

The Absolute Beginner's Guide to **Cybersecurity** 2026

From Cybersecurity Fundamentals to Practical Skills,
Threat Detection, and Defense



Alexander Oni

<packt>

The Absolute Beginner's Guide to Cybersecurity 2026

From Cybersecurity Fundamentals to Practical Skills, Threat Detection, and Defense

Alexander Oni



The Absolute Beginner's Guide to Cybersecurity 2026

Copyright © 2026 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Portfolio Director: Vijin Boricha

Portfolio Manager: Anindya Sil

Program Manager: Ankita Thakur

Content Engineer: Shubhra Mayuri

Technical Editor: Nithik Cheruvakodan

Indexer: Tejal Soni

Production Designer: Ajay Patule

Growth Lead: Ankita Thakur

Production reference: 1170926

Published by Packt Publishing Ltd.

Grosvenor House

11 St Paul's Square

Birmingham

B3 1RB, UK.

ISBN 978-1-80849-385-0

www.packtpub.com

Contributors

About the author

Alexander Oni is a bestselling instructor with over 420,000 students enrolled in his courses. With more than 10 years of experience in online teaching, Alex has created over 36 courses enjoyed by students worldwide. Alex believes in living life to the fullest by stepping out of his comfort zone, exploring new places, and trying new experiences. His online success has granted him financial freedom and the ability to travel and work from anywhere. Currently based in Bangkok, Thailand, Alex enjoys watching movies, sports, playing chess, and is an avid gamer.

Table of Contents

Preface	xv
Free benefits with your book • 0	
Part I: Cybersecurity Foundations	1
Chapter 1: Introduction to Cybersecurity	3
Technical requirements.....	3
Distinction between information security and cybersecurity.....	3
Core information security principles.....	4
CIA triad: confidentiality, integrity, and availability • 5	
Supporting principles: authentication, authorization, and accounting (AAA) • 6	
Opposing principles: disclosure, alteration, and deniability (DAD) • 7	
Putting the security principles together	8
Assets, threats, vulnerabilities, and risks • 9	
Connecting risk to the CIA triad • 11	
Summary.....	12
Chapter 2: Networking Essentials	13
Network concepts and types	14
Data transmission and communication components	15
IP addresses and MAC addresses • 16	
Practical demonstration of address identification • 17	
Protocols and ports • 18	
Protocols for email communications • 19	
Other protocols • 20	
TCP/IP protocol suite • 20	
<i>TCP/IP protocol layers</i> • 20	
HTTP and HTTPS operation • 21	
Web communication protocols and encryption • 21	
Networking devices: hubs, switches, and routers.....	23

Network segmentation and VLANs	26
Internet data transmission processes.....	27
Return path of internet data • 31	
How email works • 31	
Networking commands and tools.....	32
Summary.....	38

Chapter 3: Threat Actors and the Hacking Methodology **39**

Popular culture and misconceptions about hackers.....	39
Categories of threat actors	40
Script kiddies • 41	
Black-hat hackers • 41	
Gray-hat hackers • 41	
Hacktivists • 41	
Insider threats • 42	
Spies and saboteurs • 42	
The hacking methodology	42
Reconnaissance (footprinting) • 42	
Exploitation • 43	
Privilege escalation • 43	
Establishing persistence • 43	
Attack execution • 43	
Cover-up and avoidance of detection • 44	
Social engineering in cybersecurity	44
Baiting • 45	
Pretexting • 45	
Quid pro quo • 45	
Phishing • 46	
Vishing • 46	
Staying safe • 46	
Lunchtime attacks • 47	
Piggybacking • 47	
Tailgating • 47	
Shoulder surfing • 48	
Dumpster diving • 48	

Summary.....	49
Part II: Cyber Threats and Attacks	51
Chapter 4: Common Cyber Attacks	53
Brute force attacks	54
Phishing attacks.....	56
Examples of phishing emails • 57	
Types of phishing attacks • 61	
Spear phishing • 61	
Vishing • 61	
Smishing • 62	
High-profile invoice fraud cases • 62	
<i>Payment verification best practices • 62</i>	
Bots and botnets	63
Denial of service (DoS) and distributed denial of service (DDoS) attacks.....	64
Man-in-the-Middle attacks.....	66
Types of Man-in-the-Middle attacks • 67	
SQL injection and cross-Site Scripting (XSS) attacks	67
Supply chain attacks.....	68
Preventing supply chain attacks • 69	
Advanced cyber attacks.....	70
Business email compromise • 70	
SIM swapping • 71	
Drive-by downloads • 72	
Deepfakes • 72	
Session hijacking attacks • 73	
Summary.....	76
Chapter 5: Understanding Malware	77
Viruses and worms	78
Virus life cycle and methods of spread • 78	
Objectives and variants of viruses • 78	
Trojan horse.....	79
Major types of Trojans • 79	

Defensive measures against trojans • 80	
Adware and spyware	80
Ransomware.....	81
Data access ransomware • 81	
<i>Data sensitivity ransomware • 82</i>	
Methods of ransomware delivery • 83	
Notable ransomware attacks and trends • 83	
Rootkits	84
Symptoms of rootkit infection • 85	
Other forms of malware	85
Mobile malware	86
Mobile ransomware • 87	
<i>Removal techniques for mobile ransomware • 87</i>	
Banking trojans on mobile devices • 88	
<i>Mobile trojan removal methods • 89</i>	
Signs of mobile malware infection • 89	
Using Malwarebytes • 90	
Summary.....	92
 Chapter 6: Real-World Cyber Incidents	 93

Cyber warfare as a modern threat	94
Debates and legal frameworks of cyber warfare • 94	
The Stuxnet attack.....	95
The 2018 disinformation campaigns involving Qatar.....	96
The Estonia cyber attack.....	97
The 2014 Sony Pictures hack.....	98
Summary.....	100

Part III: Building Your Security Defenses	101
--	------------

 Chapter 7: Essential Security Controls	 103
---	----------------

Security control categories	104
Firewalls.....	104
Types of firewalls • 105	
Firewall rules and filtering criteria • 105	

Common firewall configurations • 106	
Demonstration of Windows Firewall • 106	
Encryption for data protection.....	115
Authentication	117
Biometric security mechanisms • 117	
<i>Physiological and behavioral biometric identifiers • 117</i>	
<i>Factor authentication methods • 118</i>	
Honeypots and demilitarized Zones (DMZs)	119
DMZ architecture • 120	
Wireless security.....	121
Wireless security protocols • 122	
Password security and management.....	124
Password management strategies • 124	
Password formula examples • 124	
Monitoring data breaches with Have I Been Pwned • 125	
Summary.....	126
 Chapter 8: Identity and Access Security	 127

Access control systems and identity management.....	128
The IAAA processes: Identification, Authentication, Authorization, and Accountability	129
Access control • 130	
<i>DAC • 130</i>	
<i>MAC • 131</i>	
<i>RBAC • 131</i>	
<i>ABAC • 132</i>	
Real-world application of access control models • 132	
Privileged access management (PAM)	132
Threats to privileged account security • 133	
Best practices for privileged access management • 133	
Summary.....	134
 Chapter 9: Modern Cyber Defense	 135

Zero Trust security strategy	135
Drivers of Zero Trust adoption • 136	
Core principles of Zero Trust • 136	

Key components of Zero Trust implementation • 137	
Challenges of Zero Trust • 138	
Defense in depth strategy	138
Rationale for layered security • 138	
Threat intelligence and threat hunting	141
Types of threat intelligence • 141	
MITRE ATT&CK framework • 142	
<i>Key elements of threat hunting • 143</i>	
Benefits of combining threat intelligence and threat hunting • 143	
Security compliance frameworks.....	144
AI-powered security	145
Real-world examples of AI security tools • 146	
Identifying trends and Patterns in Security Reports • 147	
Using ChatGPT for security analysis	147
Summary.....	148
 Chapter 10: Protecting Data and Systems	 149
Backup strategies and the 3-2-1-1-0 rule.....	150
Types of backups • 150	
Modern backup security practices • 151	
Common backup mistakes to avoid • 151	
Recommended backup tools and services • 152	
Cloud computing fundamentals.....	152
Cloud storage advantages and limitations • 153	
Best practices for using cloud services • 154	
Cloud deployment models • 155	
Shared responsibility model in cloud security • 156	
Security risks in cloud environments • 156	
Encryption and decryption for data protection	157
Attacks on encrypted systems • 159	
<i>Direct memory access attacks • 159</i>	
<i>Memory remnants and cold boot attacks • 160</i>	
Securing Windows 11	161
Summary.....	167

Part IV: Staying Secure in Everyday Life **169**

Chapter 11: Mobile Device Security **171**

Comparative security of major mobile operating systems 172

Mobile applications as security risks..... 172

Comparing Google Play Store and Apple App Store..... 173

Best practices for downloading mobile apps..... 175

Evaluating app reviews and ratings • 176

Analyzing app install numbers and red flags • 177

Jailbreaking iOS devices: Process, legality, and risks 181

Technical process of jailbreaking • 181

Legal and safety considerations • 181

Matching permissions to app objectives • 183

Managing and reviewing app permissions..... 184

Using permission management applications • 184

Special access and installing unknown apps • 185

Mobile app security guidelines • 187

Virtual private network (VPN) • 188

NordVPN • 189

Public Wi-Fi • 192

Configuring important security settings • 193

Lock screen and security • 193

Google Play Protect • 194

Find my phone • 194

SIM card lock settings • 200

Summary..... 202

Chapter 12: Privacy, Anonymity, and Online Safety **203**

Defining privacy, anonymity, and pseudonymity..... 204

Identity compartmentalization..... 205

Modern online tracking 209

Cookies • 209

Browser fingerprinting • 210

Cross-device tracking • 212

AI tracking • 212	
Detecting and blocking trackers • 212	
Major online tracking locations • 212	
<i>Search engines • 212</i>	
<i>Social media platforms • 213</i>	
<i>E-commerce and payment processors • 213</i>	
<i>Mobile apps and permissions • 214</i>	
<i>Data brokers and background check companies • 214</i>	
<i>Email tracking • 214</i>	
<i>Internet service providers (ISPs) • 214</i>	
Browsing in incognito or private mode • 214	
Anonymizers: tools for online anonymity.....	215
<i>Single point anonymizers • 217</i>	
<i>Proxy servers • 217</i>	
<i>VPN • 220</i>	
Networked anonymizers • 225	
<i>Tor • 225</i>	
Anonymizers and the dark web • 232	
Other anonymizing services • 234	
Summary.....	236
 Chapter 13: Cybersecurity at Home and Work	 237
Organizational cybersecurity policies and plans	237
The BYOD phenomenon in the modern workplace	239
COBO, COPE, and CYOD • 239	
Sample BYOD policy structure • 240	
The security versus ease of access paradox.....	242
Summary.....	243
 Chapter 14: Looking Ahead	 245
Applications of AI in cybersecurity	245
Malicious uses of AI by cybercriminals	246
Arup Deepfake financial scam • 246	
The Brad Pitt romance scam • 247	
Ethical and responsible use of AI in cybersecurity.....	247

Ethical hacking and responsible AI deployment • 248	
Future trends in AI and cybersecurity	249
Summary.....	249
Chapter 15: Unlock Your Exclusive Benefits	251

Unlock this Book's Free Benefits in 3 Easy Steps	252
Step 1 • 252	
Step 2 • 252	
Step 3 • 253	
Need Help? • 253	
Other Books You May Enjoy	256

Index	259
--------------	------------

Preface

Cybersecurity affects almost every part of modern life, from the devices we use and the networks we connect to, to the accounts, applications, and services we rely on every day. However, for someone new to the field, cybersecurity can quickly become overwhelming because of the volume of terminology, technologies, threats, and defensive techniques involved.

This book introduces cybersecurity from the ground up. It begins with the fundamental ideas behind cybersecurity and computer networking before moving into threat actors, common attacks, malware, and real-world cyber incidents. From there, you will explore the technologies and practices used to defend systems, protect identities and data, secure mobile devices, improve online privacy, and apply cybersecurity principles at home and in the workplace.

The emphasis throughout the book is on helping you understand not only what cybersecurity concepts mean, but also how they relate to situations you are likely to encounter in the real world. By the end of the book, you will have a broad foundation on which you can continue building your cybersecurity knowledge and skills.

Who this book is for

This book is for anyone who wants to understand cybersecurity but has little or no prior experience in the field. It is suitable for students, aspiring cybersecurity professionals, IT beginners, business professionals who want to better understand cyber risks, and everyday technology users who want to improve their security and privacy.

No previous cybersecurity knowledge is required. The concepts are introduced progressively, beginning with the fundamentals before moving into attacks, defensive technologies, privacy, mobile security, and modern cybersecurity practices.

What this book covers

Chapter 1, Introduction to Cybersecurity, introduces the field of cybersecurity and explains how it relates to information security. You will learn the core principles that underpin information security and establish the foundation needed for the rest of the book.

Chapter 2, Networking Essentials, explains how computers and other devices communicate. You will explore networks, protocols and ports, IP and MAC addresses, TCP/IP, SSL and TLS, routers and switches, NAT, network segmentation, VLANs, DNS, and the journey data takes across the

internet. The chapter also introduces useful networking commands and the basic protocols involved in email communication.

Chapter 3, Threat Actors and the Hacking Methodology, examines who carries out cyberattacks and how attacks develop. You will learn about different types of hackers, common hacking methodologies, and the stages attackers may follow when targeting a system. The chapter also introduces social engineering and the techniques attackers use to manipulate people.

Chapter 4, Common Cyber Attacks, explores many of the attacks you may encounter in cybersecurity, including brute-force attacks, phishing, botnets, denial-of-service and distributed denial-of-service attacks, man-in-the-middle attacks, SQL injection, supply chain attacks, and business email compromise. You will also examine newer and increasingly common threats such as SIM swapping, drive-by downloads, deepfake scams, and session hijacking.

Chapter 5, Understanding Malware, introduces malicious software and explains how different forms of malware operate. You will learn about viruses, worms, Trojans, spyware, adware, ransomware, rootkits, and other malware families. The chapter also examines malware targeting mobile devices, the signs of an infection, ransomware recovery, and tools that can help identify and remove malicious software.

Chapter 6, Real-World Cyber Incidents, shows how the concepts covered so far appear in actual attacks. You will examine cyber warfare and major incidents such as Stuxnet, the cyberattacks against Estonia, and the Sony Pictures hack to understand the motives, techniques, and consequences associated with significant cyber incidents.

Chapter 7, Essential Security Controls, introduces some of the fundamental technologies and practices used to protect systems and networks. You will learn about firewalls, encryption, biometrics, authentication factors, honeypots, demilitarized zones, wireless security, and password security. You will also see how firewall settings and rules can be configured in practice.

Chapter 8, Identity and Access Security, focuses on controlling who can access systems and what they are allowed to do. You will explore identity and access management, access control models, privileged access management, and the role of security controls in protecting accounts and resources.

Chapter 9, Modern Cyber Defense, moves beyond individual security tools to examine broader defensive strategies. You will learn about Zero Trust, defense in depth, threat intelligence, threat hunting, and security compliance frameworks. The chapter also explores the growing role of artificial intelligence in cybersecurity, including the use of AI tools for identifying patterns and trends.

Chapter 10, Protecting Data and Systems, explains how organizations and individuals can reduce the risk of data loss and system compromise. You will explore backups, cloud computing and cloud deployment models, cloud security risks, encryption and attacks against encryption, patching and updates, application permissions, firewall settings, browser protection, and other operating-system security features.

Chapter 11, Mobile Device Security, focuses on the security risks associated with smartphones and mobile applications. You will compare mobile platforms, learn how to identify legitimate applications, understand app permissions, and examine risks such as malicious apps, scams, and jailbreaking. The chapter also covers mobile VPNs, public Wi-Fi security, device security settings, and tools for locating lost or stolen devices.

Chapter 12, Privacy, Anonymity, and Online Safety, explores how your identity and activity can be exposed or tracked online. You will learn the differences between privacy, anonymity, and pseudonymity; examine identity compartmentalization and modern tracking techniques; and understand what private browsing can and cannot do. The chapter then introduces anonymizing technologies, including proxy servers, VPNs, and Tor, before examining Tor's limitations, the dark web, darknets, and the implications of combining different privacy technologies.

Chapter 13, Cybersecurity at Home and Work, looks at how cybersecurity practices are applied in everyday and workplace environments. You will explore cybersecurity policies, Bring Your Own Device (BYOD), mobile device management, and the considerations involved in developing a BYOD policy. The chapter also examines the balance organizations must strike between stronger security and convenient access.

Chapter 14, Looking Ahead, concludes the book by examining the evolving relationship between artificial intelligence and cybersecurity. It considers how the cybersecurity landscape continues to change and provides a starting point for continuing your learning beyond the fundamentals covered in this book.

To get the most out of this book

You do not need previous cybersecurity experience to follow this book. A basic familiarity with using computers, smartphones, web browsers, and the internet will be helpful, but the technical concepts are explained from the beginning.

Some sections include demonstrations of operating-system settings, networking tools, security software, firewalls, VPNs, and other technologies. Following these demonstrations on your own device can help reinforce what you learn, although doing so is not required to understand the core concepts.

Where practical activities involve changing device, network, or security settings, use a system on which you have permission to make those changes. Avoid experimenting with security

techniques against systems, networks, accounts, or services that you do not own or have explicit authorization to test.

Conventions used

A number of text conventions are used throughout this book.

`Code in Text` indicates commands, filenames, configuration values, protocols, ports, IP addresses, and other technical elements. For example, "The physical address listed, something such as 60-45-2E-44-5A-61"

Commands or longer technical examples may appear in separate blocks so that they can be distinguished easily from the surrounding explanation.

```
nslookup labcyber.com
```

Bold is used for important terms, user-interface elements, menu options, buttons, and other items that you may need to identify on screen. For example, "The **MAC address** stands for Media Access Control."

Italic text may be used when introducing or emphasizing terminology.

NOTE

Notes provide additional information, clarification, or useful context related to the topic being discussed.

TIP

Tips highlight practical advice or useful techniques that can help you apply a concept more effectively.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, please contact Packt through the appropriate support channels and mention the book title in your message.

Errata: Although every effort has been made to ensure the accuracy of the content, errors can occur. If you identify an error in this book, we would appreciate you reporting it through Packt's errata submission process. All valid errata will be timely updated on GitHub: <https://github.com/PacktPublishing/The-Absolute-Beginner-s-Guide-to-Cybersecurity-2026>

Piracy: If you encounter unauthorized copies of Packt publications online, please report the location or website to Packt.

Share your thoughts

Once you've read *The Absolute Beginner's Guide to Cybersecurity 2026*, we'd love to hear your thoughts! Scan the QR code below to go straight to the Amazon review page for this book and share your feedback.



<https://packt.link/r/1808493850>

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Free benefits with your book

This book comes with free benefits to support your learning. Activate them now for instant access (see the "How to Unlock" section for instructions).

Here's a quick overview of what you can instantly unlock with your purchase:



DRM-Free PDF Version

Download DRM-free PDF and ePub copies of this book.



7-Day Packt Library Access

Get 7-day unlimited access to 8,000+ books and videos. No credit card required.

Available for first-time Packt+ trial users only.



Next-Gen Reader Access

Read this book on Packt Reader with progress sync, dark mode and note-taking.

How to unlock

Scan the QR code (or go to <https://packtpub.com/unlock>). Search for this book by name, confirm the edition, and then follow the steps on the page.



UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require one

Part I

Cybersecurity Foundations

Part I — Cybersecurity Foundations brings together the essential concepts and context needed to understand the field of cybersecurity. It begins by introducing the fundamental principles of protecting digital data, computers, and networks, then covers the core networking protocols that enable communication across systems and finally examines the various **threat actors** and the stages of cyberattacks. Together, these chapters provide a comprehensive starting point for understanding how cybersecurity operates and why it is necessary.

This part has the following chapters:

- *Chapter 1, Introduction to Cybersecurity*
- *Chapter 2, Networking Essentials*
- *Chapter 3, Threat Actors and the Cyber Kill Chain*

1

Introduction to Cybersecurity

Cybersecurity is the practice of protecting digital data, networks, and workstations within cyberspace from unauthorized access and malicious threats. In this chapter, we will build a clear understanding of how cybersecurity fits within the broader field of information security, and by the end, we will be able to distinguish between the two, identify the core principles that guide cybersecurity, and recognize the mechanisms that safeguard the digital world. You will explore key concepts such as the **confidentiality, integrity, and availability (CIA)** triad, along with tools such as encryption, passwords, biometrics, checksums, and network access controls, as well as the AAA framework of authentication, authorization, and accounting. Grasping these distinctions and techniques is crucial, as they form the foundation for protecting sensitive information, ensuring trust in digital interactions, and preventing the kinds of breaches and disruptions that can have serious consequences for individuals and organizations alike.

In this chapter, we will cover the following topics:

- Distinction Between information security and Cybersecurity
- Core information security Principles

Technical requirements

All chapters in this book are conceptual and require no additional software setup. You only need your basic computer features.

Distinction between information security and cybersecurity

You often hear the terms **information security** and **cybersecurity** used interchangeably, but there is a distinction between them that can help you stand out from those who have never studied cybersecurity. While in everyday situations no one will care if you use one term instead

of the other, and people mix them up all the time, understanding the difference is important for your own knowledge and confidence. Let's see what sets information security apart from cybersecurity, using practical examples to clarify the boundaries between the two.

NOTE

All cybersecurity is information security, but not all information security is cybersecurity.

Information security is the broader field that covers all types of protection for all types of data, while cybersecurity is a specialized field within information security. When you talk about cybersecurity, the word "cyber" signals that you are dealing with the protection of data in computers, workstations, and networks that exist in the *cyberspace*. This means cybersecurity is about protecting any kind of data in digital form that could be accessed by anyone on the internet or on a network.

NOTE

Cybersecurity focuses on the protection of data, networks, and workstations that are in cyberspace. Information security, on the other hand, includes cybersecurity but also covers more.

For example, consider a 12-year-old hard drive that is not plugged into any network and is not on the internet. If you have data stored on this hard drive, protecting that data is not a matter of cybersecurity, because it is not accessible through cyberspace. The only way someone could access the data is by physically stealing the hard drive. In this case, you are dealing with information security, not cybersecurity.

Similarly, if you are talking about a physical server room in your company with metallic doors or security locks, that is also information security, because it involves physical security measures. Therefore, information security includes cybersecurity and also covers the protection of data in all other forms, including physical forms.

So now that you know the difference between cybersecurity and information security, you can move forward to learning about the core information security principles.

Core information security principles

The core information security principles form the foundation of information security, and every cybersecurity product, hardware, software, or policy is always designed to achieve at

least one of the three principles. Understanding how these principles work together is essential for grasping the basics of cybersecurity. Let's discuss them in detail next.

CIA triad: confidentiality, integrity, and availability

The CIA triad consists of confidentiality, integrity, and availability, which are commonly represented as three elements arranged around a triangle with a digital padlock symbolizing security as shown in *Figure 1.1*:

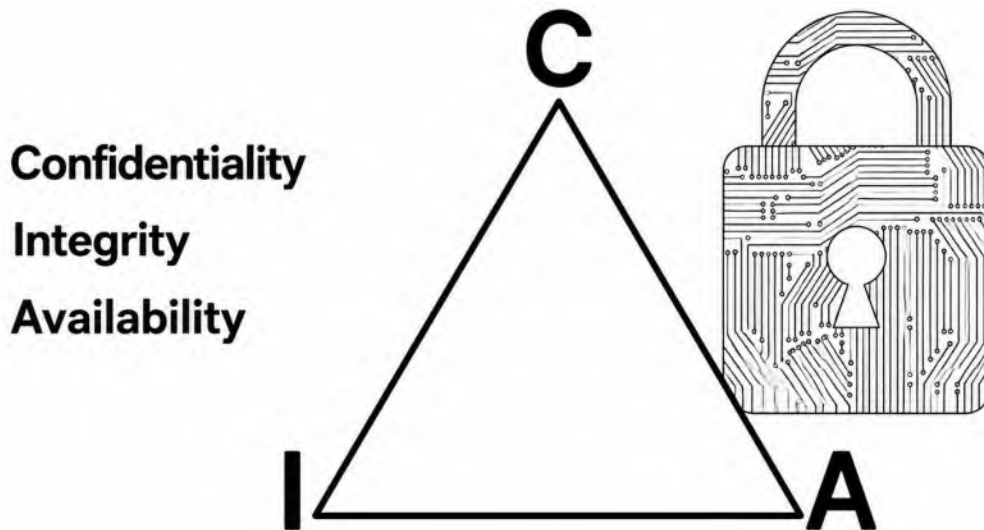


Figure 1.1: The three core information security principles: Confidentiality, Integrity, and Availability (CIA triad)

Confidentiality means that data is only accessed by those who have the right credentials. If you do not have the necessary credentials, you cannot access the data. Tools such as encryption, passwords, and biometrics are all used to achieve confidentiality.

Integrity ensures that your data has not been tampered with. If any modification has occurred, it should only be by someone who has the right to do so. Tools such as checksums and hashing are used to help you verify that data remains unaltered and trustworthy.

Availability means that your data and resources are accessible to those with the right credentials whenever they need them. Many junior security administrators tend to overlook availability, assuming that data and resources will always be accessible, but this is not always true. You use tools such as network access controls and server management to make sure that data and resources remain available to authorized users.

Before moving on, it is important to note that two additional core principles have recently been added to the CIA triad: **privacy** and **non-repudiation**.

Privacy refers to the right of an individual or user to control the use of their own personal information and to keep their online activities private. This has become a highly sensitive topic, as governments around the world increasingly seek access to user data, leading to ongoing debates about the balance between privacy and security.

Non-repudiation means that a subject or user cannot deny actions such as creating, modifying, or sending a resource. It is designed to prevent you from claiming innocence when evidence shows you performed a particular action, such as committing an illegal act. Non-repudiation achieves this by maintaining records that can be used to demonstrate, beyond dispute, who was responsible for a given action.

NOTE

Non-repudiation is closely related to accounting (discussed in the next subsection), since accounting allows you to trace what each user did with a particular file or data.

Now, let's look at the foundational mechanisms that help enforce the CIA triad in practice.

Supporting principles: authentication, authorization, and accounting (AAA)

The AAA principles form the foundation for controlling access and ensuring accountability in cybersecurity systems. They work together to ensure that only the right people have access, that their actions are controlled, and that their activities can be tracked.

Authentication is the process that ensures a user's identity is verified before access is granted to a particular kind of file. For example, when you try to access your email or log back into your Netflix account after being locked out, you are typically required to provide a password. That password is the tool used to achieve authentication, allowing the server to verify who you are.

Authorization determines what actions you are allowed to perform once you have been authenticated. For instance, if you are trying to access a confidential file on a server, authentication verifies your identity, but authorization controls what you can do with the file after access is granted. You might be able to view, modify, delete, transfer, or copy the file, but your specific permissions depend on your level of authorization. For example, a level one authorization might only allow you to view the file, while higher levels could permit editing, downloading, or even full control over the file.

The last one in here is **accounting**. This basically just keeps track of what users do with a particular kind of file or data. This is very important because if there were a data breach and a file got downloaded illegally, accounting will be able to trace who in fact downloaded the file. So, accounting can be considered a form of accountability.

Now that you've looked at the supporting principles that reinforce the CIA triad, it's also important to recognize the set of principles that work against them. These are sometimes referred to as the opposing principles to CIA.

Opposing principles: disclosure, alteration, and deniability (DAD)

Disclosure, Alteration, and Deniability or the DAD are what the bad guys, the cyber criminals, or the hackers, aim to achieve. The DAD principles and their relationship to information security threats can be described in visual terms as shown in *Figure 1.2*:

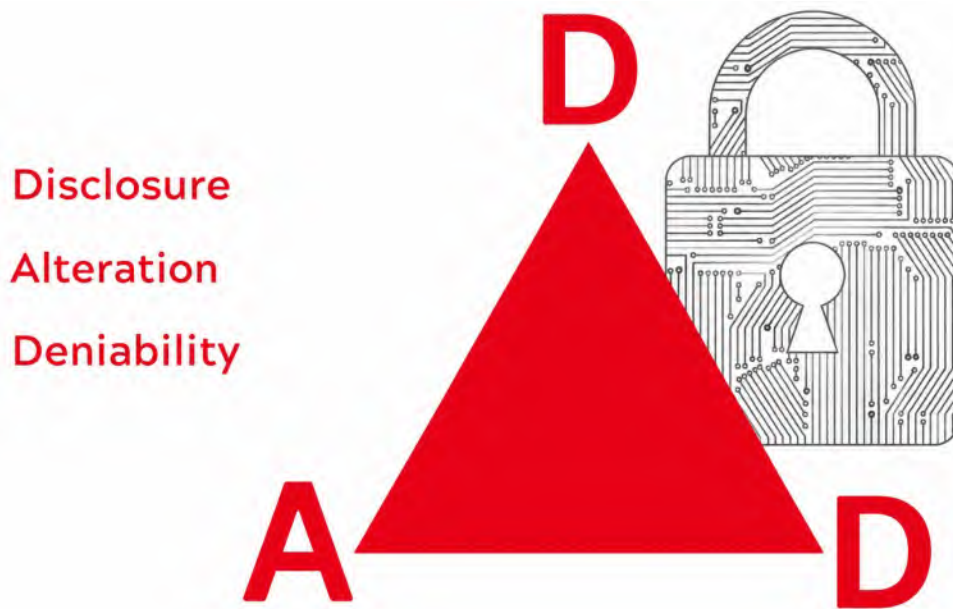


Figure 1.2: The DAD (Disclosure, Alteration, Deniability) principles targeted by cyber attackers in opposition to CIA/AAA security principles.

Disclosure is the exact opposite of confidentiality. Here, data is accessed by non-authorized users. Hackers have several tools for this, such as Trojans, brute force attacks, or even physical thefts.

The exact opposite of integrity is **alteration**, where data has been compromised or modified. Tools such as malware, viruses, and SQL injection can be used by the bad actors to achieve alteration.

The exact opposite of availability is **deniability**, where data is not made available to those who need to access it. Denial-of-service attacks and ransomware can be used by hackers to achieve deniability.

That concludes the core information security principles, covering both the foundational CIA triad and the supporting and opposing concepts. Together, these principles form the basis for understanding how cybersecurity measures are designed and evaluated.

Putting the security principles together

Now that you understand the CIA, AAA, and DAD principles, let's put them together using a simple example. This will help you understand how these principles work in a real system rather than looking at each of them separately.

Suppose you work for a company and want to access the company's payroll system to check your salary information.

The first thing you need to do is log in with a username and password so that the system can verify that you are really who you claim to be. As you learned earlier, this is **authentication**.

Once you have been authenticated, you might be allowed to view your own salary information, but you should not be able to change your salary or view the salary information of every other employee. This is where **authorization** comes in. Authorization determines what you are allowed to do after your identity has been verified.

While you are using the payroll system, the system might keep track of when you logged in, what information you accessed, and whether you made any changes. This is **accounting**, as we discussed earlier.

At the same time, the CIA principles are also being applied.

Your salary information should only be visible to people who are allowed to see it. This is **confidentiality**. Your salary and banking information should not be changed by someone who does not have permission to change it. This is **integrity**. Finally, you should be able to access the payroll system when you need it. This is **availability**.

Now, let's look at what happens when things go wrong.

Suppose a hacker manages to steal the password of a payroll administrator and uses it to access the payroll system. The hacker then reads the salary information of employees. Here, confidentiality has been compromised. As you learned in the DAD principles, this is **disclosure**.

The hacker then changes an employee's banking information. Now the data has been modified without permission, meaning that integrity has been compromised. This is **alteration**.

Finally, suppose the hacker causes the payroll system to stop working, preventing employees from accessing it. Availability has now been compromised. This relates to **deniability** in the DAD principles.

So, you can see that CIA, AAA, and DAD are not simply separate sets of terms that you need to memorize. They are closely connected and can all be involved in the same cybersecurity incident.

TIP

When you encounter security incidents later, a simple way to think about them is to ask whether someone was able to see something they should not see, change something they should not change, or prevent someone from accessing something they should be able to access. These questions will help you relate the incident back to confidentiality, integrity, and availability.

Now that you have seen how these principles work together, let's introduce another set of terms that you will encounter frequently in cybersecurity: assets, threats, vulnerabilities, and risks.

Assets, threats, vulnerabilities, and risks

When talking about cybersecurity, you will often hear people use terms such as **asset**, **threat**, **vulnerability**, and **risk**. These terms might sound technical at first, but the ideas behind them are actually quite simple.

Let's start with an **asset**.

An asset is anything valuable that you want to protect. In cybersecurity, this could be your data, computer, smartphone, user account, application, server, or even an entire network.

A company database containing customer names, email addresses, and passwords is valuable to the company and therefore needs to be protected. So it is an asset.

For anything valuable to protect, we need to think about what could potentially cause harm to it. This brings us to a **threat**. A threat is anything that has the potential to cause harm to an

asset. For example, suppose a hacker wants to steal the information stored in the customer database, they represent a threat.

However, simply having a threat does not necessarily mean that the attacker will be successful. There usually needs to be some kind of weakness that can be taken advantage of. We call this weakness a **vulnerability**. A vulnerability is a weakness that could potentially be exploited by a threat.

For example, if the administrator of the customer database uses a very weak password, a hacker might be able to guess it and gain access to the database. Here, the weak password is the vulnerability.

NOTE

One thing you should remember here is the difference between a threat and a vulnerability. Beginners sometimes confuse the two. The hacker is the **threat**, while the weak password is the **vulnerability**.

You can also relate this to a simple example outside cybersecurity. Suppose you leave a window open when you leave your house. A burglar who wants to enter your house represents a threat. The open window represents a vulnerability because it provides a weakness that the burglar could take advantage of. The valuable items inside your house are the assets that you want to protect.

This brings us to the final term, which is **risk**.

Risk is the possibility that a threat could take advantage of a vulnerability and cause harm to an asset.

Let's go back to our customer database example. The **risk** here is that the hacker could successfully take advantage of the weak password, access the database, and steal or modify the customer information.

In a nutshell, when you are trying to distinguish between these terms, you can think about them in the following way:

- An **asset** is what you want to protect.
- A **threat** is something that could cause harm.
- A **vulnerability** is a weakness that could be exploited.
- A **risk** is the possibility of that weakness being exploited and causing harm.

You will encounter these terms many times as you continue learning cybersecurity, so understanding the distinction between them now will make later concepts much easier to follow.

Now that you understand assets, threats, vulnerabilities, and risks, let's connect them back to the CIA principles you learned earlier.

Connecting risk to the CIA triad

The concepts of assets, threats, vulnerabilities, and risks are closely connected to the CIA triad because the CIA principles help us understand what could happen to an asset when something goes wrong.

This connection gives you a simple way to think about the CIA triad when looking at risks. You can ask yourself three questions.

- Can someone who should not see the information access it? If so, you have a confidentiality problem.
- Can someone who should not change the information modify it? If so, you have an integrity problem.
- Can the people who are supposed to use the information or system access it when they need it? If not, you have an availability problem.

You can apply the same questions to many different assets.

For example, think about your email account. You do not want another person reading your private emails, because that would affect confidentiality. You do not want someone modifying or deleting your emails without permission, because that would affect integrity. You also want to be able to access your email whenever you need it, which relates to availability.

TIP

At this stage, you do not need to worry about memorizing complicated definitions. What is more important is understanding how these ideas connect.

With these concepts in place, you now have a foundation for thinking about cybersecurity problems. As you move into networking and other cybersecurity topics, you will see these same ideas appear again and again.

Summary

In this chapter, we established the foundational principles of cybersecurity and information security. Starting from the distinction between information security and cybersecurity, we moved through the core CIA triad and concluded with privacy and non-repudiation. You then examined supporting AAA principles before addressing the DAD model. We also provided examples of tools that are used to establish each of these models.

The key distinction we drew is that while all cybersecurity is information security, only information security encompasses both digital and physical data protection, as illustrated by the difference between securing a networked computer and a disconnected hard drive. With this distinction in mind, you are prepared to explore how the underlying infrastructure of cyberspace supports and challenges the protection of digital assets.

Chapter 2 covers the fundamentals of networking, including how devices connect and communicate across local and global environments. We will identify key networking equipment such as hubs, switches, and routers, and understand how protocols like HTTP, HTTPS, FTP, SFTP, IMAP, SMTP, and the TCP/IP suite enable secure and reliable data transmission.

2

Networking Essentials

In the previous chapter, you learned the fundamentals of cybersecurity and the principles that guide how we protect digital information. Now, we are going to build on that foundation by looking at one of the most important areas in cybersecurity: **networking**.

Understanding networks is particularly important in cybersecurity because once devices are connected, they can communicate and exchange data. That communication is extremely useful, but it also creates opportunities for security problems. To understand how we can protect those networks, we first need to understand how they work.

In this chapter, we will discuss the fundamentals of networking, including how devices connect and communicate across local and global environments. You will first learn what defines a network and see how the devices you already use at home can form a simple network. From there, we will look at the most common types of networks you will encounter and how networks can differ depending on their size and purpose.

We will then introduce the networking devices that make communication possible, including **hubs, switches, and routers**, and look at the role each device plays in moving data from one place to another. Finally, you will begin exploring the protocols that allow devices to communicate, including familiar protocols such as HTTP, HTTPS, FTP, SFTP, IMAP, and SMTP, along with the TCP/IP suite that forms the foundation of modern network communication.

The following topics will be covered:

- Network concepts and types
- Data transmission and communication components
- Networking devices: hubs, switches, and routers
- Network segmentation and VLANs
- Internet data transmission processes
- Networking commands and tools

Network concepts and types

Think about many of the digital activities you perform every day. When you open a website, send an email, stream a video, access a file stored online, or send a message from your phone, information needs to travel from one device to another. The devices involved might be sitting next to each other in the same room, or they could be thousands of kilometers apart. The connections that allow these devices to communicate form what we call a **network**.

NOTE

A **network** is simply a system of interconnected devices that communicate or interact with each other.

For example, your home Wi-Fi is a network where your router in the living room connects to your smart TV, your computer, and maybe even your PlayStation 5. All of these devices together make up your home network. The internet itself is a massive network, basically a collection of networks. Now let's get into the different types of networks.

A **local area network (LAN)** is a network within a limited area, such as a home, school, or office. Your home network is a LAN. A LAN could also be the network for a large company if all the computers are within the same building or area.

A **wide area network (WAN)** is a much larger network that spans multiple locations, such as a network running through an entire city. The internet itself is another example of a WAN.

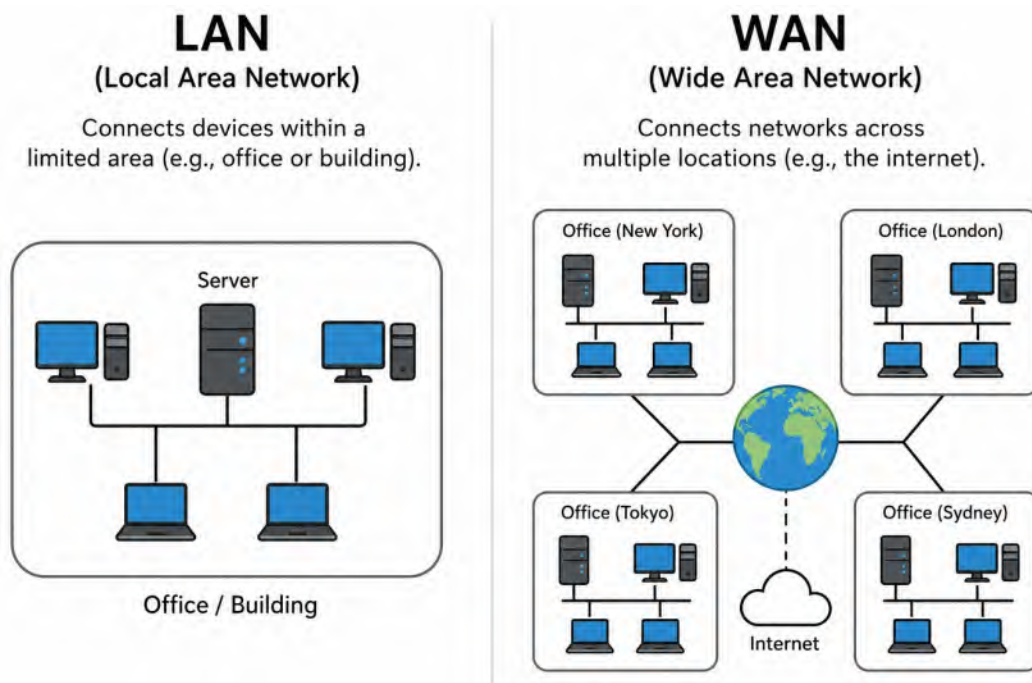


Figure 2.1: Types of computer networks: Local Area Network (LAN) and Wide Area Network (WAN) explained with examples.

A **virtual private network (VPN)** is a secure way to connect to a network remotely. VPNs are popular for security and for accessing additional content on streaming platforms.

Cloud networks are services hosted in cloud environments rather than on physical devices in a building. VPN and cloud network concepts are part of the broader network types.

The following section examines the mechanisms by which data is exchanged within a network and the methods through which networks interact with one another.

Data transmission and communication components

When you transfer data from one computer to another, that data is broken down into smaller packets, which are then transmitted across the network. Devices use four main components to communicate: **the IP address, the MAC address, protocols, and ports**. These four elements together allow computers to transfer files and data from one device to another.

Devices communicate on a network by breaking down data into packets and using addresses and protocols. Let's use an analogy to clarify how these four components, IP address, MAC address, protocols, and ports, work together in network communication. Imagine you have

won a 100-inch smart TV in a lottery, and it needs to be delivered to your home. The delivery person must know your street address, which represents the **IP address**: this identifies the building or condominium where you live. Next, your specific apartment number within that building is like the **MAC address**: it pinpoints your exact unit inside the larger structure. With both the IP address and MAC address, the delivery person can find your building and your apartment. In this section, we will discuss each in detail.

IP addresses and MAC addresses

Your computer is assigned an IP address to help other computers on the network locate it. The **IP address** allows your device to be traceable on the Internet or within a global network. There are two main types: **IP version 4** (IPv4) and **IP version 6** (IPv6). IPv4 addresses are simple, typically in the format 192.168.0.10, with each number ranging from 0 to 255. IPv6 addresses are longer and more complex, created because IPv4 addresses are running out due to the vast number of devices connected to the Internet.

IPv4 addresses are logical and dynamic, meaning they can change depending on various factors. The IP address your computer has today may not be the same tomorrow. These addresses are used for both global and local communication over the Internet or a local area network.

NOTE

IP addresses are logical, dynamic addresses used for communication over the Internet or a LAN.

The **MAC address** stands for Media Access Control. Unlike IP addresses, which are dynamic, MAC addresses are unique serial numbers assigned to every network adapter at the time of manufacture. These are physical addresses, typically written in hexadecimal format, and are used within a LAN to identify a specific device. MAC addresses are not routable across the Internet.

To extend the earlier analogy, if someone in your condominium wants to send you a parcel, they only need your apartment number (the MAC address), not your street address (the IP address). But if the parcel is being sent to another building in a different part of the city, the IP address is required. So, IP addresses are mainly used on wide area networks, while MAC addresses are used within local area networks.

NOTE

MAC addresses are hard-coded and physical. The MAC address is printed on your physical network adapter. However, MAC addresses can be spoofed, meaning a cybercriminal could pretend to be you by using your MAC address.

Practical demonstration of address identification

To see your IP and MAC addresses in action, open Command Prompt on your computer. On Windows, use the following command:

```
ipconfig /all
```

On a Mac, use:

```
ifconfig
```

This command provides information about all your network adapters and their associated IP addresses.

The output shows that your wireless LAN adapter or your Wi-Fi is the network adapter your computer is using to connect to the internet. The physical address listed, something such as 60-45-2E-44-5A-61, is the MAC address of your physical network adapter, while the IPv4 address, something like 192.168.1.33 is the IP address that identifies your computer on the network.

Notice that the lease obtained and lease expires fields show that your computer can use this particular IP address for one week. This demonstrates that IP addresses are dynamic and leased out for a period of time. The router may renew the same IP address for another week or assign a new one, depending on several factors. In contrast, MAC addresses are permanent and do not change.

You can also see the physical address for your Bluetooth network adapter listed.

TIP

Whenever you see a field labeled physical address, that refers to the MAC address. If you see an address being leased out or described as dynamic, that is the IP address. IP addresses are used to identify computers on a global network or a wide area network, while MAC addresses are used to identify computers within a local area network.

Protocols and ports

Protocols are a set of rules that determine how computers communicate with each other on a network. The protocol defines not only the order in which parts of the conversation occur but also how the conversation ends. For example, when you answer a phone call and say hello, and the caller asks for your name, there is a protocol for how the conversation proceeds and concludes. Computers use similar protocols to decide which device speaks first and how responses are structured. The **protocols** are like the delivery instructions or conditions, such as delivering only in the evening when you are home, or requiring someone to sign for the package if you are away. These rules determine how and when the delivery should happen.

The **port** is the entry point the delivery person uses to bring the TV into your apartment. This could be the front door, the back door, or even the garage, each representing a different port through which data can enter or leave your device.

Two of the most popular protocols are **HTTP** and **HTTPS**. **HTTP** stands for Hypertext Transfer Protocol, while **HTTPS** is the secure version, with the "S" indicating security. These protocols define how browsers and web servers communicate. When you open a browser such as Google Chrome, Safari, or Firefox and type in a website address, the browser communicates with the web server using either HTTP or HTTPS.

HTTP uses port number 80, while **HTTPS** uses port number 443. The protocol in use determines which port number is used for the communication. For example, when you visit <https://labcyber.com>, your browser uses HTTPS to communicate with the web server. If you click the site information icon in the browser, you will see a message stating that the connection is secure. Your information, such as passwords or credit card numbers, will be private when sent to this site. This is HTTPS in action, ensuring that your data is encrypted and secure during transmission.

If you visit a website that is not secure, such as a test site you might use for development, your browser will display a warning that the connection is not secure. When you click the site information icon, you will see a message stating that your connection to the site is not secure and that you should not enter sensitive information such as passwords or credit card numbers, as attackers could steal this data. In this case, the protocol being used is HTTP on port number 80, which does not provide security. If you attempt to log in or make a purchase on such a site, you do so at your own risk, as hackers and cybercriminals can easily steal information from sites using HTTP.

Whenever you are asked to provide sensitive information on a website, always check that the site is running HTTPS by clicking the information icon in your browser and confirming that the connection is secure before entering any important details.

Consider another scenario: Anna from HR wants to send a file to Bob in marketing. Anna's computer first needs to identify the marketing department's network, this is the **IP address**. But since there are several computers in marketing, Anna's computer also needs to know which one is Bob's, this is the **MAC address**. The **protocol** will determine how the file is sent: should it be encrypted, password protected, or restricted so only Bob can access it? The **port** is the specific channel through which the file is delivered to Bob's computer.

Protocols for email communications

When you use Yahoo Mail or another email service, you interact with email protocols that determine how your messages are accessed and stored. Email security is a significant concern because, unlike modern e-commerce sites, the original design of email did not prioritize security. As a result, you need to be especially careful when sending sensitive information via email.

When receiving emails, you rely on specific ports and protocols. The two main protocols are **Internet Message Access Protocol (IMAP)** and **Post Office Protocol (POP)**. IMAP typically uses port 143 for unencrypted connections and port 993 for SSL or TLS encrypted connections. POP uses port 110 for unencrypted connections and port 995 for SSL or TLS encrypted connections.

IMAP is the most popular protocol for receiving emails because it allows your messages to be synchronized between your email client and the mail server. This means you can access the same emails on multiple devices, such as your laptop and your phone, and see identical content on both. IMAP is less secure but offers much greater convenience.

POP, on the other hand, stores emails only on the client device. It is more secure but less convenient. When you use POP, emails are downloaded to the device you are using, such as your laptop or phone, and are then removed from the server. If you check your email on another device afterward, you will not see those same emails, except for any new messages that arrived after the initial download. This is the key difference between IMAP and POP.

NOTE

IMAP keeps your emails accessible across all devices, while POP restricts access to the device that first downloads the messages.

SMTP, or **Simple Mail Transfer Protocol**, is by far the more popular protocol for sending emails, and it is very likely that your mail server uses SMTP. SMTP port 25 is the standard port for sending emails, while SMTP port 465 is the encrypted version. Port 587 is also encrypted and uses START TLS, which can upgrade an insecure connection to a secure one.

We will cover how email works behind the scenes in a later section of the chapter.

Other protocols

Now, let us consider some other protocols: **FTP** and **SFTP**. **FTP** stands for File Transfer Protocol, and **SFTP** is the secure version, known as Secure File Transfer Protocol. These protocols govern how files are transmitted from one computer to another. For example, if Anna wants to send a file to Bob and wants the transmission to be secure, she would use SFTP, which uses port number 22. If confidentiality is not a concern, FTP would be used, which operates on port number 21.

You also have **IMAP** and **SMTP**. **IMAP** stands for Internet Message Access Protocol, which controls how Internet messages are sent. IMAP uses two port numbers: 143 for the unsecured version and 993 for the secured version. **SMTP** stands for Simple Mail Transfer Protocol, which governs how your emails are sent and received. SMTP uses three port numbers: 25 for unsecured transmissions, 465 for secure transmission (now largely deprecated), and 587 for the newer secure transmission method. Port 465 is not commonly used anymore. This concludes the introduction to protocols and port numbers.

Another topic you should be familiar with is the TCP/IP protocol, which is very important and widely used in computer security.

TCP/IP protocol suite

Transmission Control Protocol (TCP) divides a message or file into smaller packets that are transmitted over the internet and then reassembled at the destination. For example, if you wanted to send a large device or piece of machinery to a friend across the country, it would be difficult to send it as one piece. Instead, you could disassemble it into smaller parts, send them separately, and then reassemble them at the destination. This is similar to how TCP splits up data into smaller packets for more effective transmission.

Internet Protocol (IP) is responsible for addressing each packet so that it is sent to the correct destination. TCP splits the data into packets, IP ensures those packets are sent to the right place, and then TCP reassembles the packets at the destination into the original data or file.

Together, these are referred to as the **TCP/IP Protocols**, which are a set of protocols used to interconnect network devices on the internet.

TCP/IP protocol layers

TCP/IP Protocols are divided into four major layers. The first is the **data link layer**, which consists of protocols that operate strictly on a link connecting hosts on a network. When your computer connects to the internet, the actual link itself is the data link layer.

Next we have the **networking layer**, which is responsible for connecting independent networks together. This is where the IP protocol operates, focusing on linking not just individual hosts but entire networks.

Above this is the **transport layer**, which manages the actual communication between hosts and is where you find the TCP protocol.

The final layer is the **application layer**, which standardizes data exchange and includes protocols such as the HTTP and the FTP. The TCP/IP protocol suite is widely used for various types of communication, including internet browsing, email, and online gaming.

HTTP and HTTPS operation

The **Hypertext Transfer Protocol (HTTP)** defines how messages are formatted and transmitted over the web, and it also determines what actions web servers and browsers should take in response to different commands. HTTP is the foundational protocol for the World Wide Web, handling every request between web browsers and web servers.

HTTP is involved in every interaction between your browser, such as Google Chrome, and a web server. When you enter a website URL or click a hyperlink, your browser acts as an HTTP client, building an HTTP request and sending it to the IP address specified by the URL.

Every web server runs a program called a **daemon**, which is designed to wait for HTTP requests and handle them as they arrive. Then the HTTP daemon in the destination server machine receives your request and sends back the requested file or files associated with your request. HTTPS stands for Hypertext Transfer Protocol Secure. As discussed earlier, this is the secured version of HTTP. It is secured because communication between your web browser and the web server is *encrypted*.

Next, let's look at how web communication protocols and encryption work together to protect data as it travels across the network. This will help clarify the role of security in everyday internet use.

Web communication protocols and encryption

For HTTPS to work, encryption must be implemented, and this is done using either **Transport Layer Security (TLS)** or **Secure Sockets Layer (SSL)**. SSL establishes an encrypted link between your web server and the browser. If you have a website and want to establish a secure link between your web server and any browser that wants to access your website, you need to install an SSL certificate. This certificate serves as proof that your website is secured with SSL, but it also has an expiry date. Any time a browser tries to access your website, it will check to see whether the certificate has expired before completing the connection.

TLS is the successor to SSL. It is more advanced and offers a higher degree of encryption and security. SSL is becoming outdated, and TLS is now the standard.

NOTE

You should also know that SSL and TLS are used interchangeably. So don't be too confused when someone mentions SSL, when in fact they're referring to TLS. They're basically used interchangeably all the time.

To see HTTPS in action, you can check whether a website is secured by looking for the green padlock and the word "Secure" in your browser's address bar. For example, when you visit Amazon, you will see "HTTPS" and a secure connection notification. If you click on "Secure," it will state that your information, such as passwords or credit card numbers, is private when sent to the site.

The following figure shows the secure connection notification for Amazon.com, indicating that HTTPS is active and that your information is private when sent to the site.

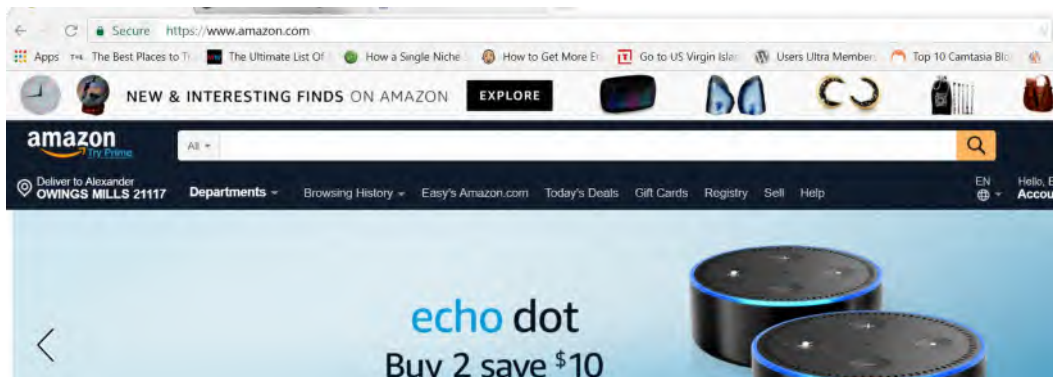


Figure 2.2: Secure HTTPS connection indicator and certificate details on Amazon.com

To obtain SSL certificates, most good web hosts will provide you with a free SSL certificate. For example, SiteGround offers this. If your web host does not provide free SSL certificates, you can go to Let's Encrypt.org, which is one of the best sites for getting a free SSL certificate.

Next, let's turn our attention to some essential networking devices.

Networking devices: hubs, switches, and routers

In the previous sections, you learned that a network allows devices to connect and communicate with one another. But for this communication to happen, networks need devices that can receive data and help move it to the correct destination.

Three important networking devices that perform this role are **hubs, switches, and routers**. At first glance, these devices can appear quite similar. They connect devices and allow data to travel across a network. However, they differ significantly in how they handle that data and decide where it should go.

One of the main differences between hubs, switches, and routers is their level of **intelligence**. In networking, intelligence refers to how much information a device can use when deciding what to do with the data it receives.

A **hub** simply passes data along. You would connect one end of a cable to a hub, and then the other end would go to the device, whether it's a laptop, a server, or another device.

Now, imagine a message comes in for computer A and passes through the hub.

You might expect the hub to simply deliver the message to device A. However, hubs are not intelligent; they do not know which device is which. Instead, the hub sends the message to every single device on the local area network, because it cannot identify device A specifically.

The hub only sees several devices connected to it and, to guarantee delivery, broadcasts the message to all devices, as shown below:

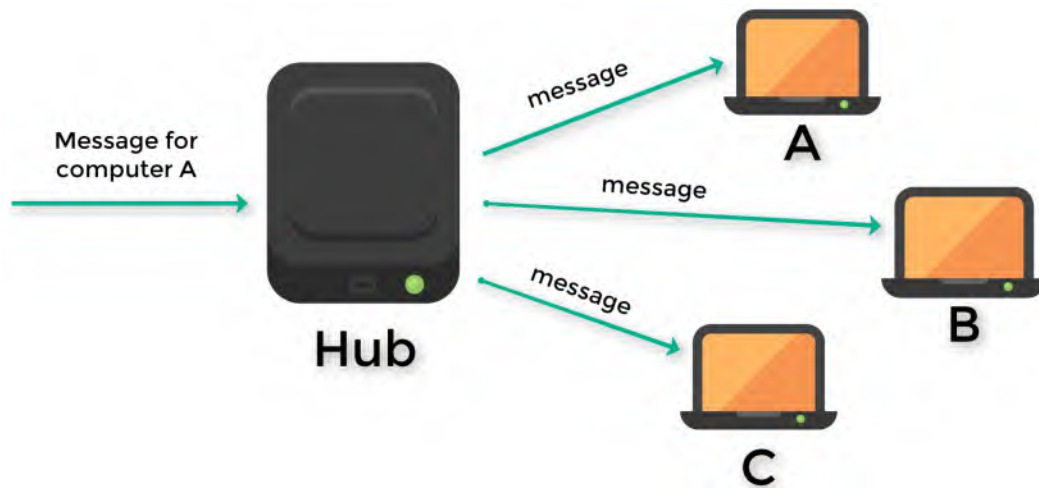


Figure 2.3: How a hub transmits a message intended for computer A on a local network with devices A, B, and C.

This approach leads to performance issues, as devices such as B and C receive messages not meant for them. Each device must check whether the message is intended for it, and if not, ignore it.

Switches and **routers**, on the other hand, are far more intelligent. In the same scenario, if a message comes in for device A, a switch or router knows which device is which and delivers the message only to device A. The router examines the destination information and determines where the data needs to go next.

It can forward the data from Device A's network toward another network as shown below:

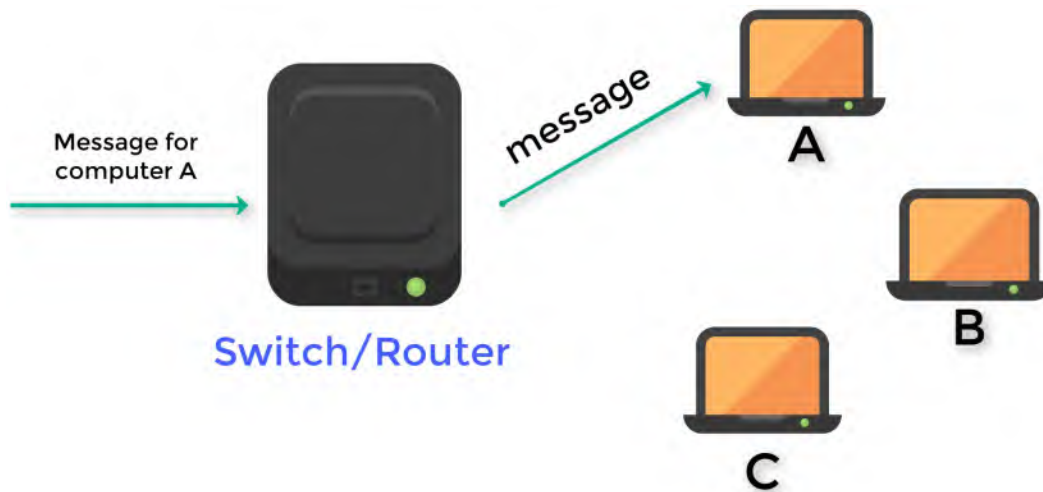


Figure 2.4: A switch/router directing the message from device A to device A

This results in improved performance and efficiency, as only the intended recipient receives the message and other devices are not disturbed.

The core difference between switches and routers is their function: a switch is used for transmitting data among devices on a local network, while a router is used for routing data among networks. In other words, a router connects networks together, while a switch connects devices within a single network.

Another key distinction is that switches use MAC addresses to perform their switching, while routers use IP addresses for their routing.

With this understanding of the basic networking devices, we can now explore how networks can be segmented and organized using VLANs.

Network segmentation and VLANs

Network segmentation is a method of dividing one large network into smaller, more manageable networks, often called subnets or segments. In a network, segmentation allows you to control who can access certain parts of your network, improving both security and management.

Imagine a house with four doors; all open, anyone can walk in and out freely, which is not secure. If you close or lock two of those doors, only certain rooms are accessible to everyone, while the others require a key. This is the idea behind network segmentation: you can have some parts of your network open and accessible, while others are restricted and require special access.

The main reasons for network segmentation are:

- **Security:** You can limit who has access to sensitive systems or data.
- **Performance:** Segmenting a large network reduces congestion, especially in environments with many computers.
- **Management:** Troubleshooting and maintaining smaller segments is much easier than dealing with one massive network. For example, if you have a network of 50 computers and divide it into 10 segments of 5 computers each, finding and fixing a problem becomes much faster.

One common way to create network segments is by using **virtual local area networks (VLANs)**. VLANs allow you to create separate virtual networks within a single physical network.

You can use VLANs to represent different groups of devices within your network. For example, a *VLAN 10* could represent all the office computers, *VLAN 20* could represent the guest Wi-Fi, and *VLAN 30* could represent security cameras connected to the network.

Without VLANs, you would have one large network where all devices are connected to the same switch and can communicate freely with each other, with no restrictions. With VLANs, the switch groups devices into separate "rooms," even if they are using the same physical cables.

Now suppose a computer in *VLAN 30* wants to communicate with another computer in *VLAN 30*. Because both computers belong to the same VLAN, the switch can forward the data between them.

The switch treats each VLAN as a separate network. Even though the HR and Marketing computers may be connected to the *same physical switch*, they are logically separated from one another as they belong to different VLANs.

Now suppose the *VLAN 30* computer wants to communicate with a *VLAN 20* camera. The switch cannot simply forward the data directly between the two VLANs because VLAN 20 and VLAN 30 are treated as separate networks. The data must instead pass through a *router or a Layer 3 switch*.

NOTE

VLANs are virtual, not physical, and communication between VLANs requires a router or a layer 3 switch with specific rules.

The cybersecurity relevance of segmentation and VLANs includes containment of threats. If a hacker compromises a device in the guest VLAN, they cannot automatically reach servers in the finance VLAN because the networks are divided. This also reduces the attack surface, as critical systems are invisible to users who do not need access.

Further, you can create a special VLAN for the most important devices and ensure that only authorized users can access them. Compliance is another factor, as many organizations are required by law to isolate sensitive data systems, such as those governed by PCI-DSS or HIPAA. **Internet of Things (IoT)** device isolation is also important, since smart cameras and sensors often have weaker security; placing them in their own VLAN ensures that if compromised, they cannot reach other computers.

Guest Wi-Fi separation is another benefit, as you do not want guests sharing the same network as employees. For example, coffee shops often have guest Wi-Fi in a separate VLAN from business systems, preventing customers from accessing internal devices such as point-of-sale machines.

With network segmentation in place, it's important to understand how data moves between network segments and across the wider internet. The next section explores the journey that data takes as it travels from one point to another online.

Internet data transmission processes

When you access a website or any online service, your request travels through several steps before reaching its destination and returning with the data you requested. Each step involves specific actions, security features, and network components that ensure that your data is delivered quickly and securely.

To help you understand this process, think of the internet as working like a post office. You write a letter, drop it off at the post office, and it is sorted and routed through various facilities until it finally arrives at the correct address. The internet does the same thing, but at lightning speed.

The first step involves your endpoint device and the **local area network (LAN)**. When you want to access a site like `lab7.com`, you enter the address on your laptop and press enter. Your device, which has a private IP address, sends the request to your home router as visualized in *Figure 2*:

Step 1 – End Point & LAN



Figure 2.5: Step 1, endpoint device connects to router, which swaps private for public IP and sends request to ISP.

The router swaps your private IP for its public IP address and forward the request to your **internet service provider (ISP)**, which acts like the post office in this analogy. Even at this stage, security features such as encryption and firewalls may be in place on your laptop or router to ensure that only safe traffic is allowed through.

Once your ISP receives the request, it checks whether it knows the IP address for the site you want to visit. The ISP applies **DNS (Domain Name System)** to resolve the domain name to the correct IP address, as visualized below:

Step 2 - Your ISP

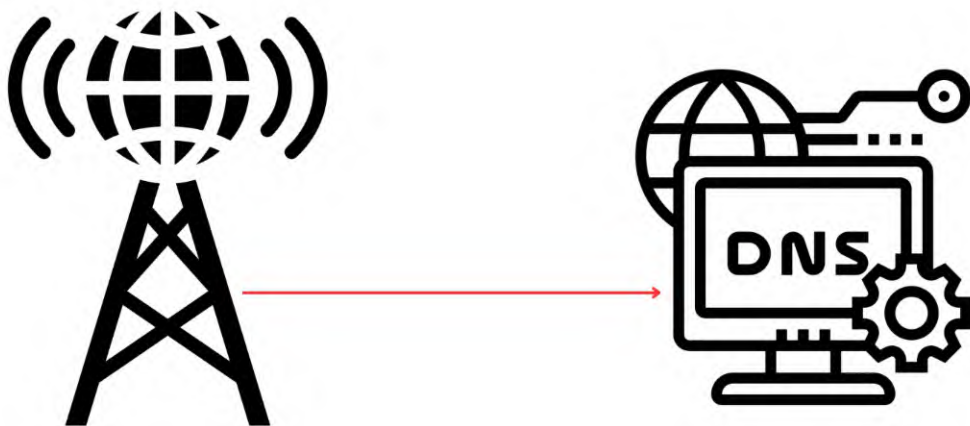


Figure 2.6: Step 2, the ISP applies DNS

Security features at this stage include ISP traffic filtering to block malicious sites and data logging.

NOTE

Data logging can be seen as an invasion of privacy since your ISP keeps track of the sites you visit.

If your ISP's DNS does not know the address, the request is forwarded to other DNS servers to find the right server for `lab7.com` in this case.

The DNS step is shown below, highlighting the process of finding the correct server and the use of DNSSEC (Domain Name System Security Extensions) to protect against DNS spoofing attacks.

Step 3 - DNS

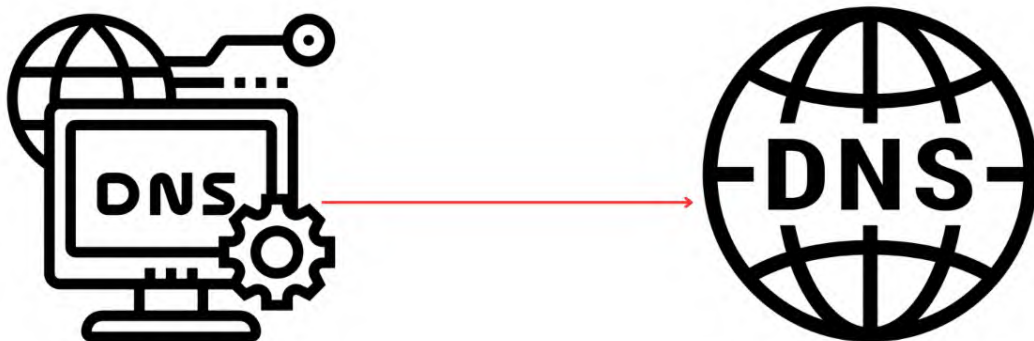


Figure 2.7: How DNS and DNSSEC help find the correct server and protect against DNS spoofing

After the DNS process, your request reaches the destination network, which is the web server for `lab7.com`, as visualized below:

Step 4 - Destination Network



Figure 2.8: Step 4 in web request flow: destination network security with firewalls and TLS/SSL certificates.

At this point, additional security features are in place, such as server firewalls to block malicious traffic and TLS/SSL certificates to ensure the legitimacy of the encrypted connection. The server processes your request and prepares to send the data back to you along the same path.

Return path of internet data

The final step in the data transmission process is the return trip, where the data from the web server travels all the way back to your computer. The data comes back through your ISP, then to your router, and finally to your device, following the same path but in reverse.

Your home router will convert the public IP address back into the private IP address of your computer, and all security measures on each hop still apply.

This process is a simplified version of how the internet works behind the scenes. If you want to explore the topic in greater depth, you can, but that goes beyond the scope of this section.

Before moving on, here is a useful tip: your ISP provides its own DNS server, but you can configure your router to use a different DNS server for improved security, privacy, and even performance. Many people notice a significant improvement in internet speed after making this change. Instead, of using your ISP's default DNS server, you can use public DNS servers such as Cloudflare, Google, or Quad. The recommended addresses are:

- Cloudflare: 1.1.1.1
- Google: 8.8.8.8
- Quad: 9.9.9.9

To change your DNS settings, log in to your home router, go to the network settings, and add the new DNS information. Make sure to write down any preconfigured DNS numbers from your ISP before making changes, so you can revert if needed.

How email works

Earlier we discussed the protocols used for emails. Now let's see how emails work on the internet. Consider the following example: Dwight wants to send an email to Meg at `meg@ghostmail.com`. The process involves several steps:

1. Dwight uses SMTP to send the email to his ISP's mail server.
2. Dwight's ISP's mail server does not know the IP address of `ghostmail.com`, so it contacts a DNS server to look up the IP address of `ghostmail.com`.
3. Once the DNS server provides the IP address, Dwight's ISP's mail server uses SMTP again to send the email to Meg's ISP's mail server.
4. Meg receives the email using either POP or IMAP, depending on her configuration.

The following diagram illustrates this process, showing the flow of the email from Dwight to Meg, including the DNS lookup and the use of the SMTP and POP/IMAP protocols:

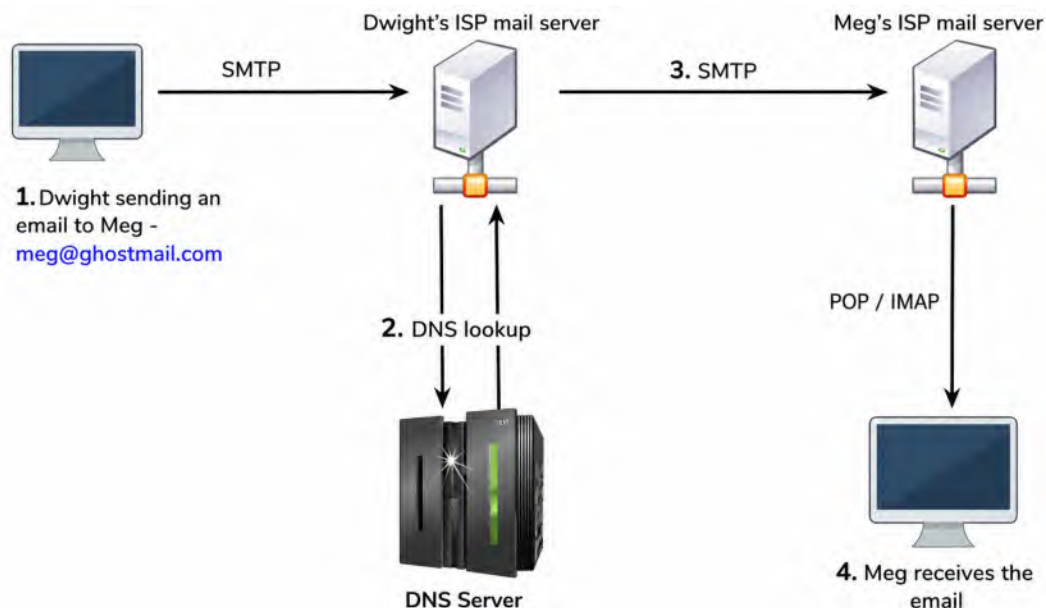


Figure 2.9: How email is delivered: SMTP, DNS lookup, and POP/IMAP in the email transmission process

Now that you have seen how the internet works behind the scenes, you are ready to try some very common networking tools and commands.

Networking commands and tools

On a Windows 11 machine, open the command prompt by pressing the Windows key and R, typing `CMD`, and pressing Enter. If you are on Linux or Mac, open your terminal.

The first command to try is the **ping** command. Make sure you have admin access to your terminal, as some commands may require it. The `ping` command is used to test connectivity and see whether you can reach a domain or website on the network. For example, to test connectivity to `imdb.com`, type the following command:

```
ping imdb.com
```

You will see an output similar to the following, showing replies from the IP address of imdb.com and indicating that zero packets were lost:

```
Pinging imdb.com [52.94.228.167] with 32 bytes of data:
Reply from 52.94.228.167: bytes=32 time=245ms TTL=235
Reply from 52.94.228.167: bytes=32 time=245ms TTL=235
Reply from 52.94.228.167: bytes=32 time=246ms TTL=235
Reply from 52.94.228.167: bytes=32 time=245ms TTL=235

Ping statistics for 52.94.228.167:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 245ms, Maximum = 246ms, Average = 245ms
```

The ping command is a very quick way to check whether you can connect to a website, but it does not provide much information beyond basic connectivity. The command's popularity comes from its speed and simplicity.

Now let's explore more advanced network commands to see the path that your data takes across the internet.

The traceroute command gives you a much more detailed view of how your data travels across the internet. When you use traceroute (or tracert on Windows), you see the exact path your data packet takes to reach a destination, such as a web server. For this example, run the following command to trace the route to labcyber.com:

```
tracert labcyber.com
```

The output is presented in the following screenshot:

```
C:\Users\onial>tracert labcyber.com

Tracing route to labcyber.com [134.209.184.67]
over a maximum of 30 hops:

  1    3 ms    1 ms    1 ms  192.168.1.1
  2    5 ms    4 ms    4 ms  100.78.0.1
  3    5 ms    20 ms   5 ms  ae8.fcr02j.cwdc.myaisfibre.com [49.228.4.99]
  4    5 ms    5 ms    5 ms  ve454.cgn05.cwdc.myaisfibre.com [49.228.4.36]
  5   16 ms   31 ms   6 ms  ae23.bgw02j.cwdc.myaisfibre.com [49.228.4.34]
  6    5 ms    5 ms    5 ms  aex.iig-cwdc-pe03.cwdc.myaisfibre.com [49.228.4.70]
  7   30 ms   30 ms   30 ms  119.31.0.114
  8   46 ms   48 ms   31 ms  unknown.telstraglobal.net [210.176.138.85]
  9   34 ms   36 ms   40 ms  i-92.sgnc-core01.telstraglobal.net [202.84.219.174]
 10  210 ms  207 ms  208 ms  i-1000.ulcn-core01.telstraglobal.net [202.84.140.142]
 11  194 ms  194 ms  194 ms  i-1008.ulco01.telstraglobal.net [202.84.178.14]
 12  189 ms  189 ms  189 ms  195.66.226.25
 13  190 ms  189 ms  189 ms  143.244.226.255
 14    *      *      *      Request timed out.
 15    *      *      *      Request timed out.
 16    *      *      *      Request timed out.
 17    *      *      *      Request timed out.
 18    *      *      *      Request timed out.
 19    *      *      *      Request timed out.
 20    *      *      *      Request timed out.
 21    *      *      *      Request timed out.
 22    *      *      *      Request timed out.
 23    *      *      *      Request timed out.
 24    *      *      *      Request timed out.
 26    *      *      *      Request timed out.
 27    *      *      *      Request timed out.
 28    *      *      *      Request timed out.
 29    *      *      *      Request timed out.
 30    *      *      *      Request timed out.

Trace complete.
```

Figure 2.10: Traceroute output for labcyber.com

The output shows that your data is sent to the public IP address for labcyber.com, which is 134.209.184.67. The first hop is to 192.168.1.1, which is the IP address of your home router. The second hop, 100.78.0.1, is likely the IP address of your internet service provider. As the trace continues, you see the packet bouncing from one router to another, including routers belonging to your hosting provider, MyAISFiber, as indicated by the domain names in the output.

As you examine the traceroute results, you notice that the latency (measured in milliseconds) for each hop is relatively low, typically between 1 and 50 milliseconds, until hop number 10. At this point, the latency jumps to over 200 milliseconds. This sudden increase suggests a

significant geographical change, such as the packet moving from one continent to another. For example, if you are in Bangkok, Thailand, and your hosting provider is also in Thailand, but the web server for LabCyber.com is located in Africa, Europe, or North America, this would explain the large jump in latency.

The traceroute output also shows that after hop 13, all subsequent hops time out. This means the packet reached a firewall on a server or router that blocks further traceroute or ping packets. Many firewalls are configured to block these types of packets for security reasons.

After completing the traceroute, use the `nslookup` command to check the IP address of the domain and perform reverse lookups. To look up the IP address for `labcyber.com`, enter the following:

```
nslookup labcyber.com
```

This returns the same IP address, `134.209.184.67`, confirming the result from the traceroute command.

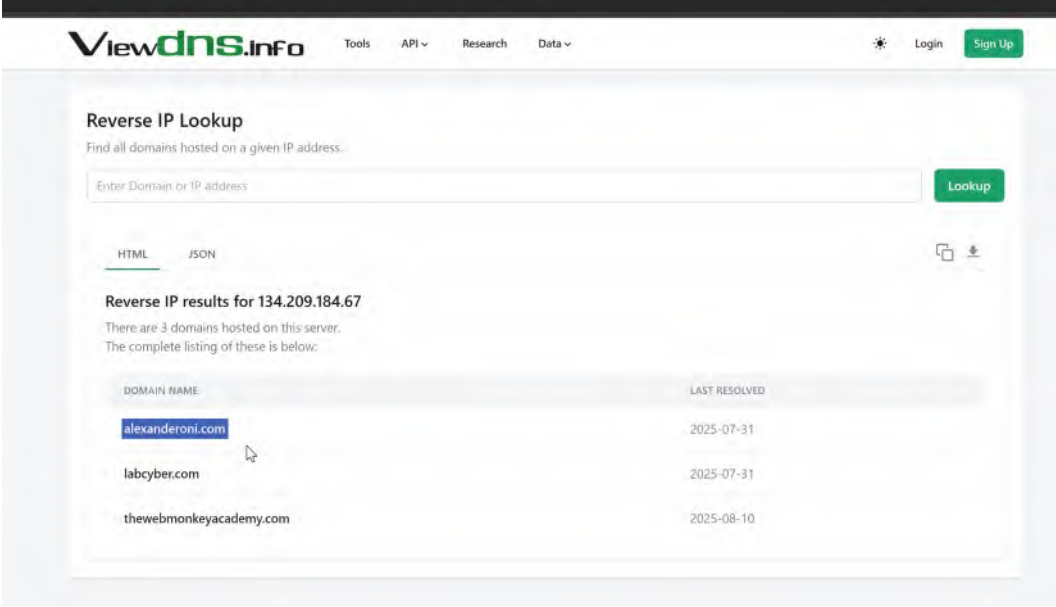
When you perform a reverse DNS lookup using the command `nslookup 134.209.184.67`, you might expect to get the domain name `labcyber.com`. However, the result you receive is actually `1382166.cloudwaysapps.com`. This happens because while domain names like `labcyber.com` are unique and map directly to an IP address, the reverse is not always true: a single public IP address can be shared by multiple domains, especially on shared hosting plans.

If your website is hosted on a shared hosting plan, such as with Cloudways, your domain shares the same public IP address with other domains. This means that a reverse lookup on the IP address will return the name provided by the hosting service, not necessarily your specific domain name.

A natural question is whether you can find out which other domains are sharing your exact public IP address. The answer is yes. You can use a tool like [viewDNS.info](https://viewdns.info/reverseip/)'s Reverse IP Lookup to discover all domains hosted on a given IP address. To do this:

1. Copy the IP address you want to investigate.
2. Go to <https://viewdns.info/reverseip/>.
3. Paste the IP address into the search field.
4. Click the Lookup button.

You will see a list of domains hosted on that server. For example, the results for 134.209.184.67 show three domains: alexandroni.com, labcyber.com, and thewebmonkeyacademy.com. In this case, all three are owned by the same person and are hosted on the same shared plan with Cloudways. The results are shown below:



The screenshot shows the ViewDNS.info website interface. At the top, there's a navigation bar with 'Tools', 'API', 'Research', and 'Data' menus, along with 'Login' and 'Sign Up' buttons. The main section is titled 'Reverse IP Lookup' with a subtitle 'Find all domains hosted on a given IP address.' Below this is a search input field labeled 'Enter Domain or IP address' and a green 'Lookup' button. The results are displayed in a table with two columns: 'DOMAIN NAME' and 'LAST RESOLVED'. The table shows three domains: alexandroni.com, labcyber.com, and thewebmonkeyacademy.com, all with a last resolved date of 2025-07-31 or 2025-08-10. The 'alexandroni.com' entry is highlighted with a blue background.

DOMAIN NAME	LAST RESOLVED
alexandroni.com	2025-07-31
labcyber.com	2025-07-31
thewebmonkeyacademy.com	2025-08-10

Figure 2.11: Reverse IP lookup results showing multiple domains sharing a single public IP address on a shared hosting plan.

The output of the Reverse IP Lookup tool lists the domains sharing the same public IP address. Thus, a reverse DNS lookup may not return your specific domain name, but rather the default name assigned by your hosting provider.

The last tool to explore is the *Whois* tool, available at: <https://whois.domaintools.com>. This tool allows you to find detailed information about a particular IP address or domain name. For example, searching for labcyber.com reveals that the domain name service is with SiteGround, while the hosting provider, as indicated by the ASN, is DigitalOcean.

Additional information such as the registrant's location (Maryland, United States) is also available, though personal contact details are often redacted for privacy. Refer to *Figure 2.13*:

DomainTools

PROFILECONNECTMONITORSUPPORT

Whois Lookup

Home > Whois Lookup > Labcyber.com

Notice: Possible depreciation

Whois Record for Labcyber.com

Domain Profile

Registrar	TUCOWS, INC. Tucows Domains Inc. IANA ID: 69 URL: http://tucowsdomains.com,http://www.tucows.com Whois Server: whois.tucows.com domainabuse@tucows.com (p) +1.4165350123
Registrar Status	ok
Dates	2,305 days old Created on 2019-04-20 Expires on 2027-04-20 Updated on 2025-04-24
Name Servers	NS1.SITEGROUND.NET (has 1,647,134 domains) NS2.SITEGROUND.NET (has 1,647,134 domains) Reverse NS
IP Address	134.209.184.67 - 2 other sites hosted on this server
IP Location	Colorado - Broomfield - Digitalocean Llc
ASN	AS14061 DIGITALOCEAN-ASN, US (registered Sep 25, 2012)
Domain Status	Registered And No Website
IP History	22 changes on 22 unique IP addresses over 13 years
Hosting History	13 changes on 9 unique name servers over 10 years

Whois Record (last updated on 2025-08-11)

Domain Name: LABCYBER.COM
Registry Domain ID: 2382396383_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2025-04-24T13:32:26Z
Creation Date: 2019-04-20T13:47:09
Registrar Registration Expiration Date: 2027-04-20T13:47:09
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Reseller: SG Hosting Inc.,
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: MD
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: https://tieredaccess.com/contact/275132bf-4462-411b-a029-0026b429034e
Name Server: ns1.siteground.net
Name Server: ns2.siteground.net
DNSSEC: unsigned
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
URL of the ICANN WHOIS Data Problem Reporting System: https://icann.org/wicf
"For more information on whois status codes, please visit https://icann.org/epp"
Registration Service Provider:
SG Hosting Inc., tucows@domains.siteground.com

Figure 2.12: Whois results for labcyber.com

Summary

In this chapter, we established the essential building blocks of networking by examining networks, local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), cloud networks, data packets, IP addresses, MAC addresses, protocols, ports, and key protocols such as HTTP, HTTPS, FTP, SFTP, IMAP, SMTP, and the TCP/IP protocol suite. Starting from foundational network concepts and types, we moved through the mechanics of data transmission and device communication, explored the structure and assignment of IP and MAC addresses, and progressed into protocol functions, port assignments, and the layered architecture of TCP/IP, before concluding with the roles and distinctions of networking devices such as hubs, switches, and routers.

The chapter's central distinction clarified how IP addresses serve as logical, dynamic identifiers for network communication, while MAC addresses are permanent, physical identifiers within a LAN, an analogy reinforced by comparing street addresses to apartment numbers.

With this foundation, you now understand the core components of a network, how devices communicate, and how data travels between them. However, understanding how networks operate is only one part of the picture. It is equally important to understand the threats that can target these networks and the methods attackers use.

In *Chapter 3*, we will explore **threat actors**, their motivations, and the **Cyber Kill Chain**, which provides a structured way to understand the different stages of a cyberattack.

3

Threat Actors and the Hacking Methodology

In this chapter, you will explore the world of **threat actors** and the *hacking methodology*, focusing on how hackers, from script kiddies, and black hats to insider threats such as compromised employees and disgruntled ex-staff, plan and execute cyberattacks. By the end, you will be able to identify the different types of hackers, understand their motivations, and break down the common steps they follow, including reconnaissance, exploitation, privilege escalation, establishing persistence, and attack execution.

Along the way, you will also examine key aspects such as the difference between external hackers and insider threats, the flexible nature of the hacking methodology, and the unique role of hacktivists. We will also introduce social engineering as a popular tactic. Recognizing how real-world attacks unfold, far removed from the dramatized action of popular culture equips you to anticipate threats, spot vulnerabilities, and build more effective defenses against the people and processes behind modern cybercrime.

In this chapter, we will cover the following topics:

- Popular Culture and Misconceptions About Hackers
- Categories of threat actors
- The Hacking Methodologies
- Social Engineering in Cybersecurity

Popular culture and misconceptions about hackers

Hugh Jackman, John Travolta, and Halle Berry star in the 2001 movie *Swordfish*, which features one of the most dramatic hacking scenes you will ever see. In this scene, Gabriel, played by

John Travolta, is searching for a highly skilled hacker and puts Stanley, played by Hugh Jackman, to the test. Stanley is given just one minute to hack into the database of the United States Department of Defense, all while under extreme pressure with a gun pointed at him. He frantically types in passwords, repeatedly gets access denied, until finally, at the last second, he succeeds and proves himself.

Scenes like this have shaped the way many people think about hacking, making it seem like a thrilling, high-stakes activity full of adrenaline and drama. In reality, the hacking process is often much less exciting than what you see in the movies.

Most real-world hacking is actually quite boring. While there are rare situations where hacking can be thrilling, in most cases, hackers are focused on gathering as much information as possible about their potential victims, striking quickly to get the data they want, and then disappearing. The process is usually not nearly as dramatic as what you see in the movies.

NOTE

The Swordfish scene is one of the most unrealistic portrayals of hacking ever made, and that's saying a lot given Hollywood's track record. If you want a more accurate depiction of hacking, the Mr. Robot series is a much better choice. Although it has some minor inaccuracies, it does a good job of showing what hacking is really like.

Despite how ridiculous the Swordfish scene is, it had a huge impact on my life. Before watching it, I wanted to be a web developer and had no interest in cybersecurity or hacking. But after seeing the movie, I, like many others, was inspired to pursue a career in cybersecurity and ethical hacking, thinking it would be as exciting as what I saw on screen. At the time, I was 15 years old, easily influenced, and I also had a huge crush on Halle Berry, which made the idea of becoming an ethical hacker even more appealing. While my expectations about meeting women like Halle Berry haven't come true, the movie still holds a special place in my heart because it inspired me to enter the field.

This scene is a great example of what hacking is not in the real world. It highlights how popular culture can create misconceptions about hackers and what they actually do. So let's talk about the bad guys, the different types of hackers out there and other types of threats that might go after you and your company.

Categories of threat actors

When you think about the different types of hackers, it's important to understand that not all of them are equally skilled or motivated by the same goals. You will encounter a range of threat actors, from those who are just starting out to highly skilled professionals, as well as those who

hack for a cause or from within your own organization. Let's go through each category in detail.

Script kiddies

The first group is known as **script kiddies**. If you compare them to a company structure, they would be like your interns. These are cybercriminals who are really not that skilled and lack much experience; they are basically learning "hacking" as they go, if you can even call it hacking. Script kiddies try to take down websites or inject malware into systems, not because they have a specific goal, but just to see whether they can do it and for bragging rights. They want to be able to tell their friends, "Hey, check me out, I took down this network or computer." In reality, they are more of a nuisance than a serious threat. In the cybersecurity world, calling someone a script kiddie is actually an insult to their hacking skills.

Black-hat hackers

The **black hat hackers** are the main threat. These individuals are very skilled and are purely motivated by financial interests. Their goal is to profit from their activities, often by stealing sensitive information, committing fraud, or selling access to compromised systems. For them, hacking is a business, and they use their skills to exploit vulnerabilities for personal gain. Black hats are extremely skilled and represent the biggest threat to you and your data.

Gray-hat hackers

There is also a special group called **gray hat hackers**. Like black hats, they are very skilled, but they are called "gray" because they often use black hat tactics for white hat objectives. Your white hat hackers are the good guys, pentesters, and ethical hackers, while black hats are the malicious ones. Gray hats fall somewhere in the middle. They might do things that are illegal, but their objective could be for something good, so the means justify the end. For example, a gray hat might hack their favorite social media platform, not to take it down, but to look for vulnerabilities. Once they find weaknesses, they report them to the platform's administrators. It's illegal to look for weaknesses without authorization, but in their reasoning, they use black hat tactics for the greater good.

Hacktivists

Hacktivists are motivated by a cause and may target a company if they disagree with its products or practices; for example, a group of hackers who are very pro-life might target a company that manufactures contraceptives, believing those products are harmful and deciding to take action against the company. Hacktivists operate based on their own beliefs, and while some people may agree with their cause, others may not.

Insider threats

These are threats that come from within your own organization. The main types of **insider threats** include the compromised employee, the disgruntled or ex-employee, the second streamer, and the spy or saboteur.

A **compromised employee** is someone whose credentials have already been hacked or stolen, often without their knowledge. This employee continues with their daily activities, unaware that hackers are using their login details to access company data.

A **disgruntled employee**, who could also be an ex-employee, is someone who is no longer happy at the company. Maybe they feel cheated out of a promotion or believe they have been treated unfairly. Their motivation is often revenge; they want to get back at the company for perceived wrongs. Threats like these are real and can be very damaging.

A **second streamer** is an employee who uses company assets to make money on the side. For example, an employee at a stock trading platform might have inside information about a particular stock and use that information to profit personally. This is illegal.

Spies and saboteurs

The most serious insider threat is the spy or saboteur. This is an employee who deliberately seeks employment at a company with the sole purpose of gaining inside access and causing as much damage as possible. This could involve a rival company planting a spy in your organization to steal information or damage data. While this might sound like something out of a movie, it does happen in the real world.

So these are the main categories of threats that you should be aware of.

Let's now take a look at the hacker methodology in order for you to better understand how hackers actually think and operate.

The hacking methodology

There is no official playbook or guide on hacking; cybercriminals do not follow a single manual or attend a school of cybercrime where they are taught a fixed sequence of steps. The process is flexible, but there are particular steps that are very common in most cyberattacks, and these are what you will examine next.

Reconnaissance (footprinting)

The very first step is usually called **reconnaissance** or **footprinting**. This is where cybercriminals try to gain as much information as they can about the target. Think of it like the movies where bad guys plan a bank robbery. They do not just walk in and announce the robbery. Instead, they do their homework: figuring out how many security guards there are,

what weapons they have, where the cameras are, and how long it will take for the police to respond. The same principle applies to sophisticated cybercriminals, who gather as much information as possible about their target before launching an attack.

Gathering information about the target involves two main approaches: **passive reconnaissance** and **active reconnaissance**.

Active reconnaissance is the point where hackers move beyond simply gathering public information and start probing for real vulnerabilities and weaknesses in your systems. Here, they look for things like **IP (Internet Protocol) addresses**, DNS servers, open ports, usernames, passwords, and details about company software.

Passive reconnaissance involves collecting easily accessible information such as email addresses, phone numbers, social media accounts, and physical locations, details that are typically public and legal to obtain.

Exploitation

Once hackers have collected as much information as possible about your company and identified potential vulnerabilities, they move into the **exploitation phase**. In this phase, attackers attempt to take advantage of the weaknesses they have discovered. Methods can include sending phishing emails, conducting social engineering attacks, exploiting weak passwords or unpatched software, and injecting malware (we will discuss these later in the chapter).

Privilege escalation

After successfully exploiting a vulnerability, the next step is **privilege escalation**. At this stage, hackers aim to increase their control over the compromised target. They may create new accounts, hijack the network, or, if their initial access was through a non-admin account, attempt to gain control of an admin account. Admin accounts provide significantly more power and access than regular user accounts, making them a primary target.

Establishing persistence

The following step is **establishing persistence**. Here, attackers work to ensure they can maintain access to the system even if the breach or attack is discovered. Techniques for persistence include creating backdoors or setting up remote access controls, allowing hackers to return to the compromised environment at will.

Attack execution

Once persistence is established, hackers proceed to the **attack execution** phase, where they carry out their intended malicious actions. These could involve data extraction, such as stealing sensitive files, data mining for valuable information, or data corruption, where files

are altered or destroyed. Attackers may also disrupt services, install malware, or manipulate system settings to achieve their goals.

Cover-up and avoidance of detection

The final phase in the hacker methodology is **cover-up and avoiding detection**. In this stage, attackers attempt to erase their tracks and ensure that victims remain unaware of the breach. Techniques include using **Internet Control Message Protocol (ICMP)** tunnels, clearing event logs, and erasing command histories, all with the goal of making sure the attack goes unnoticed.

To recap, the typical sequence of a cyberattack involves reconnaissance, exploitation, privilege escalation, establishing persistence, attack execution, and finally, cover-up. These six steps form the usual process that cybercriminals follow to successfully compromise a company.

Now let's discuss one of the most popular threat actor techniques, social engineering, and the various forms it can take.

Social engineering in cybersecurity

Social engineering is the exploitation of human emotions and interactions to extract valuable information. While the term is widely used in cybersecurity, social engineering is not unique to this field. You encounter it in negotiation, where one party tries to convince the other that they have more advantages, or in the actions of con men and fraudsters who trick people into doing things they normally would not do. Social engineering also appears in everyday relationships.

A well-known example is the movie *Catch Me If You Can*, directed by Steven Spielberg and starring Leonardo DiCaprio and Tom Hanks. The film tells the true story of Frank Abagnale, Jr., who, before the age of 20, successfully impersonated a doctor, a lawyer, and an airline pilot. His success was due to his mastery of social engineering, allowing him to convincingly adopt these roles. In real life, Frank Abagnale, Jr. eventually worked for the FBI, helping them in their fraud department.

Social engineering is a very dangerous part of cybersecurity because it exploits human error. When you work with software or hardware, you know what to expect: software is predictable, hardware is predictable, and if you have the best firewalls and anti-malware, you can expect the best results.

However, human beings are not software or hardware. While people can be predictable in some aspects, overall, human behavior is far less predictable. No matter how much training employees receive, a skilled social engineer can still manipulate them, so there is always a high probability that someone might fall victim.

There are four main tactics used in social engineering: baiting, pretexting, quid pro quo, and phishing.

Baiting

Baiting involves luring the target into taking an unfavorable action. The social engineer tries to bait the victim, often using links in emails (which overlaps with **phishing**, discussed later) or by dropping infected USB drives in strategic locations. For example, imagine you are leaving your office and see a USB drive on the ground in the parking lot. Out of curiosity, you might pick it up, take it back to your office, and plug it into your computer, accidentally infecting your entire network. This scenario is not hypothetical; it has happened in real life. Hackers deliberately drop infected USB drives around the employees of a company they want to hack, relying on curiosity to get someone to plug it in and compromise the system.

Pretexting

Pretexting is a tactic that relies on looking, acting, or sounding the part to gain trust. For instance, if someone approaches you wearing the T-shirt of your telecommunications provider, say, AT&T, and introduces themselves as an employee, you are likely to believe them just because of the shirt. Most people would not question whether the T-shirt was simply bought online. The default assumption is that someone who looks and sounds the part is legitimate, unless you are naturally very paranoid. Pretexting works by exploiting this tendency to trust appearances and convincing behavior.

Quid pro quo

Quid pro quo involves offering a service in exchange for information. For example, a contractor working on a project inside a company might ask employees seemingly innocent questions. In a real-life case, a hacker who wanted to take down a company actually got a contract to work there. While working on the computers, he asked employees questions like, *How much do you get paid? I'm thinking of working here too. What's it like? Do you get paid well? How often do you have to run security updates? How often do you have to change your password?* You might think these questions would raise suspicion, but a skilled social engineer is a master psychologist who knows exactly when and how to ask. You could become a victim without even realizing you are giving away valuable information.

Kevin Mitnick is often called the Michael Jordan of cybersecurity-related social engineering. When he was younger, he gained access to highly sensitive information through social engineering, not technical hacking such as password cracking. Many, including myself, consider him one of the greatest hackers of all time because of his mastery of social engineering. If you are interested, you should check out his books about his life as a social engineer; they are very entertaining and insightful.

Phishing

Phishing is widely regarded as the most prevalent type of cyberattack. This well-known attack method is indiscriminate. It can target individuals and organizations of any size. Phishing involves an attempt by a cybercriminal or hacker to obtain sensitive information by sending carefully crafted emails to potential victims while impersonating a trusted individual or organization.

So the email typically will contain some sort of a malicious link that when clicked on could either install malware or in most cases redirect the user to a fake website that will appear to be legitimate. In most cases, it will resemble the actual website of the company that the hacker is impersonating. Once the victim has provided their login credentials, those credentials, which would be the username and password in most cases will be recorded. The credentials will then be sent back to the hacker. So now the hacker has access to the victim's credentials. We will discuss phishing in more detail in *Chapter 4*.

Vishing

This type of attack is basically a phishing attack with a phone call. These are also very common, and I have received my own share of vishing calls.

Consider a very popular YouTube clip called "hack attack vishing." In this video, social engineers use vishing to call a man's cellular provider support desk and, with basic tools, gain access to his entire mobile account, locking him out in the process. The female social engineer tells the man she will lock him out of his own account, and he insists it is not possible because he trusts his provider.

She calls support, pretends that she has a baby (with crying sounds in the background), and talks about her family's tough times and a recent loan application. She is able to fool the support analyst into letting her log in to the man's account, change the password, and access personal information such as his social security number.

This video demonstrates how social engineers exploit human emotions, and it happens all the time, even to support staff who have received social engineering training.

Staying safe

Before we round up, what exactly are the preventive methods for phishing? How can we prevent ourselves from falling victim to phishing attacks? The best way is simply through training and education. Further, your own security alertness is critical. This is not just about knowing the tactics of phishing attackers, but also about being alert at all times.

If an email looks suspicious, your security sensors should be triggered immediately. Your thought process should be "Let me make sure that this email is legitimate before I click on that

link." And last but not least, use anti-malware software, which can also be used to fight against phishing attacks.

Apart from phishing attacks targeting individuals or organizations, many social engineering techniques are used in the workplace and understanding them is critical for employees of different companies. Let's look at these next.

Lunchtime attacks

One common attack is the **lunchtime attack**, where an employee does not log off before leaving their workstation for lunch. This scenario is risky because an insider with negative intentions could take advantage of the unattended workstation, especially if the employee was working on something important. Leaving your workstation unlocked during lunch poses a significant security risk.

Piggybacking

Piggybacking refers to when an attacker enters a secure building with the explicit permission of an employee. The employee may hold the door open or otherwise allow the attacker to enter, often out of politeness or because the attacker has convinced them to do so.

There is an example from the movie *Sneakers* (1992), featuring Robert Redford, that demonstrates how social engineers use psychological manipulation to gain unauthorized access. By first planting a believable story about a cake delivery and then returning with a box and balloons, Redford's character convinces the receptionist that he belongs and pressures him at a busy moment to allow entry. This sequence shows how attackers exploit trust, distraction, and urgency to bypass security controls. While the movie dramatizes the scenario, in real-world piggybacking, an attacker might simply wait for an employee to approach an entrance and follow closely behind, often carrying something heavy to elicit sympathy or assistance. Human nature's tendency to trust and help others is a key vulnerability that social engineers exploit.

Tailgating

Tailgating is closely related to piggybacking, but with a subtle difference. In piggybacking, you typically have the victim's knowledge or even their assistance as you enter. Tailgating involves following someone into a secure area without their knowledge or explicit permission.

To illustrate this, consider a scene from *Diamonds Are Forever*, a James Bond movie featuring the character Klaus Hergesheimer. In this clip, Bond uses a fabricated identity and a believable story about checking radiation shields to blend in and gain access to a restricted area. By acting as if he belongs and engaging in casual conversation, he avoids suspicion, and is able to slip past security. This demonstrates how attackers can use social engineering, impersonation, and timing to bypass even well-trained guards and more reliable security measures.

Shoulder surfing

Another common social engineering tactic is shoulder surfing, where someone attempts to observe you entering sensitive information, such as a password or **PIN (Personal Identification Number)**, by looking over your shoulder. While this is less common in office environments, since it is usually obvious when someone is standing too close, it can still occur, especially at places such as ATMs or shared workstations. You should remain aware of your surroundings and be cautious if someone is lingering nearby while you are entering confidential data.

Dumpster diving

Dumpster diving is another technique that attackers use to obtain sensitive information. In this scenario, a hacker goes through your company's trash to find documents, notes, or other materials that were not properly destroyed. This method is surprisingly effective because many organizations fail to shred or thoroughly destroy sensitive paperwork before disposal. Instead, employees may simply crumple up documents and toss them in the garbage. After hours, cleaning staff remove the trash, and an attacker can easily access it outside the building. By sifting through discarded materials, hackers can recover valuable information that aids in further attacks or unauthorized access.

Let's see how these tactics can work together. Imagine a hacker attempting to access a secure building. They might tailgate behind an authorized employee to enter, potentially observe sensitive information through shoulder surfing, and then search through the building's trash bags for documents containing confidential data. Even if the attacker does not succeed with one method, combining multiple social engineering techniques increases their chances of obtaining the information they seek.

To prevent social engineering attacks in the workplace, you need to focus on both awareness and practical safeguards. While employee training is an obvious and essential step, you should also remain observant of your surroundings and question unusual behavior. For example, if someone without a key card tries to enter your office or company, do not hesitate to ask questions such as, "Are you looking for someone?" or "What are you here for?" If their answers do not convince you, follow up by calling security to verify their authorization and clearance.

Proper disposal of sensitive files is also critical. When you have very important information on paper, always shred it thoroughly before discarding. This principle extends beyond paper: any physical medium containing sensitive company data, such as hard drives, USB drives, or CDs, must be properly destroyed before disposal. This ensures that even if someone gains access to these items, they cannot retrieve the information stored on them.

Summary

In this chapter, we established a clear understanding of threat actors and by dissecting the real-world capabilities and motivations of hackers, insider threats, and the step-by-step hacking methodology. Starting from popular culture and misconceptions about hackers, we moved through the categories of threat actors, including script kiddies, black hat hackers, gray hat hackers, white hat hackers, hacktivists, and insider threats such as compromised employees, disgruntled and ex-employees, second streamers, and spies and saboteurs, before breaking down the hacker methodology into reconnaissance (passive and active), exploitation phase, privilege escalation, establishing persistence, and attack execution, followed by a detailed exploration of social engineering techniques such as phishing, vishing, baiting, and tailgating.

The key distinction we established is the contrast between dramatized movie portrayals of hacking and the nuanced, multi-step reality of cyberattacks, as well as the differences between external hackers and insider threats. This chapter equips you with the practical ability to identify various threat actors, recognize their tactics, and understand the sequential phases of a cyberattack, forming a solid foundation for defending against real-world cybersecurity threats.

Chapter 4 will discuss more common cyberattacks in detail.

Part II

Cyber Threats and Attacks

Part II — Cyber Threats and Attacks brings together chapters that examine the landscape of digital dangers, from the mechanics of common cyberattacks and the varieties of malware to the impact of real-world cyber incidents. Together, the chapters in this part provide a comprehensive understanding of how attackers exploit technical and human vulnerabilities, the forms malicious software can take, and the significant consequences cyber threats have had on infrastructure and global affairs. This part equips you to recognize, understand, and contextualize the evolving nature of cyber threats. This part contains the following chapters:

- *Chapter 4, Common Cyber Attacks*
- *Chapter 5, Understanding Malware*
- *Chapter 6, Real-World Cyber Incidents*

4

Common Cyber Attacks

This chapter explores the concrete threats posed by common cyberattacks, focusing on how attackers exploit weaknesses in systems and human behavior to gain unauthorized access or control. By the end, you will be able to recognize and understand the mechanics behind brute force attacks, phishing in its many forms, including spear phishing, whaling, vishing, and smishing, as well as the roles of bots, botnets, and the command and control servers that orchestrate large-scale campaigns.

You will examine how attackers use automated software to guess passwords, craft convincing emails that prey on naivety, curiosity, and fear, and manipulate infected computers (zombies) to build botnets for attacks such as DDoS. Mastering these distinctions is crucial for defending against threats that target both technical vulnerabilities and psychological triggers, helping us protect sensitive data and maintain the integrity of systems.

In this chapter, we will cover the following topics:

- Brute force attacks
- Phishing Attacks
- Bots and Botnets
- **Denial of Service (DoS)** and **Distributed Denial of Service (DDoS)** Attacks
- Man-in-the-Middle Attacks
- SQL Injection and Cross-Site Scripting (XSS) Attacks
- Supply chain attacks
- Advanced Cyberattacks

Brute force attacks

Attackers often use a combination of methods to steal your data, and one of the oldest and most popular is the **brute force attack**. This type of attack is a trial and error method used against passwords, PIN numbers, encrypted data, and similar targets. The reason it is called trial and error is that it checks all possible key combinations.

In a brute force attack, the hacker tries every possible combination of letters, figures, and symbols in an attempt to find the correct password. Automated software is typically used to generate a very large number of consecutive guesses, so the hacker does not have to type each combination manually. This approach is considered infallible because, given enough time, the attacker will eventually find the correct password. However, it is also extremely time-consuming, especially for longer passwords.

The effectiveness of a brute force attack depends heavily on the key length. The longer your password, the more time it will take for a hacker to crack it. You can think of a brute force attack like a burglar trying to break into a safe by entering every possible combination. The more characters in the code or password, the longer it will take to crack.

Let's take a look at a concrete example to understand how the number of possible guesses in a brute force attack is calculated. Suppose your password is just two characters long. If you only use lowercase letters, uppercase letters, or numbers for each character, that gives you 26 lowercase letters, 26 uppercase letters, and 10 numbers, totaling 62 possible choices for each character. For a two-character password, the total number of permutations is 62 multiplied by 62, which equals 3,844 possible combinations.

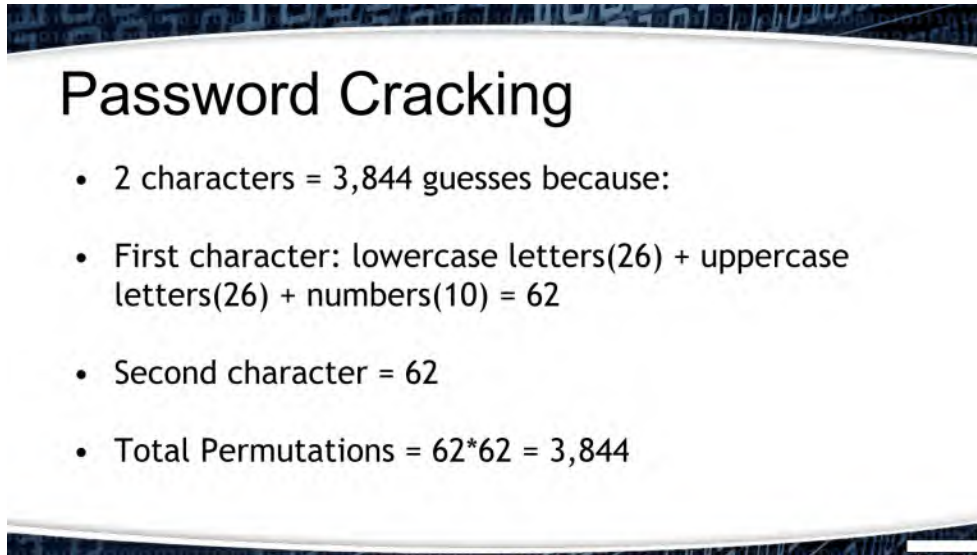


Figure 4.1: Password permutation calculation for 2-character passwords using letters and numbers

You might think that 3,844 guesses is a lot, but with automated software, this number of guesses can be generated *within seconds*. There are programs that can attempt all these combinations almost instantly, so using a two-character password is highly insecure.

There is also a special kind of brute force attack called a **dictionary attack**, where every word from a dictionary is used in an attempt to crack the password. This is why you are always advised not to use dictionary words as your password.

To defend against brute force attacks, you should:

- Use strong passwords with a minimum length of eight characters, combining uppercase letters, lowercase letters, numbers, and symbols.
- Restrict the number of times a user can attempt to log in successfully. Many websites already enforce a maximum of three login attempts.
- Enforce a timeout for users who have exceeded the specified number of failed login attempts.

When you implement all three of these measures, brute force attacks become much more difficult for anyone trying to crack your passwords.

With brute force attacks covered, let's turn our attention to phishing, a type of social engineering attack.

Phishing attacks

As also mentioned in *Chapter 3*, phishing is one of the most popular and widespread types of cyberattacks, targeting both individuals, and companies regardless of size. In a phishing attack, a hacker attempts to acquire sensitive data from a victim by sending a carefully crafted email that impersonates a trusted person or organization. In this section, I will provide real-world examples of phishing emails.

When you receive a phishing email, it typically contains a malicious link. Clicking this link can either install malware on your device or, more commonly, redirect you to a fake website that closely resembles the legitimate site of the company being impersonated. If you enter your login credentials on this fake site, your username and password are captured and sent directly to the hacker, giving them access to your account.

There are three things you should be aware of that phishing relies on, and they are naivety, curiosity, and fear. Naivety is when the victim doesn't know anything about phishing. They don't know about the tactics and so on.

Then we have curiosity; maybe the victim receives an email telling them that they're the lucky winner of a certain kind of prize and can obtain the prize by clicking on the provided link.

Finally, we have fear, which is typically the most common factor. The victim might receive an email that says something such as "We're going to close your account in 24 hours if you don't do this or you don't do that." This creates some sense of urgency and fear in the victim and compels them to act quickly.

Examples of phishing emails

Let's now look at some practical examples. The first one is for PayPal as shown in *Figure 4.2*. So here the attackers were trying to impersonate PayPal. And you can see right here they have the PayPal logo right there:

Suspended Activity

To: Jonathan Guy,

Reply-To: LimitationsPayPalsTeaminfo@gmx.com

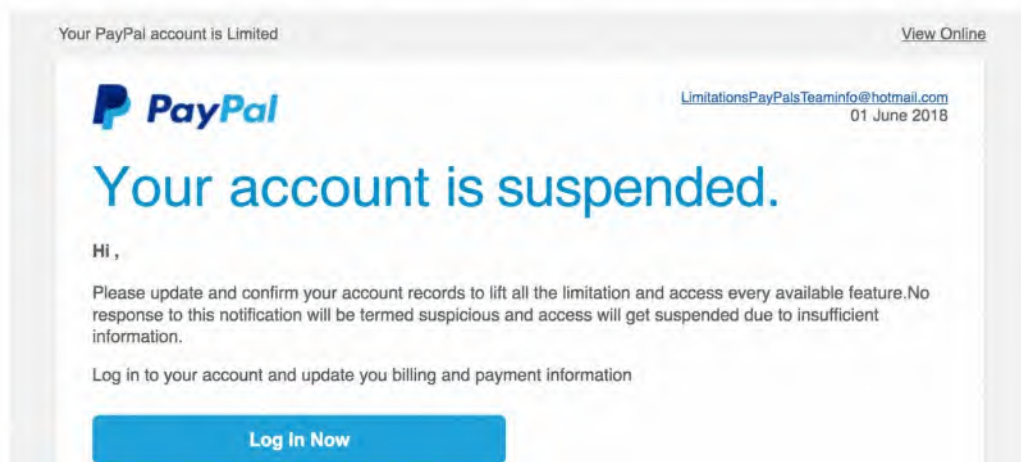


Figure 4.2: PayPal phishing email

The headline says your account is suspended, invoking fear. To add to the urgency, the message also says that no response to this notification will be termed suspicious and access will get suspended due to insufficient information.

A prominent blue button labeled "Login" is also presented to the user. When the victim clicks this button, they are directed to a login page designed to closely mimic the official PayPal login interface, but it is not legitimate.

The following example, also involving PayPal, illustrates a similar tactic:

We've temporarily suspended your account.

PHISHING



Your account has been [→]suspended

Dear client,

We've temporarily **suspended** your PayPal account due to some issues in the automatic verification process.

For this reason we suspended your PayPal account , indeed you can not make any transaction (and/or) payment until you **verify** your account informations. We will provide with all the steps you need to unlock it. Please follow these instructions after you click on the link below.

UNLOCK ACCOUNT

Follow these steps :

1. Login to your PayPal account.
2. Update your **Billing** informations.
3. Update your **Payment** method.
4. Confirm your **Identity** details.

If you do not verify your account, your funds will be lost permanently.

Please help us to clear your status and unlock your account.

Thanks,

PayPal

Please do not reply to this email. To contact us, click on [Contact](#).

[Help](#) | [Resolution Center](#) | [Security Area](#)

Figure 4.3: PayPal account suspension

This message says, "we've temporarily suspended your account" and cites issues in the automatic verification process. There is a button provided to **unlock account**. When the victim clicks on that button, it takes them to the unlock account page, where they're prompted to provide their username and password. That information is then sent to the hacker and now the hacker has access to the victim's PayPal credentials.

Phishing attacks are not limited to financial services. For instance, you might receive an email that appears to be from YouTube support, with a subject like **Inappropriate video alert**. The message claims that some videos you uploaded have been flagged as inappropriate and instructs you to click a button to edit the videos. If you do not comply, the email threatens that your channel will be suspended. Again, the email includes a large blue button labeled **Click here to edit**. Here is a screenshot:

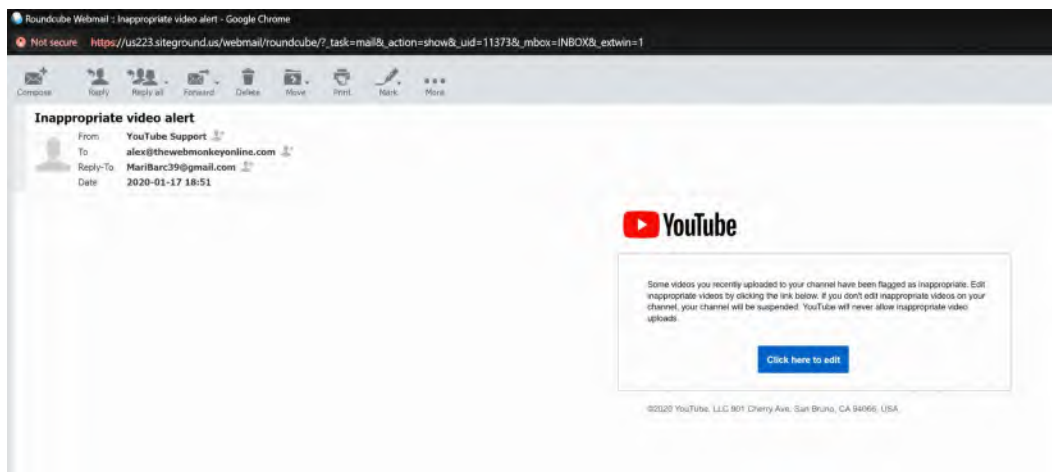


Figure 4.4: YouTube phishing email

Let's use this opportunity to show you how you can identify a phishing email. The most common and the easiest way will be for you to simply go to the sender's link.

In this example, we hover the mouse there and see that the email address points to `MariBare39@gmail.com`:

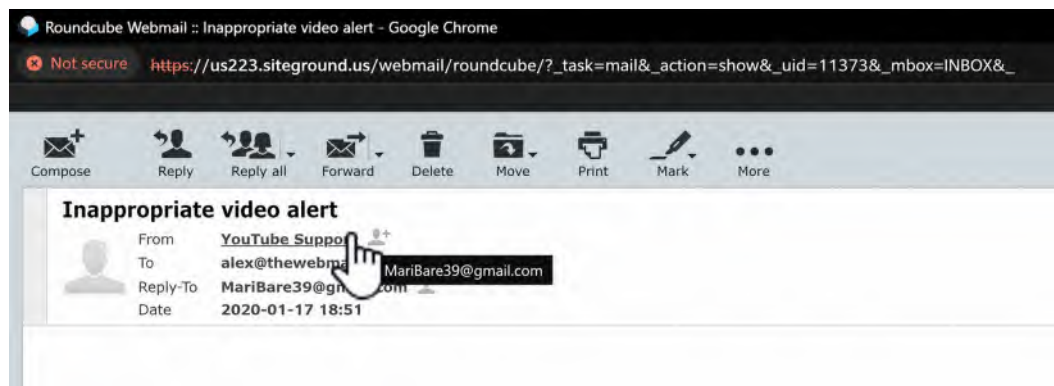


Figure 4.5: Spotting signs of phishing

If this were a legitimate email from YouTube, the from link would have been YouTube support. This is the first indicator that this is likely a phishing link.

Other indicators of phishing emails include misspellings and grammatical errors, which are common in many phishing attempts. If you notice these issues, it is likely that the email is a phishing attempt.

If you are unsure whether an email is a phishing email, the safest approach is to go directly to the actual website yourself and log in. For example, if you receive an email from PayPal saying your account has been suspended, do not click on any links in the email. Instead, open a new tab in your browser, manually type in PayPal.com, press enter, and log in with your username and password. If there is a real issue with your account, you will see an alert on your profile or account page. This is the best way to determine whether there is a genuine problem with your account. Always go to the website yourself and log in, rather than relying on any links provided in the email.

Now let's move on to the different types of phishing. We have spear phishing, vishing, and smishing.

Types of phishing attacks

There are several types of phishing attacks that you should be aware of. The classic email phishing attack is where the attacker sends the victim an email containing a malicious link.

Spear phishing

First, we have **spear phishing**, which is arguably the most dangerous form of phishing. Spear phishing targets a specific individual or a particular company. Attackers often have a lot of information about the potential victim, such as knowing that the victim recently created a new account on Netflix, attended a seminar, or made an investment. This allows the attacker to craft an email that is very convincing, including details that only someone who knows the victim would know. These attacks are very dangerous and tend to have a high success rate, depending on how much the attacker knows about the intended victim.

Whaling is another type of phishing attack, typically directed at senior executives of a company. Whaling attacks are sometimes called CEO fraud attacks because they specifically target C-level executives such as the CEO, CIO, or COO. The goal is not just to attack any employee, but to go after the most influential figures in a company, the so-called "big whips" or "big dogs."

Vishing

Another variant is **vishing**, which is phishing conducted over the phone. You might receive a call from someone claiming to be "John Smith" from Microsoft, but the caller's accent or other cues may raise suspicion. The caller might claim your computer has a virus and instruct you to visit a particular website or enter certain commands, ultimately gaining access to your computer.

NOTE

Vishing is phishing, but with phone calls instead of emails.

Smishing

Smishing is a phishing attack delivered via text messages rather than phone calls or emails. These are extremely common; you might receive a text claiming malware has been found on your computer or a message from your supposed internet provider stating your account has been suspended, urging you to click a link to update your profile. Smishing is simply phishing through SMS or text messages.

To prevent falling victim to phishing attacks, the most effective defense is training and education. When you are aware of phishing tactics, you are less likely to be deceived. Maintaining a high level of security alertness is also crucial. If you receive an email that seems suspicious, your security instincts should prompt you to verify its legitimacy before clicking any links. Security alertness is key to avoiding these attacks.

High-profile invoice fraud cases

Evaldas Rimasauskas is a name you should remember when discussing high-profile fraudsters. Over a two-year period, he managed to scam both Facebook and Google, two of the world's largest tech companies, out of more than \$100 million. His method involved registering a company in Latvia called Quanta Computer, which closely resembled the legitimate Quanta company based in Taiwan that supplied hardware to both Facebook and Google.

By purchasing a domain that looked almost identical to the real Quanta's, Rimasauskas was able to send fake invoices and forged contracts to employees in the finance departments of both companies. He impersonated real Quanta employees using these lookalike email domains, tricking the finance teams into wiring money to bank accounts he controlled in Latvia and Cyprus. This scheme ran from 2013 to 2015, until he was eventually caught, arrested in 2017, extradited to the US, pleaded guilty in 2019, and was sentenced to five years in prison, along with a \$9.7 million forfeiture and restitution order.

Payment verification best practices

To protect yourself and your organization from attackers such as Evaldas Rimasauskas and his associates, always verify payment requests through a second channel. Instead of relying solely on email, call the person making the request, arrange a video call, or meet in person if possible. Check for subtle spelling changes in domain names and be wary of urgent or confidential requests that bypass normal procedures.

For organizations, implement multi-person approval for large transactions. For example, require three different people to provide their permission before a transaction goes through. Use email authentication protocols such as SPF, DKIM, and DMARC. Conduct regular phishing simulation training to remind employees about phishing attacks. Limit publicly available information about staff roles and financial processes, if it is not necessary to inform the public

about certain aspects of your organization, keep it private and avoid sharing it on social media profiles.

Having discussed phishing and how attackers manipulate people into revealing information or taking harmful actions, we can now turn to another common tool used in cyberattacks: bots and botnets. Unlike phishing, which often relies on human interaction, bots are automated programs that can perform tasks with little or no direct involvement from an attacker.

Bots and botnets

Bots are very common in network and computer security, and the term is actually short for robots. You may also hear bots referred to as zombies or zombie computers, because in a bot attack, an attacker gains complete control over the infected computer using a Trojan horse. Once your computer is infected, the attacker can manipulate it to do anything, which is why it is called a zombie.

When your computer becomes a bot, its performance is usually severely degraded. If you notice your system is not performing as well as it used to, it could be a sign that your computer has been infected and is now part of a botnet. A **botnet** is simply a collection of bots, all under the control of a single attacker.

The person who controls a botnet is called a **bot master** or **bot herder**. These individuals use a special server known as a **command and control server** to issue commands to all the bots in the botnet. Botnets are often used to perform **Distributed Denial-of-Service (DDoS)** attacks, which require thousands of computers to be effective. Because of this, botnets are a very common tool for launching such attacks. In such attacks, the victim is positioned at the bottom of the botnet hierarchy.

Updating your antivirus and anti-malware products is one of the best ways to protect yourself from becoming part of a botnet. Not clicking on suspicious links is equally important, since clicking on a Trojan horse is a common way for your computer to become a bot. Attackers often send out emails with malicious links, and if you click on one, your computer can become infected and join a botnet. By keeping your security software up to date and avoiding suspicious links, you can greatly reduce your risk of becoming a bot or part of a botnet.

As mentioned earlier, one of the most common uses of botnets is carrying out DDoS attacks. Let's take a closer look at how DDoS attacks work.

Denial of service (DoS) and distributed denial of service (DDoS) attacks

Denial of service (DoS) and DDoS attacks are two very popular types of cyber attacks that target servers by overwhelming them with requests. In this section you will learn how these attacks work, how they differ, and what makes DDoS attacks especially difficult to combat.

A typical scenario involves a web server, such as the one for `bbc.com`, and a computer making a request to access content. The client might want to get the content for a particular page, such as the homepage. The web browser sends a request to the server asking for the content. An illustrative diagram is provided below:

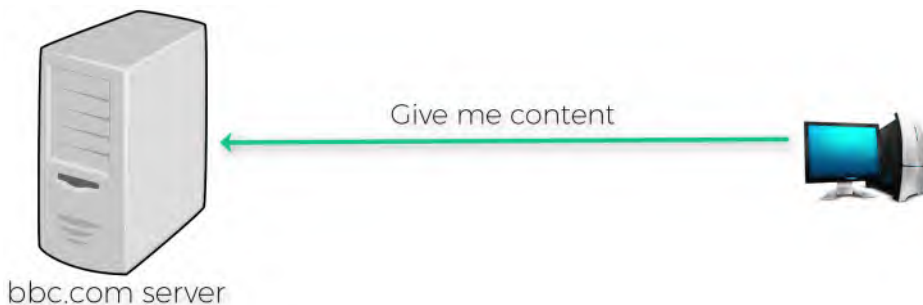


Figure 4.6: A web browser requests content from a web server, illustrating the client-server model.

The client sends a "Give me content" request to the server. The web server responds by sending back the requested content, such as the homepage or a specific article. In this exchange, the server replies, "Here you go," to the client's request.

Now, imagine a scenario where the same individual makes over 100,000 requests at the same time. The web server becomes overwhelmed by the sheer number of requests and cannot keep up, which knocks the server out of action. This is called a **denial of service attack**, where an attacker sends so many requests to a server that it becomes unavailable.

A single computer sends 100,000 "Give me content" requests to the server.

With a **DDoS attack**, the objective is the same, to knock out a server, but instead of one computer making the requests, thousands of computers all over the world send requests at the same time. This makes DDoS attacks much larger in scale and much more difficult to defend

against. DDoS attacks are more severe than DoS attacks because of the number of computers involved and the volume of traffic they generate.

So, how do you determine whether a DDoS attack is happening? The two most common signs are that a website suddenly becomes inaccessible or that you start receiving an enormous amount of spam email. These are usually the first indications that a DDoS attack is underway.

One of the most effective ways to fight against a DoS attack is to block the IP address of the attacker. Since a DoS attack comes from a single source, you can simply block that specific IP address, making it much easier to defend against compared to a DDoS attack.

With a DDoS attack, defending is much more difficult because the attack traffic comes from thousands of different sources all over the world. This makes it hard to distinguish between legitimate user traffic and attack traffic, especially when it is spread across so many sources. DDoS attacks are often carried out using **botnets**, which allow hackers to control thousands of computers and send requests simultaneously.

DDoS and DoS attacks are very common among hackers, who frequently use these attacks to make a statement or disrupt services. However, many other cybercriminals also use DDoS and DoS attacks for various purposes.

Combating DDoS attacks is challenging, but there are three major strategies you can use:

- Over-provisioned bandwidth: A company could purchase more bandwidth than they typically need, making it harder for attackers to overwhelm their web servers. This does not prevent a DDoS attack, but it makes it more difficult for attackers to succeed.
- Creating a DDoS playbook: This involves having a policy in place that tells professionals how they can combat or survive a DDoS attack. Cybersecurity specialists recommend having this in place.
- Calling a DDoS specialist: Companies such as Akamai or CloudFlare specialize in combating DDoS attacks. Contacting these experts can help you mitigate the effects of an ongoing attack.

Additionally, in the context of DoS and DDoS, attackers can abuse the ping command by sending hundreds of thousands or even millions of ping requests to a target server. This flood of useless traffic overwhelms the server, making it unable to respond to legitimate users. While a single ping is a normal diagnostic tool, sending massive numbers of pings at once is malicious and forms the basis of certain DoS and DDoS attacks.

Man-in-the-Middle attacks

A **man-in-the-middle attack** is a type of cyberattack where a hacker is able to position themselves between two computers that are communicating with each other. In this section you will learn how an attacker can intercept, steal, or modify data being exchanged between computers, and see a real-world analogy to help you understand the concept.

Imagine two computers exchanging data and information with each other. Everything appears to be working smoothly, but a hacker manages to virtually insert themselves between the two computers. This attacker can now intercept messages sent from computer 1 to computer 2 and vice versa. The hacker is able to read, steal, or even alter the data being transmitted between the two systems.

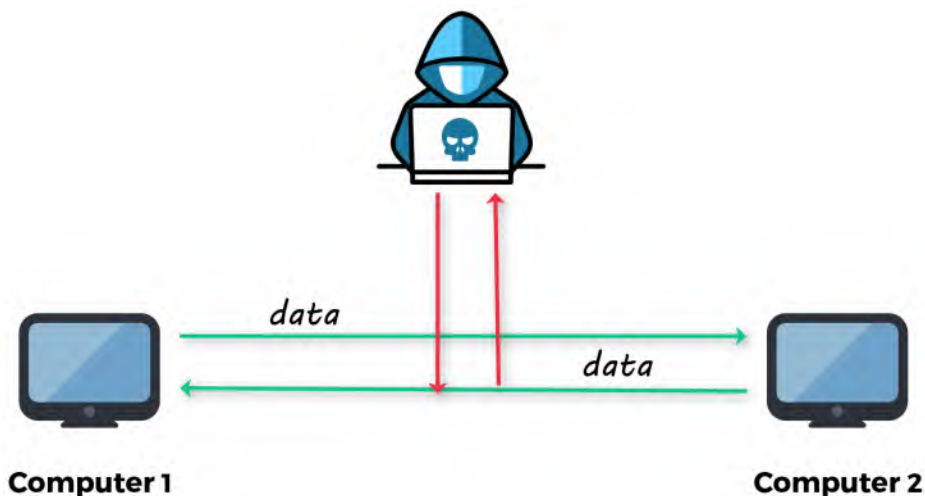


Figure 4.7: Man-in-the-middle attack intercepting data between two communicating computers

To help you visualize this, consider a real-world example from before the days of the internet and email. Suppose Jim writes a letter saying "I love you" to Jessica. The postman, acting as the hacker, intercepts the letter, edits it to say "I hate you," and then delivers it to Jessica. Jessica receives the altered message, and Jim is left wondering why she never responds. This scenario illustrates how a man-in-the-middle attack works: someone intercepts and potentially changes messages between two parties.

There are some key points to remember about man-in-the-middle attacks. For the attack to succeed, the attacker must be able to impersonate both sides of the communication. It is not enough to simply intercept the messages; the attacker must also convince both computers that they are communicating with the legitimate source or the intended target.

Types of Man-in-the-Middle attacks

There are three major types of man-in-the-middle attacks that you need to be aware of: email hijacking, Wi-Fi eavesdropping, and session hijacking.

Email hijacking occurs when an attacker gains access to someone's email account. Once inside, the attacker can read all incoming and outgoing emails and even send emails to others using the victim's address.

Wi-Fi eavesdropping is very common with unsecure wireless connections. In this scenario, an attacker hacks into an unsecure Wi-Fi network and intercepts the messages exchanged between computers.

Session hijacking involves an attacker taking over the connection between a computer and a website, rather than just between two computers. This is discussed in detail in a later section.

In the real world, man-in-the-middle attacks have been very lucrative for some hackers. For example, in 2015, cybercriminals in Belgium stole over \$6 million by gaining access to the corporate email accounts of several companies. They impersonated these companies and sent emails to clients and customers, who then sent money believing the emails were legitimate, not realizing they were actually communicating with the hackers.

SQL injection and cross-Site Scripting (XSS) attacks

SQL or Structured Query Language is a language used for database management, used to insert, modify, query, or update data in a database. SQL injection is a type of cyberattack where malicious code is executed (usually through insertion into website fields) to corrupt a database. Attackers access or manipulate sensitive data such as usernames or passwords. It has been used against major organizations such as Sony, LinkedIn, Yahoo, Microsoft, and even the CIA. This attack remains popular because it is highly effective at compromising databases.

One particular software you need to be aware of is **Havij**. Developed in Iran by cybersecurity professionals, Havij is a tool used by penetration testers to find and exploit SQL vulnerabilities. When a company hires penetration testers to assess the strength of their database, Havij is often the software of choice. However, Havij is a double-edged sword: while penetration testers use it for good, hackers also use Havij to attack databases. This makes Havij a very popular tool for both ethical and malicious purposes in the context of SQL injection.

A very similar attack to SQL injection is the **cross-site scripting attack**, also known as the **XSS attack**. In this attack, the attacker injects malicious scripts of code into a website or web application. Like SQL injection, XSS involves the use of malicious code, but the target is different. In an SQL injection attack, the attacker targets a database. In an XSS attack, the attacker targets a website or web application.

The attack is not aimed directly at a victim, but at the website that the victim visits. When the victim uses the compromised website or web application, their browser becomes infected as a result.

Combating SQL attacks involves three major strategies. First, you should limit database privileges, which restricts the amount of damage an attacker can do if they gain control of the database. Second, comprehensive data sanitization is essential. Databases must be configured so that only the correct types of characters are accepted in each field.

For example, a field reserved for phone numbers should only accept numbers, not special characters or letters. Finally, applying software patches is critical. Regularly updating and patching your software greatly improves your chances of defending against both SQL injection and XSS attacks. Many people take updates for granted, but keeping your systems patched is a key defense.

Now you will learn about supply chain attacks and how they occur.

Supply chain attacks

Supply chain attacks are a very serious threat to any company, especially when your own network is very well protected and up to date.

A **supply chain attack** is when a company is attacked, not directly by cybercriminals, but by the criminals going through a third-party company that has some sort of network access to the actual target company. For example, if company A is the target and has strong defenses such as malware protection, an active firewall, an effective security policy, and security awareness training, hackers may not be able to attack company A directly.

The most effective way for hackers to breach such a well-defended company is by targeting a third-party company that already has access to the actual target. This approach is known as a **supply chain attack**.

A prime example is the SolarWinds attack from a couple of years ago. SolarWinds is a massive company with a widely used network management tool called Orion, relied on by thousands of clients. Hackers managed to install malware onto the Orion software itself. When SolarWinds released an update for Orion to its clients, that update already contained the malware. Clients, seeing a routine update for Orion, installed it without suspicion, unaware that the malware was included. By compromising SolarWinds, the hackers were able to reach thousands of other companies.

Another one of the most notorious examples of this type of attack is the 2013 breach of Target, a major supermarket chain in the United States.

In the Target attack, hackers managed to install malware on the card readers used at checkout counters. When customers swiped their debit or credit cards, the malware captured their card details. Over 40 million customers were affected, making it one of the largest cyber attacks in United States history. The hackers did not attack Target directly. Instead, they exploited a third-party company responsible for servicing Target's air conditioning units. This company had a VPN connection to Target's network so it could access the AC systems remotely.

The attackers sent a phishing email to an employee at this third-party company. When the employee installed the phishing malware, the hackers were able to steal the VPN credentials. With those credentials, they logged into Target's network and spread the malware to the card readers. This is a textbook example of a supply chain attack, where the weakest link in the chain is exploited to reach the real target.

Supply chain attacks can take many forms, but the common thread is that attackers compromise a trusted third party to gain access to their intended victim.

Preventing supply chain attacks

Accountability through auditing is a key defense against supply chain attacks. For example, company A can send auditors to company B to verify that company B has a strong security policy, up-to-date anti-malware protection, and other safeguards in place. Company B can also audit company A in return. This mutual auditing ensures that both parties are maintaining proper security standards.

NOTE

A notable detail from the Target attack is that the third-party company did have anti-malware software installed, but it was only the free version of Malwarebytes.

Another important defense against supply chain attacks is to ensure that when you provide network access to a third-party company, you only grant the minimum access necessary for their role. For example, if company B needs access to company A's HR files, you should restrict their access to just those files and nothing else, such as marketing or financial documents. You can achieve this by using techniques such as network segmentation and carefully managing file permissions.

NOTE

If you want to understand how supply chain attacks happen in real life, you should watch the documentary titled "Target Takedown, Untangling the Infamous Server Attack Against Target" on YouTube. This short, seven-minute video covers the details of the supply chain attack against Target and provides valuable insights into how these attacks unfold. Watching it will help you see the practical aspects of supply chain attacks and reinforce the importance of the preventive measures discussed.

Now, let's move on to some more advanced cyberattacks. Unlike attacks that rely on a single technique, these attacks can involve multiple steps, careful planning, and a combination of technical methods and social engineering.

Advanced cyber attacks

As cyber threats continue to evolve, attackers are using increasingly sophisticated techniques to compromise individuals, devices, and organizations. Some of these attacks involve multiple stages, exploit a combination of human and technical weaknesses, or make use of emerging technologies to appear more convincing.

In this section, we will explore several advanced cyberattacks, including **business email compromise**, **SIM swapping**, **drive-by downloads**, **deepfakes**, and **session hijacking**.

Understanding how these attacks work will help you recognize the different methods attackers can use to gain unauthorized access, steal information, impersonate others, and compromise systems.

Business email compromise

Business email compromise is a targeted form of phishing where attackers impersonate executives, suppliers, or employees to trick victims into sending money or sensitive data.

Unlike whaling, which specifically targets senior executives, business email compromise can target anyone in the company, regardless of their position.

There are four main stages to a business email compromise attack. The first stage is reconnaissance, where attackers gather as much information as possible about their intended victim. You might see attackers researching the company using LinkedIn, social media, press releases, and public filings to identify key personnel they want to target.

The second stage is compromise or spoofing. Attackers may gain access to a legitimate email account through phishing, credential theft, or malware. If they cannot access a real account, they might spoof the email domain so that it looks legitimate. For example, if the real email is

john.smith@example.com, the attacker could substitute the letter "l" with the number "1" to create john.smith@1example.com, hoping that the victim will not notice the subtle change.

After setting up the spoofed email, attackers move to the social engineering phase. They may pose as the CEO, CFO, or a supplier, claiming that a payment is due for services rendered. The attacker will demand money via wire transfer or request confidential documents. The final step is execution, where the victim, believing the request is legitimate, transfers funds or sensitive information. Often, the scam is only discovered after it is too late to reverse the transaction.

Common scenarios include CEO fraud, where attackers impersonate the CEO to request urgent payments from finance staff; invoice fraud, where a supplier's payment details are updated to redirect funds; payroll diversion, where HR is tricked into changing direct deposit details to an attacker-controlled account; and attorney impersonation, where attackers pose as legal representatives to obtain confidential data.

SIM swapping

A common social engineering attack variant is the SIM swap attack, also called the SIM hijacking attack. In this attack, the SIM card belonging to the victim is the main target, as attackers aim to gain control over it. This is especially attractive because many people use their mobile device for two-factor authentication. When you log in to your social media or bank accounts, you often receive a PIN or authorization code on your mobile device, which you must enter to complete the login. If attackers control your SIM card, they can intercept these two-factor authentication codes.

The process typically involves several steps. First, attackers gather as much information as possible about the intended victim, such as the place of birth or the name of a favorite pet. This information is needed because, in the next step, attackers call the carrier that manages the victim's SIM card. The carrier's customer representative will usually ask security questions to verify the caller's identity. The more information attackers have, the more likely they are to convince the operator that they are the legitimate owner of the SIM card. Attackers might claim they have lost their SIM card and need to transfer their number to a new card.

Once the carrier is convinced by the attacker's answers, they will transfer the victim's number to the attacker's SIM card. With control over the SIM card, attackers can reset passwords, intercept two-factor authentication codes, and potentially drain accounts or take over social media profiles. This makes SIM swap attacks extremely dangerous, as attackers can use the victim's number to gain access to many of their accounts. In 2019, Jack Dorsey, who was then CEO of Twitter, had his Twitter account compromised through a SIM swap attack, allowing attackers to post fraudulent tweets from his account.

To protect yourself from SIM swap attacks, you have two main options. First, instead of relying on SMS-based two-factor authentication, switch to an authenticator app. Google offers a

widely used authentication app for this purpose. Second, if you still want to use your phone for two-factor authentication, enable a PIN or code with your carrier so that anyone attempting to transfer your number must provide this additional verification.

Drive-by downloads

A drive-by downloads attack is an attack where you can get infected with malware simply by visiting a site, without having to do anything special. You do not need to download anything, upload anything, or even click on any links for your system to be compromised.

In this attack, the attacker has already injected malicious code into the website. When you visit the site, that code executes automatically and scans your browser for extensions, plugins, and add-ons, and may even scan your operating system for vulnerabilities. If any vulnerabilities are found, the code exploits them and delivers the payload, which could be ransomware, a keylogger, a spy logger, general malware, or even back doors.

The defining characteristics of a drive-by downloads attack are that you, as the victim, do not need to take any action beyond visiting the website, and the attack is extremely silent. The code executes and scans your system without any notification, so you will not be alerted that anything is happening. Attackers often use malvertising in these attacks, creating banners and advertising the infected site to entice as many victims as possible to visit and become infected.

One of the worst aspects of this type of attack is that it can even affect trusted websites. For example, in 2016, the New York Times and the BBC unknowingly served malicious ads to their visitors as part of a malvertising campaign. If you visited these sites with vulnerable software, you could have been infected with ransomware.

To prevent falling victim to this kind of attack, you need to keep your browsers and plugins up to date. Remove any outdated plugins you are not using. Use reputable ad blockers to reduce your exposure to malvertising. You could also use a modern antivirus or anti-malware endpoint protection solution with web filtering. Avoid visiting suspicious or untrusted websites. For organizations, implement web gateways with URL filtering, enforce least privilege on endpoints, and regularly patch and update all systems.

Deepfakes

A **deepfake** is artificially generated or altered media, such as an image, video, or audio recording, created using **artificial intelligence (AI)** to convincingly imitate a real person. Attackers use deepfakes to impersonate trusted individuals, spread false information, or deceive victims into revealing sensitive information or transferring money.

In one high-profile case, an officer received an email about a secret transaction that needed to be carried out. The officer was suspicious, but the email also included an invitation to a video call with the chief financial officer and other colleagues. During the call, the officer recognized

the chief financial officer and several other familiar colleagues, so he believed the meeting was legitimate. However, all of the participants he saw were actually deepfakes, AI-generated video and audio designed to perfectly mimic the real people. The attackers had gone to great lengths to create convincing deepfakes of the chief financial officer and other colleagues, orchestrating the meeting so that the victim did not suspect anything was amiss. During the call, the attackers asked the officer to transfer money, and after the meeting ended, he complied.

This example demonstrates the level of sophistication and commitment attackers can show, using deepfake technology to convincingly impersonate trusted individuals and deceive victims into authorizing fraudulent transactions.

To reduce the risk of falling victim to attacks involving deepfake technology, you should implement strict approval policies for significant transactions. For example, if you are part of a company, require that any transaction over \$100,000 must be approved by at least three people, such as the chief financial officer, chief operating officer, and CEO. This multi-person sign-off process makes it much harder for attackers, since they would need to compromise several individuals rather than just one.

If your organization is too small or geographically dispersed to have multiple signatories, you should require a physical, in-person meeting before authorizing large transactions. This means the person responsible for the transaction must meet face-to-face, not over a video call, but in the same physical location, with a senior executive or someone with the authority to approve the transaction. This extra layer of verification helps ensure that attackers using deepfake technology cannot easily impersonate trusted individuals and trick you into authorizing fraudulent transfers.

Session hijacking attacks

Session hijacking is a particularly serious type of cyberattack that targets your session access and account information.

It occurs when an attacker gains access to your session cookie, which is a temporary credential that allows you to stay logged into your account without re-entering your username and password every time. For example, when you log into your Instagram account, a session cookie is created so you can close your browser and return later without logging in again. If a cybercriminal manages to steal this session cookie, they can impersonate you and gain full access to your account.

So what exactly would be the typical workflow? First of all, you have to log into your account, and when you do, a session ID will be created to represent the cookie. The attacker will then have to gain control of or gain access to that ID. The attacker then sends the ID to the server. The server thinks the attacker is you, provides the attacker with your account, and then the attacker is able to do whatever they want with your account.

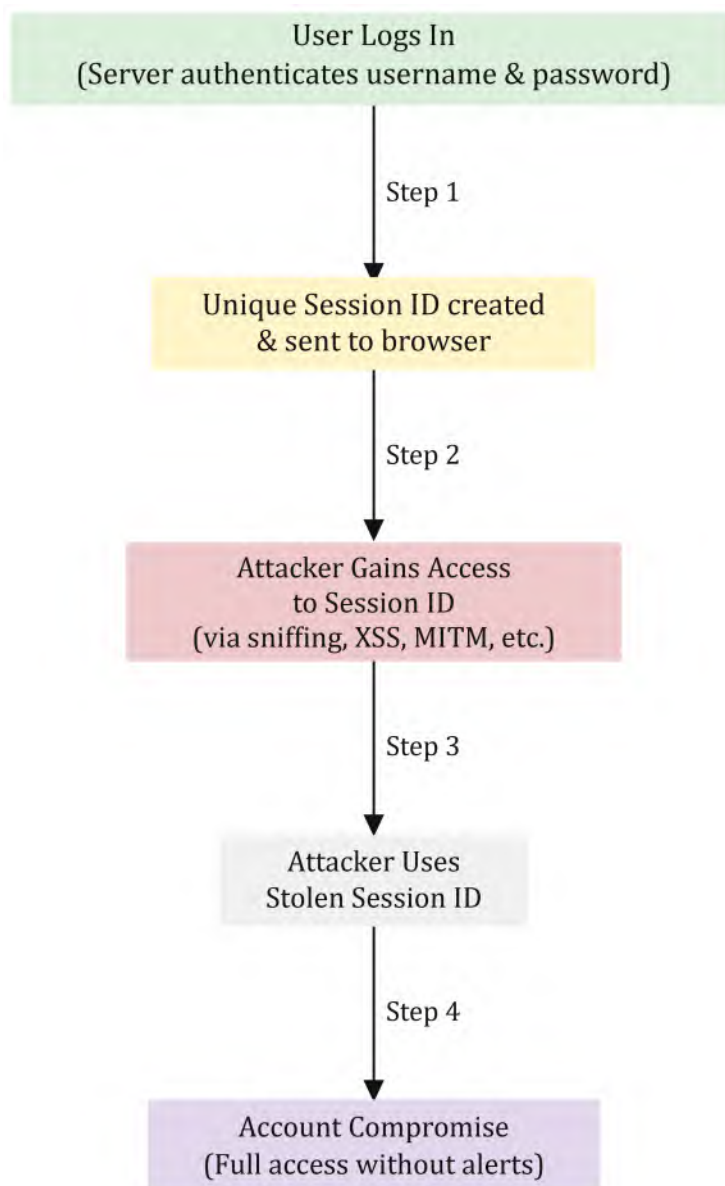


Figure 4.8: Session hijacking workflow showing how attackers gain access to user accounts by stealing session IDs.

A natural question you might have here is: how exactly will the attacker be able to gain access to the session ID belonging to the victim? There are numerous ways this could happen. First,

you have what is called **session sniffing**, where the attacker, using some sort of tool, can capture unencrypted network traffic.

You also have XSS attacks, where the attacker could inject malicious code into a site to steal the cookies from your browser. Man-in-the-middle attacks can also be used here. There is also **session prediction**, where the attacker can actually guess or calculate the session IDs if they're poorly generated. Last but not the least, attackers can use malware or keyloggers that directly steal cookies or session storage data from your device.

To give you a real-world example of this attack, consider the year when the very famous YouTuber Linus Tech Tips, a big channel with millions of subscribers, got hacked through session hijacking.

In this case, the attacker sent a convincing sponsorship opportunity email to Linus' team, which included a PDF attachment. Since receiving such emails was routine for them, opening the email and the PDF felt completely natural. However, the PDF was malicious and contained code designed to steal session cookies. Because the computer already had an active YouTube session, the malware was able to extract the session cookies for the YouTube account and send them to the attacker.

With these session cookies, the attacker gained control of the Linus Tech Tips YouTube account. Although the team eventually regained access, the attack demonstrated how quickly and easily session hijacking can compromise even high-profile accounts.

To protect yourself from session hijacking attacks, you should:

- Use HTTPS for all websites to ensure your traffic is encrypted.
- Avoid logging in on public Wi-Fi networks or always use a VPN when connecting from untrusted locations.
- Log out of sessions when you are not actively using them.
- Clear cookies on all shared devices to prevent others from accessing your session.

These steps are especially important for individuals, but organizations need to take additional measures to secure their users and systems.

For organizations, you need to implement additional defenses to protect against session hijacking. Use secure cookies with both HTTP-only and secure flags, enforce session timeouts, and require re-authentication for sensitive actions. Regenerate session IDs after each login and always encrypt all traffic using TLS.

A critical point to remember is that an attacker does not need to be on the same network as the victim to perform session hijacking. Attackers can steal session cookies remotely using malware, phishing, or even malicious browser extensions, as demonstrated in the Linus Tech Tips cyberattack.

Summary

In this chapter, we explored some of the most common cyberattacks used to target individuals, organizations, networks, and applications. We began with **brute force attacks**, where attackers repeatedly attempt different password combinations, before examining **phishing attacks** and their variants, including spear phishing, whaling, vishing, and smishing. These attacks demonstrate how cybercriminals can exploit both technical weaknesses and human behavior to gain access to sensitive information.

We then discussed **bots and botnets** and how compromised devices can be controlled through command and control servers to carry out large-scale attacks. This led to **DoS and DDoS attacks**, which attempt to make systems or services unavailable by overwhelming them with traffic. We also examined **man-in-the-middle attacks**, **SQL injection**, **cross-site scripting (XSS)**, and **supply chain attacks**, highlighting the different ways attackers can intercept communications, exploit applications, and databases, or compromise trusted third parties to reach their intended targets.

Finally, we explored more advanced attacks, including **business email compromise**, **SIM swapping**, **drive-by downloads**, **deepfakes**, and **session hijacking** with examples that demonstrate how modern cyberattacks can combine social engineering, malware, stolen credentials, artificial intelligence, and other techniques to compromise victims.

Throughout the chapter, we also examined practical defensive measures, including strong passwords, security awareness, regular patching, multi-factor authentication, access controls, transaction verification, and secure session management.

By recognizing common attack methods, identifying warning signs, and applying appropriate security measures, you will be better prepared to reduce the risk and protect systems, accounts, and sensitive information from cyber threats.

Chapter 5 will introduce you to malware and its types along with the most effective methods to protect against them.

5

Understanding Malware

Malware is one of the most common and persistent threats in cybersecurity. The term malware, short for *malicious software*, refers to software intentionally designed to disrupt systems, steal information, gain unauthorized access, or perform other harmful activities.

In this chapter, we will explore the major types of malware and examine how they operate. By the end, you will be able to distinguish between viruses, worms, Trojans, adware, spyware, and rootkits, and understand how each can compromise a system. Along the way, we will introduce important terms such as an executable file, a network connection, a backdoor Trojan, a keylogger, and a spyware scanner, while clarifying the differences between self-replicating worms, host-dependent viruses, and user-triggered Trojans.

Understanding these differences is important because malware does not always behave in the same way or require the same defenses. Recognizing how malware enters a system, what it does once installed, and how it spreads can help you select appropriate security measures. These can include anti-malware software, regular updates, security awareness training, backups, and disaster recovery plans. Together, these measures can reduce the likelihood and impact of malware attacks, helping protect sensitive information, maintain system availability, and prevent costly disruptions.

In this chapter, we will cover the following topics:

- Viruses and Worms
- Trojan Horses
- Adware and Spyware
- Ransomware
- Rootkits

- Other forms of malware
- Mobile malware

Viruses and worms

You may have heard of viruses, worms, and Trojans before, but it is important to understand their differences and how they operate.

Viruses and worms are both forms of malicious code designed to change the way a computer or network operates. You need to remember that these threats target not only individual computers but also entire network systems. The main difference between viruses and worms is that a virus requires an active host or an already infected system to run, while a worm is self-replicating and self-propagating. This means that worms can spread themselves without any help, reproducing and moving across networks and computers on their own.

Virus life cycle and methods of spread

A virus typically goes through four basic stages from development to causing harm on a computer system. The first stage is when the virus attaches itself to an executable file or a Word document. This is how viruses usually embed themselves. They then spread through email attachments, infected websites, and flash drives, which are the three main ways viruses move from one system to another.

Once a virus gets onto a computer or network, it can remain dormant until the infected file or system is activated. For example, a virus could be programmed to become active only when a user visits a specific website. This shows how sophisticated some viruses can be, waiting for a particular trigger before causing harm.

Worms, even though they are more advanced than viruses, actually operate in a very simple way. They first spread themselves or enter systems through network connections or downloaded files. Once inside, worms make copies of themselves and continue to spread via a network or an internet connection, much like Agent Smith from the movie *The Matrix*, who replicates himself repeatedly.

Objectives and variants of viruses

When it comes to viruses, you need to remember that their objectives can vary widely. While worms are destructive in almost all cases, viruses can have a range of behaviors. Some viruses are purely destructive, aiming only to destroy files. Others are designed to slow down system performance without actually destroying anything. There are even some viruses that are non-destructive and simply remain latent on a system, not causing any harm but just existing there.

To defend against viruses and worms, the three best methods are:

1. Use antivirus and anti-malware products, which are highly effective at detecting and removing these threats.
2. Restrict the use of flash drives, since both viruses and worms can spread rapidly through them.
3. Always scan email attachments before downloading or opening them, as email attachments remain one of the most popular ways for worms to spread. Make sure attachments are from trusted sources or scan them before downloading to your system.

By following these three methods, you can significantly reduce the effectiveness of viruses and worms on your computer or network system.

Trojan horse

The story of the Trojan horse from Greek mythology is the origin of the term **Trojan** in cybersecurity. According to the story, the Greeks were unable to conquer the city of Troy due to its high walls and skilled defenders. They built a large wooden horse, hid soldiers inside, and presented it as a gift. The Trojans, believing it to be a sign from the gods, brought the horse into their city. At night, the hidden soldiers emerged, opened the gates, and allowed the Greek army to enter and capture Troy. This story illustrates how a Trojan malware operates: it appears to be something harmless or beneficial but secretly contains a threat.

Trojans are extremely dangerous because they disguise themselves as legitimate software, often games or useful applications. You might think you are installing a helpful program, but behind the scenes, the Trojan is performing malicious actions. Sometimes, the software even provides the legitimate promised feature, making it harder to detect the threat.

Trojans are highly sophisticated, as they can take the form of a game, video, song, or application. The major distinction between a Trojan and a virus or worm is that Trojans cannot self-replicate. While viruses and worms can spread themselves to other systems, a Trojan relies on you to install or run it. This limitation is fortunate, as self-replicating Trojans would be even more destructive.

Major types of Trojans

There are four major types of Trojans that you should be aware of. The first is the **Backdoor Trojan**. A backdoor Trojan allows a hacker unauthorized access to a system in order to control it. With a backdoor, a hacker can penetrate your computer and take control of the system.

We also have the **Info Stealer Trojan**. This type of Trojan steals data from infected computers, which could include credit card information, passwords, addresses, and other sensitive details.

Some adware can be more malicious, such as those hijacking your browser. There might be search pages. For example, you might set your home page to Google, but when you open your browser, it takes you to a different page instead. This is adware at work. There are even more sinister forms of adware that track your web usage, which are known as **spyware**. In this sense, spyware can be considered a form of adware that specifically tracks your web activity.

Spyware is designed to spy on you, monitoring your computer, and internet use. One example is a key logger, which records every keystroke you make on your keyboard. Spyware can also take screenshots of what you are viewing on your screen. This data can then be sent back to hackers, who may use it to steal credit card information, passwords, and other sensitive details. Alternatively, the data might be sent to advertising agencies to learn about your interests and serve you targeted advertisements.

The two best ways to protect yourself against adware and spyware are to think carefully before using free software and to use spyware scanners. While some free software is genuinely free with no strings attached, many free programs require you to install adware as well. If you can afford it, it is often recommended to purchase the premium version of the software to avoid adware. Additionally, you can use one of the many available spyware scanners to regularly check your computer system and ensure there is no adware or spyware malware running.

Ransomware

Ransomware is a type of malware that hijacks your data, holding it hostage until a ransom is paid, often in Bitcoin. Ransomware attacks can be compared to a kidnapping scenario you might see in movies or hear about in real life. Ransomware does not involve kidnapping people, but rather your data. Your data, whether company or personal data, becomes the hostage. Ransomware attacks depend on two main factors, resulting in two variants **Data Access Ransomware** and **Data Sensitivity Ransomware**:

Data access ransomware

This variant focuses on denying you access to your files. The attackers encrypt your data, making it inaccessible until you pay the ransom. Once payment is made, usually in Bitcoin, the hackers provide you with a decryption key to regain access to your files.

NOTE

Bitcoin has become synonymous with ransomware attacks, and you may have noticed that it often carries a negative association because of this link.

A typical data access ransomware demand screen includes instructions for Bitcoin payment and uses threatening language to pressure the victim.

Figure 5.2 shows a typical example of the kind of threatening message a victim would receive:

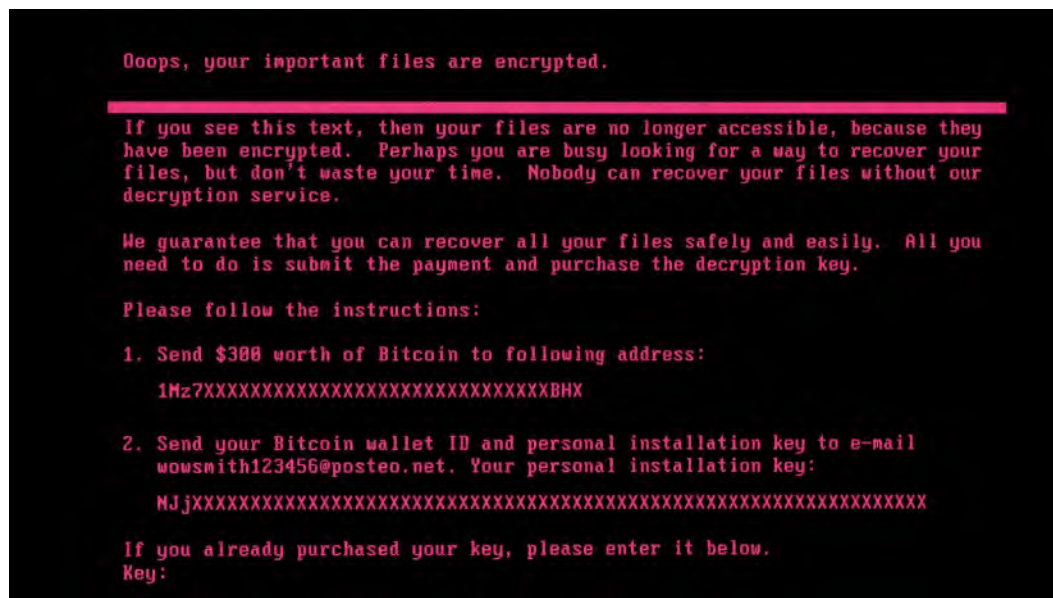


Figure 5.2: Ransomware message demanding Bitcoin payment for file decryption, illustrating a typical cyber extortion scenario.

The message states that your important files are encrypted and that nobody can recover your files without their decryption service. It instructs you to send \$300 worth of Bitcoin to a specified address and to provide your Bitcoin wallet ID and personal installation key to an email address. The tone is designed to make you feel hopeless, emphasizing that the only way to recover your data is to pay the ransom.

However, there is a significant limitation to this type of ransomware attack. If you have backups of your data, you may not care about the encrypted files because you can simply restore them from your backup. This makes the data access ransomware variant less effective against individuals or companies that are security-aware and maintain regular backups.

Data sensitivity ransomware

The second variant, data sensitivity ransomware, is far more troubling. With this type, the issue is not access to the data, but the sensitivity of the information itself. The attacker threatens to release sensitive data, such as tax records, salaries, or potentially embarrassing videos or pictures, if you do not pay the ransom.

Thus, in this kind of ransomware attack, the real danger is not about whether you have a backup of your files or videos, but about the sensitivity of the information itself. If the public learns about confidential data such as tax records or salaries, it could cause serious

reputational damage. In these situations, the hacker holds all the power, and the number of backups you have becomes irrelevant. This makes data sensitivity ransomware extremely dangerous and highly feared by companies.

Methods of ransomware delivery

Ransomware attacks can be delivered in several ways:

- *Phishing* is a common method, where you might receive an email with a malicious attachment or link
- *Malvertising* is another technique, involving malicious advertisements that can infect your system
- *Drive-by* downloads occur when you visit an infected website and ransomware is downloaded without your knowledge
- Pirated software from the black market is also risky, as it can contain ransomware.
- Finally, infected USB drives can be used to spread ransomware, especially in business environments where plugging in a compromised USB can infect an entire network.

Notable ransomware attacks and trends

In 2017, ransomware losses exceeded \$5 billion. New forms of ransomware and defensive measures are constantly evolving, and ransomware has now spread to mobile devices, not just computers. Another trend is **ransomware as a service**, where hackers develop ransomware software and then provide or sell it to other criminals who want to launch attacks. This means that the people who create the ransomware are not always the ones carrying out the attacks, they simply supply the software to others. In 2021, the largest known ransomware payout was made by an insurance company for \$40 million.

NOTE

Ransomware has become so notorious that it is sometimes called the Hans Gruber of the digital world. Hans Gruber, the main antagonist in the 1988 movie *Die Hard* starring Bruce Willis, is known for taking hostages.

Some of the most significant ransomware attacks in recent years include the Colonial Pipeline attack, which shut down the largest pipeline in America, and the JBS Meat Plant attack. Acer, one of the largest PC manufacturers, was also targeted, as well as CNA Financial and Ireland's Health Service Executive. These examples illustrate just a small portion of the many ransomware incidents that have occurred.

To defend against ransomware attacks, you should maintain regular backups, which are effective against data access ransomware. For data sensitivity ransomware, security training is

crucial, train employees not to click on phishing links or engage in risky online behavior. Additionally, efficient disaster recovery plans are essential. These plans enable a company to respond quickly and effectively if a ransomware attack occurs. Any company with a solid security policy should have such plans in place, greatly improving their chances of minimizing losses from ransomware.

Rootkits

Rootkits are considered one of the most dangerous forms of malware, deserving special attention. You can think of a rootkit as a burglar hiding in your attic, unseen but always present, waiting to strike when you least expect it. Rootkits are the hardest malware to detect and remove. They allow viruses and other malware to hide in plain sight by disguising them as essential system files. Not only do rootkits have their own destructive features, but they can also enhance other malware by making them appear as legitimate files.

Rootkits can even bypass encryption and evade anti-malware programs. Most forms of rootkits begin to run as soon as your system starts to boot, even before you reach your desktop, making them extremely difficult to detect and remove. If you ever have a rootkit infection, the recommended solution is to wipe out your hard drive, since you can never be 100% sure that a rootkit has been fully removed, even with specialized scanning software.

Now let's talk about the five different levels of rootkits as illustrated in *Figure 5.3*:

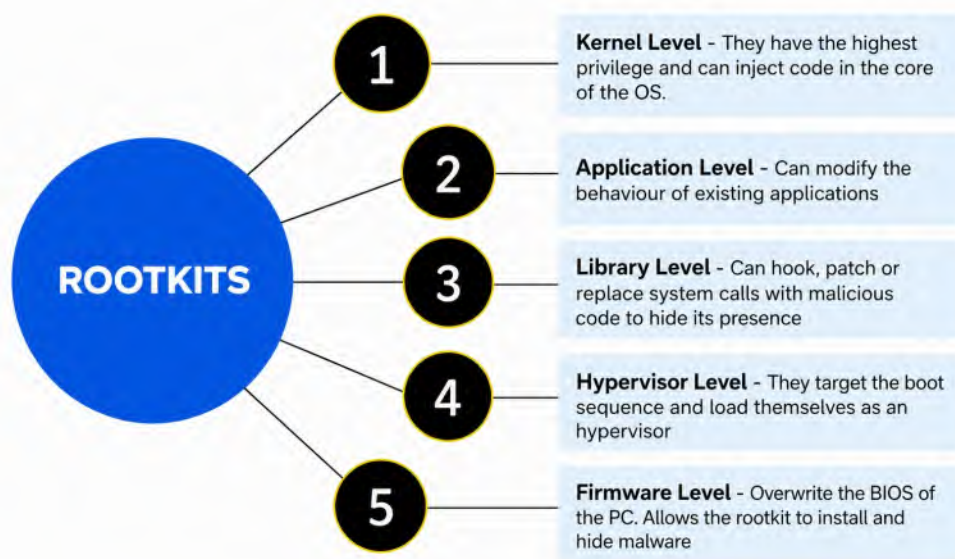


Figure 5.3: Rootkit levels

The very first one is the **kernel level rootkit**. This type of rootkit runs once your system starts to boot and can execute the highest levels of commands on your system. It has the highest privilege and can inject code into the core of your operating system. These are easily the most dangerous forms of rootkits. It basically can turn your PC into a complete zombie.

Next is the **application level rootkit**. These only run after your system has finished booting and work by modifying the behavior of existing applications, similar to how viruses operate.

The third type is the **library level rootkit**, which can hook, patch, or replace system calls with malicious code to hide its presence. These rootkits are masters of disguise.

The fourth type is the **hypervisor level rootkit**, which also runs when your system begins to boot. Hypervisor level rootkits target the boot sequence and load themselves as a hypervisor, which is a program that can create a virtual machine. This means a rootkit can create virtual machines inside your PC, which is a very alarming capability.

Another type of rootkit is the **firmware level rootkit**, which runs when your system boots and specifically targets your BIOS. Firmware level rootkits allow malware to install itself and remain hidden by affecting your BIOS directly.

NOTE

All types of rootkits, represent a very troublesome set of malware that can be extremely difficult to detect and remove.

Symptoms of rootkit infection

It is very important that you are able to identify when you might have a rootkit infection. The first symptom is that your anti-malware or antivirus software stops working. If you discover that your protection software is no longer functioning, you probably have a rootkit infection. Another symptom is unexpected changes to your Windows settings, such as pinned items on your taskbar or your desktop background image changing without your input. Frozen input devices, such as your mouse, keyboard, or webcam, are another sign; if these devices freeze for no reason, you just might have a rootkit infection. Finally, high network usage on an idle computer is a warning sign. If you are not running applications but notice a lot of network activity, you probably have a rootkit infection.

Other forms of malware

So, we have already talked about all the major types of malware out there. We've discussed viruses, worms, Trojans, spyware, ransomware, and a few others. Now let's round up this discussion on malware by talking about a few other ones.

Browser hijackers are a less malicious form of malware, similar to adware. They hijack your browser and redirect you to specific pages, often changing your homepage to a different website. The main goal of browser hijackers is to make money by feeding ads to you, not to steal information or destroy files. Most are developed by advertisers who want to track your usage habits, making them more annoying than dangerous.

Rogue security software pretends to be legitimate programs that remove malware but are actually malware themselves. Once installed and activated, they can disable any real security software on your system. You often encounter these on websites promising better security or virus removal. The safest way to protect yourself from rogue security software is to install software only from known vendors such as Kaspersky, McAfee, or Norton.

When you hear words such as malware and viruses, you probably think about desktops and regular computers. However, nowadays malware to specifically infect mobile devices is on the rise. Let's discuss these next.

Mobile malware

Think about how much information is stored or accessed through a modern smartphone. Mobile devices are commonly used for email, social media, online banking, shopping, messaging, and accessing workplace systems. They may also contain personal photographs, saved passwords, contact information, and authentication codes. This makes them attractive targets for attackers who want to steal information, gain access to accounts, monitor users, or commit financial fraud. Mobile malware is malicious software specifically designed to compromise smartphones, tablets, and other mobile devices.

Malware specifically designed to attack mobile devices has grown tremendously in the last few years. For example, in May 2018, G DATA, a security blog, reported that its researchers had found 846,916 new Android malware samples in Q1 2018, averaging 9,411 per day. At that point, it forecast roughly 3.4 million new Android malware samples for the full year. Later, its November 2018 report stated that researchers had identified almost 3.2 million new Android malware samples through Q3 2018, representing an increase of more than 40% over the same period in 2017 (<https://blog.gdatasoftware.com/2018/05/30735-new-malware-every-10-seconds/>).

Kaspersky, a leading security vendor, reported that in the same quarter, they detected more than 1.7 million malicious mobile installation packages, which was over 400,000 more than in the previous quarter (<https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/>).

Mobile malware is typically administered through the use of apps, and these apps can come in all shapes and sizes.

You may encounter apps that do not handle your data as you expect, but otherwise do nothing malicious. Some apps are specifically created to exploit software or zero-day vulnerabilities and steal your data. Others focus on delivering pop-up ads for quick monetization. There are also highly malicious apps designed to spy on you, steal your data, wipe your data, or hold your device for ransom. Security vendors generally classify these threats as mobile malware. Let's break down the most common types.

Mobile ransomware

The first type to consider is ransomware. The concept behind mobile ransomware is the same as discussed earlier: once your phone is infected, you are denied access until you pay a ransom. The developer of the malware holds your phone hostage, typically demanding payment in Bitcoin or another cryptocurrency. After payment, the developer may provide a key or code to decrypt your files or restore access to your phone.

Mobile ransomware incidents have increased dramatically in recent years. In 2017 alone, the number of mobile ransomware attacks rose by more than 415%. This surge was partly due to the success of the WannaCry ransomware, which targeted desktops and PCs. Cybercriminals recognized the potential for attacking mobile devices, and the number of incidents has continued to grow.

Removal techniques for mobile ransomware

Mobile ransomware can take the form of crypto ransomware, which encrypts your files to prevent access, but this type is more common on regular computers. On mobile devices, especially Android, you are more likely to encounter locker ransomware, which blocks access to your device by locking the user interface. The main ways your phone can become infected include installing malicious apps, running infected software updates, or clicking on spam links received via text message or email.

If you or someone you know has been infected by ransomware on a mobile device, you can use specific techniques to remove this form of malware. The first step is to switch off your phone and then turn it back on in **safe mode**. You will see the text "safe mode" displayed on your screen.

How you can boot your Android device into safe mode depends on the specific phone model. For example, on a Samsung S7, you power up the device and hold both the volume up and volume down buttons while the phone boots. On other devices, you might need to hold the power button throughout the boot process or use a different combination. The key is to ensure your phone starts in safe mode.

Safe mode disables all apps that did not come pre-installed on your phone. You will notice that some apps, such as Facebook and Instagram, appear normal, while others, such as Uber or

YouTube Studio, are grayed out. The grayed-out apps are those you installed after purchasing the phone.

So, if your phone starts acting strangely after you install a new app, safe mode lets you test whether that app is the cause. Boot your phone into safe mode and check whether it works properly. If the issues disappear, the recently installed app is likely responsible.

Here are the detailed steps to remove ransomware from your Android device:

1. Boot your phone into safe mode.
2. Open your class="keyWord">Settings.
3. Look for the section labeled **Apps** or **App Information**.
4. Tap on **Apps** to view your application list.
5. Find the suspicious or unfamiliar app you think is ransomware.
6. Tap the app in the list and select the option to **Force stop** the app.
7. Uninstall the application.

An example of the Apps list on an Android device, where the user is about to select an app for removal.

Now, let's talk about the mobile Trojan horse malware.

Banking trojans on mobile devices

Trojans are notorious for disguising themselves as legitimate applications. For example, you might download a game from the App Store, thinking you are just playing a fun game, but in reality, the app could be performing malicious actions in the background. One particular form of Trojan that has gained notoriety in recent years is the **banking Trojan**.

Banking Trojans are a very dangerous form of malware specifically designed to attack banking applications. For Android users, the threat is especially severe: 98% of all known banking Trojans target Android devices. While there has not yet been a recorded incident of a banking Trojan successfully infecting an iPhone, you should still remain vigilant and security conscious regardless of your device.

A banking Trojan typically operates through a six-step process:

1. You download the Trojan application onto your phone. Later, you run a legitimate banking application.
2. The Trojan, running in the background, detects the banking app and overlays its own interface on top of the real one.
3. You unknowingly enter your username and password into the Trojan's fake interface.

4. The Trojan copies your credentials and sends them to the criminal who designed the malware.
5. The criminal logs in with your credentials and performs unauthorized financial transactions.

To counteract banking Trojans, security experts introduced two-factor authentication, requiring you to receive an SMS in addition to entering your username and password. However, banking Trojans have evolved and can now bypass two-factor authentication, so you are still at risk even with this security measure.

One particularly example is the Acecard banking Trojan malware. Unlike regular Trojans that can overlay only one banking application, Acecard can overlay the interfaces of 30 different banking applications, making it especially dangerous.

Mobile trojan removal methods

To remove a Trojan horse from your phone, you have three main options:

1. Uninstall the malicious application, which is usually the most effective method.
2. Run the Malwarebytes application to detect and remove Trojan malware from your device.
3. If you suspect your phone has connected to an infected router, reset the router to its default factory settings.

These are the primary ways you can remove a Trojan horse from your mobile device.

Signs of mobile malware infection

You might notice several clear symptoms if your mobile device is infected with malware. The first is a significant slowdown in speed and performance, your phone may feel sluggish, and apps can take much longer to open or install. Another major sign is the sudden appearance of pop-up ads, which are extremely annoying and a strong indicator of infection. A third symptom is a surge in your data usage, which can lead to spikes in your phone bills; this suggests that applications are running in the background and consuming your data. Finally, increased battery consumption can also be a warning sign. However, do not immediately assume malware is the cause of reduced battery life, first confirm that your battery is in good condition. If your battery is fine, then malware could be draining your device's power.

Now that you know the major symptoms of a malware infection on your mobile device, you need to understand how to prevent your device from becoming a victim. One protection software you can use is Malwarebytes, discussed next.

Using Malwarebytes

When you first open the Malwarebytes app on your device, you will likely see a notification about critical issues found, such as your last device scan being set to 'never' and your database version being out of date. The database contains a list of all known malware, so you should update it immediately by clicking 'update now.' You also have the option to run a full scan, but for the app to be most effective, you need to enable certain protections.

To make Malwarebytes truly effective, enable real-time protection. This feature allows the app to run in the background, monitoring your device as you send emails or download files and helps prevent malware attacks.

You will also see an option to enable device administrator, which is a very useful setting. When you enable device administrator for Malwarebytes, you are granting the app full control to protect your device in any way necessary. Once you choose to enable device administrator, you will see a note explaining that this permission allows Malwarebytes to perform a wide range of actions to protect your device, including anti-ransomware remediation, sending SMS commands, and enabling real-time protection through file monitoring. This screen is shown below:

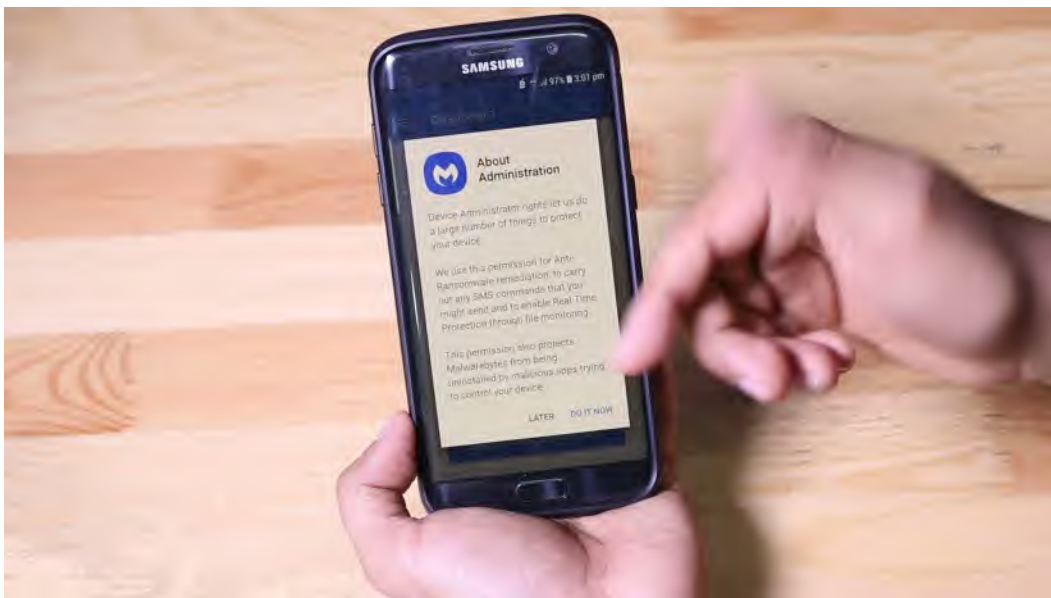


Figure 5.4: Granting device administrator rights to the Malwarebytes app for enhanced device protection and anti-ransomware features

You can then proceed by selecting 'do it now' to grant these permissions. You may be concerned about the 'erase all data' permission, but Malwarebytes will only use this in extreme

emergencies to protect your device from severe malware threats. You can reduce the severity of this outcome by keeping daily backups, so make sure you back up your phone regularly.

To further configure the app, open the menu and select 'Settings.' Under the scanning options, you can allow the app to scan your phone after a reboot, perform a deep power scan, or use a power-saving scan. You can also schedule scans to run automatically, such as during the night.

Enabling real-time protection is a crucial step. To do this, you must allow the app access to your data, including information about your web activity, uploads, and downloads. Scroll down to the 'Usage Data Access' section, find Malwarebytes, and enable usage tracking.

This setting gives Malwarebytes the ability to monitor which other apps are running on your phone and what actions they are performing. The following figure shows the 'Usage Data Access' screen with usage tracking enabled for Malwarebytes.

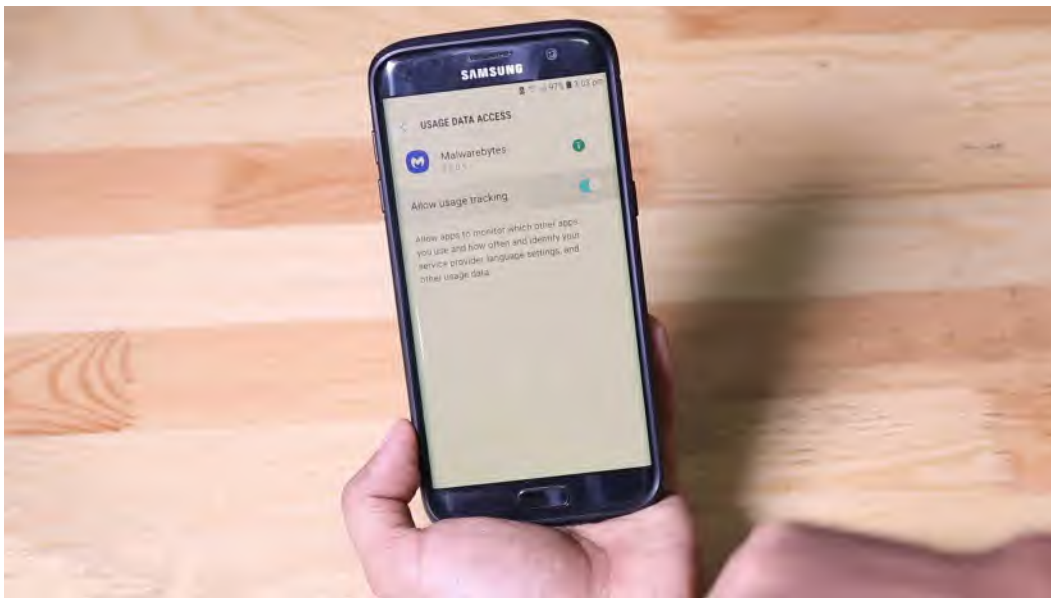


Figure 5.5: Enabling usage tracking for Malwarebytes on an Android device to allow app activity monitoring.

You can also enable the option to scan links sent via SMS, which is highly recommended for additional protection.

If you decide to use the premium version of the app, you get access to features such as scanning for malware and bad apps, real-time protection, and the ability to detect ransomware before it can lock your phone. This is extremely important for avoiding ransomware attacks, and the cost is very low, about a dollar per month. The app offers a 30-day free trial, so you can try out all the premium features before deciding to pay.

If you choose not to upgrade after the free trial, you can still scan your phone for malware using the free version, but you will lose real-time protection, which is a very important feature for keeping your phone safe.

Summary

Malware continues to evolve, but understanding how different types of malicious software operate is an important first step toward defending against them. Throughout this chapter, you saw how viruses, worms, Trojans, adware, spyware, and ransomware share the goal of compromising systems or information, but differ significantly in how they spread, what they target, and the damage they can cause.

The most important lesson is that there is no single defense against every form of malware. Protecting systems requires multiple measures working together, including antivirus and anti-malware software, regular backups, security awareness training, appropriate security policies, and disaster recovery planning. Just as importantly, you need to understand how your own actions, such as downloading files, installing applications, or interacting with suspicious content, can contribute to an infection.

Now that you have a clear understanding of how malware operates and the defenses available against it, you are better prepared to recognize potential threats and respond appropriately.

In *Chapter 6*, we will move from individual threats and attack techniques to examining how cyberattacks unfold in practice. You will review notable cybersecurity incidents and see how the concepts covered so far come together in real attacks, the consequences they can have for individuals and organizations, and the lessons that can be learned from them.

6

Real-World Cyber Incidents

Cyberattacks have consequently become tools not only for criminals seeking financial gain, but also for groups pursuing political, strategic, or military objectives. An attack against a single organization can interrupt supply chains, halt business operations, expose sensitive information, or cause significant financial losses. At a larger scale, attacks against critical infrastructure or government systems can disrupt essential services and create tensions between countries.

Understanding cybersecurity therefore requires more than learning about individual threats and defensive technologies. It also requires examining what happens when these threats are used against real targets. This chapter confronts the realities of cyber warfare by examining how digital attacks have disrupted infrastructure, economies, and even international relations in the real world.

By the end of this chapter, you will be able to distinguish cyber warfare and cyber espionage, understand the tactics used by nation-state sponsored cyber gangs, and analyze landmark incidents such as Stuxnet, the Estonia 2007 attacks, the Qatar 2018 disinformation campaigns, and the Sony Pictures breach.

You will also explore key terms such as denial-of-service attacks, plausible deniability, and the Tallinn Manual (NATO CCDCOE, Tallinn, Estonia), while unpacking debates about attribution and the legal boundaries of digital conflict.

The ability to recognize the mechanisms and motives behind these incidents, whether sabotage of power grids or targeted hacking of media agencies, equips us to better assess risks, respond to threats, and navigate the blurred lines between espionage and open cyber warfare.

In this chapter, we will cover the following topics:

- Cyber warfare as a modern threat
- The Stuxnet attack
- The 2018 disinformation campaigns involving Qatar
- The Estonia cyber attack
- The 2014 Sony Pictures hack

Cyber warfare as a modern threat

Cyber warfare is not a new phenomenon. It has been a part of international conflict for over 20 years. Cyber warfare refers to attacks against a country's infrastructure, which can include power grids, communication lines, transportation systems, and even the internet. These attacks can be carried out directly by a government or through nation-state-sponsored cyber gangs. Governments often use these gangs to conduct cyberattacks while maintaining plausible deniability, allowing them to claim they are not involved if the attacks are discovered.

Cyber warfare marks a major shift from the basics of cybersecurity and malware into the realm of international conflict and digital attacks on a national scale. With ongoing wars in Ukraine and the Middle East, and tensions involving China and Taiwan, you see how cyber warfare is intertwined with modern global conflicts. In this section, you will explore what cyber warfare means, how nation-state-sponsored cyber gangs operate, the legal debates surrounding these activities, and the different types of cyber warfare actions that can target a country's infrastructure.

Debates and legal frameworks of cyber warfare

There is significant debate among experts about what activities truly constitute cyber warfare and what responses are appropriate. The boundaries are not clear-cut, leading to ongoing confusion and gray areas. For example, some argue that cyber espionage, such as a spy stealing secrets from one country and selling them to another, should be considered cyber warfare, while others see it as a separate category.

Some experts argue that espionage is fundamentally different, but you can also view it as an integral part of cyber warfare. To illustrate this, consider the Cold War between the United States and the Soviet Union: although no direct shots were fired, both sides engaged in extensive spying, which you might think of as a form of "cold" warfare. In the digital age, cyber espionage functions as "cold cyber warfare," where nations gather intelligence and undermine each other without open conflict.

This lack of consensus extends to questions about proportional responses. For instance, if China were to shut down America's power infrastructure, is it justified for America to retaliate

by targeting China's power or water infrastructure? These unresolved questions highlight the absence of universally accepted standards for defining or responding to cyber warfare.

A notable attempt to clarify these issues is the Tallin manual, now in its second edition, which was prepared by an **NATO — North Atlantic Treaty Organization** Cooperative Cyber Defense Center of Excellence. This manual aims to explain when cyber attacks violate international law and how countries may respond to such violations. However, it is not legally binding, and while respected in the West, countries like China, Russia, Iran, and North Korea do not necessarily recognize its authority.

Beyond espionage, you also see other types of cyber warfare activities, including sabotage of water plants, ATMs, banks, denial of service attacks, attacks against electrical power grids, propaganda campaigns, and economic disruption. These actions target a country's infrastructure and stability, often blurring the line between traditional and digital conflict. To ground these concepts, let's examine three real-world examples of cyber warfare.

The Stuxnet attack

The first is the **Stuxnet** attack, which you may have heard described as the world's first digital weapon. Stuxnet was a worm designed specifically to target centrifuges, which play an important role in enriching uranium. In 2010, Stuxnet was used to sabotage centrifuges at the Natanz nuclear facility in Iran. The attack is widely believed to have been designed by the United States and Israel. At the time, Iran was attempting to develop its own nuclear weapon, a process that requires uranium enrichment. Stuxnet targeted this process by increasing the pressure in the valves connected to the centrifuges, causing repeated malfunctions, and ultimately disrupting Iran's nuclear program. At the end of its operation, Stuxnet had destroyed about 984 centrifuges, reducing Iran's nuclear enrichment capacity by 30%.

What makes Stuxnet particularly alarming is that it infiltrated the Natanz plant in 2009 but went undetected until 2010. This demonstrates how sophisticated and stealthy digital weapons can be, and raises questions about the kinds of destructive cyber capabilities that may exist today.

The point here is that if you had weapons like **Stuxnet** 14 years ago, you can only imagine the kinds of destructive digital weapons that exist today, possibly developed by countries such as Russia, China, or the United States. This is a genuinely frightening prospect when you consider the evolution of cyber capabilities.

NOTE

If you want to learn more about the Stuxnet incident, there is a book called *Countdown to Zero Day* that documents this attack in detail.

Stuxnet spread via a USB drive. Someone introduced Stuxnet into a USB, plugged it into a computer at the nuclear facility, and, being a worm, it was able to propagate itself to other networks and began attacking systems that controlled the centrifuges.

This highlights how malware can be militarized to become cyber weapons. The attackers in this case did not need to launch airstrikes or invade Iran; inventing the Stuxnet worm, getting it onto a USB drive, and plugging it into a computer was enough to cause significant damage. Although no one has definitively proven that the United States or Israel was behind the attack, the nature, and intent of Stuxnet have led many to believe these two countries were responsible.

You should also be aware that Stuxnet has since been redesigned and repurposed by many cyber attackers. This highlights a major downside of cyber weapons. There might be a very sophisticated form of malware that only a government could sponsor. However, eventually, the code for that malware gets released, and other cyber attackers and cyber criminals can then adapt it to their own advantage. Much of the original code developed for Stuxnet has been modified and is now used to attack businesses and companies worldwide.

The 2018 disinformation campaigns involving Qatar

One of the most striking examples of cyber conflict involving the United States, Saudi Arabia, and Qatar emerged around the **2017-2018 Gulf diplomatic crisis**, when political tensions between Qatar and several neighboring countries spilled into the digital world. The dispute involved Saudi Arabia, the UAE, Bahrain, and Egypt, which accused Qatar of supporting terrorism and interfering in regional affairs. These claims were denied by Qatar.

During this period, Qatar was accused of supporting online campaigns intended to discredit senior officials and other influential individuals associated with Egypt, Saudi Arabia, the UAE, and Bahrain. Reports suggested that approximately 1,200 individuals were targeted as part of these activities, demonstrating how cyber operations can be directed not only at computer systems but also at individuals whose reputations or political influence make them valuable targets.

A notable individual target was American Republican fundraiser Elliot Brody. Qatar is believed to have hacked into his computer, uncovering incriminating files, including allegations of a sensitive nature. This led Brody to sue the Qatari government, although the lawsuit did not appear to progress significantly.

The wider regional conflict also included attacks against media organizations. The conflict escalated when Saudi Arabia retaliated by infiltrating the computer systems of the Qatari media agency. Saudi actors then launched their own disinformation campaigns, further intensifying the situation. The result was a chaotic exchange of cyberattacks and counterattacks. This incident illustrates how cyber warfare can manifest as both technical intrusions and information manipulation. Hacking can be used to obtain sensitive information, while leaks and disinformation can be used to influence public opinion, damage reputations, and place political pressure on an adversary.

The Estonia cyber attack

Now, let's consider the cyber attacks against Estonia in 2007. These attacks were allegedly conducted by the Russian government, although they have denied any involvement. However, it is undeniable that the attacks originated from Russia. The background to this incident involves the end of the Second World War, when the Russians drove the Nazis out of Estonia and erected a bronze soldier statue in Tallinn, the capital of Estonia, to commemorate their victory. The statue may also have been intended to honor a hero from the war, though that detail is uncertain.

The controversy began when in 2007, the Estonian government decided to move the statue from the center of Tallinn to a cemetery on the outskirts. This action caused significant backlash in Russia, where it was seen as highly disrespectful. In response, there were numerous **distributed denial of service attacks (DDoS)** launched from Russia. These attacks targeted Estonian banks, media outlets, and ATMs, and persisted for about three weeks.

While the Russian government denied any involvement, it is plausible that Russian nation-state-sponsored cyber gangs carried out the attacks, either with direct support from the government or with the government simply ignoring their actions. DDoS attacks are often carried out by groups of motivated individuals rather than governments, so it is possible that Russian hacktivists organized the attack without official support. The undeniable fact is that the attacks originated from Russia.

NOTE

Estonia is often cited as the first country to experience a major cyber attack targeting its national infrastructure, specifically through a DDoS attack.

Once Estonian authorities realized that their websites were being overwhelmed by traffic from unusual countries such as Egypt and Vietnam, they quickly identified the situation as a DDoS attack. To defend against it, Estonia had to take the drastic step of disconnecting its internet infrastructure from the rest of the world.

This meant that people inside Estonia could only access Estonian websites, and those outside the country could not reach any Estonian-based sites. As a result, Estonia was effectively cut off from the global internet, which created a very alarming situation for its people and government.

This incident demonstrates how cyber warfare can be triggered by political or cultural disputes, and how attacks can be carried out by actors who may or may not have direct ties to a government, allowing for plausible deniability.

Note that governments and national infrastructure are not the only targets of politically motivated cyberattacks. Private companies can also find themselves at the center of international disputes, particularly when their products, actions, or public influence attract the attention of governments or politically motivated groups. In these cases, an attack against a company can have consequences that extend well beyond financial loss, affecting employees, customers, and even international relations. Let's discuss a private attack next.

The 2014 Sony Pictures hack

One of the most notorious examples of a private company becoming a high-profile target is the 2014 attack against Sony Pictures, which coincided with the release of the controversial movie *The Interview* starring Seth Rogen, a comedy depicting a fictional plot to assassinate North Korean leader Kim Jong Un. North Korea strongly objected to the film before its release. In June 2014, a North Korean government spokesperson condemned the movie and warned of retaliation if it was released. Several months later, a group calling itself the **Guardians of Peace (GOP)**.

The attack began on the Monday before Thanksgiving, when employees attempting to log into their computers were confronted with a graphic of a red skeleton, accompanied by gunshot sounds and a message stating "Hacked by #GOP." The warning threatened to release sensitive data later that night if an unspecified demand was not met.

Figure 6.1 shows the threatening message and imagery that greeted Sony Pictures employees during the attack:



Figure 6.1: Ransom note displayed during the Sony Pictures hack, illustrating a real-world cyberattack and its effect on organizations.

Sony's IT staff responded quickly, but before they could intervene, the malware had already spread throughout the company's network. It propagated from computer to computer and network to network, ultimately erasing all data stored on more than 3,000 computers and affecting over 800 servers.

To ensure that the data could not be recovered, the attackers used a specialized deleting algorithm that overwrote the data in seven different ways. This meant that Sony not only lost its data, but also had no way to recover it. As a result, the company was forced to revert to using fax machines, blackboards for communication, and paper checks to pay employees.

Before destroying the data, the hackers also exfiltrated it. Over the next three weeks, they released confidential files and data on public file sharing sites, including unfinished movie scripts, internal emails, more than 47,000 social security numbers, and even four unreleased Sony films, which were leaked to piracy websites for free viewing. The attackers escalated their threats by warning of a "9-11 style" attack against theaters planning to show *The Interview*.

Attribution for the Sony Pictures hack remains difficult, but the **FBI — Federal Bureau of Investigation** and the United States government ultimately blamed the North Korean government, citing the timing of the attack with the release of *The Interview*. In response, the North Korean government publicly denied involvement in the attack but praised it as a righteous act, suggesting that supporters of the regime could have been responsible. As a result, it is widely believed that hackers sympathetic to North Korea carried out the attack.

Summary

The incidents examined in this chapter demonstrate that cyberattacks are not confined to computers and networks; their consequences can extend into politics, business, national security, and everyday life. From the attacks against Estonia to politically motivated campaigns and attacks on private companies such as Sony Pictures, each case shows how digital systems can become targets during wider political, economic, or international disputes.

The chapter drew a critical distinction between cyber warfare and cyber espionage, highlighting the ongoing debate over definitions, the use of plausible deniability, and the unique challenges of attribution in digital conflict. The examples also highlight how attackers can operate across borders, use compromised systems located in other countries, and conceal their identities, making it difficult to determine who is ultimately responsible. Even when an attack appears to support the interests of a particular country or group, proving direct involvement can be considerably more difficult.

Most importantly, these incidents demonstrate why cybersecurity must be considered in a broader context. Understanding the technical details of an attack is important, but so is understanding the motivations behind it, the people and organizations being targeted, and the consequences that follow.

Part III

Building Your Security Defenses

Part III — Building Your Security Defenses brings together the core strategies and tools needed to protect networks, systems, and data from a wide range of threats. Across these chapters, you will learn how to implement essential security controls, manage identity and access, apply modern defense principles like Zero Trust, and design robust protections for critical information. Together, these topics form a comprehensive approach to building practical and effective security defenses.

This part contains the following chapters:

- *Chapter 7, Essential Security Controls*
- *Chapter 8, Identity and Access Security*
- *Chapter 9, Modern Cyber Defense*
- *Chapter 10, Protecting Data and Systems*

7

Essential Security Controls

So far, you have seen how cyber threats can cause real consequences for individuals, organizations, and even entire countries. The incidents in the previous chapter demonstrate why understanding threats is important, but identifying a threat is only the beginning. The next question is, *what can we do to protect ourselves against it?*

This chapter focuses on essential security controls, or the practical defenses that stand between our networks and the constant threat of unauthorized access, malicious activity, and data loss. Security controls can take many forms, from technologies that filter network traffic and detect suspicious behavior to policies and procedures that determine how systems and information should be protected.

By the end of this chapter, you will be able to identify, configure, and distinguish between critical tools such as firewalls (including network and host-based firewalls), DMZ setups, symmetric and asymmetric encryption methods, and wireless security protocols such as WPA2 and WPA3.

We will also clarify key distinctions such as default deny versus default allow firewall configurations, the difference between public and private key encryption, and the specific roles of encryption and authentication in wireless security.

Mastering these controls is crucial, as they form the foundation for protecting sensitive information, ensuring that only trusted users and devices gain access, and keeping our networks resilient against both external and internal threats.

In this chapter, we will cover the following topics:

- Security control categories
- Firewalls
- Encryption for Data Protection
- Authentication
- Honeypots and Demilitarized Zones (DMZs)
- Wireless Security
- Password Security and Management

Security control categories

As discussed earlier, a security control is something that is designed to give a system or a digital asset the properties of confidentiality, integrity, availability, and non-repudiation. Security controls can be divided into three different categories: **technical**, **operational**, and **managerial**.

The technical category includes controls that are implemented as a system. Examples of technical controls are firewalls, anti-malware, and open system access control. These are also referred to as **logical controls**. The operational category consists of controls that are implemented primarily by people rather than systems. Examples include security guards and training programs. These are operational security controls. Managerial security controls provide oversight over information systems. Examples of managerial controls are risk identification tools and security policies.

Now, let's look at the technical control, firewalls, next.

Firewalls

You are now going to explore one of the most important security tools available— firewalls. Firewalls have existed since the early days of the internet and play a crucial role in protecting your data and systems from cyberattacks. Firewalls act as security systems that monitor and control incoming and outgoing network traffic based on a set of rules. You can think of a firewall like a security guard at an airport, inspecting data as it passes through to ensure nothing harmful gets in or out.

In this section, you will learn what firewalls are, how they work, and the different types you might encounter, including both physical devices and software solutions such as Windows Defender. You will also see how firewalls use rules to control network traffic and how these rules can be customized to fit your needs.

Types of firewalls

Firewalls can be either physical devices or software applications, or sometimes both. There are two main types of firewalls. The first type is **network firewalls**, which are usually physical devices placed in your office or building, or built into your router. These protect entire networks from outside threats. For example, your home Wi-Fi router almost certainly has a default firewall built in.

The second type is **host-based firewalls**, which are software installed on individual devices. These protect the specific device from threats, even those coming from within the same network. Examples include Windows Defender firewall and the macOS firewall.

Firewall rules and filtering criteria

Firewall rules can be created to block traffic from a specific IP address or range, such as one known to belong to a hacker or scammer. You can also set rules based on ports, for example, allowing only web traffic on ports 80 and 443 while blocking everything else. Protocol-based rules let you allow or block specific protocols like HTTP, HTTPS, FTP, or SFTP. Application-based rules enable you to allow certain applications, such as a game, to connect while blocking unknown or unwanted applications. This flexibility allows you to tailor firewall behavior to your specific needs.

These rule types relate to different parts of your network. The following diagram shows a firewall filtering traffic between devices and the internet based on rules for IP addresses, ports, protocols, and applications:

Firewalls

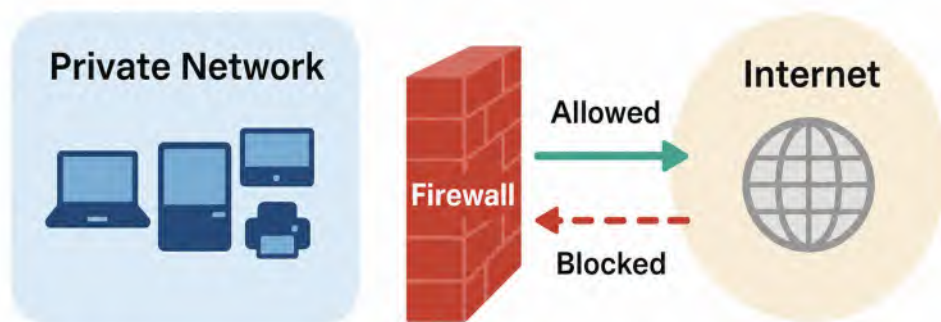


Figure 7.1: Firewalls

Common firewall configurations

There are two common firewall configurations: **default deny** and **default allow**. With default deny, you block everything by default and only allow the specific traffic you need, making it the most secure option. Default allow, on the other hand, permits all traffic unless it is explicitly blocked, which is less secure but more commonly used in home environments, such as on your local router.

Demonstration of Windows Firewall

To help you understand how firewalls work in practice, here is a quick demonstration using Windows Defender on Windows 10 Home Edition.

1. Press the Windows key and search for "Windows Defender firewall"
2. Open the Windows Defender Firewall application. You will see the main Windows Defender Firewall screen, which displays the status for Private networks and Guest or public networks. The Advanced Settings link is located on the left side of the window.
3. Click "Advanced settings" in the left sidebar to access more detailed configuration options.

This opens the Windows Defender Firewall with Advanced Security window, where you can view and manage firewall profiles and rules. By default, most Windows machines have three firewall profiles: **domain profile**, **private profile**, and **public profile**.

The next figure shows the Advanced Security interface, including the Domain Profile, Private Profile, and Public Profile sections.

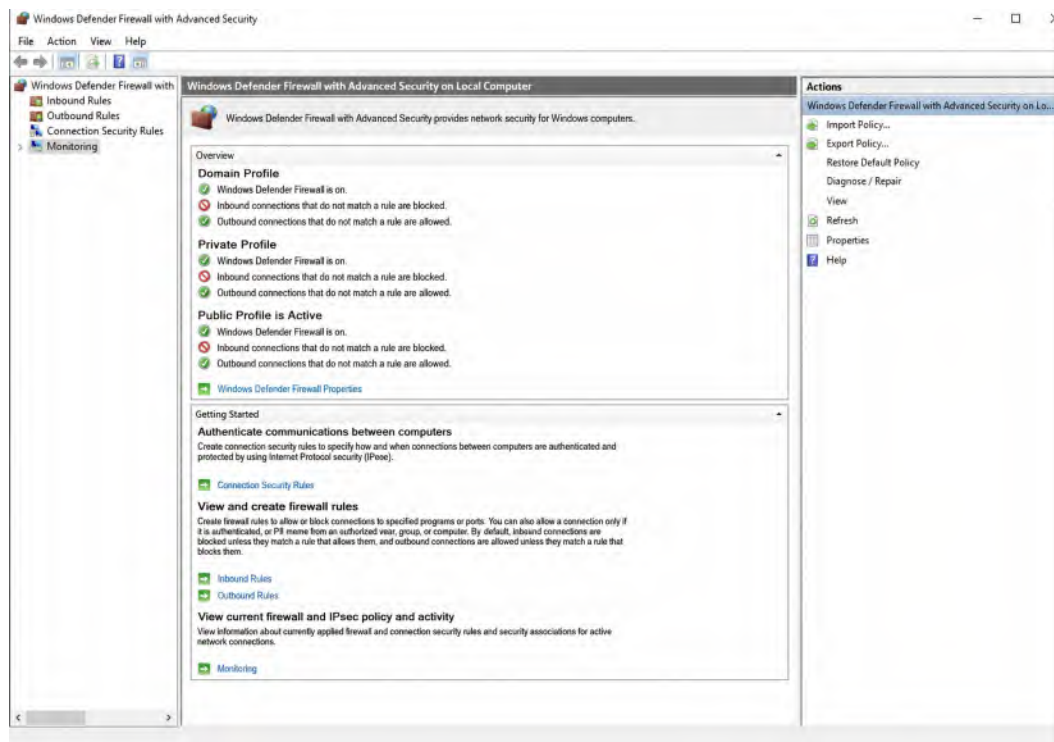


Figure 7.2: Windows Defender Firewall profiles: domain, private, and public, with status and rule enforcement details.

The domain profile is used for special networks where your computer can authenticate itself, typically managed by a domain controller. The private profile is for your home or a private network, while the public profile is for public Wi-Fi environments such as coffee shops, airports, or hotels.

As mentioned earlier, every firewall, whether hardware-based or software-based, uses rules to filter traffic. The firewall filters both incoming (inbound) and outgoing (outbound) network traffic. On the left side of the Advanced Security window, you will see options for **Inbound Rules** and **Outbound Rules**. Inbound rules control traffic coming into your computer from external networks, such as the internet. For example, you might see inbound rules for applications like the Apache HTTP server or video games, which are enabled to allow necessary network communication.

A list of applications such as Dropbox, FileZilla, and Firefox that have specific inbound rules configured in Windows Defender Firewall. Each rule is associated with a profile, public, private, or domain, and you can enable it for one or all profiles.

The action column shows whether traffic is being blocked or allowed, and there is no override set for these rules. The program column lists the executable path for each application, and you can also view the local and remote addresses, as well as the protocol (TCP or UDP) used by each rule. The same structure applies to outbound rules, which control traffic leaving your computer for the network or internet. Here, you will find rules for applications such as Skype, Spotify, and Candy Crush, even if you have not played Candy Crush in a long time.

To monitor and log firewall activity, select the Monitoring option in the left sidebar. This section allows you to configure whether your firewall will monitor and log traffic for the domain, private, and public profiles. You can expand each profile to view its general and logging settings as shown below:

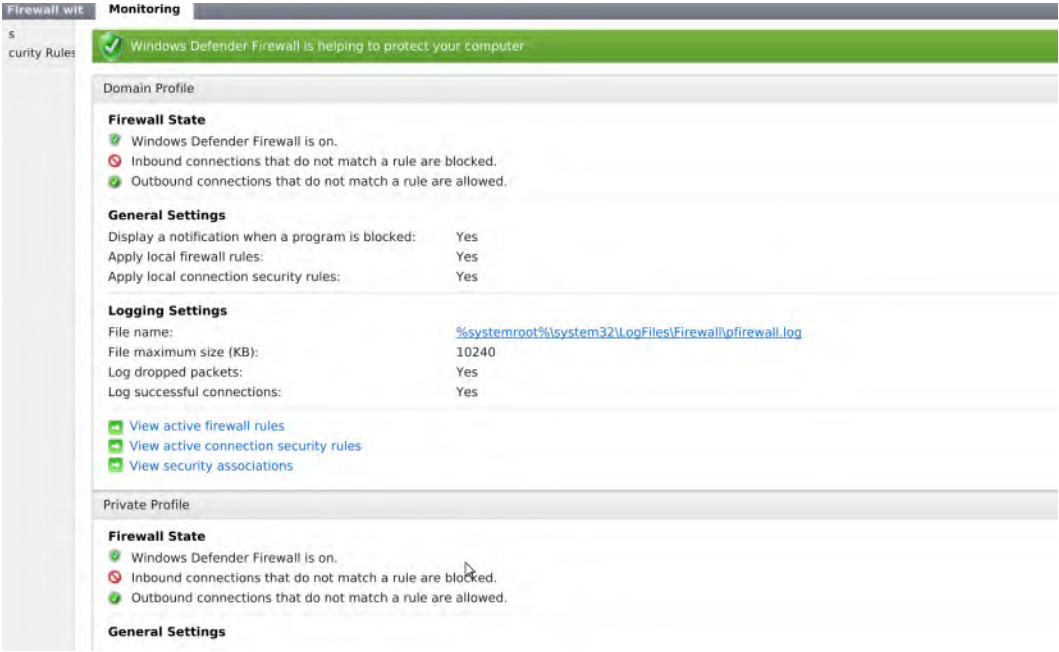


Figure 7.3: Windows Defender Firewall monitoring settings, showing firewall state, general settings, and logging options for domain and private profiles.

When you expand a profile, under General Settings, you will see options such as "Display a notification when a program is blocked" (set to Yes if you want to be notified), and "Apply local firewall rules" (also set to Yes).

The Logging Settings section lets you specify the log file name, the maximum file size, and whether to log dropped packets and successful connections. By default, on Windows 10 Home Edition, the options to log dropped packets and successful connections are usually set to No for all profiles. If you want your firewall to log traffic, you need to enable these options.

To enable logging for your firewall, follow these steps:

1. Open Windows Firewall with Advanced Security.
2. Right-click on it and select **Properties**.
3. In the Properties window, you will see three profiles: Domain, Private, and Public.
4. For each profile, locate the Logging section and click **Customize**.
5. Change the settings for "Log dropped packets" and "Log successful connections" from No to Yes.

This allows your firewall to log both dropped and successful connections for each profile.

You also have the option to change the default location where the traffic reports are stored, though you should only do this if you have a specific reason. Additionally, you can increase the size limit for the log file, but again, only adjust this if necessary.

Typically, inbound connections are blocked by default, and you must explicitly allow the specific connections you want to permit. This is because inbound traffic may include unwanted connections from outside your network. Outbound connections, on the other hand, are usually allowed by default, since you are initiating the access to external websites or services.

The next figure shows the Windows Defender Firewall settings dialog, where inbound connections are set to 'Block (default)' and outbound connections are set to 'Allow (default)':

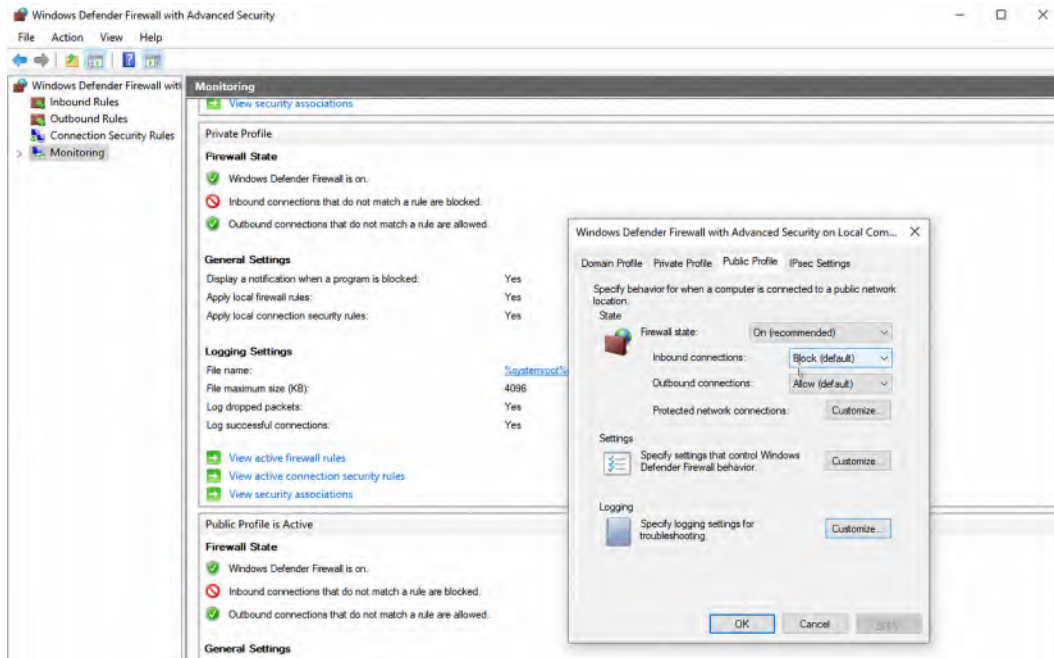


Figure 7.4: Windows Defender Firewall settings, showing default inbound connections blocked and outbound connections allowed

Most Windows machines come with pre-configured rules that allow you to access the internet and use various services by default.

When you view the monitoring section, you will see log files for the public, domain, and private profiles. These files monitor the firewall logs. A typical firewall log includes fields such as *date*, *time*, *action*, *protocol*, *source IP*, *destination IP*, and *port number*.

The following code block shows an example of a firewall log file as displayed in Notepad:

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags
tcpsyn tcpack tcpwin icmptype icmpcode info path

2021-05-05 10:42:19 ALLOW UDP 192.168.1.5 74.125.24.121 59075 443 0 - - - - -
SEND
```

```
2021-05-05 10:42:19 ALLOW UDP 192.168.1.5 74.125.24.125 59076 443 0 - - - - -  
SEND  
2021-05-05 10:42:19 ALLOW UDP 192.168.1.5 192.168.1.255 138 138 0 - - - - -  
RECEIVE  
...
```

Notice the version, software, and fields at the top, followed by entries showing the date, time, action (such as ALLOW), protocol (UDP or TCP), source and destination IP addresses, port numbers, and other details. This information helps you investigate network activity and troubleshoot issues.

You are now going to see how to create a sample outbound rule in Windows Defender Firewall to block all internet connections for Google Chrome.

First, you verify that you can currently access the internet using Google Chrome by navigating to a website such as webmonkeyacademy.com. After confirming that Chrome can access the internet, you return to the firewall to begin creating the outbound rule.

To start creating a new outbound rule, do the following:

1. Go to the **Outbound Rules** section.
2. Click the **New Rule** option in the Actions panel on the right. The New Outbound Rule Wizard provides options for selecting the type of rule to create. You can choose to create a rule for a specific program, a port number, use a predefined rule, or create a custom rule based on specific port numbers, programs, and other criteria.
3. Since you want to target Google Chrome specifically, select **Program** and click **Next**.
4. You are then prompted to specify the program path. Click **Browse** and navigate to the default installation path for Chrome, which is typically on your C drive under Program Files (x86), then Google, then Chrome, then Application.
5. You are then prompted to enter a name and optional description for your new outbound rule. For this example, set the name to "Google Chrome Test," and the description asks, "Can we block internet traffic with Chrome?" The following code shows the exact text entered for the rule name and description:

```
Name: Google Chrome Test  
Description (optional):  
Can we block internet traffic with Chrome
```

6. After entering the details, click Finish to create the rule.

Once the rule is applied, try refreshing a page in Google Chrome. You will see a message stating that your internet access is blocked, confirming that Chrome can no longer access any website. Opening a new tab and attempting to visit a website will also fail, demonstrating that the outbound rule is working as intended.

To manage the rule, return to the Windows Defender Firewall with the **Advanced Security** window. The new rule, "Google Chrome Test," is listed at the top under Outbound Rules, as shown below:

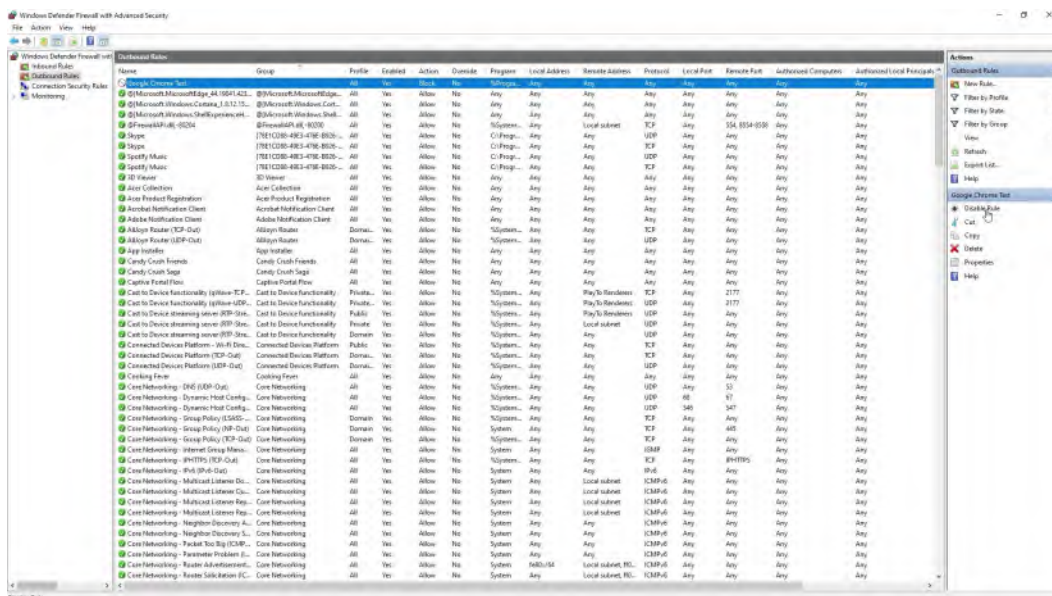


Figure 7.5: Blocking outbound traffic for Google Chrome with Windows Defender Firewall

The rule is enabled, applies to all profiles, and its action is set to block any traffic from the specified program. The program path is also displayed. If you delete the rule and refresh a page in Chrome, you will regain internet access, confirming that the rule was responsible for blocking traffic.

You can also create a rule based on a port number. For example, if you want to block all internet traffic regardless of the browser, you can select port 80, which is used by HTTP.

The following code block shows how you specify the protocol and port in the New Outbound Rule Wizard:

```
Does this rule apply to TCP or UDP?
```

- TCP

```
Does this rule apply to all remote ports or specific remote ports?
```

- Specific remote ports: 80

After specifying the port, you choose whether the rule applies to TCP or UDP services, then proceed to the next step, where you can select to block the connection. You continue through the wizard, clicking Next at each step, until you finish or cancel the process.

The next code block shows the profile selection step in the wizard:

```
When does this rule apply?
```

- Domain (applies when a computer is connected to its corporate domain)
- Private (applies when a computer is connected to a private network location, such as a home or workplace)
- Public (applies when a computer is connected to a public network location)

If you decide not to proceed, you can simply click cancel to exit the wizard.

The process for creating an inbound rule is nearly identical. You click on **New Rule** under **Inbound Rules**, and you can choose to block a program, block a port number, or select other options.

The following code block shows the initial step for creating a new inbound rule:

```
What type of rule would you like to create?
```

- Program (rule that controls connections for a program)
- Port (rule that controls connections for a TCP or UDP port)
- Predefined (rule that controls connections for a Windows experience)
- Custom (custom rule)

You follow the same steps as with outbound rules, selecting the type of rule and proceeding through the wizard.

The following figure shows the Windows Defender Firewall with Advanced Security interface, highlighting the available outbound rules options in the Actions pane:

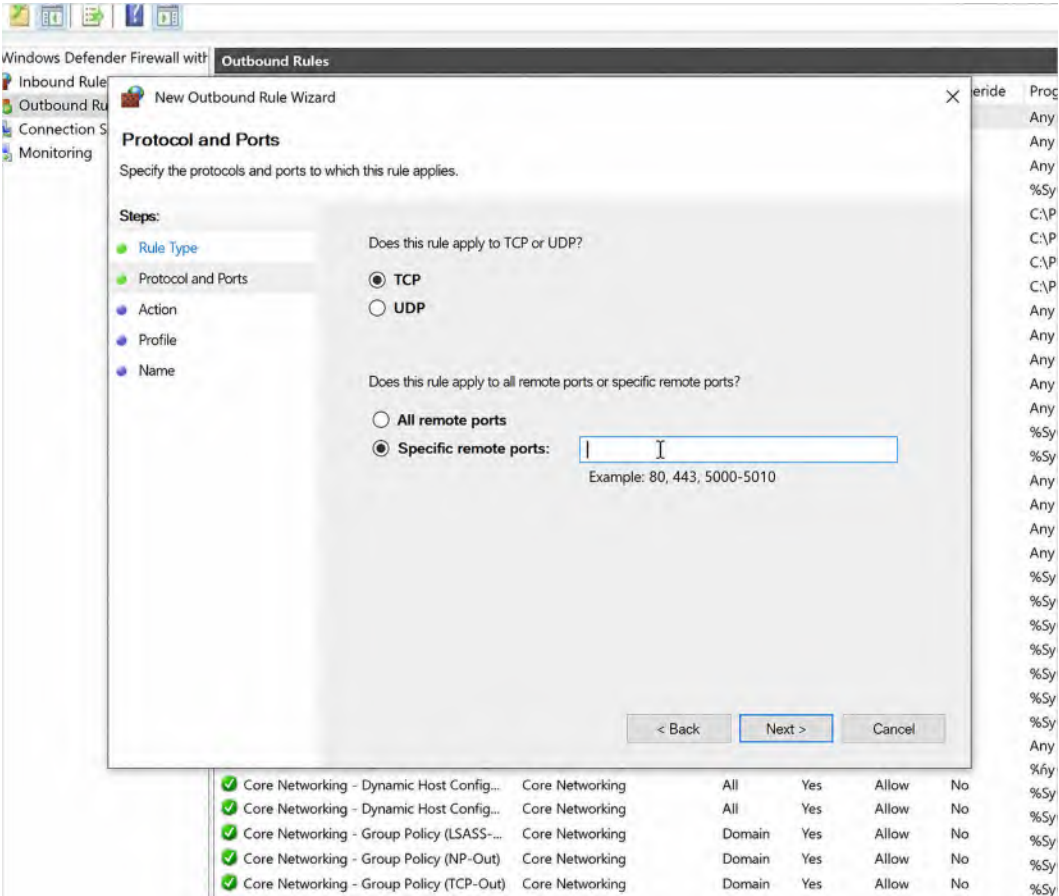


Figure 7.6: New outbound rule options

On the right side of the Windows Defender Firewall with Advanced Security window, you have options to import or export firewall policies. If you want to import a policy from another machine or server, click "Import Policy," confirm with "Yes," and select the policy file to import. To export your current policy for use on another machine or server, click "Export Policy." If you encounter issues with firewall settings, use the "Diagnose and Repair" link or restore default policies if something has broken.

Firewalls provide an important layer of protection by controlling the traffic that enters and leaves a network. However, once data is allowed to travel across a network, it may still be exposed to interception or unauthorized access.

This brings us to another essential security control, **encryption**, discussed next.

Encryption for data protection

Encryption is the process of making information hidden or secretive. The word "encryption" comes from two words: "en," which means to make, and "crypto," which means hidden or secret. In other words, encryption is all about making certain kinds of data or information private so that only people with the right access will be able to view that information.

Encryption uses a key to transform readable information into a form that cannot easily be understood by someone who is not authorized to access it. Once the information has been encrypted, the readable data, known as **plaintext**, is transformed into unreadable data called **ciphertext**.

Decryption is the reverse process. It uses the appropriate key to transform the ciphertext back into plaintext so that the information can be read and used again.

You may also come across the term **cryptography**, which is often confused with encryption. Cryptography is the broader science of protecting information and enabling secure communication. Encryption is one of the techniques used within cryptography. Cryptography also covers other concepts and techniques used to protect the confidentiality, integrity, and authenticity of information.

NOTE

The important distinction to remember is that encryption is a process, while cryptography is the broader field that studies and develops methods for securing information and communications.

There are two major types of encryption:

1. **Asymmetric Encryption:** This uses two different keys for encrypting and decrypting. For example, if a sender wants to send a message, they will use a public key to encrypt the plain text. The plain text then becomes a cipher, which will have to be decrypted using a private key by the receiver. So, it's basically using a public key to encrypt the plain text, turning it into a cipher, and then the receiver uses a private key to decrypt the cipher, turning it back into a plain text message.
2. **Symmetric Encryption:** This uses just one single key. The sender and the receiver use the exact same key to both encrypt and decrypt the message.

Decryption using a private key by the receiver is a core part of asymmetric encryption. In this process, you use a public key to encrypt the plaintext, turning it into a cipher, and then the receiver uses a private key to decrypt the ciphertext, converting it back into plaintext. This is shown in the diagram below:

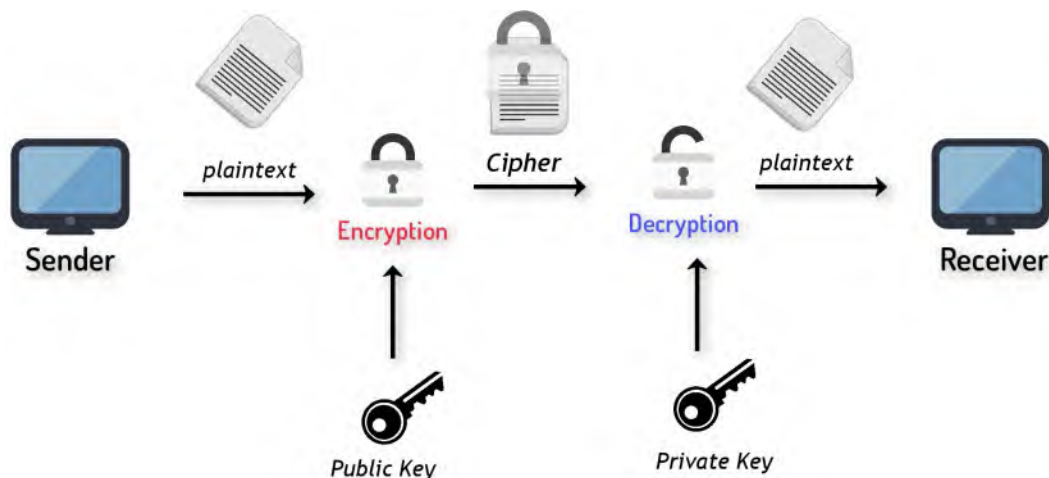


Figure 7.7: Public key encryption and decryption process showing sender, receiver, and use of public/private keys for secure communication.

In symmetric encryption, the process is similar, except that both the sender and the receiver use the exact same key for both encryption and decryption.

The next diagram demonstrates the symmetric encryption process, where a single secret key is used for both encrypting and decrypting the message.

There are a few types of asymmetric encryption you should know about. The first is the RSA algorithm, which stands for Rivest, Shamir, and Adleman. For symmetric encryption, the main types are the **Data Encryption Standard (DES)** and the **Advanced Encryption Standard (AES)**.

NOTE

We will discuss encryption and decryption in more detail in *Chapter 10*.

Encryption helps protect data by ensuring that even if it is intercepted or accessed without authorization, it cannot be easily understood. However, protecting the data itself is only one part of security. Organizations must also ensure that the person attempting to access that data or system is actually who they claim to be. Let's discuss this next.

Authentication

Authentication is the process of verifying that a user, device, or system is who or what it claims to be. The most familiar example is entering a username and password when signing in to an account. However, passwords are only one method of authentication. Security systems can verify identity using something you *know*, such as a password or PIN, something you *have*, such as a security token or smartphone, or something you *are*, which includes unique physical characteristics.

One increasingly common way of verifying identity is through **biometric authentication**. Rather than relying on something a person must remember or carry, biometric security mechanisms use characteristics unique to the individual, such as fingerprints, facial features, or voice patterns, to help determine whether access should be granted.

Biometric security mechanisms

Biometrics is a security mechanism used to authenticate and provide access based on the verification of physical characteristics. The general idea is that everyone is unique in some way; whether it is your voice, the way you talk, your walk, fingerprints, or eyelashes, there is always something that distinguishes you from others.

The opening scene from *Mission Impossible 5*, starring Tom Cruise, provides a memorable example of a security system using biometrics. In the clip, the system detects an impersonator by analyzing the way the individual walks, ultimately identifying the person as a fake.

Physiological and behavioral biometric identifiers

There are two general types of biometric identifiers. **Physiological characteristics** refer to the shape or composition of the body, such as fingerprints, DNA, retina scans, face, and hand geometry. **Behavioral characteristics** are more advanced and refer to the behavior of a person, including voice, gestures, and gait. The Mission Impossible clip demonstrated behavioral characteristics, as the cameras detected the impersonator simply by analyzing the way the person was walking.

Biometric systems typically involve a database that stores the biometric data for comparison. Therefore, every individual that is supposed to have access will already have their eye scans, their fingerprints taken, and the way they walk or talk would have been recorded. All this data is compared to every other individual walking in, just to make sure that they are actually the right person. If there is a match in the database, then the system knows that the individual is the right person. If there is a mismatch, then the system knows that the person is unauthorized.

Accuracy has improved and the cost has been reduced over time. Back in the early days, implementing biometrics was extremely expensive, but now things have gotten cheaper and, as a result, it is becoming increasingly common. You can even see nowadays that many laptops require a fingerprint scan before you can gain access.

Using more than one of authentication methods can provide stronger protection through **factor authentication**, discussed next.

Factor authentication methods

Let's come back to Mission Impossible again. In one clip, William Donlow attempts to access a black vault lockdown, where only one person is allowed in the room and must pass through a series of security checks. The first is a voiceprint identification and a six-digit access code, which only gets him into the outer room. Next, he has to pass a retinal scan. Finally, the intrusion countermeasures are only deactivated by a double electronic keycard.

The most popular form of factor authentication is **two-factor authentication**. Here, a user provides two authentication factors to verify who they are, which provides an additional layer of security. All forms of factor authentication add extra layers of security, but what exactly are these authentication factors?

As the clip suggests, there is the knowledge factor, which is something the user knows, like a password. In the clip, the user types in a six-digit code. The knowledge factor could include things such as passwords, usernames, or keyphrases. There is also the possession factor, which is something the user has, like a token or a mobile device. In the clip, the user had a keycard. Finally, there is the inheritance factor, which is something the user is, biometrics. In the clip, the individual provided both a voiceprint and an eye scan. Even though the individual went through four security checkpoints, in reality, he actually went through three authentication factors.

However, note that using two factors from the same category would not constitute two-factor authentication. For instance, if you combine a username and a password, even though you have to provide both, they both fall under the same category, which is the knowledge factor. As a result, this would still be considered a single-process authentication factor method.

Similarly, a retina scan and a voice print, belongs to the same category, the inheritance factor and will be counted as one factor.

While two-factor authentication does improve security, it is not foolproof; cards can be stolen, and fingerprints can even be lifted. That is why **three-factor** and **multi-factor authentication** methods are used for further improvements. **Multi-factor authentication** can even include additional factors, such as a time and location factor. In this case, an individual could be required to be at a specific place at a specific time, in addition to providing the inheritance, knowledge, and possession factors, in order to gain access to certain information.

Honeypots and demilitarized Zones (DMZs)

You can also strengthen your network defenses using tools such as **honeypots** and **DMZs**.

A **honeypot** is a computer system or network that is deliberately set up as a decoy to attract cybercriminals. Instead of giving attackers access to real, valuable systems, a honeypot gives them something that *looks* like a worthwhile target. While attackers attempt to gain access, cybersecurity professionals can observe their activities and learn more about the techniques they use.

To make this work, a honeypot is designed to behave like a real system. It might contain applications, services, files, and other resources that an attacker would expect to find on a genuine computer or server. The more convincing the honeypot is, the more useful it can be. Experienced attackers may recognize obvious signs of a decoy, so honeypots are often designed to make their behavior and environment appear as realistic as possible.

Honeypots can generally be divided into two types based on their purpose: **research honeypots** and **production honeypots**.

A **research honeypot** is used to *learn about* cyberattacks. It provides a controlled environment where cybersecurity professionals can observe how attackers discover systems, attempt to gain access, and behave after gaining access. This information can help researchers understand new attack techniques, identify patterns in attacker behavior, and develop better ways to defend real systems.

A **production honeypot**, on the other hand, is deployed as part of an organization's current network. Its purpose is to attract suspicious activity away from genuine systems while also providing an early indication that someone may be attempting to compromise the network. For example, imagine an organization has several important servers on its network and also deploys a honeypot that appears to contain valuable information. An attacker searching the network may discover the honeypot and attempt to access it. Because legitimate users generally have little or no reason to interact with a honeypot, activity detected on it is a useful warning sign for the security team.

NOTE

In simple terms, a research honeypot helps you learn from attackers, while a production honeypot helps you detect and observe suspicious activity in a real environment. In both cases, the basic idea is the same: provide attackers with a convincing decoy and use their interaction with it to better understand and defend against potential threats.

DMZ architecture

A **demilitarized zone (DMZ)** is a physical or logical subnetwork that separates a local area network from other untrusted networks. The DMZ acts as a barrier between the real local area network of a company or business and the outside world, such as the internet.

External facing servers and resources are placed in the DMZ so that they are accessible from the internet, but the internet LAN is kept off limits. In the most popular DMZ setup, you use two firewalls: one facing the internet and another facing the local area network. The DMZ sits between these two firewalls.

For example, a company may have servers that need to be accessible to people outside the organization, such as web servers, email servers, or DNS servers. Instead of placing these servers directly inside the internal LAN, you can place them in the DMZ. Users on the internet can then access the services they need, while the company's internal network remains separated and protected.

The following illustration shows the internet on the left, the LAN on the right, and the DMZ in the center, separated by two firewalls. Servers in the DMZ act as a barrier between the outside world and the internal LAN of a company or a business.

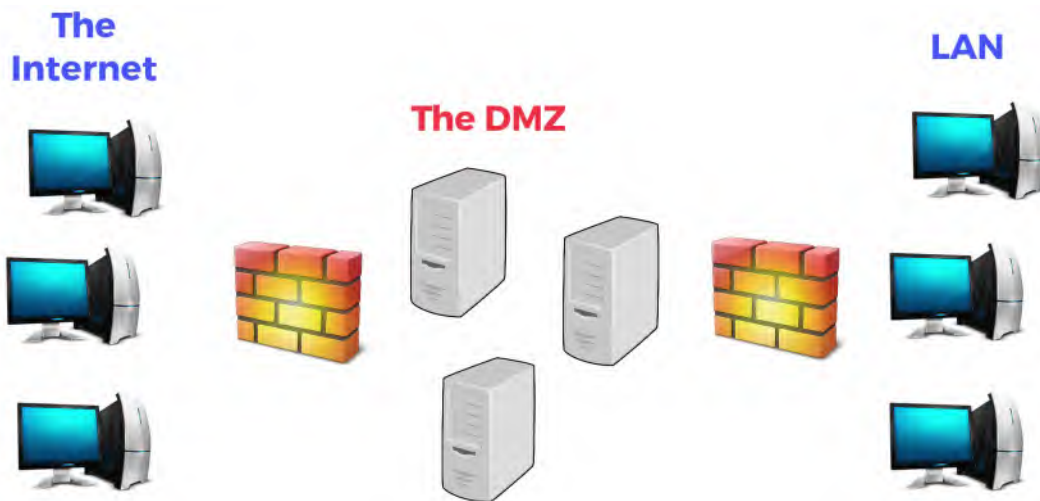


Figure 7.8: Network architecture showing a DMZ between two firewalls, separating the internet from the internal LAN.

The real objective behind DMZs is to add an additional layer of security. This means that even if an attacker manages to compromise a server in the DMZ, they do not automatically gain access to the internal network. They would still need to get through the second firewall and its security rules. In this way, the DMZ helps limit how far an attacker can go and reduces the exposure of important internal systems.

Wireless security

Wireless security is often overlooked, yet it is extremely important because most connections to a network or the internet are now wireless. Wireless security is the prevention of unauthorized access, but it also includes preventing damage to computers using wireless networks.

There are two main security objectives that wireless security tries to achieve. The first is encryption, which ensures that wireless communication is unintelligible to anyone except those with the correct encryption keys. Even if a hacker gains access to the traffic between two computers, if the connection is encrypted, they will not be able to decode what is being transferred. The second objective is authentication, which ensures that only authorized users whose identity has been verified can join and use the network.

Wireless security protocols

Wireless security protocols have evolved significantly since the introduction of Wi-Fi, with each new protocol aiming to address the vulnerabilities of its predecessors. The four main protocols you will encounter are WEP, WPA, WPA2, and WPA3.

The very first protocol, **Wired Equivalent Privacy (WEP)**, was introduced in September 1999. WEP was quickly found to be extremely vulnerable and was officially abandoned by the Wi-Fi Alliance in 2004. The Wi-Fi Alliance, a non-profit organization that owns the Wi-Fi trademark, sets the standards for wireless security and determined that WEP was simply not secure enough. If you find yourself on a network using WEP, you should take immediate action to upgrade, as it is considered a very poor security protocol.

To address WEP's weaknesses, **Wi-Fi Protected Access (WPA)** was developed. WPA was a significant improvement over WEP but still relied on some of the same exploitable elements, leaving it vulnerable to attacks. While WPA is better than WEP, it is still not considered a strong security protocol today.

The next major advancement was **WPA2**, which brought a massive improvement by introducing the **Advanced Encryption Standard (AES)**. AES is the same encryption standard used by the U.S. Government to protect sensitive data, making WPA2 a very strong choice for most networks. However, WPA2 is still susceptible to certain attacks, such as brute force attacks where hackers attempt to guess your password. Additionally, on public networks using WPA2, other users on the same network could potentially observe your activity and traffic.

The most recent protocol is **WPA3**, launched in 2018. WPA3 offers protection against all types of attacks and is currently the best wireless security protocol available. However, WPA3 is not yet supported by many routers, switches, or even some laptops and mobile devices, especially older models. You should be aware of these compatibility limitations when considering an upgrade to WPA3.

Now that you understand the differences between these wireless security protocols, you will see how to check which protocol your own network is using.

To check which wireless security protocol your network is using, open your control panel, go to Network and internet, and select Wi-Fi. Let us take an example with the connected Wi-Fi network named Resident Evil, inspired by the video game series. After clicking on the network, you will see the security type listed; here, it is WPA2-Personal as shown below:

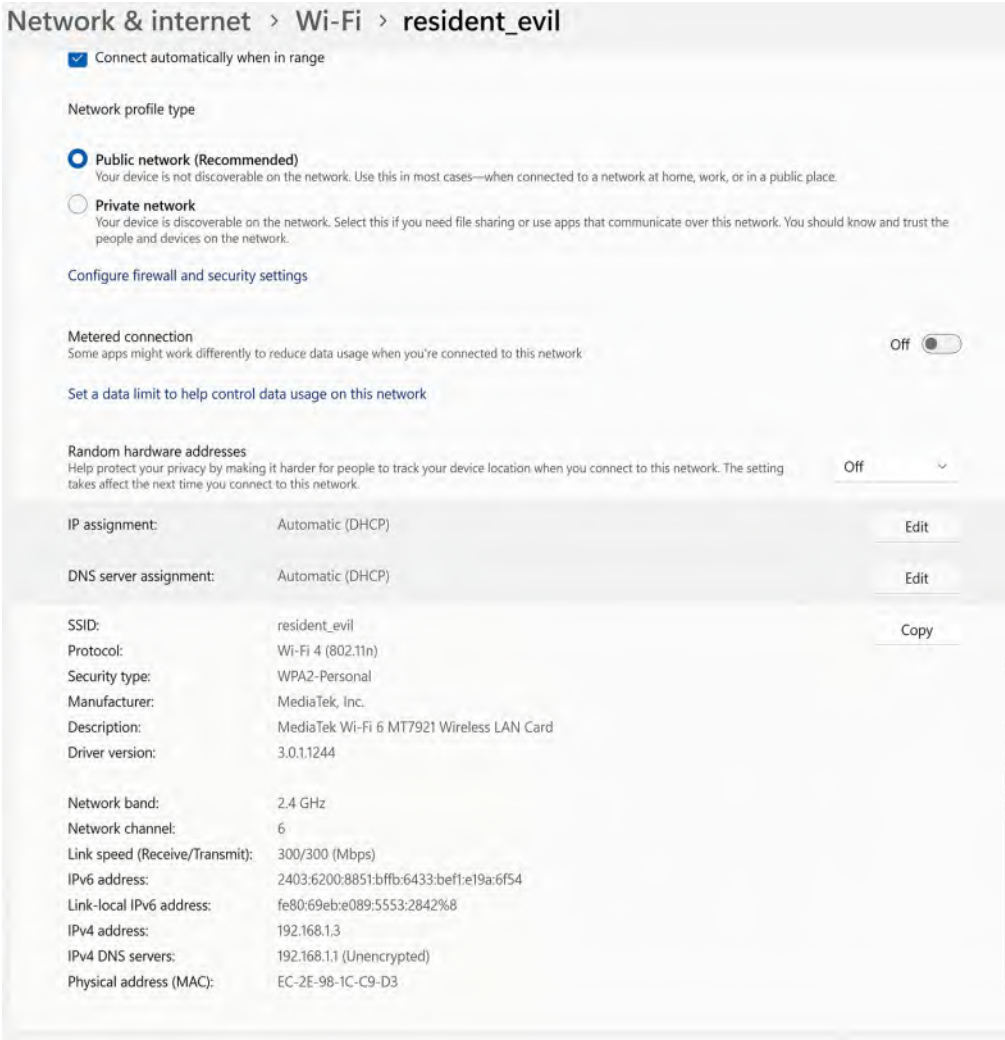


Figure 7.9: Wi-Fi network settings showing WPA2-Personal security for a private home network

If you are wondering why WPA3 is not being used, remember that sometimes the limitation is due to the router or device compatibility in your home or office. For a personal home network, WPA2 is a very good choice, especially if you are the only user and it is not a public network. WPA3 is more necessary for enterprise or large office networks.

TIP

At a minimum, you should be using WPA2. If you discover that your network is using WEP or WPA, you need to upgrade your security settings.

No section or module talking about cyber defenses would be complete without discussing passwords. Let's get into it.

Password security and management

Passwords are the most common way you protect your accounts, whether it's your email, websites, or other online services. In this section, you will learn what makes a strong password, how to manage multiple passwords across different accounts, and practical strategies for creating and remembering secure passwords.

A strong password should meet several key criteria to ensure your accounts remain secure. You need at least eight characters in total, and your password must include a mix of numbers and letters. Make sure to use at least one capital letter, and also include at least one symbol, such as a hashtag or a dollar sign. If your password satisfies these four criteria, most platforms will recognize it as very strong and accept it when you create a new account.

Password management strategies

Managing passwords can be challenging because you likely have many accounts: social media, email, third-party websites, your bank, and more. Many people make the mistake of using the same password for all their accounts, but this is risky. If one password is stolen, all your accounts could be compromised.

To keep your accounts secure, use different passwords for different categories of accounts. One approach is to have a unique password for your email and bank accounts, another for your social media accounts, and a third for all other types of accounts. When creating accounts on third-party websites, especially those you do not use often, avoid using your primary email account. Instead, use a secondary email account (such as a separate Yahoo or Gmail address) for these less important sites. Reserve your primary email account for your most important and frequently accessed websites.

Password formula examples

When you create your own passwords, having a formula makes it much easier to remember them. This approach ensures that you never forget your passwords, and it also makes them nearly impossible for hackers or cybercriminals to guess unless you reveal the formula yourself.

Here is how you can build a password formula that is both memorable and secure. Start your password with four letters that identify the account, using a capital letter as the first character. For example, use "Email" (with a capital E) for your email account, "Face" (capital F) for Facebook, "Inst" (capital I) for Instagram, and "Bank" (capital B) for your bank account. After these four letters, add a set of four numbers that you are familiar with, such as "1885" or "1945." You can assign different number sets to different accounts or use the same set for multiple accounts if you prefer. If you ever enter the wrong set of numbers, you will know to try the other one.

Following the four numbers, add another letter that refers back to the account, such as the "L" in "Email," the "B" in "Facebook," the second "T" in "Twitter," or the "A" in "Instagram" and "Bank." Finally, end your password with a symbol you commonly use, such as "@," "#," or "\$." This formula makes your passwords easy to remember, and if you ever forget which number set you used, you can quickly try the alternatives.

TIP

Never rely solely on passwords to secure your accounts, especially for your most important ones. Always combine your passwords with an additional security measure, such as two-factor authentication or multi-factor authentication, whenever these options are available. Activate these extra protections on all platforms that support them to maximize your account security.

Monitoring data breaches with Have I Been Pwned

To help protect your accounts, use the third-party service haveibeenpwned.com (note that the "A" is missing in "Pwned"). This platform tracks data breaches and notifies users if their email accounts or passwords have been compromised. To use the service, enter your email address and click the "Pwned" button to check if your email has been involved in a breach. If not, you can use the Notify Me link to provide your email address and receive notifications if your account is ever breached in the future. You can also check if your passwords have been compromised by entering them on the site.

The Notify Me feature allows you to receive alerts if your email account appears in a future data breach. This service is reliable and effective, as demonstrated by a real notification received for a secondary Gmail account that was involved in a breach. Even if the affected account is not your primary one, this shows that the service works and provides timely alerts. It is strongly recommended that you sign up for Have I Been Pwned to stay informed about potential compromises to your accounts.

Summary

In this chapter, we explored the essential security controls used to protect modern networks, systems, and data from unauthorized access, interception, and attack. We began with **firewalls**, examining how they monitor and control network traffic and how network firewalls differ from host-based firewalls in where and how they provide protection.

From there, we moved to **encryption**, looking at how data can be transformed into an unreadable form to protect its confidentiality. We compared **symmetric encryption**, where the same key is used to encrypt and decrypt data, with **asymmetric encryption**, which uses separate public and private keys. We also introduced widely used algorithms such as **AES** and **RSA** and considered where each type of encryption is most appropriate.

We then examined **authentication mechanisms**, including passwords, biometric security, and **multi-factor authentication (MFA)**. These controls help verify that users are who they claim to be and reduce the risk of unauthorized access, particularly when multiple authentication factors are combined. Password management strategies were also discussed as an important part of maintaining strong authentication practices.

The chapter also introduced defensive technologies such as **honeypots**, which are designed to attract and observe malicious activity, and **demilitarized zones (DMZs)**, which create a controlled area between internal networks and untrusted external networks. These mechanisms demonstrate how network architecture itself can be used to reduce exposure and limit the potential impact of an attack.

Finally, we turned to **wireless security**, examining how protocols such as **WPA2** and **WPA3** protect wireless communications. By comparing these standards with older and less secure protocols such as **WEP** and **WPA**, we saw how wireless security has evolved in response to increasingly sophisticated threats.

Taken together, these controls illustrate an important principle of cybersecurity: no single defense is sufficient on its own. Firewalls control traffic, encryption protects data, authentication verifies identity, network segmentation limits exposure, and wireless security protects communications over the air. When these controls are used together, they form multiple layers of defense that make systems and networks significantly more difficult to compromise.

With this foundation, you are now better equipped to recognize, evaluate, and apply the security controls that protect both wired and wireless environments. *Chapter 8* moves to identity and access management.

8

Identity and Access Security

Every system contains resources that should not be available to everyone. An employee may need access to certain files to perform their job, an administrator may require additional permissions to manage systems, and an external user may only be allowed to access a specific service. Making sure the right people have the right level of access is therefore an important part of cybersecurity.

This is where identity and access security comes into play. It focuses on identifying users, verifying that they are who they claim to be, and controlling what they are allowed to access once their identity has been confirmed. These measures help protect sensitive systems and data from both external attackers and unauthorized activity within an organization.

By the end of this chapter, you will be able to design and manage access control systems that enforce the principle of least privilege, apply identity and access management best practices, and address the unique risks posed by privileged access. You will examine key concepts such as **identification, authentication, authorization, accounting (IAAA)**, and explore distinctions between access control models such as discretionary, mandatory, role-based, and attribute-based access control, as well as the mechanisms behind privileged access management.

Mastering these tools and distinctions is critical because effective access control not only prevents unauthorized actions but also limits the damage a single compromised account can cause, helping us reduce insider threats, prevent privilege creep, and maintain accountability across complex environments.

The following topics will be covered in this chapter:

- Access control systems and identity management
- The IAAA Processes: Identification, Authentication, Authorization, and Accounting

- Access Control Models
- Privileged access management (PAM)

Access control systems and identity management

Identity and access management is a very important part of cybersecurity. An **access control system** is a set of technical controls that governs how subjects interact with objects, such as networks, servers, files, and databases. You use access control systems to determine who can do what. For example, maybe Bob can print documents, Nancy can print documents and access the client database, and Eric, as the admin, can read and edit all files. This is the basic idea behind access control systems.

When you look at identity and access management, it is broken down into four main processes, known as the **IAAA**. The first is **identification**. To have an access control list or system, you need a list of users, which you create through identification. Every user should have a unique ID. If multiple users share the same ID, it becomes difficult to determine who performed a specific action, especially if something goes wrong.

Authentication is the next process, where an individual proves they are who they claim to be when trying to access a resource. Authentication is simply saying, "I am Bob, and these are my credentials to prove it." For example, Bob might need to provide a password, or maybe even a fingerprint, to prove his identity.

After authentication, you move on to **authorization**, which determines what rights each subject has on a given resource. It is important to understand the difference between authentication and authorization, as these terms are often confused. Authentication is about proving *who you are*. For example, imagine you want to enter the Pentagon, which is a highly secure and classified building. Not just anyone can enter. If you are authenticated, maybe you are a military official or a government employee, you might be allowed into the lobby. However, just because you are authenticated and can enter the lobby does not mean you are *authorized* to access the office of the commander. Authorization is what determines what an authenticated user is actually allowed to do. In a system, your ability to write, edit, view, or download documents all depends on your level of authorization.

NOTE

Authentication is about proving your identity, while authorization is about what actions you are permitted to take.

The final process is **accounting**, which involves tracking authorized usage of resources and alerting when unauthorized use is detected or attempted. Accounting ensures accountability by keeping a record of what actions users perform on the system.

Everybody's actions are kept track of so that if something goes wrong, you can quickly identify what exactly went wrong.

The IAAA processes: Identification, Authentication, Authorization, and Accountability

The following diagram illustrates the four main processes: identification, authentication, authorization, and accountability:

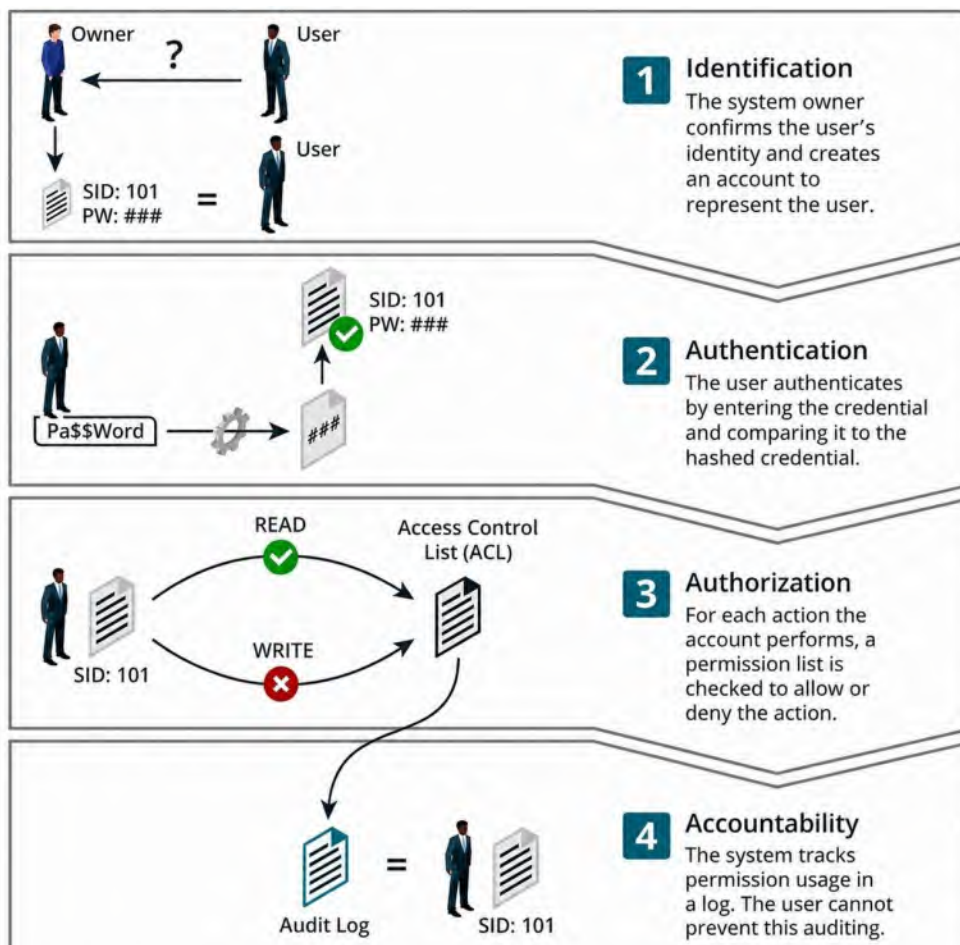


Figure 8.1: IAAA processes

In the identification step, the system owner confirms the user's identity and creates an account, assigning a unique SID (such as 101) and a password. The owner could be a system administrator or an IT administrator responsible for account creation. During authentication, user 101 provides their user ID and password, which are checked against the stored credentials. Once authenticated, authorization determines what user 101 can do, such as being allowed to read documents but not write to them. Finally, accounting tracks everything user 101 does, recording actions in an audit log.

TIP

The servers and protocols that implement these functions are simply referred to as authentication, authorization, and accounting, or AAA. Whenever you hear someone mention AAA in cybersecurity, you now know exactly what they are talking about.

Access control

Access control in cybersecurity refers to a set of rules and processes that govern permissions. The main goals of access control are to prevent unauthorized access, ensure users have only the access they need—which is known as the principle of least privilege—and reduce both insider and outsider risks.

NOTE

Access control is at the heart of cybersecurity, and if you could describe cybersecurity in one term, it would be access control, since this is the number one reason cybersecurity exists.

There are four main models of access control:

- Discretionary access control or DAC
- Mandatory access control or MAC
- Role-based access control or RBAC
- Attribute-based access control or ABAC

You will look at each of these models in detail, starting with **DAC**.

DAC

As the name suggests, discretionary means that the owner of the resource, such as a server or a file, determines who will have access to that particular resource. Permissions in this model are very flexible but depend heavily on the owner's choices. For example, on your own personal

laptop, computer, or mobile device, you can choose to share a particular folder with your fellow coworkers or friends, or keep it private for yourself.

The pros of DAC are that it is very easy to manage, especially for small groups, and it is also easy to set up. However, the cons include the risk of oversharing and poor control in large organizations. As the number of users grows, it becomes increasingly difficult for a single person to decide who among thousands should have access to a particular file, making this model less practical for larger environments.

MAC

MAC is a model where access is controlled by a central authority based on predefined rules, making it mandatory rather than optional. This approach is commonly found in military and government systems. MAC uses security labels, such as "Top Secret" or "Confidential," to control access to resources. For example, a "Top Secret" label might only be accessible to the president of the United States, while a "Confidential" label could be accessible to the vice president. These security labels determine who can access which resources.

The pros of MAC are that it is quite possibly the most secure type of access control. It is very hard to bypass. The cons, however, are that it is very inflexible, which tends to be the trade-off in security: the more secure, the less flexible, and the more flexible, the less secure. When organizations implement MAC, it is typically difficult for them to adapt to using new kinds of technology.

RBAC

In **RBAC**, permissions are granted based on a person's role in the organization. This is very common in businesses, organizations, and companies. For example, all finance department employees get access to the payroll system, while all IT admins can manage IT services. The IT manager will not be able to access the payroll system, and vice versa, people from finance will not be able to access the IT database. The pros are that RBAC scales very well and is much easier to manage than DAC. The cons are that you can have the issue of role creep if roles are not regularly reviewed, which often happens in large organizations.

Role creep refers to the situation in which you might have an employee who started in finance and had access to finance resources, but then moved to marketing or HR, and the permissions from their previous role were not removed. This means the employee keeps their old access while gaining new permissions in their new department, accumulating access to more resources than they should have. This is the main risk with role-based access control if roles are not regularly reviewed and updated.

ABAC

Finally, we have **ABAC**. In this model, access decisions are made based on attributes related to the user, the resource, and the environment. You have to meet certain attribute requirements before you can access a resource. These attributes could include the time of day, your department, your clearance level, or even the device you are using. You might need a specific identification, like a password or a security token, or you might only be allowed access during certain hours. For example, you might only be able to log into the CRM if you are in the sales department *and* you are connecting during work hours. Everything is determined by attributes.

This model is highly flexible and precise, but it is also much more complex to set up and maintain compared to the other models. Different organizations will choose the access control model that best fits their needs.

Real-world application of access control models

To see how these models work in practice, consider a hospital environment. Doctors can view all patient records but cannot change the patient's billing records; this is an example of RBAC since doctors have access based on their job role. In the same hospital, security administrators can modify user access, which is an example of MAC, as a central authority (the security admin) decides who can access what. If the chief surgeon has a private training folder and selects which residents can access it, this is DAC, because the resource owner (the chief surgeon) decides access. Finally, if a remote doctor accesses patient records using a secure VPN and multi-factor authentication, this is ABAC, since access depends on attributes such as VPN use and successful MFA authentication.

To summarize, DAC, MAC, RBAC, and ABAC each have different decision makers and best use cases: DAC is controlled by the resource owner and works best for small or personal systems; MAC is managed by a central authority and is common in military or government settings; RBAC is based on job roles and is typical in large organizations; and ABAC uses attributes and is suited for complex environments. The main drawbacks are oversharing for DAC, inflexibility for MAC, role creep for RBAC, and complexity for ABAC.

Privileged access management (PAM)

Privileged access management, or PAM, is a critical topic as you move deeper into cybersecurity. Privileged access refers to accounts that have more privileges or authorizations than a standard account. Examples include domain admin accounts on Windows, root accounts in Linux, database admin accounts, and cloud superuser accounts. These accounts are considered privileged because they can perform actions that standard accounts cannot.

Privileged access management involves securing accounts with elevated permissions, highlighting the importance of protecting these sensitive accounts.

Threats to privileged account security

Privileged accounts can do actions such as install or uninstall software, change security settings, access or delete sensitive data, and create or modify other user accounts. Further, they can bypass most security controls, often have broad organization-wide access, and can hide malicious activities such as log wiping or disabling monitoring. This makes them highly attractive targets for cybercriminals and hackers. Once a cybercriminal gains control of a privileged account, they can operate behind the scenes and evade detection due to the power of these accounts.

The main risks and challenges associated with privileged access include **privilege creep**, where users accumulate unnecessary permissions over time, and shared accounts, which are common in IT departments and result in zero accountability. Poor password hygiene is another issue, with privileged accounts often using weak, reused, or default passwords. Inactive accounts also pose a risk when privileged accounts are left active after employees leave, creating opportunities for unauthorized access by insiders or attackers.

Best practices for privileged access management

To manage privileged access effectively, you need to put practices in place that reduce the opportunities for privileged accounts to be misused. Because these accounts can make significant changes to systems, access sensitive information, or modify security settings, they can cause considerable damage if they are compromised or used incorrectly.

One of the most important practices is the **principle of least privilege**. This means giving users only the permissions they need to perform their responsibilities and nothing more. For example, if an employee only needs permission to view certain files, there is no reason to give them permission to modify or delete those files. Privileged access should also be provided only when it is actually required rather than automatically giving users permanent administrative privileges.

You should also avoid shared privileged accounts wherever possible. If several administrators use the same account, it becomes difficult to determine who performed a particular action. Giving each administrator an individual account creates greater accountability because their activities can be associated with a specific user.

Another important measure is **multi-factor authentication (MFA)**. A privileged account protected only by a password could be compromised if that password is stolen or guessed. MFA requires an additional form of verification, making it more difficult for an attacker to gain access even if they obtain the password.

Privileged activity should also be monitored and logged. Organizations need to know when privileged accounts are being used and what actions are being performed with them. Unusual activity, such as an administrator accessing sensitive systems at an unexpected time or making unauthorized configuration changes, can then be identified and investigated.

It is also important to rotate privileged credentials regularly, particularly for highly sensitive accounts. Changing passwords and other credentials reduces the amount of time a compromised credential can remain useful to an attacker. Credentials should also be changed immediately when there is reason to believe they have been exposed.

Finally, organizations should remove privileged access when it is no longer required. When an employee changes roles or leaves the organization, their old permissions and accounts should be reviewed and removed promptly. Regularly reviewing privileged accounts can also help identify accounts that are no longer being used.

Summary

In this chapter, you explored the foundations of identity and access security and how organizations control who can access their systems, data, and resources. You examined the four core IAAA processes: identification, authentication, authorization, and accounting.

You then looked at how access decisions can be implemented through different access control models, including discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC). Each model approaches access differently, allowing organizations to choose controls based on their security requirements and environment.

Finally, you examined **privileged access management (PAM)** and why accounts with elevated permissions require additional protection. Practices such as applying the principle of least privilege, using multi-factor authentication, avoiding shared accounts, monitoring privileged activity, rotating credentials, and promptly removing unnecessary access can reduce the risks associated with these powerful accounts.

Together, these concepts reinforce a central principle of access security: users should be able to access the resources they need, but only at the level necessary to perform their responsibilities. With this understanding of identity, authentication, permissions, and privileged access, we can now turn our attention to the broader technologies and approaches used to defend against today's cyber threats. In *Chapter 9*, you will explore modern cyber defense and how organizations use these defenses to detect, prevent, and respond to attacks.

9

Modern Cyber Defense

Modern cyber defense is about more than just building higher walls; it's about using multiple strategies to detect, contain, and respond to threats. In this chapter, we will learn how Zero Trust, defense in depth, and threat intelligence and threat hunting can help protect against credential theft, lateral movement, insider threats, and other attacks.

We'll explore concepts and tools such as multi-factor authentication, microsegmentation, UEBA, endpoint protection, SIEM, and the MITRE ATT&CK framework. We'll also examine security compliance and AI-powered security, including how tools such as ChatGPT can help analyze security incident reports. Together, these approaches provide a layered, proactive, and adaptive way to protect modern systems and data.

In this chapter, we will cover the following topics:

- Zero Trust Security Strategy
- Defense in Depth Strategy
- Threat Intelligence and Threat Hunting
- Security Compliance Frameworks
- AI-Powered Security
- Using ChatGPT for Security Analysis

Zero Trust security strategy

Zero Trust is a security strategy built on the idea that no user, device, workload, or network location should be trusted by default. Instead, every request to access a resource must be explicitly verified based on factors such as identity, device security, location, context, and the sensitivity of the resource being accessed.

Unlike traditional security models that often place significant trust in users or devices once they are inside the corporate network, Zero Trust treats trust as something that must be continuously evaluated. Access is granted according to the principle of least privilege, meaning users and systems receive only the permissions they need, for only as long as they need them.

This approach has become increasingly important as organizations adopt cloud services, support remote and hybrid work, and face attacks involving stolen credentials and compromised devices. In this section, you will explore the drivers behind Zero Trust adoption, its core principles, the key components of a Zero Trust architecture, how it works in practice, and the challenges organizations may encounter when implementing it.

Drivers of Zero Trust adoption

The need for Zero Trust starts with the fact that the traditional network perimeter is no longer enough. In the same company, you might have an employee working at headquarters in the United States and another working remotely from Australia. Work is now global, and users, devices, applications, and data are no longer confined to a single physical space or network. With cloud services and remote and hybrid work, being inside the corporate network is no longer enough to establish trust.

You also have to consider lateral movement. If an attacker gains access to one account, device, or system, they may be able to move through the network and gain access to other resources. Credential theft is another major driver, as many attacks begin with stolen or compromised passwords. Just because a user provides a valid password does not mean they are the real person; it could be an attacker using stolen credentials. Zero Trust therefore requires more than simply trusting a user after they have logged in.

Insider threats are also a concern, as employees, contractors, or compromised accounts can cause serious damage if they are trusted by default or given more access than they need. These risks have made traditional perimeter-based security less effective on its own. Zero Trust addresses this by verifying access based on factors such as identity, device health, context, and the resources a user needs to access. These drivers show why organizations can no longer rely on network location or valid credentials alone to establish trust. To address these risks, Zero Trust follows a set of core principles that determine how access should be verified, granted, and controlled.

Core principles of Zero Trust

Zero Trust is built on several core principles. First, you must verify explicitly. Never trust by default, and always validate identity, device health, and context before granting access. You must authenticate and authorize based on available data, including user identity, device, location, time, and the resource being accessed. This means you make sure that John is in fact John and that the device and circumstances of his request meet your security requirements.

The second principle is least-privilege access. Give users only the access they need to perform a specific task and only for as long as they need it. This can include just-in-time and just-enough access. For example, if an administrator needs elevated access to a web server for five minutes, you can grant the required privileges for that period and automatically revoke them afterward. This limits the amount of access available if an account or credentials are compromised.

Finally, you must assume breach. Design your security controls with the possibility that an attacker may already have compromised a user, device, or system. Instead of allowing unrestricted access after initial authentication, continue to evaluate access and use controls such as segmentation and monitoring to limit lateral movement and reduce the potential impact of a breach. Together, explicit verification, least privilege, and assuming breach form the foundation of a Zero Trust strategy.

Key components of Zero Trust implementation

Key components of Zero Trust include **identity and access management (IAM)**, strong authentication such as **multi-factor authentication (MFA)** or passwordless methods, and micro-segmentation to break large networks into smaller zones and control access between them.

Device security is also critical. Continuously validate device health by ensuring that devices are updated, patched, not jailbroken, and running appropriate endpoint protection. Data should be encrypted both in transit and at rest. Continuous monitoring, using technologies such as **user and entity behavior analytics (UEBA)** and anomaly detection, can help identify activity that differs from a user's normal behavior. For example, if John usually logs in at 10 a.m. and works on HR files, but suddenly logs in at 9:15 a.m. and accesses marketing files, that is an anomaly you need to investigate.

Policy decisions should be enforced based on risk. For example, if a remote employee named Nancy logs in from home, she may be required to complete MFA and use a compliant laptop that is patched and meets the organization's security standards. Access is limited to the applications she needs for her role. If unusual behavior or other risk signals are detected, the system can require additional verification, restrict access, or block the request.

Organizations can also use guidance such as **NIST SP 800-207** and the CISA Zero Trust maturity model to help structure and assess their Zero Trust initiatives.

Challenges of Zero Trust

Zero Trust can be complex to implement. Applying multiple layers of security may require redesigning access policies, networks, and workflows, which can be time-consuming. Legacy systems can add to this complexity because they may not support modern authentication methods or granular access controls.

There are also cultural challenges. Employees who are used to entering a username and password for broad access may face additional verification or access restrictions, which can feel disruptive and affect productivity. You must balance these trade-offs between security and user experience.

Integration is another challenge, as identity and access management, **endpoint detection and response (EDR)**, **security information and event management (SIEM)**, cloud security, and monitoring tools need to work together. Zero Trust is not a single tool you can buy; it is a security strategy that requires multiple technologies, policies, and processes to work together effectively.

Defense in depth strategy

Defense in depth is a security strategy that uses multiple layers of defense to protect your systems and data. Instead of relying on a single tool or control, you combine different types of security measures so that if one fails, others are still in place to stop or limit an attack. You will explore why layered security is important, how different defensive layers work together, and how modern technologies can strengthen this approach.

Rationale for layered security

To understand defense in depth, imagine you are looking at a bank's security setup. You might see a security guard at the entrance, security cameras monitoring the building, and a heavy door protecting the vault. If you were trying to rob the bank, getting past one control would not be enough. You would still have other layers of security to overcome before reaching the money. The bank makes it as difficult as possible to reach its most valuable assets by using multiple layers of defense.

The same idea applies to cybersecurity because no single security control is perfect. Firewalls can be bypassed, passwords can be stolen, and anti-malware software can miss new malware. Defense in depth therefore uses multiple, overlapping security controls so that if one fails or is bypassed, others remain in place. This approach strengthens overall security by reducing single points of failure, covering gaps left by individual security controls, and improving the ability to detect and respond to attacks before significant damage occurs.

The following figure shows the benefits of layered security controls in cybersecurity defense strategies:

Benefits

-  Reduces the chance of a single point of failure.
-  Slows down attackers, increasing the chance of detection.
-  Covers gaps left by individual security tools.
-  Enhances compliance with regulatory frameworks (NIST, ISO 27001, GDPR).



Figure 9.1: Benefits of layered security controls in cybersecurity defense strategies

The core principles of defense in depth are as follows:

- **Layered security:** Use multiple controls at different levels, such as the network, endpoint, application, and data layers.
- **No single point of failure:** If one control fails or is bypassed, other controls remain in place.
- **Diversity of defense:** Use different types of security controls rather than relying on a single technology or approach.
- **Depth over perimeter:** Do not protect only the network boundary; internal systems, applications, identities, and data also need protection.

For example, if a bank only had a security guard and no other protections, a group of attackers could overpower the guard. However, if the bank also has security cameras, they could alert security teams or law enforcement. Even if attackers get past the guard, they still have to deal with the secure vault door. Each additional layer makes it more difficult for them to reach their objective.

The same approach can be applied across different layers of a cybersecurity environment, as shown in *Figure 9.2*. Perimeter and network defenses can include firewalls and intrusion detection systems, while endpoints can use endpoint protection and anti-malware. Applications can use authentication and access controls, and sensitive data can be protected through encryption and other data security controls. Monitoring and response provide visibility across these layers so that suspicious activity can be detected and investigated.

Layers of Defense

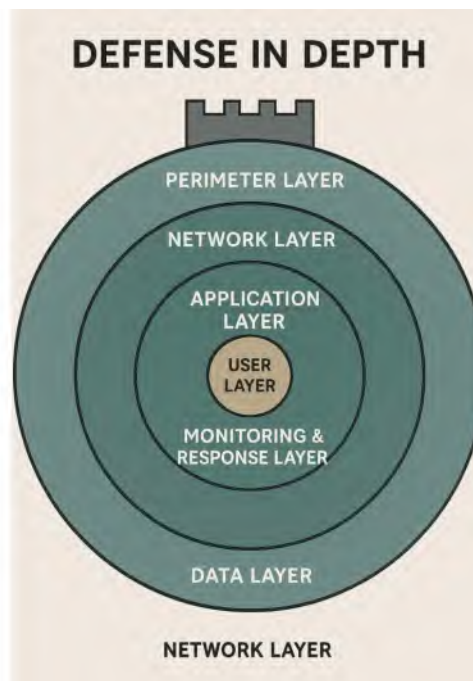


Figure 9.2: Layers of defense in depth

The idea is to stack defenses so that if one layer is bypassed, others remain to prevent, detect, or limit an attack. The more layers an attacker must overcome, the more opportunities you have to detect their activity and respond before they reach their objective.

However, defense in depth also brings challenges. Implementing multiple security controls can increase cost and complexity, particularly if the tools do not integrate well. Overlapping tools can generate excessive alerts and false positives, creating fatigue and making the environment more difficult to manage. Balance is therefore important: you need enough layers to provide effective protection without introducing unnecessary controls that disrupt users or business operations.

Threat intelligence and threat hunting

Let's now take a look at a modern approach towards cyber defense: threat intelligence and threat hunting. You need to get intelligence about threats or even hunt proactively for threats because waiting for alerts or attacks is no longer enough. You cannot simply put security controls in place and then wait for a breach to occur before identifying and addressing the weaknesses that attackers have exploited.

Threat intelligence (TI) is knowledge about threats, adversaries, and the tactics and techniques they use. It helps organizations understand current and emerging cyber threats and what they should be looking for. **Threat hunting (TH)** means proactively searching for threats that may be hidden inside the environment or may have bypassed existing security controls. Instead of waiting for an alert, you actively look for signs of suspicious or malicious activity.

Types of threat intelligence

Threat intelligence helps you stay updated on the latest techniques attackers are using, including new social engineering scams, phishing techniques, malware, and other emerging threats. Threat intelligence can be divided into four main types, as shown in *Figure 9.3*:



Figure 9.3: The four types of threat intelligence

There are four different types of **threat intelligence**:

- **Strategic:** This is high-level, long-term intelligence focused on trends and risks. For example, an organization might track the growing threat from state-sponsored groups targeting its industry or critical infrastructure.
- **Tactical:** This provides information about adversary **tactics, techniques, and procedures (TTPs)** and can be aligned with frameworks such as MITRE ATT&CK.
- **Operational:** This provides intelligence about specific attacks or campaigns, including the adversaries involved, tools they use, and attack vectors.
- **Technical:** This includes **indicators of compromise (IOCs)**, such as malicious IP addresses, domains, file hashes, and phishing URLs. These indicators can be used to identify or investigate potentially malicious activity.

Each type of threat intelligence provides a different view of the threat landscape and together, they provide the context security teams need to better understand and respond to threats.

Knowing that attackers use particular tactics and techniques is only part of the picture. You also need a structured way to understand how those behaviors relate to different stages of an attack. This is where the MITRE ATT&CK framework becomes useful.

MITRE ATT&CK framework

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. You can think of it as a structured way of understanding how attackers operate, from gaining initial access to moving through an environment, collecting information, and achieving their objectives.

The ATT&CK Matrix for Enterprise organizes adversary behavior into tactics and techniques. Tactics represent what an attacker is trying to achieve, such as Initial Access, Execution, Persistence, Credential Access, Lateral Movement, Exfiltration, or Impact. Techniques describe how the attacker may achieve that objective. For example, an attacker trying to gain initial access could use phishing to trick a user into opening a malicious link or attachment.

MITRE ATT&CK also provides information about how these techniques have been observed in real-world attacks. Each technique has an identifier and can include descriptions, related techniques, and examples of how known threat actors or malware have used it. ATT&CK includes matrices for different environments, including Enterprise and Mobile, allowing you to explore adversary behavior relevant to the systems you are protecting.

This makes MITRE ATT&CK useful for both threat intelligence and threat hunting. Threat intelligence can tell you which tactics and techniques particular adversaries are using, while threat hunters can use that information to search their environments for signs of the same

behaviors. Instead of looking only for known malicious files or IP addresses, you can look for patterns of activity that indicate how an attacker may be operating.

Key elements of threat hunting

The first key element is the hypothesis. Threat hunting involves thinking about different attack scenarios and asking questions such as, *"What if the attacker did this?"* or *"What if the attacker did that?"* Your hypothesis can be based on threat intelligence, known attacker techniques, unusual behavior, or knowledge of your environment. For example, you might ask: what if an attacker is using PowerShell to run suspicious scripts at night?

Once you have a hypothesis, you need the right data to investigate it. Data collection is therefore a critical part of threat hunting. You might collect logs and telemetry from endpoints, servers, networks, cloud environments, and SIEM systems. You then use analysis tools to examine this data. These could include EDR platforms, network analysis tools, and behavioral analytics.

During the hunt, you search this data for anything that could indicate an attacker's presence. For example, you might look for unusual account activity, lateral movement, persistence mechanisms, suspicious PowerShell activity, or command-and-control traffic. If something stands out, you investigate further to determine whether it is a genuine threat and identify which systems or accounts may be affected.

You have several tools that can support threat hunting. SIEM and security analytics platforms such as Splunk, Elastic, and IBM QRadar can help you collect, search, and analyze security data. You also have EDR and XDR platforms such as CrowdStrike, SentinelOne, and Microsoft Defender that can provide visibility into endpoint and other security activity. While you do not need to memorize every tool, it is helpful to understand the types of tools available and how they can support a threat hunt.

You can also use **open source intelligence (OSINT)** when investigating threats. OSINT means gathering intelligence from publicly available sources. For example, tools and services such as VirusTotal, Shodan, AbuseIPDB, and AlienVault OTX can help you investigate suspicious IP addresses, domains, files, and other indicators. These additional sources can provide useful context when deciding whether something you discover during a hunt is actually malicious.

Benefits of combining threat intelligence and threat hunting

When you combine threat intelligence and threat hunting, you create a feedback loop. Threat intelligence provides **indicators of compromise (IOCs)** and information about adversary tactics and techniques, giving you a starting point for what to look for. At the same time, threat hunting may uncover new indicators or attacker behaviors that can be fed back into the threat intelligence cycle. In this way, threat intelligence guides your hunting, and your hunting improves the intelligence.

For example, a financial institution might receive threat intelligence about a new phishing campaign delivering a specific type of malware. Threat hunters can use the indicators from that intelligence to search endpoints for signs of the malware. They might also look for suspicious PowerShell activity if the malware is known to use PowerShell to execute commands. PowerShell is a legitimate administration tool, but attackers can misuse it to run malicious commands. If hunters discover early signs of infection, they can investigate and contain the threat before it causes further damage.

Threat intelligence platforms (TIPs) such as Recorded Future, Anomali, and ThreatConnect can help you manage and operationalize intelligence from different sources. By combining threat intelligence and threat hunting, you can improve the detection of advanced threats, reduce attacker dwell time—the time between an intrusion and its discovery—and improve incident response. Each hunt can also provide new information that strengthens future detection and hunting activities.

However, there are also challenges. You need skilled analysts who understand cybersecurity, data analysis, and adversary behavior. Large volumes of logs, alerts, and intelligence can become overwhelming without proper filtering, while false positives can waste investigation time. Commercial intelligence feeds and platforms can also be costly, particularly for organizations that need multiple sources of threat data.

Security compliance frameworks

Cybersecurity is not just about defending against hackers; organizations also need to follow applicable laws, regulations, standards, and security frameworks. These provide requirements or guidance for protecting sensitive information, managing security risks, and demonstrating accountability. Compliance can also help organizations avoid legal or financial penalties and build trust with customers, regulators, and partners.

Although they are often discussed together, not all compliance requirements are the same. Some are regulations or laws, while others are standards or security frameworks. **ISO/IEC 27001** is an international standard for **information security management systems (ISMS)**, focusing on managing information security risks and continual improvement. The NIST **cybersecurity framework (CSF)** provides a flexible approach organized around six functions: Govern, Identify, Protect, Detect, Respond, and Recover. **Payment card industry data security standard (PCI DSS)** applies to organizations that store, process, or transmit payment card account data and includes requirements for areas such as access control, encryption, and monitoring.

For example, the **general data protection regulation (GDPR)** is a European Union regulation focused on protecting personal data and giving individuals rights over how their data is used. Serious violations can result in significant financial penalties, including fines of up to 4% of

worldwide annual turnover for the preceding financial year. **Health Insurance Portability and Accountability Act (HIPAA)** establishes requirements relevant to protecting health information in the United States. SOC 2 is commonly used by service and cloud providers to demonstrate controls related to security, availability, processing integrity, confidentiality, and privacy.

Adopting relevant security frameworks and standards can bring several benefits. You can improve security maturity, provide a structured approach to managing security, and build confidence with clients and partners. Instead of relying on ad hoc security practices, organizations can use established requirements and guidance to develop a more consistent security program.

However, compliance also brings challenges. Cost and resources can be significant, especially for smaller organizations. Complexity is another issue because an organization may need to satisfy several overlapping requirements depending on its industry, location, and the data it handles. Requirements and frameworks also evolve, so organizations need to keep up with changes.

One of the biggest risks is checkbox security: doing only what is necessary to pass an audit or demonstrate compliance rather than focusing on actual security. Meeting the requirements of a framework, standard, or regulation does not mean that you cannot be attacked or breached. Compliance provides an important foundation, but organizations still need to assess their own risks and implement additional defenses where necessary.

AI-powered security

AI-powered security is transforming how you defend against cyber threats, with security products and services such as Microsoft Defender and Gmail already using artificial intelligence and machine learning to help protect users. You will see how AI is applied in cyber defense, examples of AI-powered security tools, the benefits they provide, and the challenges that come with using them.

AI can detect anomalies by learning patterns of normal activity and identifying behavior that differs from that baseline. This can help detect potential insider threats, lateral movement, and other suspicious activity. AI can also analyze files and network activity to identify malicious patterns and help detect new or changing malware that traditional signature-based methods might miss.

Natural language processing and machine learning can help identify phishing attempts by analyzing email content, links, domains, and other characteristics associated with social engineering. AI can also analyze behavioral signals, such as typing patterns, mouse movements, and login behavior, to identify activity that does not match the legitimate user's normal behavior.

The following figure highlights how AI helps with phishing detection, behavioral biometrics, and automated response:

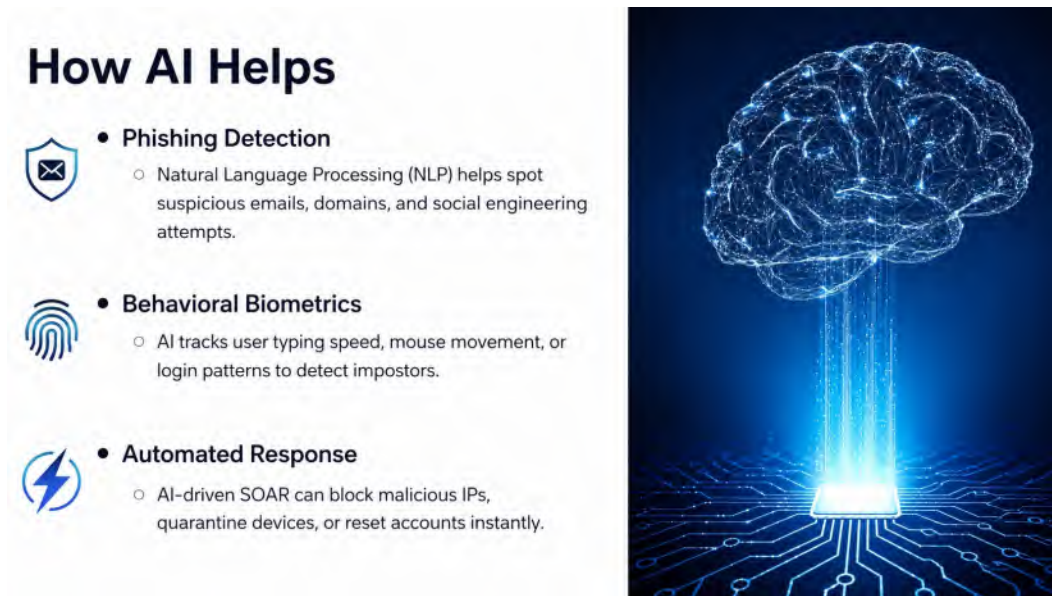


Figure 9.4: How AI assists cybersecurity

AI can also support automated responses to threats. For example, security systems can use AI-driven analysis together with predefined policies to block malicious IP addresses, quarantine compromised devices, or trigger actions on suspicious user accounts. This can help security teams respond more quickly and contain potential threats before they spread.

Real-world examples of AI security tools

There are already several real-world examples of AI-powered security tools. Microsoft Defender and Microsoft Sentinel use machine learning and analytics to help detect and investigate threats across devices and environments. Darktrace uses AI to analyze network and system behavior and identify anomalies. Google Gmail uses AI and machine learning to detect spam and phishing emails, while CrowdStrike Falcon uses AI and machine learning as part of its endpoint detection and response capabilities.

The benefits of using AI in security include the ability to identify suspicious activity and potentially detect new or unknown threats that signature-based systems may miss. AI can also reduce the workload for security analysts by analyzing large volumes of security data, filtering noise, and prioritizing events that require attention. It can help improve response times and operate across large, distributed environments such as cloud, **Internet of Things (IoT)**, and mobile environments.

However, adversarial AI presents a significant challenge because attackers can also use AI. For example, while you might use AI to help detect phishing emails, attackers can use generative AI to create more convincing phishing messages. They may also attempt to manipulate or evade machine learning models. This means that the same underlying technology that strengthens cyber defense can also help attackers improve their techniques.

You also need to be aware of false positives and false negatives because AI is not perfect. Poor or incomplete training data can cause an AI system to miss threats or incorrectly flag legitimate activity. Bias and transparency are additional concerns, as some AI models can be difficult to explain. This is often referred to as the black box problem, where it may not be clear why a model reached a particular conclusion. Finally, cost and expertise are important considerations because AI-powered security solutions can be expensive and require skilled staff to implement, monitor, and maintain them effectively.

Identifying trends and Patterns in Security Reports

AI can also help you identify trends and patterns in security reports. For example, you can use ChatGPT to analyze a weekly security incident log for changes in attack frequency, common attack types, recurring targets, or unusual activity.

You might use the following prompt:

```
From the following report, identify trends in attack frequency and attack types.  
Summarize the findings and suggest actions to mitigate future attacks.
```

When analyzing security reports with AI, follow your organization's policies for handling sensitive data and verify AI-generated findings against the original data before acting on them.

Using ChatGPT for security analysis

Your security logs may contain different attack types, such as brute force attacks, SQL injection, ransomware, phishing, and DDoS attacks. ChatGPT can analyze the report and summarize the frequency of each attack type, daily attack trends, the most targeted systems, and attack outcomes. It can also suggest actions to mitigate future attacks. This helps you identify patterns over time and better prepare for similar attacks.

ChatGPT can also compare multiple security reports to identify recurring patterns and anomalies. For example, you might compare logs from your firewall and IDS or IPS to see whether the same IP addresses, attack types, or targeted systems appear across them.

To do this, upload the security incident reports, such as two reports in CSV format, and provide a clear and specific prompt. For example:

```
Analyze the following two security incident reports. Identify:  
- Recurring IP addresses and the attack types they are associated with.  
- Commonly targeted servers across both reports.  
- Trends in attack frequency for each attack type over the week.  
- Any unique or distinct findings in each report.
```

ChatGPT can then compare the reports and identify recurring IP addresses and their associated attack types, commonly targeted servers, trends in attack frequency, and findings that are unique to each report. You can use the same approach with reports from firewalls, anti-malware tools, IPS, IDS, or threat intelligence platforms to identify correlations or anomalies that might otherwise go unnoticed.

Summary

In this chapter, we explored a modern approach to cyber defense, starting with Zero Trust and its principles of explicit verification, least-privilege access, and assuming breach. We then examined defense in depth and how multiple layers of security can reduce single points of failure. We also looked at threat intelligence and threat hunting, including the different types of threat intelligence, the MITRE ATT&CK framework, and how intelligence can guide proactive threat hunting.

We also examined security compliance frameworks and the importance of balancing compliance with effective security. Finally, we explored AI-powered security, including anomaly and phishing detection, automated response, and the use of tools such as ChatGPT to analyze security reports and identify trends. Together, these strategies show how modern cyber defense combines identity and access controls, layered protection, proactive threat detection, compliance, and AI-assisted analysis to build a more resilient security environment.

In the next chapter, you will examine the security controls and practices used to safeguard these assets against unauthorized access, compromise, and data loss.

10

Protecting Data and Systems

Protecting data and systems is about more than just preventing loss; it's about building practical defenses against the real-world threats that put our information at risk every day. In this chapter, we will learn how to protect our files from ransomware, hardware failures, human error, natural disasters, and cloud account breaches using strategies such as the 3-2-1-1-0 rule, offline and immutable backups, and regular backup verification.

In this chapter, we'll distinguish between full, incremental, and differential backups, understand why cloud sync services like Google Drive and Dropbox are not substitutes for a complete backup strategy, and explore cloud security, encryption, and attacks on encrypted systems. We'll also look at practical Windows 11 security features for protecting our files, privacy, and system access. These safeguards matter because a single incident, whether it's a failed four-terabyte WD drive, a stolen device, or a cloud outage, can result in permanent data loss if we are not properly prepared.

In this chapter, we will cover the following topics:

- Backup strategies and the 3-2-1-1-0 rule
- Cloud computing fundamentals
- Encryption and decryption for data protection
- Securing Windows 11

Backup strategies and the 3-2-1-1-0 rule

Data is one of your most valuable assets, and backups are your safety net when things go wrong with your hard drives or other storage devices. You need to back up important data regularly because you can lose access to your files for many reasons. Ransomware is a major threat, especially for businesses, and reliable backups can help you restore encrypted data without relying on the attacker for recovery.

Hardware failure is another risk. Hard drives and SSDs can fail without warning. For example, a four-terabyte WD drive failed after just over a year of use, and even after trying everything to recover the files, some were permanently lost, including irreplaceable videos. Fortunately, copies of important documents had been stored in the cloud and could be retrieved. This experience shows why you should never rely on a single physical drive to protect important data.

You also need to consider human error, such as accidentally deleting files, as well as fire, flood, theft, or compromised cloud accounts. To protect against these risks, you can follow the 3-2-1-1-0 rule:

- **3 copies:** Keep three copies of your data: the primary copy and two backups.
- **2 different storage media:** Store backups on different types of media, such as an external drive and cloud storage.
- **1 copy off site:** Keep one backup in a different physical location so that a single disaster cannot destroy every copy.
- **1 offline or immutable copy:** Keep one backup disconnected from your systems or protected from modification or deletion for a defined period.
- **0 backup errors:** Regularly verify and test your backups to make sure they can actually be restored.

The goal is not simply to have several copies of your files, but to make sure that one incident cannot destroy or compromise all of them.

Types of backups

You need to understand the different types of backups to choose the best approach for protecting your files. The three main types are full, incremental, and differential backups.

A **full backup** copies all the selected data, giving you a complete backup at that point in time. This is a good starting point when you first begin backing up your data. The downside is that full backups can take more time and require more storage.

An **incremental backup** only copies files or data that have changed since the last backup. For example, if you perform a full backup on Monday morning and then run an incremental backup Monday night, only the changes made since the morning backup are saved. Another incremental backup on Tuesday saves only the changes made since Monday night's backup. Incremental backups are fast and require less storage, but restoration may require the original full backup and all subsequent incremental backups.

A **differential backup** copies all changes made since the last full backup. For example, if you perform a full backup on Monday and run a differential backup on Thursday, it includes the changes made since Monday. Restoring is generally simpler than with incremental backups because you need the last full backup and the most recent differential backup. The tradeoff is that differential backups grow larger as more data changes after the full backup.

Whatever backup type you use, you need to verify that your backups actually work. Run restore tests regularly, such as quarterly for a business environment, to make sure your backups are not only present but can also be recovered when you need them.

Modern backup security practices

Modern backup security is about making sure your backups remain protected even if your primary systems are compromised. In addition to following the 3-2-1-1-0 rule, you should consider the following security practices:

- **Immutable storage:** Store backups so that they cannot be modified or deleted for a defined period. This can help protect against ransomware and accidental deletion. Services such as AWS S3 Object Lock and Wasabi provide immutability features.
- **Encryption:** Encrypt backup data both at rest and in transit. Strong encryption protects your backups if storage media or backup data are accessed by unauthorized users.
- **Access controls:** Restrict access to backup systems and use strong authentication, such as multi-factor authentication, particularly for administrative accounts.
- **Monitoring and testing:** Monitor backup jobs for failures and regularly test restoration. A backup is only useful if you can successfully recover the data when you need it.

These practices help ensure that backups remain available and usable even when your primary systems are affected by hardware failure, human error, or a cyberattack.

Common backup mistakes to avoid

One common mistake is storing backups on the same device as your original files. If that device fails or is compromised, you could lose both the original data and the backup.

Another mistake is not testing the recovery process. If you discover that your backup is corrupt only during an emergency, it is already too late. You should also remember to back up mobile

devices such as phones and tablets. Many people focus on their laptops or computers and overlook their phones, even though important photos, videos, and other data may be stored there.

Relying only on cloud synchronization services such as Google Drive or Dropbox can also be a problem. Sync services are useful for keeping files available across devices, but synchronization is not the same as a complete backup strategy. Changes or deletions can be synchronized across devices, so you should understand the service's versioning and recovery features and maintain separate backups where necessary.

Recommended backup tools and services

There are many tools available depending on your operating system and backup requirements. On Windows, options include built-in backup features, Macrium Reflect, and Acronis Cyber Protect. On macOS, you can use Time Machine or Carbon Copy Cloner. Cross-platform and command-line options include Duplicati, Restic, and BorgBackup.

For cloud backup and storage, services such as Backblaze, IDrive, and Wasabi provide different options for storing backup data remotely. The right tool depends on how much data you need to protect, how frequently you need to back it up, your recovery requirements, cost, and whether you need features such as encryption or immutable storage.

Cloud computing fundamentals

Cloud computing allows you to access data, applications, and computing resources over the internet instead of relying only on software or storage installed on your physical device. The term "cloud" is essentially a metaphor for computing resources available over a network. For example, services such as Google Drive and iCloud allow you to store and access files online, while web-based applications such as Microsoft 365 allow you to work with documents and spreadsheets through a browser.

Cloud computing is broader than cloud storage. It can provide storage, applications, servers, databases, processing power, and other computing resources on demand. Services such as **Amazon Web Services (AWS)** provide many of these capabilities, while Google Drive, Dropbox, and iCloud are familiar examples of cloud-based storage and synchronization services.

A simplified cloud topology is shown in *Figure 10.1*. Your client device connects over a network to the cloud service, which processes requests and stores or retrieves data from the provider's underlying infrastructure.

The actual infrastructure may include many servers and storage systems distributed across multiple locations:

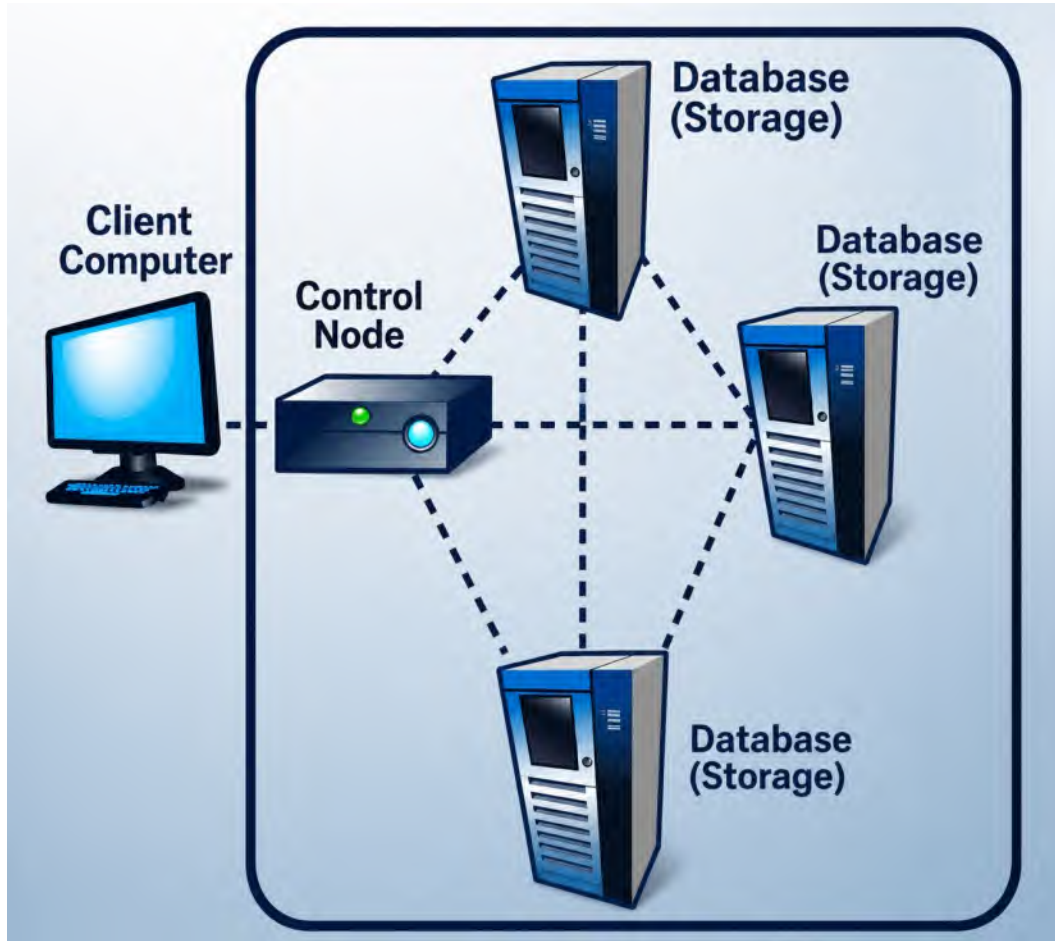


Figure 10.1: Basic topology of a cloud computing service

Cloud storage advantages and limitations

One of the biggest advantages of cloud storage is accessibility. You can access your files from different devices and locations as long as you have the required network access. For example, you can upload files online and share them with a business partner in Australia without having to transfer a physical storage device. This can improve efficiency and collaboration.

Cloud storage can also make it easier to synchronize files across devices, expand storage without purchasing additional local hardware, and maintain remote copies of important data. However, these advantages come with several limitations that you need to consider.

The first is control. When files are stored on your own physical drive, you have direct control over the storage device. With cloud storage, you depend partly on the provider's infrastructure, policies, availability, and terms of service. Privacy and security are also important because your data is stored on infrastructure operated by another organization. You need to understand how the provider protects your information and what security and privacy controls are available.

You also need to consider availability. If a cloud provider experiences an outage, some services or data may become temporarily unavailable. For example, an Amazon Web Services outage in 2012 affected services used by major customers, including Netflix, demonstrating how problems at a cloud provider can also affect the organizations that depend on it. Similarly, if your own internet connection fails and you do not have an offline copy, you may not be able to reach cloud-only files.

Finally, you should consider questions around data ownership, location, and jurisdiction, particularly when storing sensitive or regulated information. You need to understand the provider's terms and where your data is stored, as these factors can affect your organization's privacy, legal, and compliance requirements.

Best practices for using cloud services

When using cloud services, think carefully about the type of data you are storing and how sensitive it is. Sensitive information, such as medical, financial, or personal records, requires stronger protection than ordinary files. If sensitive data needs to be stored in the cloud, use an appropriate service and protect it with controls such as encryption, strong authentication, access restrictions, and secure sharing settings.

For less sensitive files, such as music, videos, or everyday documents, services such as Google Drive, Dropbox, and iCloud can provide convenient storage and access. However, cloud synchronization should not be treated as your only backup. Keep separate backup copies of important data according to the backup strategy discussed earlier in this chapter.

You should also avoid depending on a cloud service without understanding how you would recover your data if the provider became unavailable. Depending on your requirements, you might keep important files locally, maintain backups with a separate service, or use more than one storage location. The goal is to avoid creating another single point of failure.

Major providers and services include Google Drive, Dropbox, iCloud, Microsoft OneDrive, and cloud platforms such as Amazon Web Services. Each offers different storage, security, synchronization, and management capabilities, so you should choose a service based on your requirements rather than price alone.

Now that you understand the fundamentals, advantages, limitations, and safe use of cloud services, you are ready to look at the different ways cloud environments can be deployed.

Cloud deployment models

Cloud deployment models describe how cloud resources are made available and managed. The main models are public, private, hybrid, and multi-cloud, each offering different levels of control, flexibility, scalability, and cost.

A **public cloud** provides computing resources through a third-party cloud provider and typically serves multiple customers using shared infrastructure with logical isolation between them. Public clouds can be cost-effective and highly scalable because you can increase or reduce resources as your needs change without maintaining the underlying physical infrastructure yourself. They also provide broad accessibility, allowing you to access applications and data from different locations.

However, you have less direct control over the underlying infrastructure, and security depends on both the provider and how you configure and use the services. Your data may also be subject to requirements around its geographic location, so you need to understand the provider's available regions and your data residency requirements.

A **private cloud** is a cloud environment dedicated to a single organization. It provides greater control over infrastructure, security configurations, and where data is stored, making it useful when you have specific security, privacy, or regulatory requirements.

The trade-off is cost and complexity. A private cloud may require significant infrastructure, management, and in-house expertise, depending on how it is deployed. Scaling can also require more planning and resources than using an on-demand public cloud, and greater control does not eliminate risks such as insider threats or misconfigurations.

A **hybrid cloud** combines private or on-premises infrastructure with public cloud services. For example, you might keep sensitive workloads or data in a private environment while using the public cloud for less sensitive workloads or additional capacity when demand increases. This gives you flexibility in deciding where different workloads should run.

However, hybrid environments can be more complex to manage because you need to integrate different infrastructures and maintain consistent security policies across them. You may also experience latency when moving data between environments, and maintaining multiple environments can increase cost.

A **multi-cloud approach** uses cloud services from more than one cloud provider. For example, you might choose one provider for particular security or computing capabilities and another for its storage services. This can give you access to different provider capabilities and reduce dependence on a single vendor.

Multi-cloud can also improve resilience and flexibility, but it introduces additional management and security complexity. You need to manage identities, configurations, data, monitoring, and security policies consistently across different providers.

Understanding these deployment models helps you choose the right approach for your organization's requirements and balance cost, flexibility, security, scalability, and control.

Shared responsibility model in cloud security

Regardless of which cloud deployment model you use, you need to understand the concept of shared responsibility. When you store data or run services in the cloud, you cannot rely solely on the cloud provider to handle every aspect of security.

In general, the cloud provider is responsible for security of the cloud, including the underlying infrastructure, physical data centers, hardware, and networking. You, as the customer, are responsible for security in the cloud, which can include protecting your data, managing identities and user access, and correctly configuring the cloud services you use. The exact division of responsibility varies depending on the provider and the type of cloud service.

Security risks in cloud environments

Cloud environments introduce security risks that you need to consider when storing data or running applications in the cloud. Some important risks include misconfigurations, account hijacking, ransomware, insecure APIs, and supply chain attacks.

One of the most important risks is **misconfiguration**. Cloud resources can become exposed when storage, access permissions, network settings, or other services are configured incorrectly. Attackers do not always need advanced techniques; a simple configuration error may expose sensitive data or provide unauthorized access.

Another major risk is **account hijacking**. If attackers compromise a cloud account, they may gain access to the data and services available to that user. **Phishing** and **credential stuffing**, where attackers try credentials stolen from other services, are two ways cloud accounts can be compromised. Using multi-factor authentication, strong access controls, and monitoring for suspicious sign-ins can help reduce this risk.

Cloud ransomware is another concern. Attackers may encrypt, delete, or otherwise disrupt access to cloud-hosted data and systems. Regular backups, immutable copies, appropriate access controls, and secure configurations can help organizations recover from these attacks.

API exploits can occur when attackers take advantage of insecure or misconfigured application programming interfaces. APIs should therefore be securely configured, authenticated, monitored, and regularly tested for vulnerabilities.

Supply chain attacks target third-party software or services that your organization depends on. Attackers may compromise a trusted provider or software component and use that access to reach its customers. Before using a cloud provider or third-party service, you should evaluate its security practices and continue monitoring the risks associated with that service.

To protect your cloud environment, use encryption, enable multi-factor authentication, and follow the principle of least privilege by giving users only the permissions they need. You should also regularly review configurations and monitor your cloud environment using security management tools provided by your cloud platform. AWS Config and services such as Microsoft Defender for Cloud and Google Cloud Security Command Center can help identify configuration and security issues.

Encryption and decryption for data protection

Encryption and decryption are important technologies for protecting data. Encryption takes readable data, known as **plaintext**, and transforms it into unreadable **ciphertext** using an encryption algorithm and key. For example, a plain text message such as "I LIKE TEA" could be encrypted into unreadable characters such as "54&Hbun!40". Decryption uses the appropriate key to turn the ciphertext back into readable plaintext.

When protecting stored data, you can apply encryption at different levels. For example, you might encrypt an entire disk, a particular partition, or individual folders, as shown in *Figure 10.2*:

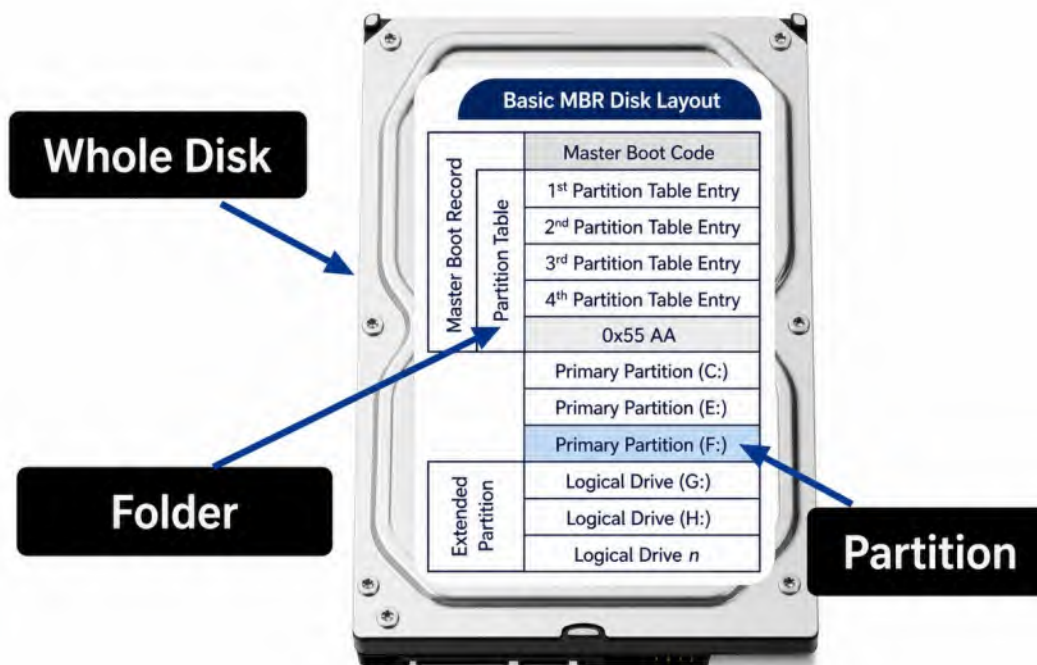


Figure 10.2: The three levels of storage encryption

Encryption is particularly useful for protecting data if a device or storage medium is lost or stolen. If someone steals an encrypted hard drive, USB drive, or laptop, strong encryption can prevent them from simply reading the data without the required key or credentials. This is also useful if a computer needs repairs and you do not want technicians to have access to private files. Encryption therefore provides an important layer of protection for sensitive data stored on physical devices.

However, it is important to understand what encryption does not protect you against. Encrypting a hard drive does not stop malware or rootkits from infecting a running system. Once encrypted data is unlocked and being used, an attacker who compromises the system may still be able to access it. Encryption keys may also be present in system memory while encrypted storage is unlocked, creating opportunities for attacks that target the running system rather than trying to break the encryption itself.

This is why an encrypted hard drive is not automatically immune to attack. Attackers may try to obtain passwords or encryption keys, compromise the system before or after it boots, or target sensitive information stored in memory.

Attacks on encrypted systems

Several techniques can be used to attack systems that use encrypted storage, including rootkits and bootkits, password attacks, direct memory access attacks, attacks involving hibernation data, and memory-remanence or cold boot attacks.

Rootkits and bootkits can compromise a system at a privileged level and potentially interfere with the trusted startup process or access data after it has been decrypted. One defense is Secure Boot, which helps prevent unauthorized boot software from loading by verifying trusted components during startup. Secure Boot is an important protection, although it does not prevent every type of rootkit or malware attack.

Password attacks target the credentials used to unlock encrypted data. An attacker may try many possible passwords until the correct one is found. Strong, unique passphrases and properly configured encryption systems make password guessing significantly more difficult. The security of encrypted storage therefore depends not only on the encryption algorithm but also on how its keys and credentials are protected.

Direct memory access attacks

Direct memory access (DMA) allows certain hardware devices to communicate directly with system memory without requiring the processor to handle every data transfer. This improves performance, but it can also create a security risk. If an attacker can use a DMA-capable interface to access memory while an encrypted drive is unlocked, they may be able to search that memory for sensitive information, including encryption keys.

For example, an attacker with physical access could connect a specially configured device through a DMA-capable interface and use another system or specialized tools to attempt to read the target computer's memory. If an encryption key is present in memory and can be recovered, the attacker may be able to use it to access the encrypted data.

Interfaces and expansion buses associated with DMA have historically included technologies such as FireWire, Thunderbolt, ExpressCard, PCMCIA, and PCI Express. However, modern operating systems and hardware can include protections such as IOMMUs and kernel DMA protection that restrict what connected devices can access. You should therefore use these protections where available and restrict or disable unnecessary external interfaces, particularly on systems that handle sensitive data.

Another potential source of sensitive memory contents is the Windows `hiberfil.sys` file. When Windows hibernates, it saves information from system memory to disk so that the system can restore its previous state. Because memory may contain sensitive information, including cryptographic material, the hibernation file needs to be protected as part of the encrypted system. Full-disk encryption and appropriate system configuration can help prevent an attacker from simply accessing this data offline.

Memory remnants and cold boot attacks

Last but not least is the memory remanence attack, also known as a cold boot attack. Data stored in memory does not necessarily disappear immediately when a PC is turned off. For a short period, remnants of that data may remain in RAM, and cooling the memory can slow down how quickly the data degrades. If encryption keys are present in memory, an attacker with physical access may attempt to recover them.

The attack can work as follows:

1. The attacker cools the PC's memory to help preserve its contents. For example, aerosol cooling spray can be used to rapidly cool the memory modules.
2. The attacker restarts or powers down the PC.
3. Instead of allowing Windows to start normally, the attacker boots into another environment, such as from a bootable flash drive.
4. Specialized tools are used to capture and scan the remaining contents of memory for encryption keys.
5. If the encryption key is recovered, the attacker may be able to use it to access the encrypted drive's data.

This attack is more difficult to execute in practice because the attacker generally needs physical access to the system at the right time and must recover the memory contents before they degrade.

This type of attack may be more practical as an inside attack. For example, in a company, office, or school where the attacker knows the victim's routine, they might know exactly when that person is going to shut down their laptop and leave. The attacker could then quickly gain physical access to the device and attempt to recover information from memory.

Physical security is therefore an important defense against cold boot attacks. You should protect your laptop or PC from unauthorized physical access and use the security protections provided by modern hardware and operating systems. Attacks such as DMA and cold boot attacks show that while encryption provides strong protection for data at rest, it still needs to be combined with physical and system-level security.

That concludes the attacks and how to combat them. Now let's take a look at some of the security and privacy features available in Windows 11.

Securing Windows 11

Let us start off by taking a look at the patching and updates feature for Windows 11. In your settings, scroll down to **Windows Update** and click in. Here, you can check for available updates and see whether a restart is required. Security updates can fix vulnerabilities that attackers might otherwise exploit, so they should be installed in a timely manner. In business environments, organizations may test updates before deploying them more widely to reduce the risk of compatibility or stability problems.

Under **Advanced options**, you can also review optional updates, including driver updates. Driver updates may contain security, compatibility, or stability fixes, so you should review them according to your system's needs. You can also configure **Active hours**, which helps prevent Windows from restarting your computer while you are using it. For example, if you normally use your computer from 6 a.m. to midnight, you can configure your active hours accordingly.

Another useful Windows 11 security feature is **Controlled folder access**. To find it, open **Windows Security**, go to **Virus & threat protection**, and select **Manage ransomware protection**. Controlled folder access helps prevent unauthorized or untrusted applications from making changes to files in protected folders.

The following screenshot shows the controlled folder access feature enabled under **Ransomware Protection**:

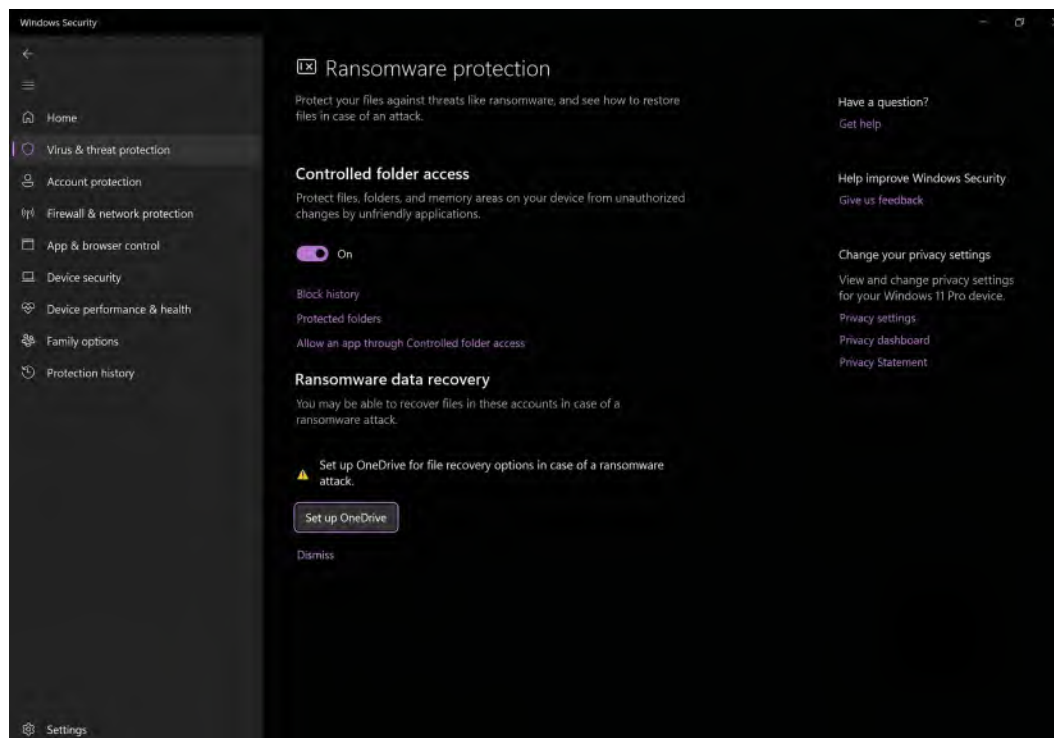


Figure 10.3: Enabling controlled folder access for ransomware protection in Windows Security settings

Once **Controlled folder** access is enabled, you can review the **Protected folders** and add your own. Windows can protect folders containing documents, pictures, music, and videos. If you have another folder containing important files, you can add it to the protected list. You should also review blocked applications because legitimate applications may sometimes need permission to access these folders.

The following screenshot displays the list of protected folders, including the option to add or remove folders:

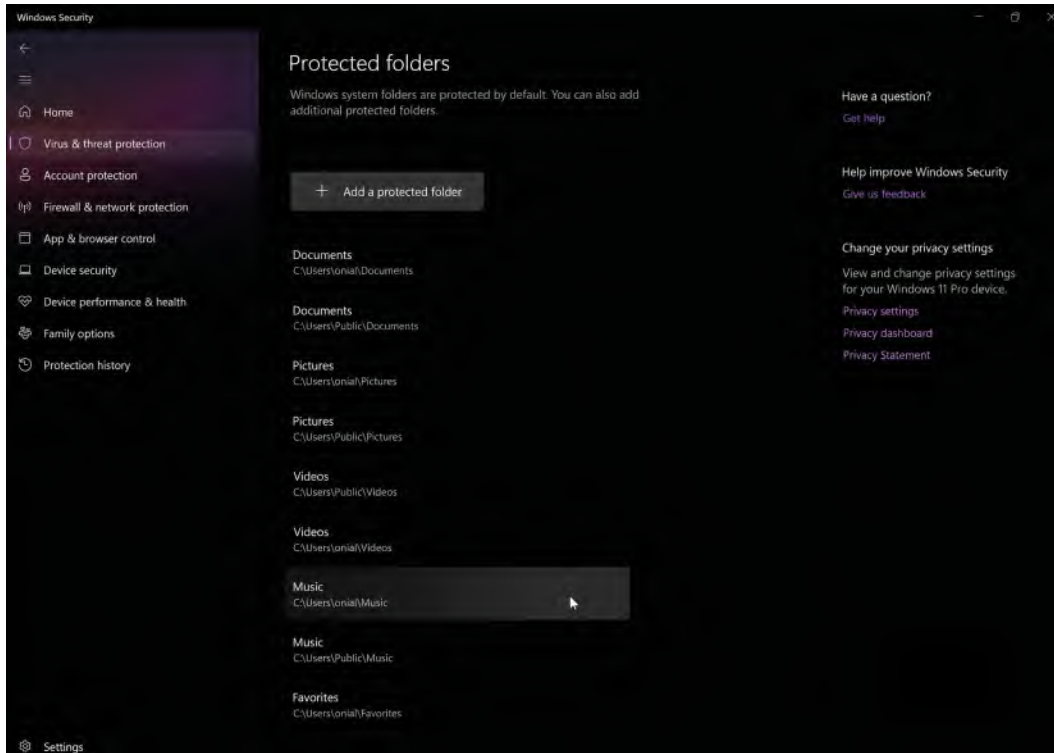


Figure 10.4: Protected folders settings in Windows Security

It is highly recommended to enable this feature, even if you do not have any special folders to protect, as it will at least safeguard the default folders that come with your Windows installation. However, you should review any blocked applications to make sure legitimate programs are allowed when necessary.

You also have the option to delete the diagnostic data that Microsoft has collected on your device. You can do this if you wish, but deleting existing diagnostic data does not necessarily stop Windows from collecting new diagnostic data from your system. Personally, I leave this setting as it is, since deleting the existing data does not change the ongoing collection settings. You can also adjust the feedback frequency, which controls how often Windows asks for your feedback. By default, it is set to **Automatically**, but you can change it to **Once a week** or **Never** if you prefer.

The following screenshot shows you how to delete diagnostic data and set the feedback frequency:

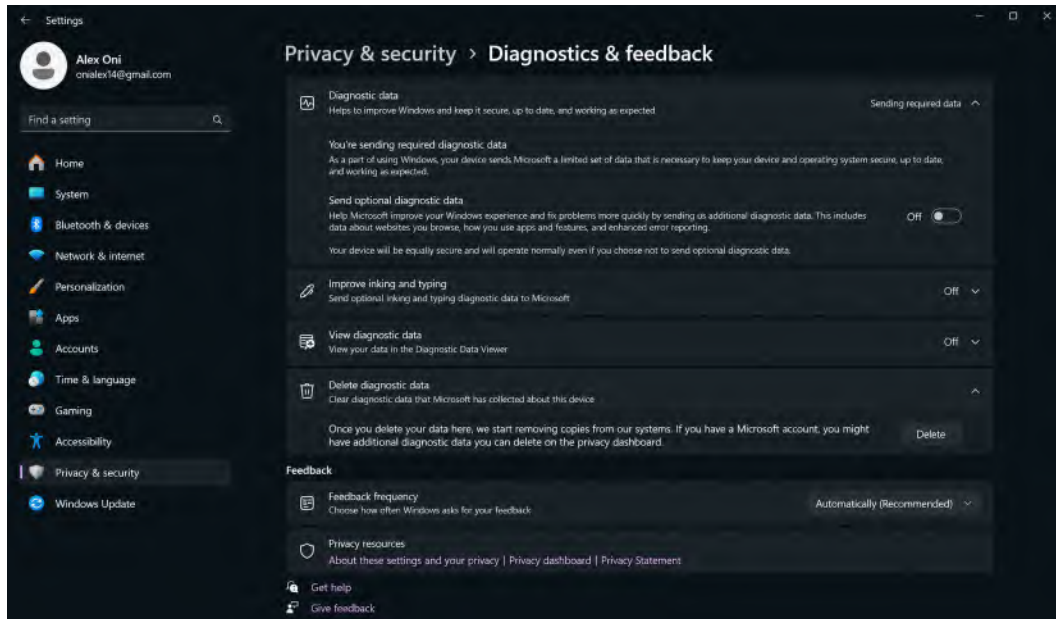


Figure 10.5: Windows privacy & security settings

You should also review app permissions, particularly access to your location, camera, and microphone. For location, check which applications actually need access and turn it off for those that do not. The same principle applies to your camera. For example, if you rarely use the camera on your computer, you can keep access restricted and enable it when you need it for something such as a Zoom meeting or an interview. If you use the camera regularly, you can leave it enabled but make sure only applications you are comfortable with have access.

The following screenshot shows the Windows 11 **Privacy & security** settings for camera access, where you can toggle camera permissions for individual applications:

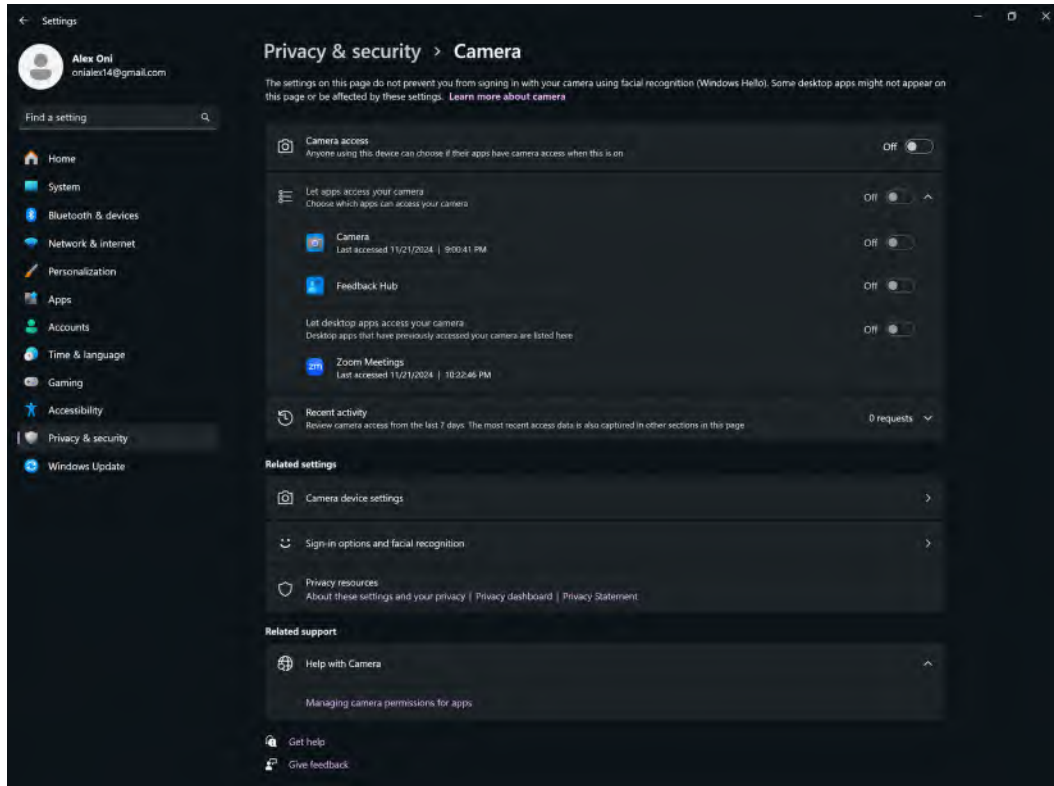


Figure 10.6: Windows privacy & security camera settings

The same applies to the microphone. For example, you might allow microphone access for Camtasia and Zoom if you use them for recording or meetings, while disabling it for applications such as Copilot or Snipping Tool if they do not need it. The important thing is to review your location, camera, and microphone permissions and provide access only where it is required.

Another useful security feature is Dynamic Lock, which can automatically lock your computer when you move away from it. It works by pairing your PC with a device such as your mobile phone. Once configured, Windows can lock the computer when it detects that the paired device is no longer nearby.

The following screenshot shows the Dynamic Lock setting in the Windows 11 **Accounts** | **Sign-in options** menu, where you can enable or disable this feature:

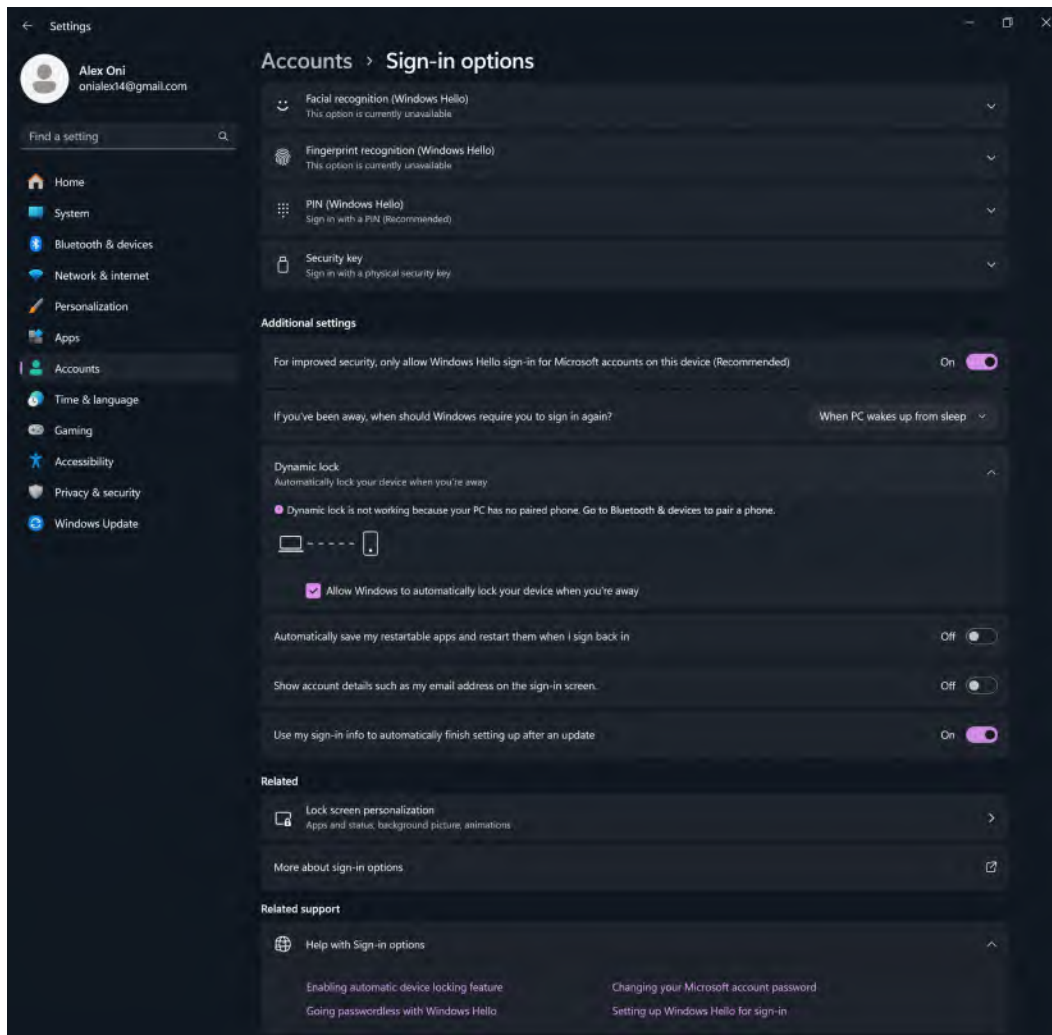


Figure 10.7: Windows sign-in options settings

Dynamic Lock is particularly useful in a workplace environment, where you do not want someone accessing your computer after you leave your desk. If you live alone and work from home, you may have less need for it, but it is still useful to know that the option is available.

You can also use a Windows **Hello PIN** to sign in. The PIN is tied to the particular device and works with Windows Hello's security mechanisms, making it different from a traditional password that might be used across multiple services.

You should also review **Protection history** in **Windows Security** to see detections and actions taken on files and applications. For example, Windows Security might flag FileZilla as a potentially unwanted application. This does not necessarily mean that the application itself is malicious.

False positives can occur when a legitimate file or application is identified as suspicious. Do not automatically assume that every flagged file is malicious, but do not automatically allow it either. Verify the file, its source, and the reason for the detection before deciding whether to allow, quarantine, or remove it.

Finally, you can improve your privacy on Wi-Fi networks by using random hardware addresses, where supported. Instead of always presenting the same MAC address when connecting to Wi-Fi networks, Windows can use randomized addresses. This can make it more difficult to track your device across networks using a persistent MAC address. You can review this option under your Wi-Fi settings and enable it according to your network requirements.

Summary

In this chapter, we established the importance of protecting data and systems through reliable backups, secure cloud services, encryption, and system-level security. Starting with the 3-2-1-1-0 rule and backup types, including full, incremental, and differential backups, we explored modern backup security practices, common mistakes, and recommended tools and services. We then examined cloud computing, including its advantages and limitations, deployment models, shared responsibility, and common security risks.

We also explored how encryption protects data and how attacks such as direct memory access and cold boot attacks can target encrypted systems. Finally, we looked at practical Windows 11 security and privacy features for protecting files, managing access, and securing the system. With these principles and tools, you can build a layered approach to keeping your data secure, available, and recoverable.

In the next chapter, you will learn about mobile device security.

Part IV

Staying Secure in Everyday Life

This part brings together the essential aspects of staying secure in everyday life, from protecting our mobile devices to safeguarding our privacy and anonymity online. The chapters in this section will guide you through practical strategies for cybersecurity at home and work and conclude by exploring how emerging technologies like artificial intelligence are shaping the future of digital safety. Together, these chapters provide a comprehensive approach to navigating the evolving risks and responsibilities of our connected world.

This part contains the following chapters:

- *Chapter 11, Mobile Device Security*
- *Chapter 12, Privacy, Anonymity, and Online Safety*
- *Chapter 13, Cybersecurity at Home and Work*
- *Chapter 14, Looking Ahead*

11

Mobile Device Security

Mobile device security is now a daily concern for billions, as smartphones and tablets have become our primary gateways to communication, work, and entertainment. In this chapter, we will learn how to recognize and avoid fake apps, understand the risks posed by mobile malware, and make informed decisions about app permissions and security settings on platforms such as Android and iOS.

We will use real-world examples, such as the fake Facebook Messenger app and misleading developer names like "WhatsApp Inc.", to practice identifying red flags, and we will compare the strengths and weaknesses of Google Play Store and Apple App Store, including the importance of app vetting, install counts, and developer contact information. Mastering these techniques matters because even reputable app stores can host malicious apps that threaten your data, privacy, and devices, making it crucial to spot warning signs and apply practical protections in our everyday mobile use.

In this chapter, we will cover the following topics:

- Comparative security of major mobile operating systems
- Mobile applications as security risks
- Comparing Google Play Store and Apple App Store
- Best practices for downloading mobile apps
- Jailbreaking iOS Devices: Process, legality, and risks
- Managing and reviewing app permissions

Comparative security of major mobile operating systems

According to GSMA's Mobile Economy 2026 report, the global mobile population amounted to 5.8 billion unique subscribers, around 70 percent of the world's population. The average person spends 3.6 hours a day inside mobile apps, according to Sensor Tower's State of Mobile 2026 report. Meanwhile, 49.3 percent of all worldwide website traffic was generated through mobile phones as of August 2026, according to StatCounter.

Unfortunately, with this tremendous rise in mobile device usage, the number of mobile malwares has also grown rapidly. McAfee, one of the world's leading cybersecurity companies, reported that while it took 20 years to reach 2 million malware samples on the PC, it took just 5 years to do the same on mobile. While we will look at all the major forms of mobile malware and how they are able to infect mobile devices later in the chapter, let's start by comparing the security of the top two major mobile operating systems: **Android** and **iOS**.

The major advantage of using Android is that it is highly configurable and offers the highest levels of configuration among the three. However, by default, Android has very weak security settings, by far the weakest of the three. If you use an Android device, be ready to adjust the default security settings, for example, by enabling a screen lock, turning on device encryption, and reviewing app permissions. Just because you run Android does not mean you cannot provide good security for the device; you just have to be ready to take the necessary steps and precautions.

The major pro of iOS is that it is very consistent and reliable, and the major con is that iOS tends to be the most expensive. And contrary to popular myths and beliefs that only Android is susceptible to malware, iOS devices are also vulnerable. Nevertheless, if you want a mobile device that offers good levels of configuration as well as good levels of security, iOS is the best choice.

Mobile applications as security risks

Mobile applications are at the heart of your smartphone experience, enabling everything from taking photos to transferring money. These apps are what truly distinguish smartphones from older cell phones. However, while apps provide convenience and functionality, they also introduce significant security risks.

Think of your smartphone as a house: without doors or windows, everything inside is secure. The internet connection on your phone acts as a door, and each app you install is like adding a window. The more apps (windows) you have, the more opportunities there are for attackers, such as burglars, to enter and access your data. As a result, increasing the number of apps on your device raises your risk of being targeted by mobile malware or cybercriminals.

In the following sections, you will learn how to distinguish between legitimate and fake apps, understand the differences between the Apple App Store and Google Play Store, and discover practical steps to protect your device when downloading and using mobile applications.

Comparing Google Play Store and Apple App Store

Google Play Store and **Apple App Store** are the two main platforms where you can download mobile applications, but they differ significantly in growth, app availability, and security. As of June 2026, it is estimated roughly that the Google Play Store had 2,556,036 apps available, while the Apple App Store offered 2,587,092 apps.

In this section, we will compare these two stores, examine their security differences, and explain why, when it comes to security, one is considered more secure than the other, starting with the four major reasons for this difference:

Strict app vetting policies: Apple enforces a very strict policy and security requirements for publishing applications on their platform. Before an app can be published on the Apple App Store, it must go through a rigorous vetting process. While Google does attempt to filter out bad apps from good ones, the requirements for publishing on the Google Play Store are not as stringent as those of the Apple App Store.

- **Update policies and security implementations:** Apple requires users to download and install updates as soon as they are available, making it mandatory and therefore receive protections quickly. In contrast, Google gives users the option to delay or skip updates can make their devices go without important security fixes for longer periods, making them more vulnerable to threats compared to iOS users, who are required to update.
- **Hardware control and security:** Apple has full control over the hardware they manufacture, ensuring that security is a top priority in their devices. Android devices, however, are produced by many different manufacturers, and not all of them prioritize security. Many Android manufacturers focus more on design or customer experience than on security features.
- **Device fragmentation:** The fourth and final reason for the security gap between Android and Apple devices is something known as device fragmentation. Before you can use a mobile device, you need both the hardware (your phone) and the software (the operating system).

The following chart illustrates the distribution of Android OS versions, highlighting the extent of fragmentation across devices:

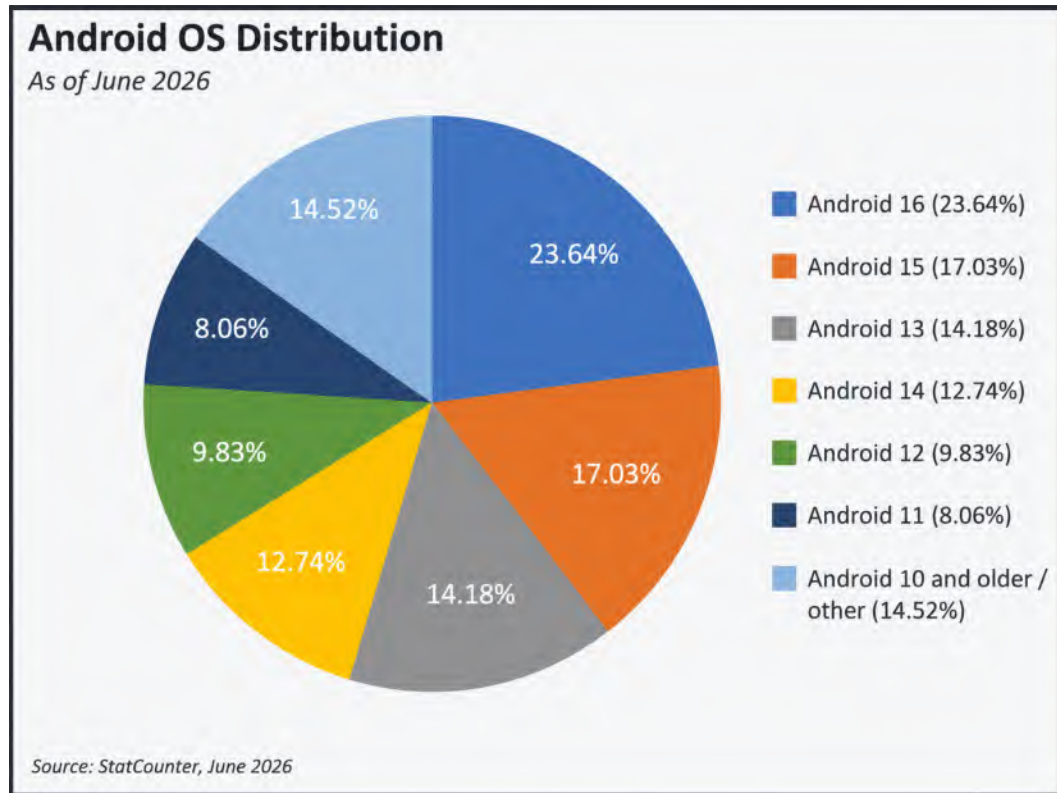


Figure 11.1: Android OS version distribution as of June 2026, illustrating platform fragmentation

The more versions that exist between hardware and operating systems, the more compatibility issues can arise. Apple benefits from having very limited versions of both their operating system and hardware.

Understanding the differences between these app stores helps you make informed decisions about where and how you download apps. Being aware of their unique security approaches can guide you toward safer mobile device use.

Best practices for downloading mobile apps

When you navigate Google Play Store, you will see a wide variety of content, including movies, books, music, and apps. If you want to download a popular app or an app associated with a major application, you need to be extremely careful to ensure you are downloading the correct version. Facebook, for example, has many associated apps with similar names. You will find the main Facebook app, but also Facebook Lite, Facebook Creator, Moments by Facebook, and more.

If you try to download an app like Facebook Messenger, you will find even more types of messenger apps for Facebook. If someone wanted to infect users, they could create a crafty name like "Facebook Lite Messenger" or "Facebook Fast Messenger." Many people are not security conscious; they see "Facebook" and "Messenger" and assume it is the legitimate application, then download it without further thought. This is a risky move, so always be extremely careful when downloading apps with names similar to popular ones.

Let's discuss how to evaluate: For instance, an ethical hacker might use AI tools to scan a company's network for vulnerabilities, helping the company fix security gaps before attackers can exploit them. This kind of testing is done with permission and aims to strengthen defenses rather than cause harm. the credibility and security of apps when we're in similar situations.

Evaluating app reviews and ratings

Before downloading an app like ChatGPT on Google Play Store, check information such as the developer, the number of reviews, and the overall rating.

For example, as shown in *Figure 11.2*, ChatGPT has 54.4 million reviews, which is a good sign:

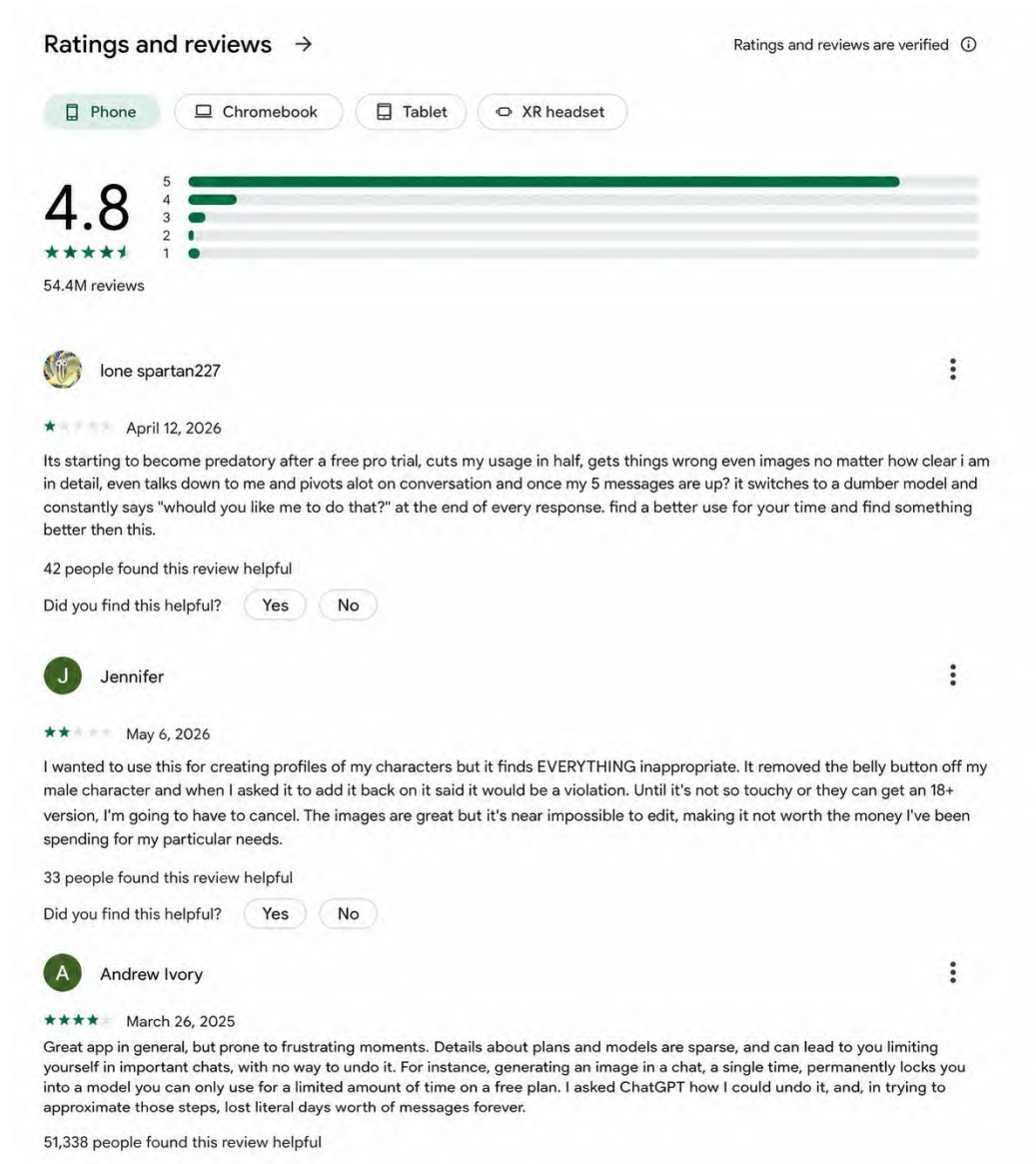


Figure 11.2: User reviews and ratings distribution for the Facebook Local app on Google Play Store

If you scroll down, you will notice a few negative reviews, which are actually helpful. Negative reviews show that real people have used the application, and it is not just filled with fake positive feedback. You should be cautious if you find an app with only five-star reviews and stating, *"This is the best app ever, this app changed my life,"* or similar overly positive comments. Apps with nothing but great reviews are often a big red flag.

TIP

You can read through some of the reviews to get a general idea of whether the app is right for you. Typically, focus on the two-star or three-star reviews, as those tend to be more constructive than either the one-star or the four- and five-star reviews.

In this case, some users report issues with limits or incorrect outputs, others like its usability but mention complicated models of use. There are both positive and negative reviews, so you should spend time reading them. If you notice many complaints about the app constantly crashing, collecting a lot of data, or requiring excessive permissions, you should avoid such applications.

Analyzing app install numbers and red flags

Be wary of apps with "update" in their title, especially when searching for tools such as "updates" on Google Play Store. While not every app with "update" in the title is bad, the chances of them being good are actually quite low. For example, you might see apps like "Updates Checker" by various developers.

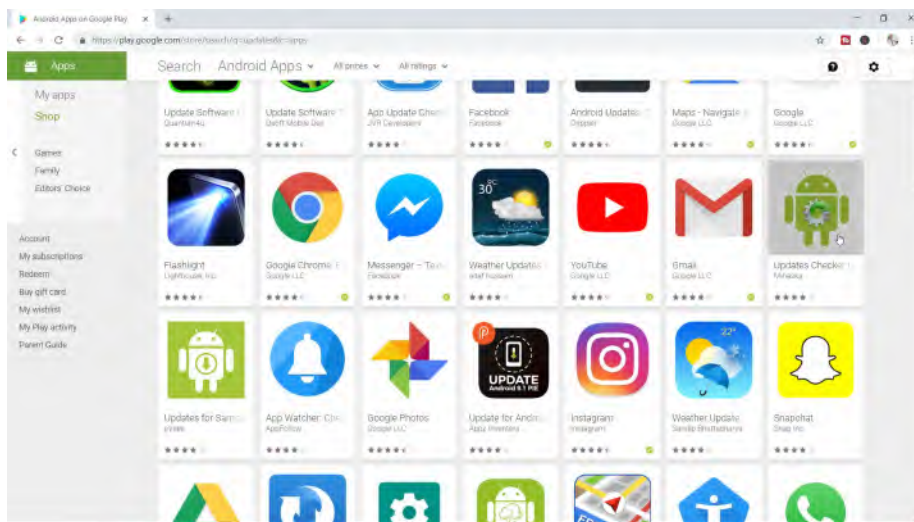


Figure 11.3: Risks of downloading Android apps with "update" in the title

The reason you should avoid using apps such as "Updates Checker" is because if you already have an app installed on your phone, you should have it set to download updates automatically whenever they are available. You do not need a separate application to notify you that there is an update ready for your Facebook or WhatsApp app.

Another important factor to verify whether an app is legitimate is to check its author. In this example, the author is "Mihaska." Click on the author's name to see more information. If the author has created only one single application, this is another red flag. While this does not guarantee the app is bad, it does make it more suspicious. It is less suspicious if the author has created multiple apps. Typically, having 10, 15, or 20 different apps is a good sign.

When you scroll down on the main page for the app, in the additional information section, you will find the number of installs, which in this case is 100,000+:

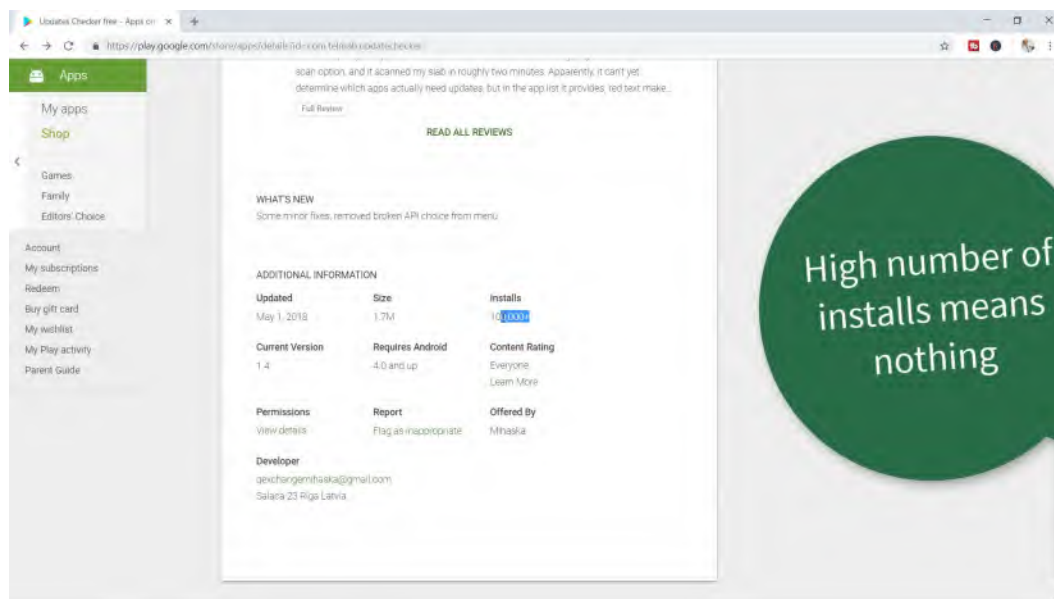


Figure 11.4: High install numbers do not guarantee app safety or quality

Do not let this number fool you. Some people believe that if an app has hundreds of thousands of installs, it must be a good application, but that is absolutely false. A high number of installs doesn't mean the app is legitimate or guarantees safety because some of the most successful malicious apps have had millions of installs.

Another important detail to check when evaluating an app on Google Play Store or Apple App Store is the developer's contact information. If the developer does not provide a real physical address or uses a suspicious-looking email address, this is a major red flag.

For example, in *Figure 11.4*, you can find the developer's email and physical address in the app listing. Here, an address like "Salekha 23, Latvia" might look real, but you should verify whether it actually exists. Similarly, an unusual email address such as `queueexchange.mihaska@gmail.com` can be a sign that the app is not trustworthy.

Let's consider another example. When searching for a popular app like YouTube in Google Play Store, you will see many different versions and variations of the same. The official apps such as "YouTube," "YouTube for Android," "YouTube for Google," "YouTube Kids," and "YouTube Studio," are all published by Google LLC, which provide a real address and website, confirming its legitimacy. However, you will also find many other apps with similar names and icons that are not official. Always verify these details to assess the authenticity of both the app and its author.

The following figure shows the search results for "YouTube" in Google Play Store, with a variety of apps using the YouTube name and logo:

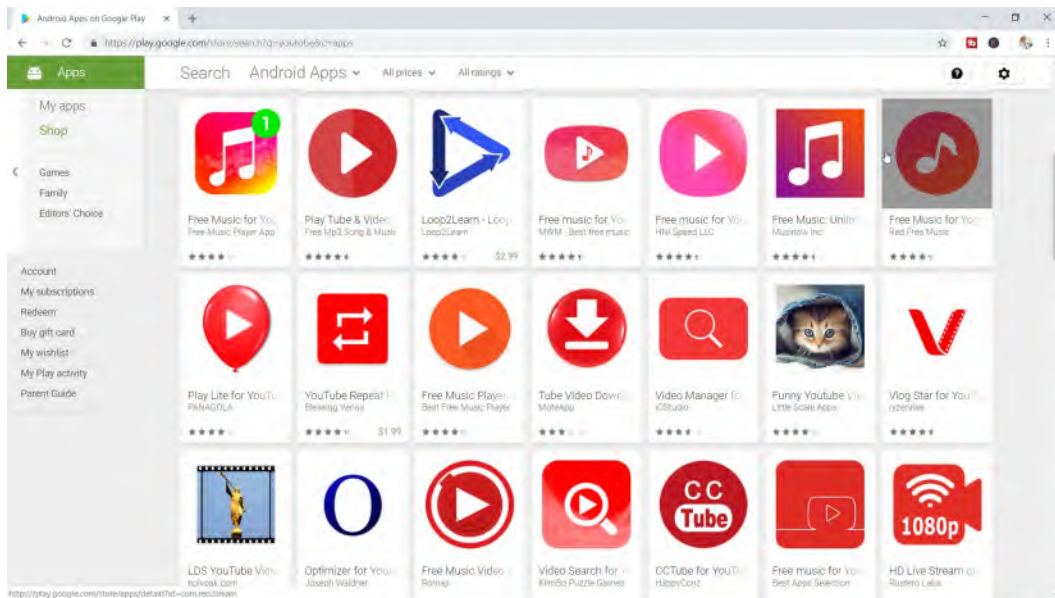


Figure 11.5: Search results for YouTube-related apps on Google Play, illustrating the prevalence of unofficial and potentially misleading apps

You might notice a green check mark on some app icons in the search results. This check mark does not indicate that the app is verified or endorsed by Google. It simply means that the app is already installed on your connected Android device. You will also encounter many unofficial apps with names like "Free Music for YouTube Music Player," "Free Music for YouTube Player," and other variations. Be extremely cautious with apps that try to associate themselves with a

well-known app such as YouTube, as having "YouTube" in the title does not guarantee authenticity or safety.

The article "*WhatsApp scam tricks over a million Android users into downloading fake version of the app - don't get caught out*," published by Mirror in 2017 illustrates the points we discussed with a real-world example. This case highlights the risk of downloading apps that appear to be popular, like WhatsApp, YouTube, or Facebook, but are actually fake.

In this incident, the developers created a fake app called "Update WhatsApp Messenger" and even listed the developer as WhatsApp Inc. to deceive users. This fake app was installed over a million times, demonstrating that a high install count does not guarantee an app's legitimacy. Once installed, the app displayed ads on victims' phones, generating revenue for the developers.

Nicholas Cresadus, a security researcher at Avast, explained that the fake app was being used to generate revenue through ads, but also emphasized that this kind of scam is far from unique. There was also a fake Facebook Messenger app that was downloaded 10 million times, showing just how widespread and successful these fake apps can be. This example reinforces why you must be especially careful when downloading apps that mimic popular services, as attackers often use similar names and branding to trick users.

The article highlights several important questions you should ask before downloading any app:

1. What is the name of the developer? If the developer's name does not match the app, be wary.
2. Do the reviews and ratings seem suspect? Hundreds of genuine reviews are a good sign, but a few glowing reviews may be fake.
3. Do the performance and promises seem over the top? Outlandish claims or requirements to rate the app five stars to activate it are suspicious.

You should be extremely careful about the kinds of apps you install on your phone, as many people have downloaded fake applications and suffered consequences like data loss or intrusive ads. Remember that even reputable app stores like Google Play Store can contain malicious apps that have been downloaded millions of times.

Jailbreaking iOS devices: Process, legality, and risks

The term **jailbreaking** is often confused with **unlocking**, but they are not the same. Unlocking allows your phone to use any network carrier, so your device is not restricted to a single provider. With an unlocked phone, you can insert any SIM card and use it for calls, texts, and internet access, but this does not alter the device's operating system or security controls.

If you have ever watched the TV show *Prison Break*, you might associate the idea of jailbreaking with breaking out of confinement. Jailbreaking your iOS device is similar in concept: you are removing the restrictions imposed by Apple to gain more control over your device.

Technical process of jailbreaking

At the core of your mobile device is a program called the **kernel**, which acts as the master controller for everything on your device and is one of the first programs to load when you power it on. Jailbreaking works by applying **patches**, small programs that modify the default behavior of the kernel. These patches change how the kernel operates, allowing you to bypass Apple's restrictions.

Apple tries to counter jailbreaking by releasing new hardware and software updates. Every time a new iOS update is released, jailbreak developers must create new code to bypass the latest protections. This creates a constant cat-and-mouse game between Apple and those who develop jailbreaking tools.

Legal and safety considerations

A common question is whether jailbreaking your iOS device is legal. Apple has confirmed that it is legal to jailbreak your device. However, in some countries, such as Australia, Canada, New Zealand, and possibly India, jailbreaking is not permitted. The legal status is often unclear, as digital laws can be murky and fall into gray areas without clear definitions. As far as Apple is concerned, jailbreaking is legal, but you should check the laws in your own country.

An even more important question is whether jailbreaking is safe. The answer is that it is a risk. You cannot say that it is completely safe, nor can you say that it is completely unsafe. It is similar to flying on a plane: generally safe, but accidents can happen. When you jailbreak your device, you accept both potential positive and negative consequences, so you need to weigh the risks before proceeding.

Here are the four major reasons why you may not want to jailbreak your iPhone device:

- **Loss of warranty and lack of customer support:** If anything goes wrong after you jailbreak your device, Apple customer support will not help you; you are on your own. This is the main reason many people avoid jailbreaking.
- **Consequences of freedom:** While jailbreaking gives you the freedom to install any updates or apps and customize your iPhone however you want, unlimited freedom is not always a good thing. For example, you might install apps from untrusted sources that contain malware, or make changes that accidentally disable important security features. These actions can expose your device to risks like data theft or system instability.
- **Any updates you install after jailbreaking can break your device:** If you jailbreak your iPhone and then try to install a new update, you risk making your device unusable.
- **Possibility of unpredictable negative results:** When you jailbreak your iPhone, you never really know what will happen. For example, your device could become unstable, crash unexpectedly, or lose access to important security updates. Even if the process is done properly, the chances of negative results are reduced, but there is always a risk.

So, should you jailbreak your iPhone? If you are happy with what your iPhone or iPad does for you and do not need further customization, you do not need to jailbreak your device. If you are extremely unhappy with Apple's restrictions, you could decide to jailbreak your phone, but you alone will face the consequences. Ultimately, you need to weigh the advantages and disadvantages and decide whether jailbreaking is right for you. Alternatively, you may want to consider buying an Android device instead.

These are just examples of the kinds of permissions that apps can request for. Now, Android in particular, would always force applications to declare these permissions that they require whenever you choose to install them. This way, Android tries to protect you by letting you know the kinds of permissions you'll be granting to applications should you choose to accept the permissions those apps demand.

You should understand that this is basically a take-it-or-leave-it situation. If an app says it needs access to your address book and your camera, you cannot selectively deny one permission and still install the app. Most applications will not function or will not even install if you do not accept all the permissions they require. So, you either accept the permissions and install the app, or you look for another app that does not require the same permissions.

Matching permissions to app objectives

Permissions must always match the objectives of the application. This is one way you can spot a potentially fake or malicious app. For example, if you install the Instagram application, it is reasonable for it to request access to your videos, pictures, and address book, since it is a social media app and these permissions align with its purpose:

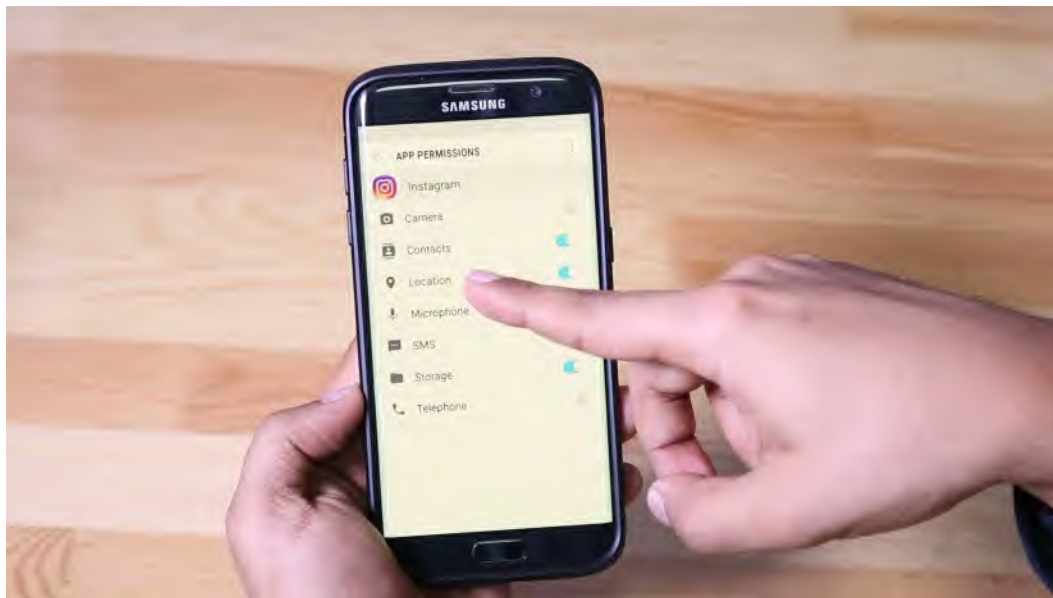


Figure 11.6: App permissions granted to Instagram, illustrating typical access needed for a social networking app

However, if you install an app that is supposed to help you download videos from YouTube, and it requests permission to send SMS messages on your behalf, that is a red flag. You should question why an app designed to download videos would need access to your text messages. This mismatch between the app's stated purpose and the permissions it requests is a warning sign.

The permissions requested by an app must always match the core objectives of that application. This is a key way to protect yourself from downloading and installing malicious apps. Also, new permissions prevent automatic updates. Typically, when you install an app on your phone, you can choose to have that app automatically update itself whenever a new update is available.

Managing and reviewing app permissions

As we discussed previously, Android prevents apps from automatically updating themselves if new permissions are added. The purpose of this restriction is to protect you from an app going rogue by introducing new malicious features. For example, if you've previously installed an application that only required access to your camera, and a month later an update for that app requests a new permission, such as access to your address book, Android will block the app from updating automatically.

When you notice that an app you previously allowed to auto-update now refuses to update itself, this is a sign that a new kind of permission has been added. You should review the new permissions requested and then decide whether to update the app or look for an alternative. Some apps may continue to function after you revoke their permissions, but many will not work properly if you remove the default permissions they require. When you try to run these apps, you will typically see a prompt asking for access to features like your camera. If you deny the request, the app will not run.

To check the kinds of permissions that your installed apps have access to, open the **Settings** app on your Android device and select **Apps** (which may also be labeled as **Default apps** or **App permissions**).

If you want to see the specific permissions that an app has access to, you can scroll through its permission list. For example, Rebtel, which is an app used for making international calls, will have access to your contacts, location, microphone, and telephone, which are all reasonable for its function. Thus, the app permissions for Rebtel will include toggles for camera, contacts, location, microphone, SMS, storage, and telephone. There is nothing unusual about the permissions granted to Rebtel in this case.

Using permission management applications

To help you manage app permissions more effectively, you can install an app called **ASpotCat**. This app allows you to quickly and efficiently review and manage the permissions that your apps have access to and ensure that only appropriate apps have access to sensitive information. When you open ASpotCat, you can choose to list apps by permission, by bookmarks, or alphabetically.

If you select "**List apps by permission**," you will see all the different types of permissions that apps can request, such as access to body sensors, calendar, camera, contacts, and more. For example, if you want to check which apps have access to your calendar, you can tap on "**calendar**" and see a list of apps such as My Bank, Facebook Messenger, and Smart Switch that have this permission. Similarly, you can check which apps have access to your location and see a list that might include apps like Smart View and Body Weight. If you notice an app that should not have access to your location, you can disable that permission.

Special access and installing unknown apps

You can review the special access settings on your Android device by following these steps:

1. Navigate to **Settings | Apps**. Tap the gear or settings button, and you can access **Special Access**.

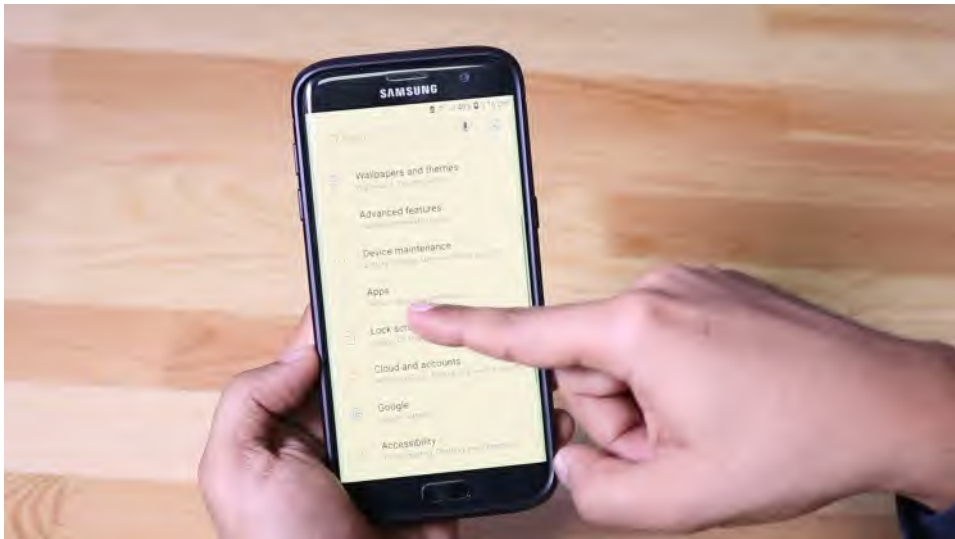


Figure 11.7: Navigating to the Apps section in Android settings to check app permissions

2. From there, scroll down to **Install unknown apps**.

By default, Android prevents apps from installing applications from third-party sites. You will see a list of apps that are not allowed to install unknown applications. For example, if you receive a link in Chrome to download an app, your phone will block the installation if Chrome is on the disallowed list.

If you want to allow a specific app, such as Facebook, to install unknown applications, you can select it and turn on the permission:

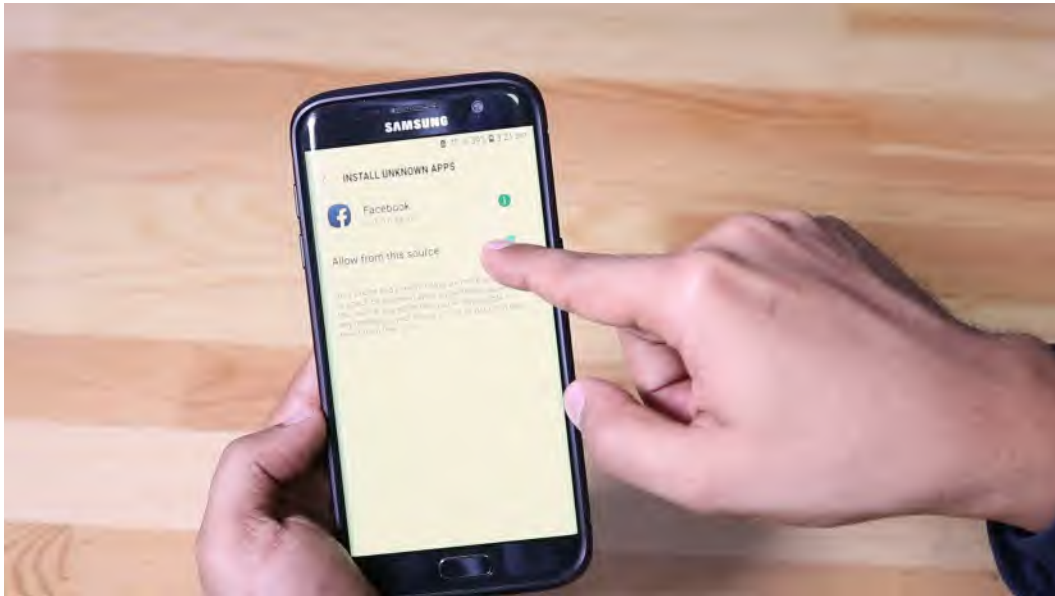


Figure 11.8: Enabling the third-party app Facebook to be installed in Android

However, you will see a warning that your phone and personal data are more vulnerable to attack by unknown apps if you enable this setting.

Now, to check for app permissions on an iPhone, start by navigating to your **Settings | Privacy** tab. Here, you will see the different types of permissions that can be granted to apps, such as access to your calendars, contacts, camera, and microphone.

For example, if you want to see which apps have access to your calendars, tap on **Calendars**. If no apps are listed, then none have access. Under **Contacts**, you might see apps like Messenger, Line, or a banking app, which is normal if you use those features. To check camera access, tap on **Camera**, and you will see a list of apps such as ClassDojo, Snow, Facebook, Slack, and Line that have permission to use your camera. This method allows you to review which apps have access to specific tools on your phone.

If you want to disable a permission, such as preventing Facebook from accessing your microphone, tap on **Microphone** and turn off the toggle next to **Facebook**. This immediately revokes the app's access to your microphone.

Another useful feature is the ability to reset your location and privacy settings. To do this, go to **Settings | General | Reset | Reset Location and Privacy**. This will reset all apps, so they no longer have access to your location or privacy-related data. Remember that some apps will not function properly until you grant them the necessary permissions again.

Mobile app security guidelines

To help you stay safe when downloading and using applications on your phone, follow these four main tips:

1. **Avoid apps from third-party sites:** Only download your apps from the Google Play Store or the Apple App Store. Do not trust applications from third-party sites, no matter what they promise or how appealing they sound. Stick to the official app stores to reduce your risk.
2. **Less is more:** The more apps you have installed, the less secure your device becomes. If you have apps that you have not used for several months, delete them. If an app has not worked for you or served its purpose, remove it from your phone. Keeping only the apps you actually use helps minimize your attack surface.
3. **Restrict permissions:** Review the permissions granted to each app on your device. If an app has access to your camera, videos, or other sensitive data and you feel it should not, restrict those permissions. Only allow apps to access the data they genuinely need to function.
4. **Run updates:** Always install updates as soon as they become available, especially if you use an Android phone. Do not delay updates, as they often contain important security fixes. Keeping your apps and operating system up to date is critical for your protection.

Virtual private network (VPN)

Using a **VPN** can allow you to access region-restricted content simply by changing your IP address. For example, if you are in China and want to access YouTube or Facebook, you can use a VPN to make it appear as though you are connecting from England, where there is no such censorship.

When you introduce a VPN, the connection changes. Now, the connection between your mobile device and the VPN is encrypted, as indicated by a padlock in *Figure 11.9*:



Figure 11.9: How a VPN encrypts connections and allows users to choose IP addresses from different countries

This means that any data you send between your device and the internet becomes encrypted. VPN also allows you to choose an IP address from a variety of countries, depending on the VPN service you use. Once you select an IP address from one of these countries, VPN completes your request to connect to the internet using the new IP address. This setup helps protect your privacy and can bypass applications or services that restrict content based on your location.

When choosing a VPN service for your mobile device, it is important to select a reputable provider. Avoid free VPNs, as they can be dangerous and may mishandle your data. If you are going to invest in security, choose a trusted VPN provider like **NordVPN**, which is a fast, secure, and affordable option, available on both Google Play Store and Apple App Store.

NOTE

Before you go any further, pay attention to similar VPN providers like FreeVPN Master, FreeVPN Unlimited, and FreeVPN Unlimited 2019. Never install free VPNs, as they tend to do more harm than good. If you are going to use a VPN service, make sure that it is one that you have paid for.

NordVPN

Now, let's explore how to use NordVPN on your mobile device:

1. Download and install NordVPN. Click on the **OPEN** button to launch the app:

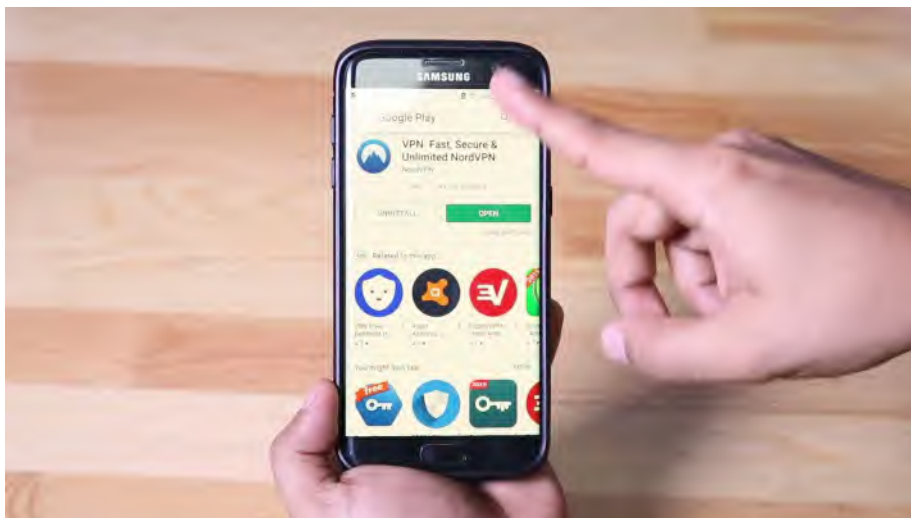


Figure 11.10: NordVPN app is ready to be opened on a Samsung device

2. Once the app opens, you will need to sign up if you do not already have an account with NordVPN. If you already have an account, go ahead and log in with your credentials. After logging in successfully, you will notice blue dots on the map in the main interface, which represent the servers that NordVPN has all over the world. You can connect to any one of these countries:

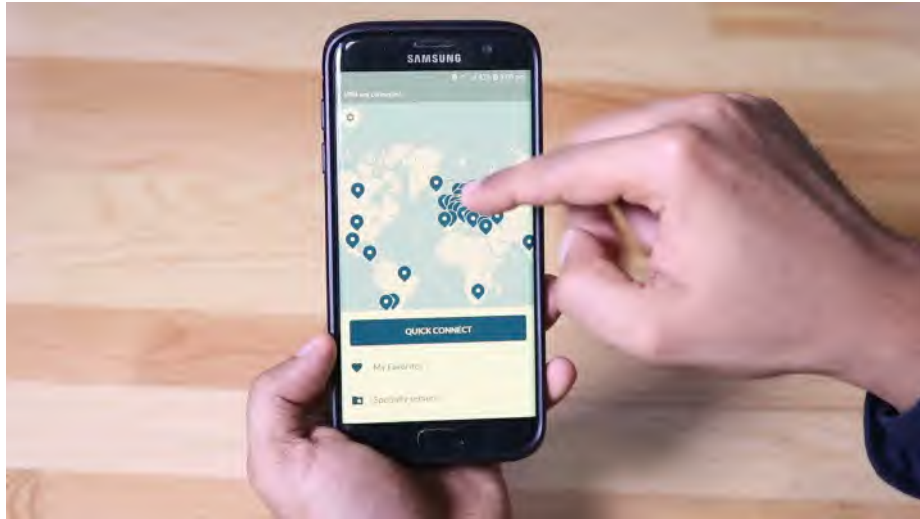


Figure 11.11: NordVPN world map interface with server locations

If you expand the window, you will see that there are many servers across Europe, as well as in Southeast Asia, including countries like Thailand and Vietnam. You can scroll through the list of countries, ranging from Albania to Argentina, Australia, Brazil, Chile, France, Ireland, Italy, Mexico, and more.

3. If you want to connect to a particular country, for instance Thailand, click on **Thailand**. The app will prompt you for permission to connect to VPN:

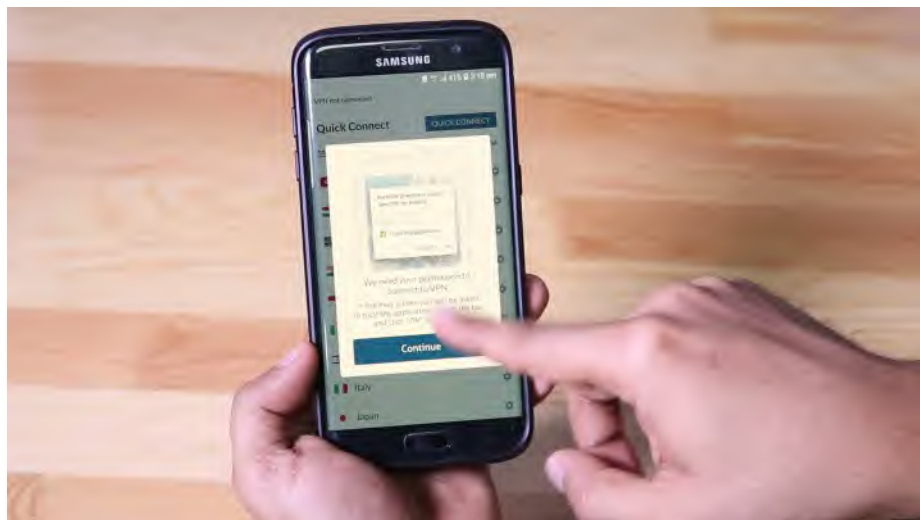


Figure 11.12: Permission to connect to the VPN of a country

4. Click **Continue**, and when NordVPN requests application permissions to control your traffic, select that you trust the application, then click **OK** and **Continue** as needed. After a few seconds, you will see the status turn green, indicating that you are now connected to Thailand:

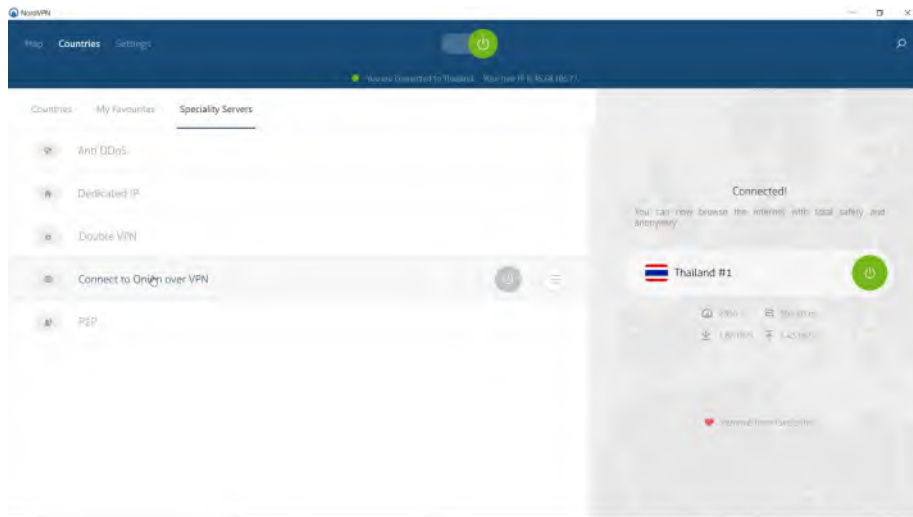


Figure 11.13: VPN connected to Thailand

NordVPN also offers specialty servers, which are advanced features you probably do not need for everyday use. These include peer-to-peer connections and other sophisticated options, but you do not need to worry about them for basic VPN usage.

5. You can enable additional features in the NordVPN app to boost your security. It is recommended that you turn on the **CyberSec** setting, which helps protect you from malware and phishing attempts. Click the toggle next to **CyberSec** to activate this protection:

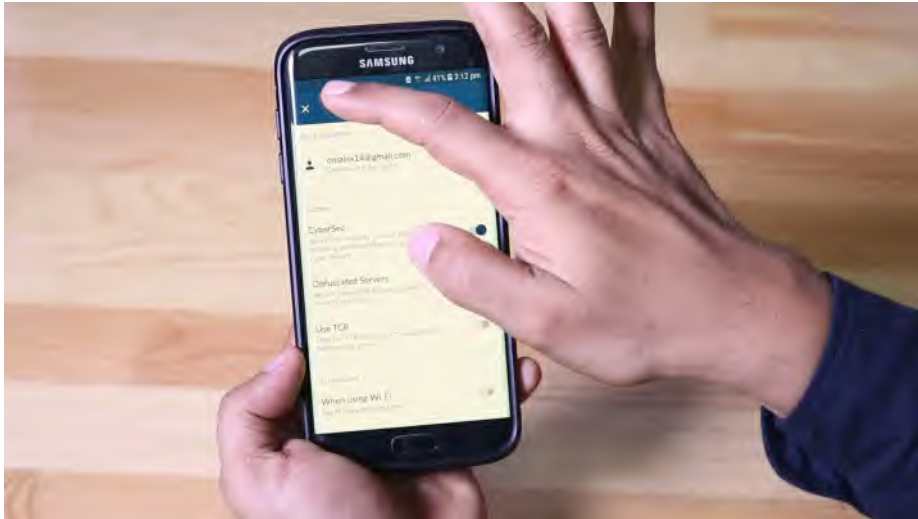


Figure 11.14: Enabling CyberSec security features in the NordVPN mobile app settings to protect against malware and phishing attempts

6. All other settings are optional and generally not necessary for most users. However, CyberSec is one that you should definitely enable if you decide to use NordVPN.
7. All other settings are optional and generally not necessary for most users. However, CyberSec is one that you should definitely enable if you decide to use NordVPN.

Public Wi-Fi

If you often walk in public places such as conference centers, public libraries, coffee shops like Starbucks, or if you travel frequently and work in airports, you have likely encountered public Wi-Fi networks. When you connect to a free public Wi-Fi network, you are at significant risk of attacks from cybercriminals and hackers. As a rule, do not connect to free public Wi-Fi networks. It is safer to use the internet service provided by your mobile network carrier.

If you do not have a data plan and must use public Wi-Fi, only access websites that use **HTTPS**. Websites that start with HTTPS encrypt the information sent between your device and the website, making it much harder for attackers to intercept your data. Never send sensitive information such as passwords or credit card details over public Wi-Fi.

A VPN is another tool you can use for protection on public Wi-Fi. It encrypts all data sent between your mobile device and the websites you access, providing an extra layer of security.

Configuring important security settings

To round up this section, let's review a few more important security settings on your Android device.

Lock screen and security

Under your device settings, navigate to **Lock Screen and Security** | **Phone Security**, and set up at least one type of screen lock. This could be a PIN, fingerprint, or both:

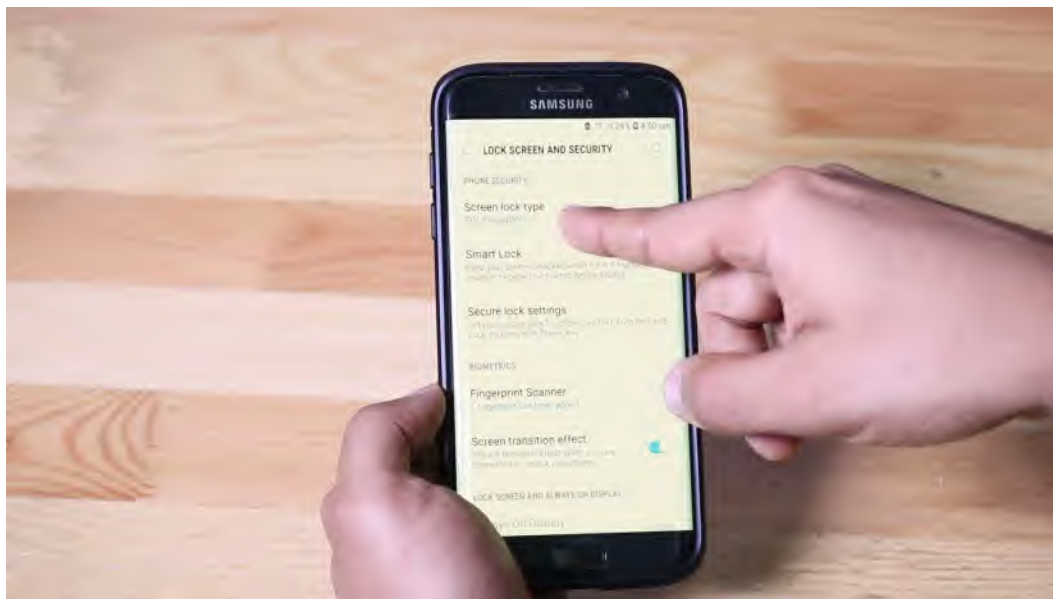


Figure 11.15: Lock screen and security settings on an Android device, highlighting screen lock type and fingerprint options

Google Play Protect

Google Play Protect regularly scans your device for malicious apps and notifies you if any security risks are found. Keep this feature activated to help protect your device from harmful apps:

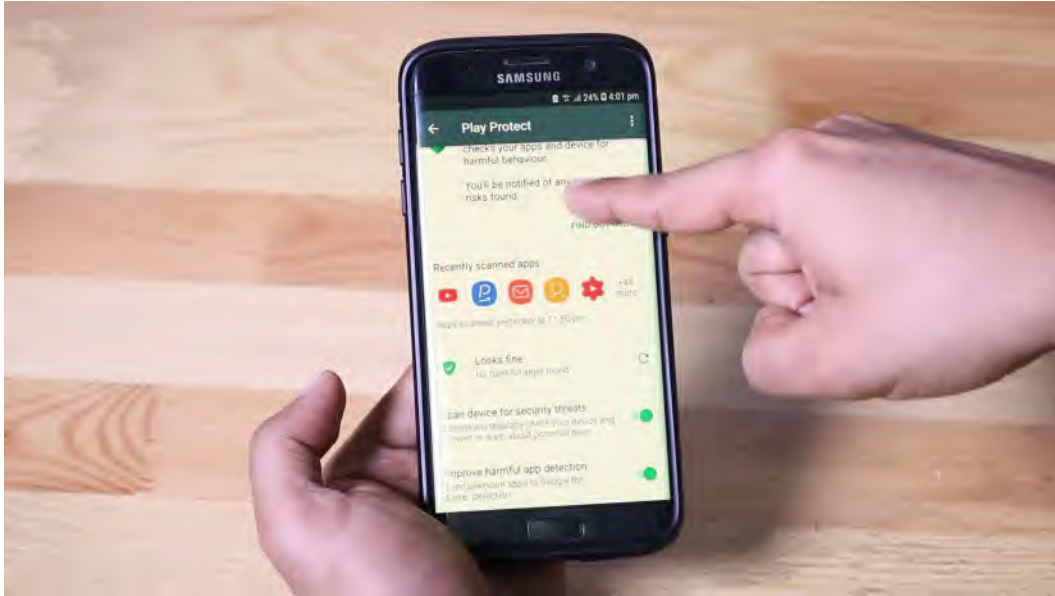


Figure 11.16: Google Play Protect settings for scanning the device and improving harmful app detection on an Android phone

The Play Protect interface includes a notification that no harmful apps were found and displays toggles for both security options. If Google Play Protect is not activated, your device may be at greater risk. Make sure that Play Protect is working and updating your apps regularly.

Find my phone

After checking Play Protect, go back to the main security settings and enable **Find My Mobile** and its related options: activate remote controls, Google location service, and send last location:

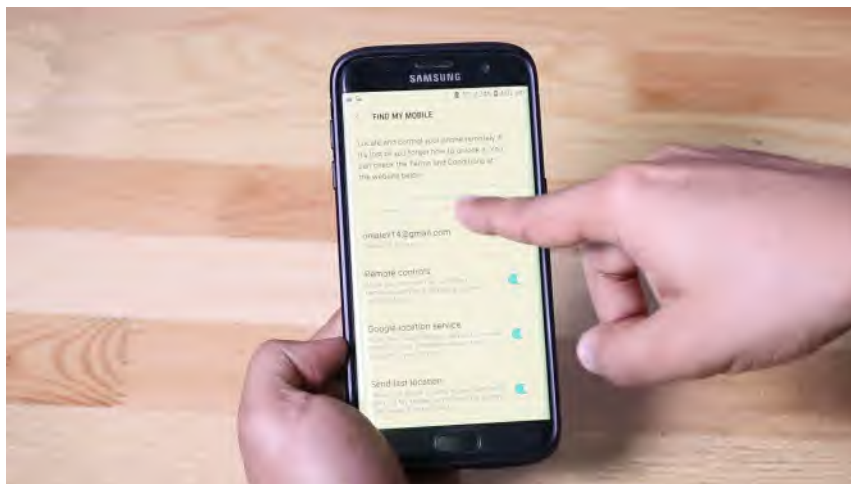


Figure 11.17: Options under Find My Mobile setting in Samsung

If you misplace your phone or it gets stolen, you can use the Find My Mobile feature to ring your phone and trace its location. In more serious situations, such as theft, you have the option to erase all the data on your phone remotely. You can also retrieve your calls and messages and even extend your battery life. For Samsung devices, use the findmymobile.samsung.com website to track your phone:

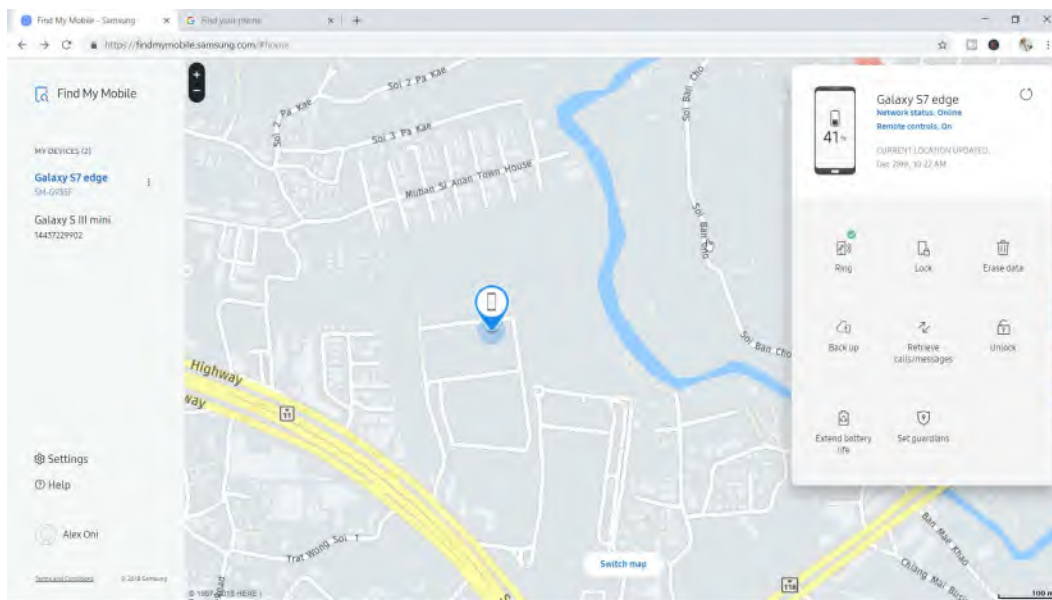


Figure 11.18: Find My Mobile interface for locating, ringing, locking, or erasing a lost Samsung phone

If you use a different kind of Android device, Google provides its own Find Your Phone feature. To access it, go to `google.com` and search for **Find My Phone**, then log in with your Google account. Once your phone is registered with Google, its last known location and select it from the list of devices:

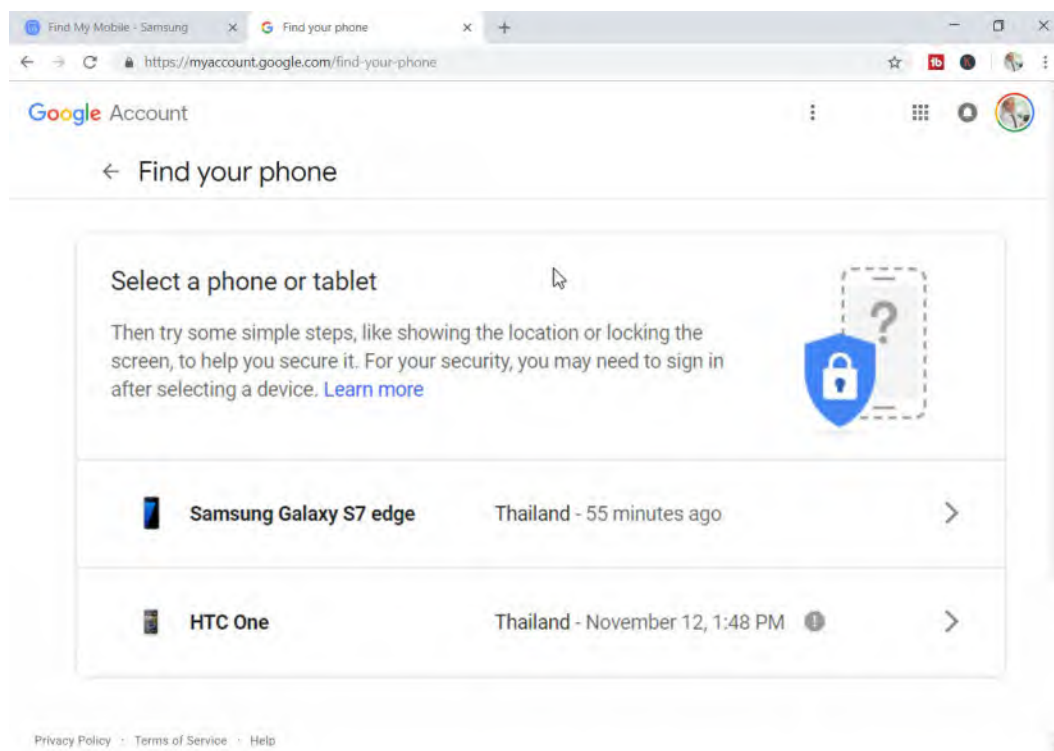


Figure 11.19: Google Find My Device interface showing registered Android devices and their last known locations

After selecting your device, you may be prompted to enter your password to verify your identity. The Google Find Your Phone feature offers similar options to Samsung's service: you can lock your phone, try calling it, sign out, or erase your device.

You can also attempt to locate your phone on a map:

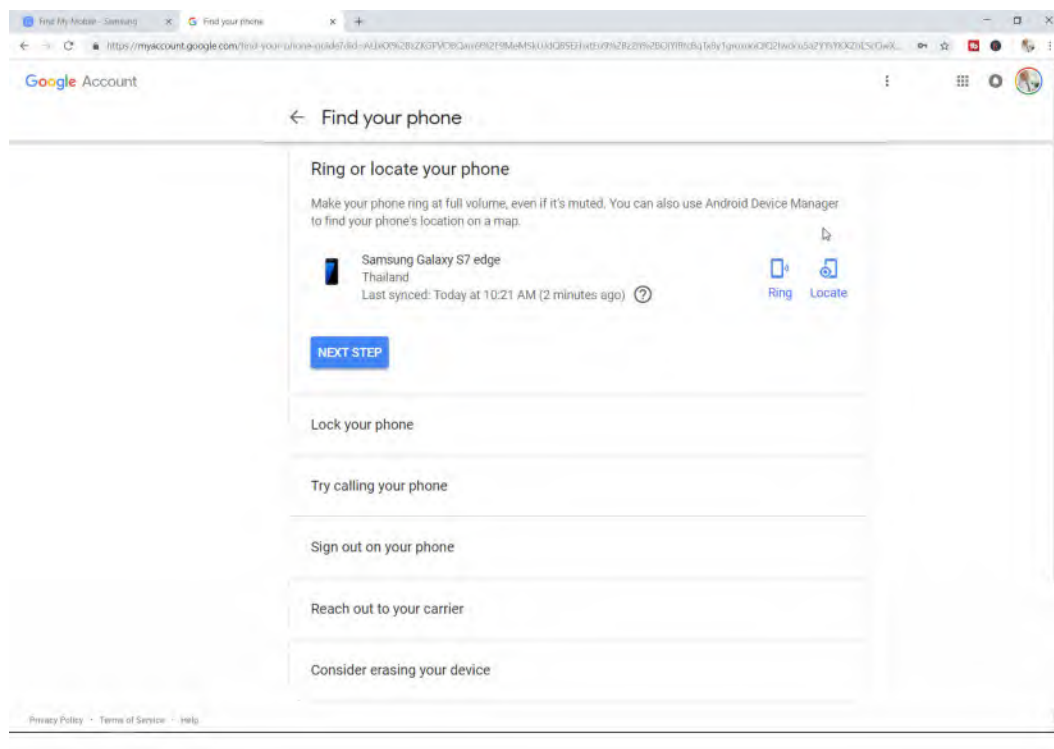


Figure 11.20: Google Find Your Phone interface showing options to ring, locate, lock, call, sign out, contact carrier, or erase the device

When you use the **Locate** feature, Google attempts to pinpoint your device's location on a map. The service is very accurate and can show your phone's location down to a specific area, such as a condo next to a well-known shopping mall.

You can also view your device's battery level and access additional security options like erasing or securing your device:

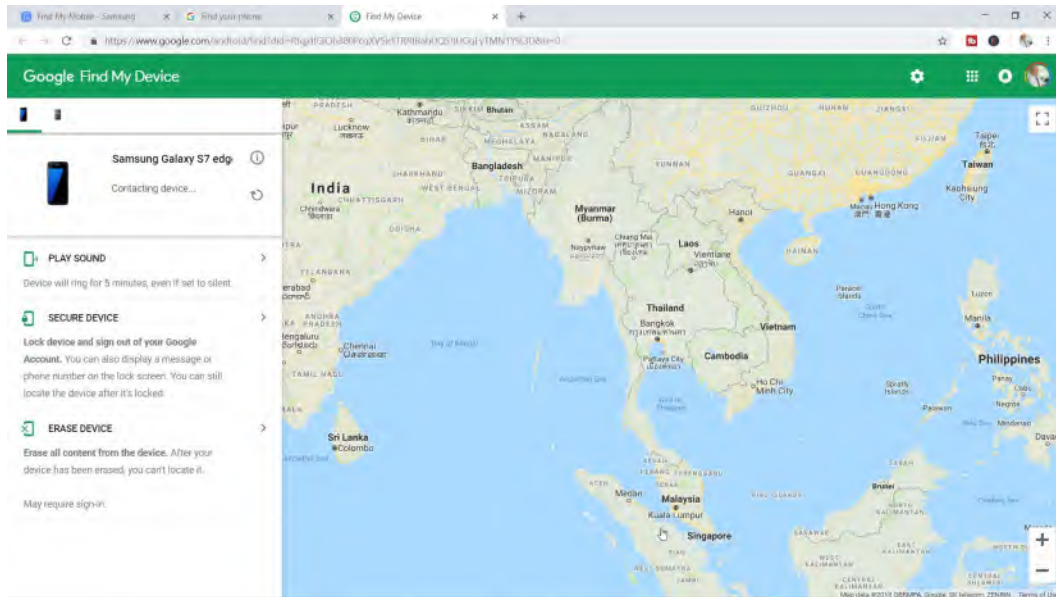


Figure 11.21: Google Find My Device interface showing real-time device location on a map of Southeast Asia

Be sure to activate the **Find My Phone** tools under your Android security settings to take advantage of these features. Scroll further to find the **App Permission Monitor** and ensure it is turned on. This lets you monitor which permissions your apps are using.

Find My iPhone

One particular kind of tool you should use if you have an iPhone is the **Find My iPhone** service. This tool allows you to physically locate your iPhone if it is misplaced or stolen. To set it up, log in with your Apple ID and password, and follow the setup instructions provided. The process is similar across iPhones, other iOS devices, and Macs, with clear instructions available for each platform.

Find My iPhone service has many options located in its main menu, actions such as physically locating your device, locking it, or erasing all information from your phone if it is lost or stolen and you want to prevent unauthorized access to your data.

You can also play a sound on your iPhone, which is helpful if you have misplaced it somewhere in your house and need to track its physical location:

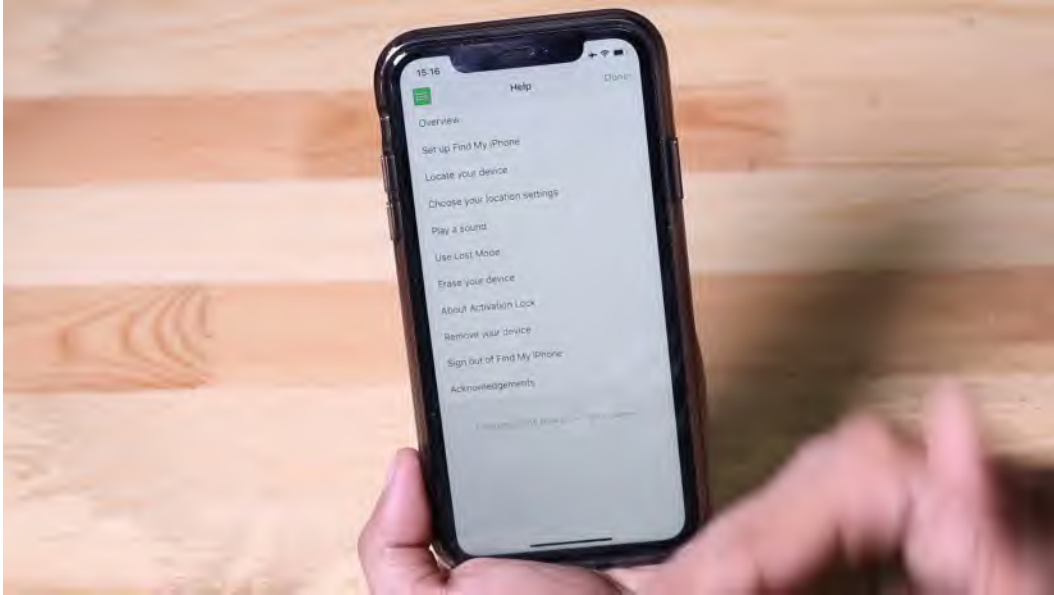


Figure 11.22: Find My iPhone help menu options for locating and securing a lost device

You cannot perform these actions directly from your missing iPhone, but you can use the Find My website from your Mac or any regular computer to control your device remotely.

SIM card lock settings

Finally, under **Other Security Settings**, you have the option to set up a SIM card lock. The following figure shows the SIM card lock settings screen, where you are prompted to enter your current SIM card PIN:

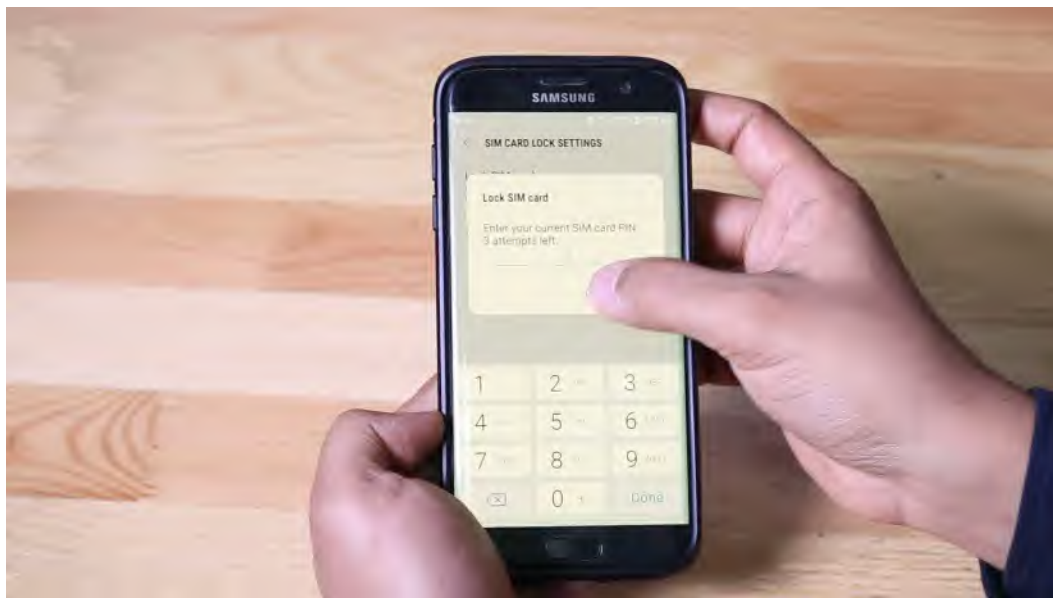


Figure 11.23: Locking a SIM card by entering the current SIM card PIN in a smartphone security settings screen

Basically, that PIN will be used to lock and unlock your SIM card if you want to go through this process. While not everyone uses this, enabling a SIM card lock can further enhance your phone's security.

You can also make your passwords visible whenever you're typing them just briefly, or you can just make sure they're never visible again. Also make sure that your security policy updates are set to update automatically as well:

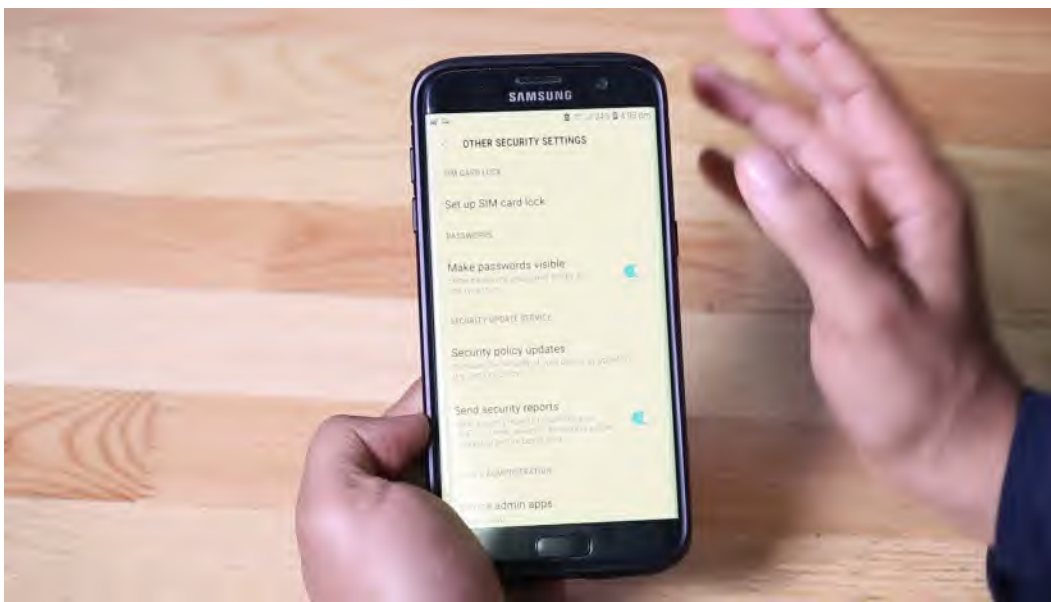


Figure 11.24: Key Android security settings, including SIM card lock, password visibility, and automatic security policy updates

These are the major security settings that you should configure on your Android. Make sure you have some form of screen lock type, Google Play Protect is working, Find My Mobile is active, your security updates are working properly, and of course, your app permission monitor is set to on. Staying aware of mobile device security risks and following best practices for app management, permissions, and device settings will help you keep your personal information safe.

Summary

In this chapter, we established how to identify legitimate versus fake mobile applications using practical techniques such as analyzing developer information, evaluating app reviews and ratings, and scrutinizing install numbers and visual clues within Google Play Store and Apple App Store. Starting from global mobile usage trends and the rapid growth of mobile malware, we moved through a comparison of Android and iOS security characteristics.

We then examined how app vetting, security updates, and device fragmentation impact overall device safety, before focusing on best practices for downloading apps, verifying authenticity, and understanding app permissions. The key distinction we drew is that a high install count or a familiar app name does not guarantee legitimacy, malicious apps can mimic official ones, and even reputable app stores can host dangerous downloads, making careful scrutiny of developer details and app characteristics essential.

This chapter equips you with the practical skills to confidently assess mobile apps for security risks and to make informed decisions when installing and managing applications on our devices. *Chapter 12* will take you through some essential security controls.

12

Privacy, Anonymity, and Online Safety

Privacy, anonymity, and online safety are no longer abstract ideals, they are daily challenges for anyone navigating the modern internet. From browsing websites and using social media to shopping online or accessing cloud services, our activities constantly generate data that can be collected, tracked, shared, or exposed. As a result, understanding how to protect personal information and control what others can learn about you online has become an important part of cybersecurity.

In this chapter, you will build the practical skills and understanding needed to control your personal information, keep your identities compartmentalized, and defend against tracking techniques that seek to link your actions across devices and accounts. You will work hands-on with tools like VPNs (including NordVPN and TunnelBear), ProtonMail, temporary email providers such as TempMail.org, Google Voice, VirtualBox, and privacy-focused browsers and extensions such as Brave, Firefox, uBlock Origin, and Privacy Badger, while making clear distinctions between privacy, anonymity, and pseudonymity, and also learning the principles of identity compartmentalization.

Mastering these techniques is crucial because even the most advanced privacy tools can be undermined by a single misstep, such as reusing an email address or logging into a personal account on a compartmentalized VPN. The real goal is to develop habits and strategies that keep your online lives separate, untraceable, and safe from both commercial trackers and AI-powered behavioral profiling.

In this chapter, we will cover the following topics:

- Defining Privacy, Anonymity, and Pseudonymity
- Identity Compartmentalization
- Modern Online Tracking Techniques
- Major Online Tracking Locations
- Browsing in Incognito or private mode
- Anonymizers: Tools for online anonymity

Defining privacy, anonymity, and pseudonymity

When you think about privacy, anonymity, and pseudonymity, you are dealing with very important and very interesting topics that shape your control over information and access in the digital world.

Privacy means that you are in control of your own personal information. Many people mistakenly believe that privacy means only you have access to your data, but that is not entirely true. Privacy is about control: you decide who can access your information and, more importantly, what they are allowed to do with it. For example, your doctor or hospital knows about your illnesses or medical history. Even though this information is private, you want them to have access to it, and you expect them not to share it publicly. In many countries, there are laws that make it illegal for medical institutions to reveal patient data. This is still privacy, because you have chosen to share your information with them and can control how it is used.

Anonymity, on the other hand, means your true identity is hidden. No one can link your online activities to who you really are. For instance, you might post a message on an online forum as a guest without logging in or creating an account, allowing you to be anonymous. You can also use services such as Tor to help hide your identity. However, achieving 100% anonymity today is extremely difficult due to advanced fingerprinting, metadata collection, and AI-powered correlation. These technologies make it much harder to remain completely anonymous online.

Pseudonymity is often confused with anonymity, but they are not the same. Pseudonymity simply means that you consistently maintain a false identity online. It has to be consistent. The classic example here would be on YouTube, where you probably follow certain YouTubers who use pseudonyms. It's not their real name and they have never revealed their true identity or in some cases even their face. This encompasses pseudonymity.

The one big risk of pseudonymity or using pseudonyms is that if your true identity is ever revealed online, then your past activity can be linked to you instantly. That is the one risk involved with pseudonymity. So even though you can hide your true identity, you can hide your face, you can use a fake name, your posts, your general behavior, your attitude toward certain kinds of topics or social issues, your writing style—all of this can be linked back to you. So do keep that in mind. Pseudonymity and anonymity are not the exact same thing. They are very, very different.

So now that you know what privacy, anonymity, and pseudonymity are, here are a few examples of each one. For privacy, a very good example would be using encrypted mail. Services such as ProtonMail allow you to encrypt your emails and send them securely, which ensures privacy. For anonymity, think of using a VPN, a virtual private network, and then paying for the VPN with cash and never actually logging into any account. Finally, pseudonymity, as already described, could be you running a YouTube channel with a fake username, a fake avatar, and never revealing your face or your true identity.

These examples show that privacy, anonymity, and pseudonymity offer different ways to control how much information about your identity is exposed online. However, protecting your identity is not only about hiding information; it is also about keeping different parts of your online activity separate. This brings us to identity compartmentalization.

Identity compartmentalization

If the same usernames, email addresses, accounts, or other identifying details are used across different activities, those activities may eventually be linked back to the same person. **Identity compartmentalization** the practice of separating different online identities and activities so that information from one area cannot easily be connected to another. This section will discuss the types of online identities you can create, the core principles for keeping them distinct, and practical examples of how this works in real life.

You may have seen the meme that shows four different profile pictures of the same person, in this case, Chef Gordon Ramsay, across various platforms. The point of this meme is to highlight how people project different personalities or aspects of themselves depending on the platform.

For example, LinkedIn is professional, Facebook is about family, Instagram is about fun, and Tinder is about being available for dating, as shown below:



Figure 12.1: How people present different personas on LinkedIn, Facebook, Instagram, and Tinder

So, what types of identities can you actually create online? There are four main types:

- **Personal identity:** This includes your real name, home address, phone number, bank information, family details, and even your date of birth. You use this identity for important accounts such as medical or banking services where your real information is required.
- **Professional identity:** This covers your LinkedIn profile, work email, business website, and other work-related accounts.

- **Pseudonymous identity:** You might use this for gaming, forums, or creative projects. For example, your PlayStation Network username is likely not your real name, which is a typical use of a pseudonymous identity.
- **Anonymous identity:** This is used for highly sensitive tasks such as whistleblowing, activism, or sensitive research, where you do not want your real identity or even a consistent pseudonym to be linked to your actions.

The core principles of identity compartmentalization are as follows:

- Always use separate accounts for each identity. Never use the same email address across different identities.
- Use separate devices or at least different browsers or browser profiles for each identity.
- Use unique credentials for each identity. Do not reuse passwords.
- Avoid cross-contamination by not logging into your personal accounts from your anonymous device, as this defeats the purpose of compartmentalization.

For example, a journalist might have a personal laptop for their personal identity, which they use for home banking, personal email, and family calls. For the professional identity, they might use a work laptop for interviews, writing articles, and managing media accounts. If they wanted to contact whistleblowers, anonymity would be a high priority. Therefore, for their anonymous identity, they would use a separate laptop or device, ideally running a Linux operating system in a virtual machine with Tor.

The main benefit of identity compartmentalization is that it limits the damage if one identity is compromised. For example, if your professional identity is breached, your personal identity remains protected, and vice versa. It also makes it much harder for data brokers and AI tracking systems to build a unified profile of you. Compartmentalization also improves operational security for sensitive activities.

NOTE

AI tracking online is extremely advanced, and if you use the same accounts across devices, AI and data brokers can easily identify you and your habits.

There are four major mistakes people make when trying to compartmentalize their identities:

1. Using the same recovery email for multiple identities. You must have separate recovery emails for each identity.
2. Logging into personal accounts while connected to a compartmentalized VPN. For example, if you use a secure VPN for anonymous activities and then log in to your personal email, you defeat the purpose of compartmentalization.

3. Reusing usernames or avatars across compartments. Using the same username or avatar for multiple identities undermines compartmentalization, yet many people still do this.
4. Mixing financial transactions between compartments. Never use the same payment methods or financial accounts across different identities.

Now, what are the most useful tools you could use for compartmentalization? Your browser is a very important one. For example, the Brave browser allows you to create different profiles. To do this in Brave:

1. Open the Brave browser to a blank page.
2. Go to your settings.
3. Under "More tools," click to add a new profile.
4. Name the new profile (for example, "private") and click "Done"

Now, anything you search for or any sites you visit will be linked only to this specific profile. You can open Brave again and choose another profile for a different identity. This is an effective way to compartmentalize within your browser.

Other tools you can use for identity compartmentalization include VirtualBox, which allows you to create virtual machines. With VirtualBox, you can install multiple operating systems, such as Mac or Linux, on your Windows computer, all running at the same time. This is a practical way to keep your identities separated at the operating system level.

NOTE

The VirtualBox website provides the download link and documentation for getting started with virtualization.

ProtonMail is another valuable tool, offering what is arguably the most secure form of email available. You can sign up for a free account and use it to send anonymous emails and maintain privacy, making it a much better choice than mainstream services such as Gmail or Yahoo Mail.

Temporary email providers, such as TempMail.org, are also useful. When a website requires you to create an account to access content, you can generate a temporary email address, sign up, and gain access without exposing your real email. However, you might prefer to create a dedicated email account specifically for these types of signups, which can be more convenient than repeatedly using temporary services. The choice depends on your personal preference.

Google Voice is another option, allowing you to create phone number accounts online for added separation between your real identity and online activities.

Finally, VPNs such as NordVPN are commonly used for identity compartmentalization. While there are many VPN providers available, and VPNs will be discussed in more detail later, they are an important part of your toolkit for keeping identities and activities separate.

After compartmentalizing your identities, it is also important to understand that separating accounts does not necessarily prevent your activities from being observed or connected. Websites, applications, advertisers, and other parties can collect information about how you behave online, sometimes without you being fully aware of how much information is being gathered. This brings us to another important aspect of online privacy, which is tracking.

Modern online tracking

Tracking is the process of collecting information about your online activities and behavior over time. When you visit websites, search for information, click links, make purchases, or interact with content, information about these activities may be recorded. Tracking can involve obvious information, such as the websites you visit, as well as less noticeable details, such as your device type, approximate location, browsing patterns, and interests.

This information can be used for many purposes. Advertisers, for example, may track your activity to build a profile of your interests and show you more personalized advertisements. Data brokers may collect information from multiple sources and combine it into detailed profiles that can be used or sold for marketing and other purposes. Governments may use certain forms of tracking for law enforcement, intelligence, or security purposes.

Tracking can also be misused. Cybercriminals may collect information about potential targets to make phishing attacks, scams, or other forms of social engineering more convincing. Information gathered from different sources can sometimes reveal far more about a person than any single piece of data would on its own.

Let's go through some common tracking methods.

Cookies

Cookies are a way for a website to know who you are by storing pieces of text on your computer. For example, when you create an account on a site, log in, and then close your browser without logging out, you can return later and still be logged in because the site reads the cookie it stored on your device. This cookie allows the site to recognize you and keep your session active without requiring you to log in again. First-party cookies store your preferences and login sessions for the site you are visiting.

However, third-party cookies are more intrusive, as they can track you across multiple sites. Most modern browsers attempt to block third-party cookies by default, but workarounds still exist.

Super cookies are even more persistent than regular cookies, as they can be stored in unusual places such as your flash storage, making them very difficult to delete. Evercookies take persistence further by regenerating themselves even after you try to delete them, making them extremely hard to remove. These methods all contribute to how you are tracked online.

Browser fingerprinting

Browser fingerprinting is another technique that collects information such as your browser type and version, installed fonts and plugins, screen resolution, time zone, hardware information, and even your audio and canvas rendering output, which is unique for each device. This combination of details can make your device highly identifiable online. Tools like `amiunique.org` can show you how unique your fingerprint is compared to others. The purpose of this site is to show you exactly how unique your fingerprint is on the internet and how identifiable you are compared to millions of other users.

The homepage of `amiunique.org` invites you to check your fingerprint uniqueness by clicking the SEE MY FINGERPRINT button in the center of the page as shown below:

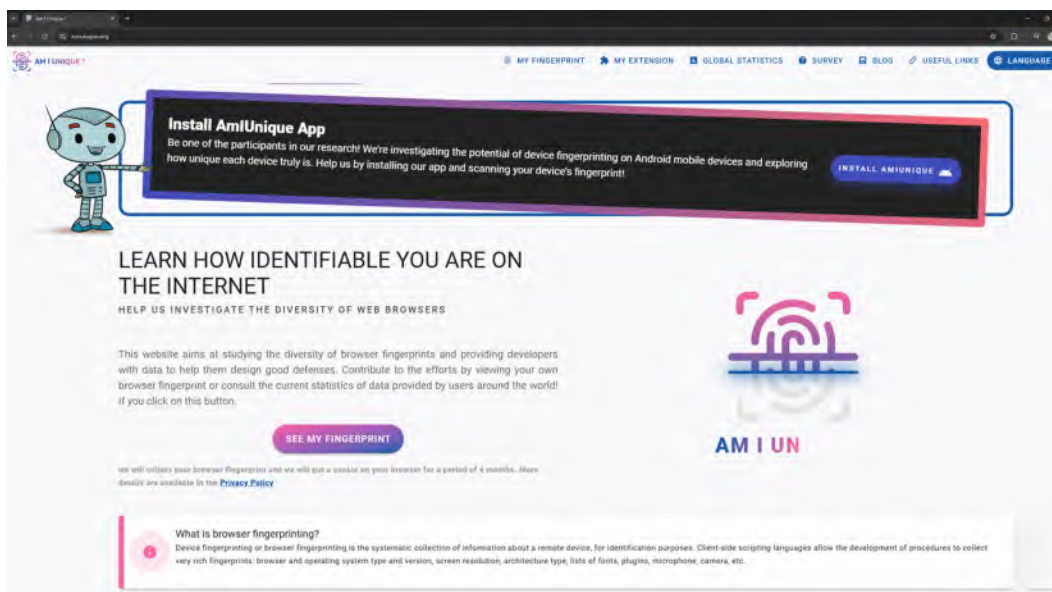


Figure 12.2: AmlUnique homepage

When you click to see your fingerprint, the site analyzes your device and browser details, such as your operating system, browser type and version, language, time zone, screen size, and more. In the example screenshot below, the result shows that you are unique among over 4 million fingerprints in their dataset:

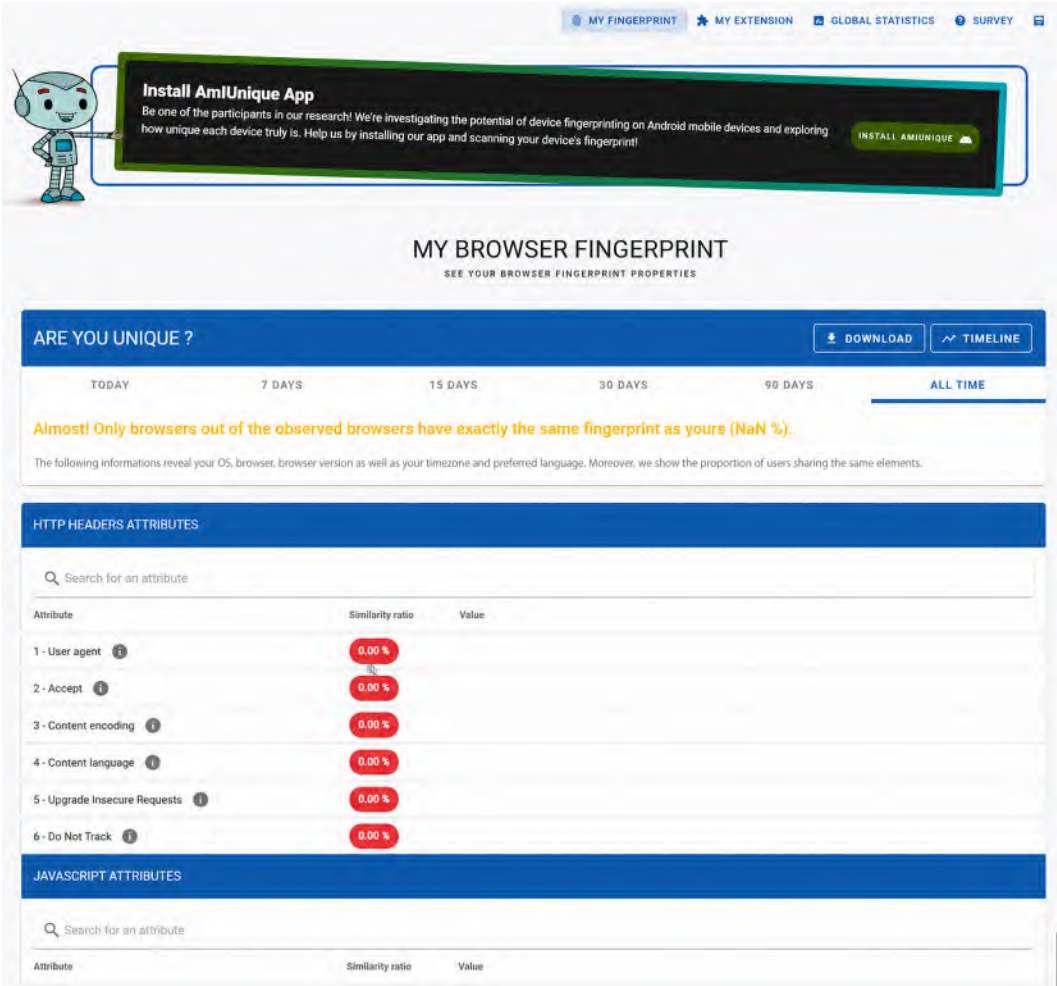


Figure 12.3: How browser fingerprinting can uniquely identify users based on device and browser attributes.

The page displays detailed information it has collected, including your OS (Windows), browser (Chrome), language (English), time zone, content language, cookie status, screen width, and screen height. You can try this yourself by visiting amiunique.org to see whether your fingerprint is unique on the internet.

Cross-device tracking

A cross-device tracking technique can link your phone, tablet, and laptop activity through shared elements such as logged-in accounts, IP addresses, Bluetooth, and Wi-Fi signals. For example, if you have the same Gmail account open on both your computer and your mobile device, trackers can easily determine that both devices belong to the same person. Even without cookies, advertisers can track you across devices using these shared identifiers.

AI tracking

The most advanced method of tracking today is **AI behavioral tracking**. This technique uses AI to detect patterns in your behavior, such as your mouse movement, typing speed, and style, scrolling behavior, and purchase patterns. Even if you use a VPN, change your IP address, or practice identity compartmentalization, there are subtle behavioral traits, like how you move your mouse or scroll, that you probably would not think to change. AI can track these unique behaviors, making it extremely difficult to hide from these trackers.

Detecting and blocking trackers

There are several options for detecting and blocking trackers. You can install browser extensions on browsers such as Brave or Google Chrome. Examples include uBlock Origin, Privacy Badger, NoScript, and ClearURLs. You can also use private browsers such as Firefox, Brave, or LibreWolf with hardened settings. For email privacy, tools such as ProtonMail and SimpleLogin allow you to create aliases. For more advanced, network-level protection, you can use services such as Pi-hole or NextDNS.

However, keep in mind that these measures are not enough on their own. Even with "do not track" enabled, many sites will ignore your request. Privacy laws exist, but many websites still choose to track you regardless. Many trackers are invisibly embedded in scripts, ads, or images, and are very advanced and sneaky.

Ultimately, your privacy depends on a combination of tooling, compartmentalization, and, most importantly, your own habits. Even with the best privacy tools and strategies, your attitude and habits toward privacy are what truly matter.

Major online tracking locations

Online tracking happens in many places, and each location collects different kinds of information about you. Search engines, social media platforms, and other services gather and use your data for different purposes.

Search engines

Search engines collect a wide range of data, including your search queries, click history, IP address, and device information. The main reason for this data collection is to build interest

profiles and sell you targeted advertisements. Companies such as Google and Baidu, along with their ad networks, are the primary entities tracking you through search engines. With the rise of AI models and tools such as GPT, people are starting to use search engines less, which may change how this tracking works in the future. For better privacy, you can use alternatives such as DuckDuckGo, Startpage, Brave Search (via the Brave browser), or self-hosted options such as SearXNG, which do not track your searches.

Social media platforms

Social media platforms collect highly personal information, including your posts, likes, shares, friend lists, direct messages (metadata), and facial recognition data from images. The information gathered here is often more personal than what is collected by search engines. Social media also creates **shadow profiles**, where platforms collect data on non-users through friends' uploads and contact syncing. For example, even if you do not have an Instagram account, if a friend uploads a photo with you and tags your name, Instagram can still associate that information with you. Through contact syncing, these platforms can learn even more about you.

The main companies involved in this kind of tracking are Meta (which owns Facebook and Instagram), X (formerly Twitter), TikTok, and LinkedIn. To protect your privacy, you should disable contact syncing, review your privacy settings regularly, and avoid reusing personal photos across platforms.

NOTE

You may have seen the meme where Mark Zuckerberg is talking to a child who says, "My dad says you're spying on us," and Zuckerberg replies, "He's not your real dad." This meme is funny, but it also highlights just how much information social media platforms collect about you. There is even a saying that social media platforms know more about you than you know about yourself, which shows how much data you give them.

E-commerce and payment processors

Next, e-commerce and payment processors are major locations for online tracking. The data collected here includes your purchase history, payment methods (such as credit or debit cards), delivery address, and your browsing history on the site. These companies want to track your payment processes so they can predict your future purchases and adjust pricing, a practice known as dynamic pricing. For example, if you have bought a certain product before at a specific price, they may offer it to you again at the same or a slightly higher price, knowing you are likely to buy it. Companies such as Amazon, Alibaba, Shopify stores, PayPal, and Stripe are examples of those that track you through your payment processor. To protect your privacy, use

guest checkout whenever possible and privacy-respecting payment options, such as privacy.com cards or cryptocurrency where legal.

Mobile apps and permissions

Mobile apps and permissions are another significant source of data collection. Apps on your device can collect your location, contacts, microphone input, camera feed, background activity, motion sensors, and more. The main reason is to sell you ads and to sell your location data to brokers. This applies to all kinds of apps, including games, weather apps, dating apps, and fitness trackers. To protect your privacy, review the permissions you grant to these apps and uninstall any apps you do not use.

If there's any application you haven't opened within the past three months on your phone, delete that app. You do not need it, and if you ever do need it again, you can always reinstall it later.

Data brokers and background check companies

Data brokers and background check companies are another major tracking location. These companies can collect everything from your browsing history to your home address, political affiliation, and even income estimates. Examples include Acxiom, LexisNexis, Experian Marketing, and Oracle Data Cloud. To protect your privacy, use opt-out services such as Privacy Bee or Delete Me, or manually request removal from broker lists.

Email tracking

Email tracking is also common. Data collected through email tracking includes whether you opened the email, your IP address, location, and device information. Marketing services such as MailChimp and HubSpot, as well as sales tracking tools, use this data. To protect yourself, disable remote content in your email client and use an alias for signups.

Internet service providers (ISPs)

Last but not least, **internet service providers (ISPs)** also track you. They collect data such as websites visited, DNS requests, and traffic patterns, even if the traffic is encrypted. ISPs track this information for legal compliance, marketing partnerships, and usage analytics. The best way to combat ISP tracking is to use a VPN or DNS over HTTPS.

Browsing in incognito or private mode

Incognito or private mode is a feature in browsers such as Firefox that many people use to avoid leaving traces of their online activity. When you use incognito mode, your searches, browsing history, and cookies are not stored by your browser.

However, there is a common misconception that going incognito makes you completely private online. This is not true, because two important things are still stored and recorded even in

incognito mode: your bookmarks and your downloads. These remain tracked and monitored by your browser regardless of private mode.

You need to be careful with what you bookmark and download, even when using incognito mode. In addition, your employer and your ISP can still recognize and track your activity. Routers and remote servers are not affected by your browser mode; they identify you by your IP address and can monitor your online actions regardless of whether you are in incognito mode. For example, searches for illegal downloads can still be monitored by your ISP.

If you are at work, do not assume that using incognito mode will hide your activity from your employer. If you are using company equipment, your employer can monitor exactly what you are doing on your computer, even in private mode.

Websites and apps can also recognize you in incognito mode, especially if you log in to sites such as Facebook or Amazon. While your browser will not keep a record of your visit, these sites will know you logged in and can track your activity. Apps such as keyloggers and security software can also monitor your actions, regardless of browser mode.

Finally, some browser extensions may continue to track your activity even in incognito mode. Ideally, extensions should not be active in private mode, but in Firefox, certain extensions have been known to remain active.

TIP

Always be cautious about what you do in incognito mode. While your searches and cookies are not stored, you are not completely private and can still be tracked and monitored.

While it may not be possible to prevent every form of tracking, there are tools that can help reduce the amount of information exposed and make it more difficult to associate online activity with a particular user.

This brings us to anonymizers, discussed next.

Anonymizers: tools for online anonymity

Anonymizers are very useful tools and services designed to conceal or obscure identifying information, such as your IP address, as you use the internet, thereby making it difficult for others to track your activity.

The obvious advantages of using anonymizers are that they make it much harder for hackers to target you and for identity theft to occur, since your online actions become difficult to trace. Anonymizers also ensure privacy, which is extremely important for anyone concerned about

their personal information. Another major benefit is the ability to bypass censorship, which is especially valuable in countries with heavy internet restrictions, such as China. For example, if you are not allowed to use sites such as YouTube or Facebook, anonymizers can help you bypass those restrictions and gain access.

The basic topology of using an anonymizer involves your computer making an HTTP request, which is then routed through the anonymizer before reaching the internet. The anonymizer changes your IP address, so the website you are visiting sees a different IP than your real one, making your request anonymous and hiding your activity from anyone trying to track you.

The following figure illustrates this simple anonymizer topology, showing a computer making an HTTP request with its original IP address, which is then changed by the anonymizer before reaching the internet:



Figure 12.4: Anonymizer topology

Overall, there are two main types of anonymizers: single-point and networked anonymizers.

Single point anonymizers

A **single point anonymizer** passes your requests through a single intermediary to protect your identity, with a classic example being a proxy server. The topology for this is very similar to the simple anonymizer example shown in *Figure 12.4*. A **networked anonymizer** is more effective but also more complex, as it routes your communication through a network of computers, multiple points, before reaching the internet. The best-known example of this is Tor, which will be discussed in more detail later. In this setup, your request passes through several nodes, making it much harder to trace. The types of anonymizers are visualized below:

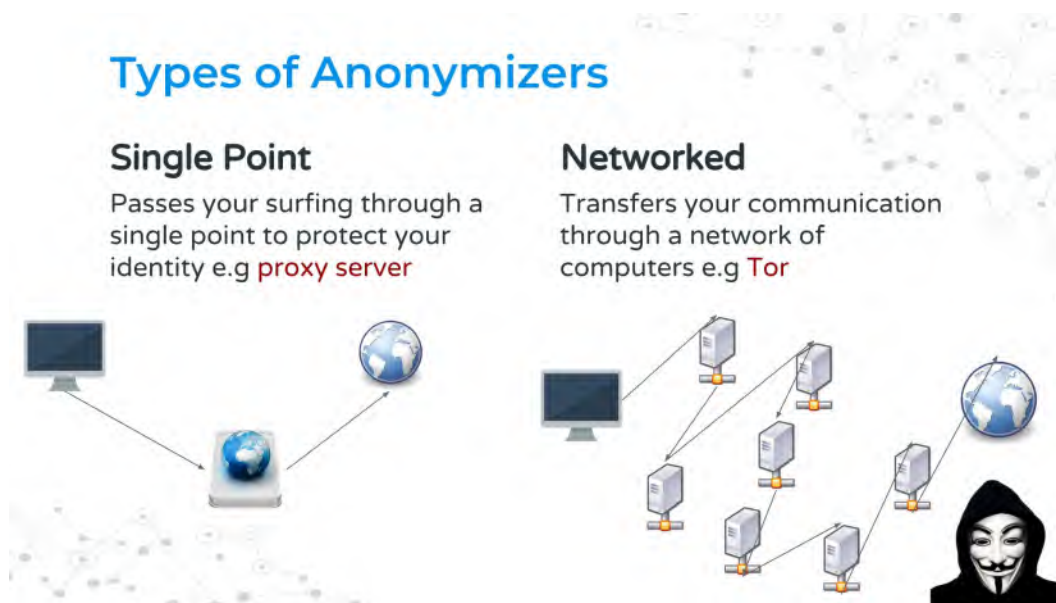


Figure 12.5: Types of anonymizers: single point (proxy server) vs. networked (Tor), with example network topologies

You will now look at the first type of anonymizer in detail: the proxy server.

Proxy servers

A **proxy server** acts as an intermediary between your device and the internet, providing you with a proxy IP address that can help you defeat restrictions and censorship. When you use a proxy, your public IP address is hidden and replaced with a different IP address to access the website you want to visit, effectively bypassing your ISP. This makes proxies useful for accessing blocked sites or downloading files, especially torrents.

However, proxies are not perfect. The first issue you will encounter is speed. Any anonymizer introduces some delay, but with proxies, the slowdown can be significant depending on the server you choose. Reliability is another concern, as not all proxies are trustworthy or stable, so you need to perform due diligence before selecting one. The most important limitation is that proxies generally provide no encryption. While some proxy servers may encrypt the initial connection between your computer and the web server, the actual traffic exchanged is usually not encrypted, which is a major security risk.

One recommended proxy server is Hidester, which is simple to use and offers several useful features. To use it, go to hidester.com, enter the URL of the site you want to visit, and choose between a U.S. or a European server. You can also access additional features by clicking the gear button to the right, where you can choose to encrypt the URL, allow cookies, or remove scripts from the site. The site page is shown below:

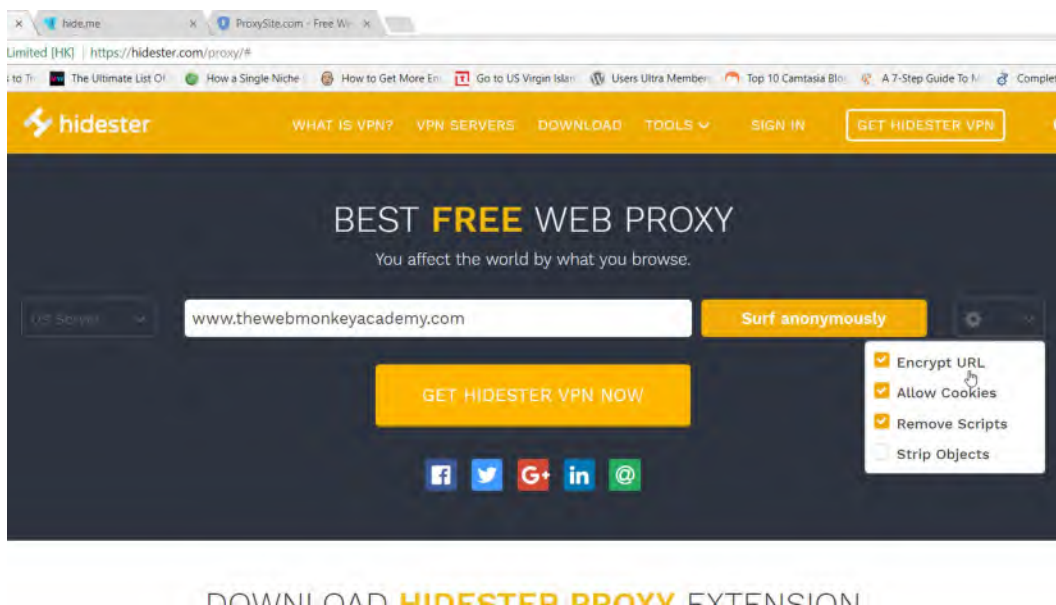


Figure 12.6: Web proxy interface showing options to encrypt URLs, allow cookies, and remove scripts for anonymous browsing.

One other useful feature of Hidester is that, apart from hiding your IP address, you can also choose to change the browser and operating system you appear to be using. For example, even if you are on Windows 10 with Chrome, you can tell Hidester to make it look like you are running Windows XP with Firefox 8. This adds an extra layer of security by allowing you to pretend to use a different operating system or browser.

An example is shown below:

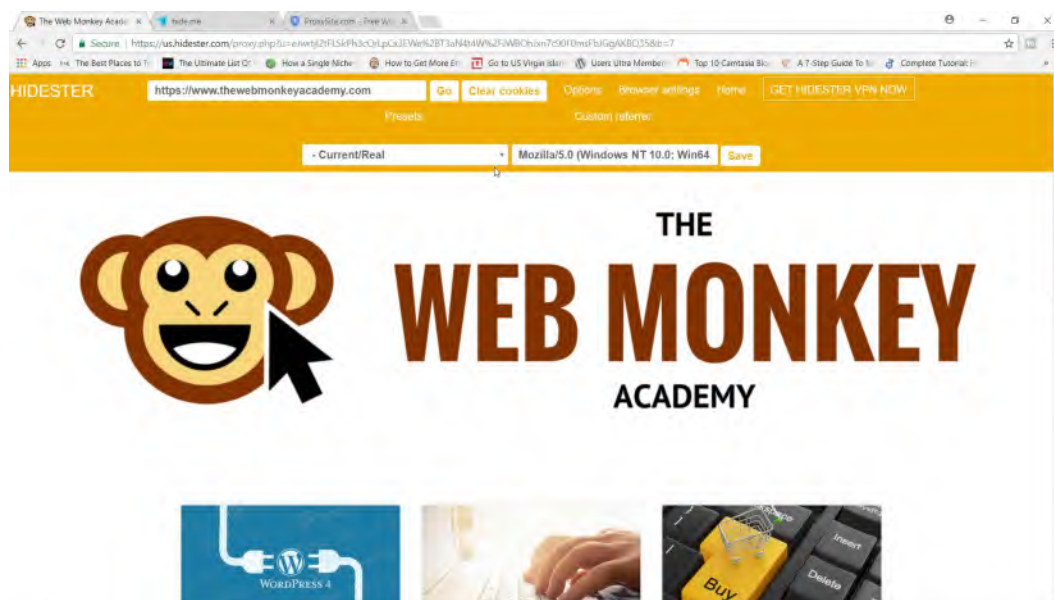


Figure 12.7: Demonstration of using the Hidester proxy service to access a website and modify browser and OS settings for privacy.

Another proxy server is hide.me, which is also free and excellent. When you visit the main site, hide.me, you will see a "free proxy" option. Click on "free proxy" to access the tool. You can choose from three different servers: one in the Netherlands, one in Germany, and one in the United States. Just like Hidester, hide.me gives you options to allow cookies, encrypt the URL, remove scripts, and more. You paste your target URL into the input field and then visit anonymously.

When you try to visit a site anonymously through hide.me, you may sometimes encounter a message saying that the server is currently busy and unable to process your request. This is a common issue with free proxies, as many people around the world use them, so occasional downtime or slow performance is to be expected.

Another popular option for accessing sites anonymously is [ProxySite.com](https://proxysite.com). You can use proxysite.com to easily access major platforms such as YouTube, Facebook, Twitter, and others directly from the [ProxySite.com](https://proxysite.com) interface. The proxysite.com homepage allows you to select an EU or US server. You also have quick access buttons for sites such as YouTube, Facebook, Twitter, Reddit, Imgur, and Google.

For example, if you click on YouTube, you can watch videos anonymously without needing to sign in. However, if you try to access Facebook, you will still need to log in with your credentials. This means that while proxies can hide your activity from your ISP, the site you log into, such as Facebook, will still know exactly what you are doing. You should always be aware of this limitation when using proxies.

Apart from these features, the process is similar to other proxies: you paste your URL, choose a server location (such as the United States or Europe), and click Go. Performance may vary; proxysite.com is not as fast as Hidester for example, but it still provides access to the desired site. You can also adjust privacy settings such as allowing cookies or removing scripts, just as with Hidester and hide.me.

NOTE

These three proxy servers, Hidester, Hide.me, and proxysite.com, are recommended for basic anonymous browsing. If you have experience with other proxies, you are encouraged to use them.

Now you will explore one of the most popular anonymizing tools available: a virtual private network or VPN.

VPN

You already walked through using VPNs on mobile devices in *Chapter 11*. VPNs are a fantastic way for enhancing security and also enhancing your privacy. A VPN changes the way your computer connects to the World Wide Web. A typical VPN topology includes your computer, the VPN server, and the internet.

Normally, your computer connects directly to the internet, but when you introduce a VPN server, the situation changes. Unlike a proxy server, a VPN server encrypts all the traffic between you (the client) and the VPN server itself. This means your requests, your IP address, and all data sent between you and the VPN server are encrypted.

The next diagram shows how the VPN server acts as an intermediary, encrypting the traffic between you and itself, while the connection from the VPN server to the internet is not encrypted:

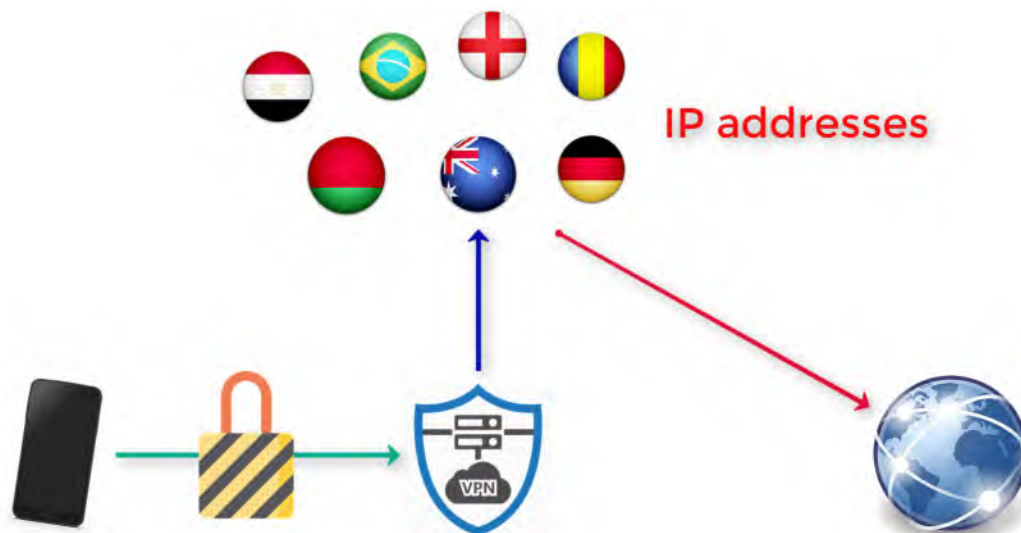


Figure 12.8: VPN connection

The communication between the VPN server and the internet is not encrypted, since the initial connection between you and the VPN server is already secure. This is one of the main ways a VPN server is more than a proxy server: it not only acts as an intermediary but also encrypts your traffic.

TIP

Keep in mind that while a VPN can provide optimal privacy in theory, it does not guarantee total privacy. This is an important limitation to remember.

Besides the obvious advantages of bypassing your ISP's restrictions and censorship, VPNs are also widely used in the business world. Employees can access their company's intranet from different cities or countries simply by using a VPN, making VPNs very popular for business use.

Although anonymizer services such as proxies or VPNs can often slow down your internet connection, there are cases where using a VPN can actually increase your speed. For example, a 2017 article from 9to5Mac reports that NordVPN confirmed that using a VPN can bypass Verizon's throttling of all video streams. Verizon, one of the largest ISPs in the United States, offers so-called unlimited plans, but in reality, these plans have bandwidth caps, especially for video services such as YouTube or Netflix. By using a VPN, you can bypass these caps and avoid throttling on your video streams.

We already discussed NordVPN in *Chapter 11* and how it is one of the most popular tools for protecting your identity online, especially on mobile devices. Now let's look at some other VPN offerings.

TunnelBear is a popular VPN service that provides a simple way to use VPN protection across computers and mobile devices. It allows you to connect to VPN servers in different locations, encrypting your internet traffic and masking your regular IP address.

The following figure shows the TunnelBear interface with a map of the world with various server locations marked, including Japan, India, Singapore, several countries in Europe, the United States, Mexico, Canada, and Brazil. The interface also displays your current data usage out of the 500 megabytes available for the month on the free plan, and offers an upgrade option for more data:

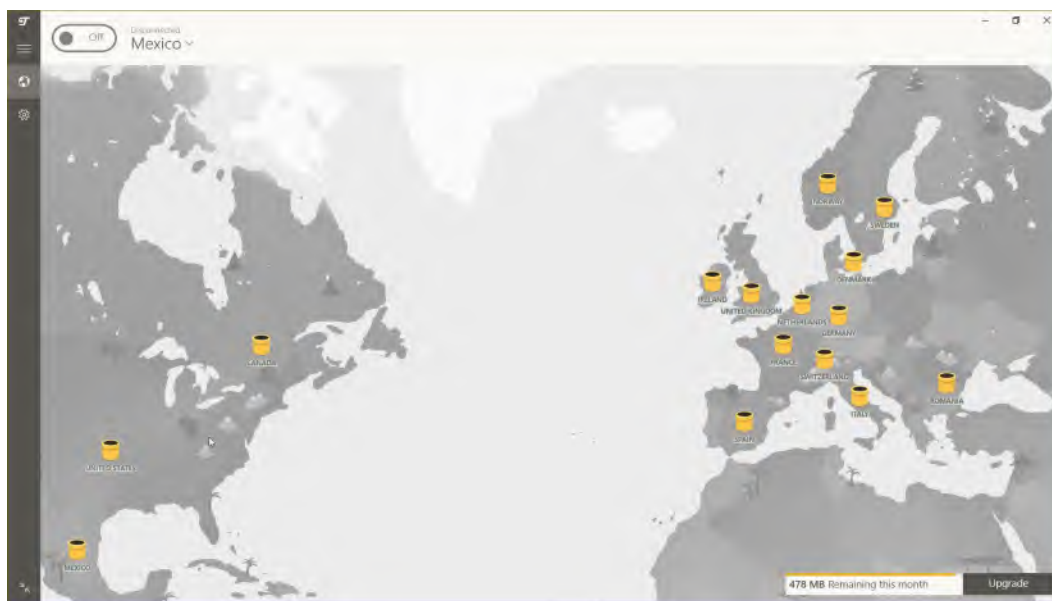


Figure 12.9: Geographic distribution of VPN servers across North America and Europe, showing available server locations for user connections.

This visual map helps you select which country you want to tunnel your connection through.

Additionally, in the TunnelBear settings, you can access options such as launching TunnelBear on start-up and doing a TCP override, but the most important settings are under the **Security** tab. Here, you find two very important features: VigilantBear and GhostBear:

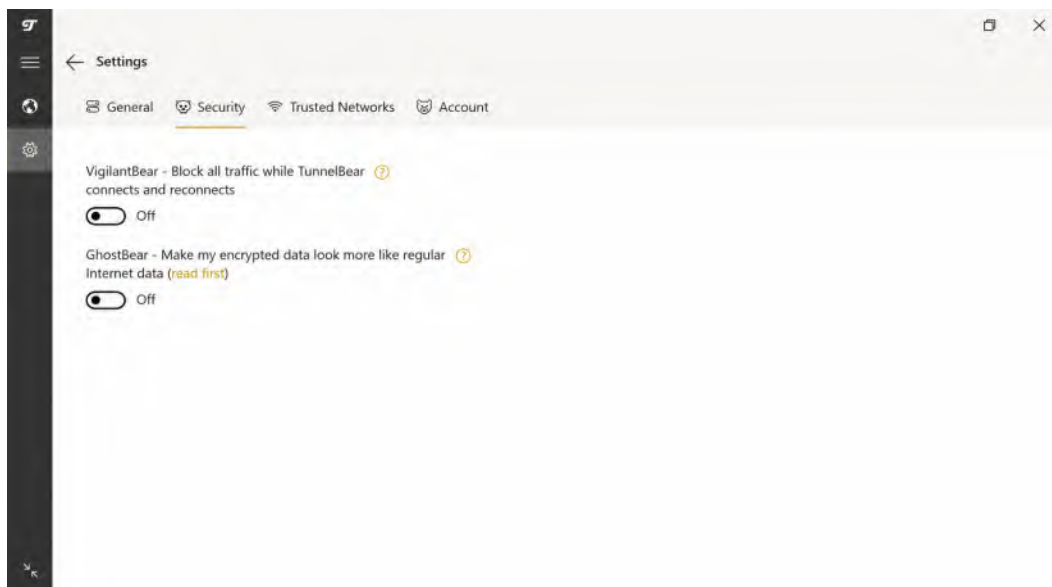


Figure 12.10: TunnelBear security settings showing VigilantBear and GhostBear options for enhanced VPN protection

VigilantBear blocks all traffic while TunnelBear connects and reconnects. This means that no internet traffic is allowed unless TunnelBear is fully activated and working. If your VPN loses connectivity and tries to reconnect, you do not want any internet traffic to leak during that period. Turning this on will really enhance your privacy.

GhostBear is a feature you should use only in specific situations. Sometimes, your ISP may recognize that you are using a VPN and block your connectivity because your traffic becomes encrypted. When you turn on GhostBear, TunnelBear makes your encrypted data look more like regular internet traffic, which can fool your ISP and help you connect. If you are trying to use TunnelBear and cannot connect to the internet, this is the ideal time to turn on GhostBear.

GhostBear is toggled on by default while VigilantBear remains off.

However, if you are using TunnelBear and connecting to the internet without any issues, you do not need to turn on GhostBear. Enabling it adds another layer of security but will slow down your internet speed even further.

You also have options for trusted networks and your account details, but these are less critical for basic use. TunnelBear is very simple to use, and you are encouraged to try out the free version to see whether it meets your needs. If you like it, you can upgrade to the paid version for more features and data.

Other VPNs you might consider are CyberGhost and PureVPN. CyberGhost is less expensive than NordVPN but not quite as good, though still a solid choice. PureVPN is reputed to be the fastest, though this is not confirmed personally. NordVPN remains the recommended favorite, but if you want a free option, TunnelBear is a great place to start.

VPN myths

A common myth is that a free VPN is just as good as a paid VPN. Many people wonder why you should pay for a VPN when there are free options available, but there are several reasons to consider a paid service. With a paid VPN, you get much larger data allowances, while free VPNs typically restrict you to 500 megabytes to 1 gigabyte per month.

Paid VPNs also offer faster speeds and better security, including stronger encryption; most free VPNs provide only 128-bit encryption, whereas paid VPNs can offer up to 256-bit encryption. In short, you get what you pay for: paid VPNs deliver better service, speed, and security.

Another myth is that VPNs always reduce your internet speeds. While it is true that VPN encryption can slow down your connection, with a paid VPN the speed difference is almost negligible. You should not worry that paying for a VPN will make your internet unusably slow. In fact, VPNs can sometimes increase your speed in specific situations, such as bypassing ISP throttling on video streams.

A third myth is that VPNs provide complete anonymity. This is not true. Even with strong 256-bit encryption, your activity can still be tracked; it is just much more difficult. Additionally, VPN providers often keep logs of user activity, which can be subpoenaed by a court.

Another important limitation is that the use of a VPN can be detected by observers such as your ISP or a nation-state. If someone is monitoring your traffic and notices that they cannot see the specific requests you are making, it becomes fairly obvious that you are using a VPN. This can prompt them to take further steps to investigate your activity. Additionally, some websites and services may suspend or block your account if they detect that you are connecting through a VPN.

Platform support also varies: some VPNs support Android, Windows, and Mac, while others may only support Windows. Latency is another factor, as VPNs with more servers distributed globally can offer lower latency, while those with servers only in the United States and Europe may result in higher latency if you are connecting from other regions.

To summarize, VPNs can provide you with a significant amount of privacy, but not complete anonymity. Not all VPNs are equal or safe. Some VPNs offer faster speeds but are more expensive, while others are cheaper but slower.

Another very popular tool for achieving anonymity online is Tor. Let's discuss this next.

Networked anonymizers

Networked anonymizers take anonymity a step further by routing internet traffic through multiple intermediary systems rather than relying on a single server. This makes it more difficult for any one point in the connection to link the user directly to their online activity.

One of the best-known examples of this approach is **Tor (The Onion Router)**, discussed below

Tor

Tor is widely recognized as a highly effective tool for providing anonymity when you are browsing the internet. Tor routes traffic through a network of independently operated servers, called relays, adding multiple layers of separation between you and the websites you visit.

To get started with Tor, go to torproject.org and click the Download Tor button. Tor is free and available for Windows, Linux, and Mac, so you should download the version that matches your operating system.

NOTE

Note that Tor is different from VPNs. While VPNs are primarily focused on privacy, Tor is focused on anonymity. This is a key distinction between the two tools.

On the Tor download page, you will find several important tips from the developers about using Tor safely, summarized below:

- First, always use the Tor browser. Tor does not protect all of your computer's internet traffic by default; it only protects applications that are specifically configured to send their traffic through Tor. To avoid configuration problems, you are strongly advised to use the Tor browser.
- Avoid torrenting over Tor. If you use torrents, do not use them with Tor, as this is not a good combination. For torrenting, you are better off using a VPN.
- Finally, do not enable or install browser plugins when using Tor. The Tor browser will block plugins such as Flash, RealPlayer, and QuickTime, because these can be manipulated to reveal your IP address.
- Always use HTTPS versions of websites. Tor will encrypt your traffic within its own network, but whether your traffic is encrypted all the way to the final destination depends on whether the website itself supports HTTPS. This is similar to how a VPN works: your traffic is encrypted between your computer and the VPN server, but from the VPN server to the internet, encryption depends on the website. To help with this,

Tor browser includes HTTPS Everywhere, which forces the use of HTTPS encryption with major websites that support it.

- Always disconnect before opening any files you have downloaded through Tor. Opening such files while online can reveal your real IP address, just as browser plugins can be manipulated to expose your identity.

Once you have downloaded and installed Tor, you will see the Tor browser icon. Click on the icon to launch the browser. You will be greeted with the Tor browser welcome screen, which confirms that you are now free to browse the internet anonymously.

To check that everything is working correctly, click the "Test Tor network settings" link in the center of the welcome page.

You will see a confirmation page stating, "Congratulations, this browser is configured to use Tor," along with the IP address that the world will see, which is not your real IP address:

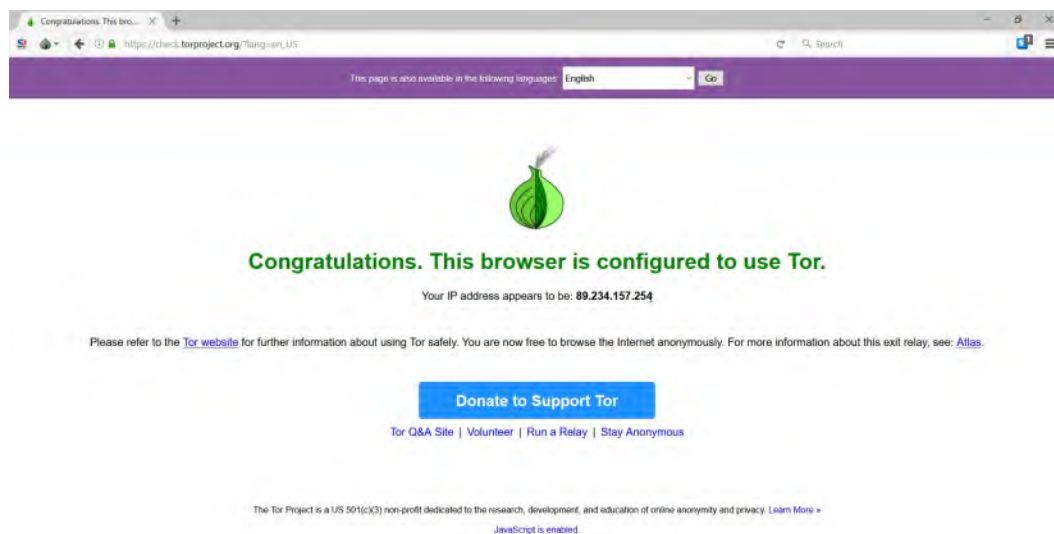


Figure 12.11: Confirmation page showing successful Tor Browser configuration and assigned exit node IP address for anonymous browsing

You can further customize your Tor network settings by clicking the onion icon and selecting "Tor network settings." Here, you will find three additional configuration options. If you are in a country where Tor is censored, such as China or Iran, you can check the first box to help with your connection. If you are using a proxy, enable the second option. The third box is for situations where your firewall only allows connections to certain ports. These settings help Tor determine the best way to connect in challenging environments. On the right, you will also see an "S1" indicator, which means HTTPS encryption is enforced everywhere, ensuring that every site you visit uses HTTPS.

If you want to further reduce the risk of someone discovering that you are using Tor, you can use Tor through a VPN.

Tor through VPN

In this setup, the initial request you make from your computer to the Tor network is encrypted, and this traffic passes through the Tor network to your VPN provider, which then relays your request to the internet.

The main advantages of this topology are that it bypasses all blocked exit nodes, your VPN provider will not see your real IP address (making you truly anonymous because the Tor network sits between your computer and the VPN server), and you are protected from malicious exit nodes due to the encrypted data entering and exiting the Tor network.

This encryption here is provided by your VPN server.

The main disadvantage is that the VPN provider can still see your traffic, so your privacy is not absolute. However, you do achieve real anonymity because your VPN provider does not know your real IP address.

To connect to Tor through your VPN using NordVPN, you need to use the specialty servers feature.

1. Go to the Countries tab in NordVPN.
2. Click on Specialty Servers.
3. Click on "Connect to Onion over VPN"

When you click this option, NordVPN will automatically select the best server for connecting you to Tor through your VPN. Refer to the following screenshot:

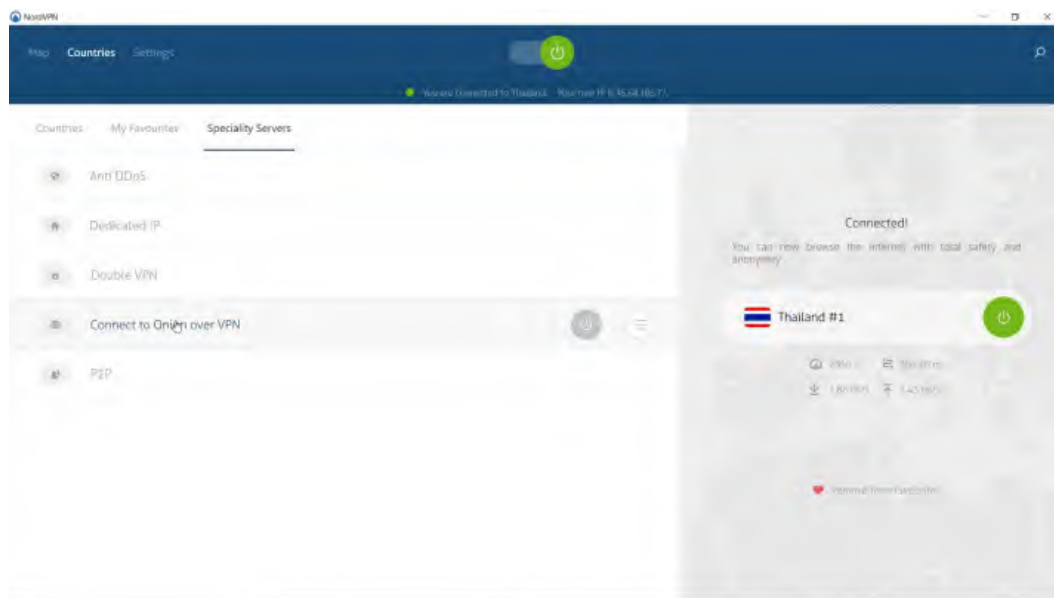


Figure 12.12: NordVPN interface showing specialty servers, including Onion over VPN, and connection status to a Thailand server

Connecting to your VPN through Tor is more secure, but very few VPN providers offer that service. Still, connecting to Tor through your VPN is a very secure way to browse online, and most VPNs with this feature have similar settings.

NOTE

You can also configure Tor to use a bridge relay instead of connecting directly to the public Tor network. This is only necessary if you are in a situation where it is critical to hide the fact that you are using Tor, such as in countries where Tor is censored. However, combining Tor with a VPN already provides a very high level of privacy and anonymity, so using a bridge relay is taking things to the extreme.

Now let's look at the actual Tor topology and how Tor works behind the scenes.

How Tor works

You are likely already familiar with the topology of a VPN, where your computer connects to a VPN server, which then connects to the internet.

This diagram shows how your Tor client (Alice) obtains a list of Tor nodes from a directory server as the first step:



Figure 12.13: Step 1 of how Tor works: Alice's Tor client obtains a list of Tor nodes from a directory server.

Once your computer has the list of possible paths, your Tor browser randomly selects one path to the destination server:

How Tor Works: 2

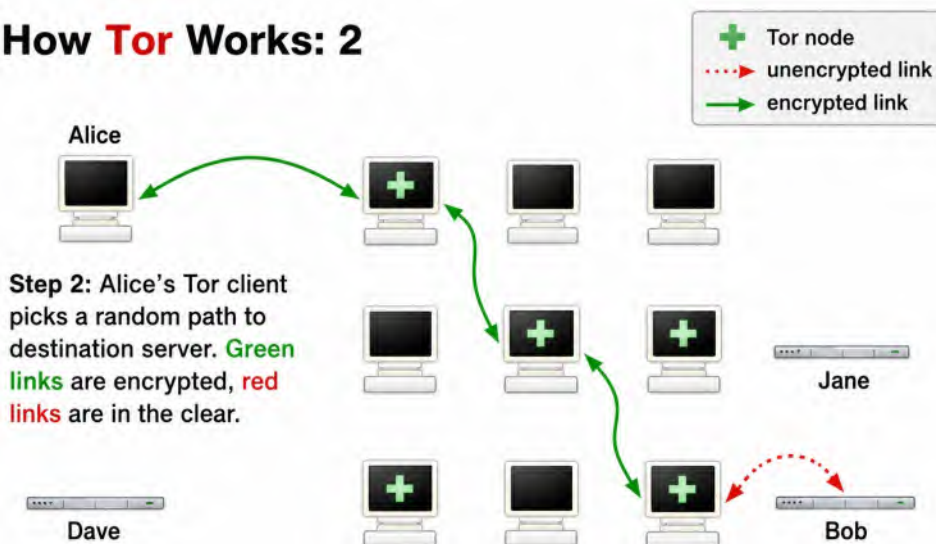


Figure 12.14: How Tor routes encrypted traffic through random nodes to reach a destination server

For example, if you are trying to reach facebook.com (represented by Bob), your traffic passes through several Tor nodes, with each link between nodes encrypted (shown with green arrows). The final link between the last Tor node (the exit node) and the destination server is unencrypted (red dotted arrow). This is similar to a VPN in that the last segment of the journey is not encrypted.

If you use Tor again, your client will choose a different pathway each time, ensuring that the same path is never reused. This dynamic routing is a core feature of how Tor maintains anonymity.

Tor weaknesses

Now that you've been introduced to Tor, you need to understand the major weaknesses of using this particular kind of technology.

The very first major weakness of using Tor is that if you use Tor, you could be marked as an extremist or a person of interest. For example, an article from Silicon Angle is titled "NSA's XKEYSCORE dissected: All Tor users marked as extremists." According to this article, the NSA has a rule in its XKEYSCORE program that marks all Tor users as extremists, regardless of their intent.

This policy is quite extreme, but when you think about it, you can understand where they are coming from. There are good people who use Tor purely for the reasons of staying anonymous,

but there are also bad people who use Tor to commit illegal acts like selling drugs or dealing in child pornography. Since authorities cannot differentiate between the intent of users, they unfortunately have to label every single Tor user as an extremist or a person of interest. Thus, it is advised to keep in mind that you do run the risk of being labeled as a person of interest if you decide to use Tor.

You should also know that the NSA and other intelligence agencies around the world are constantly looking for ways to make Tor less effective. There is a constant battle between the authorities, who want to make Tor ineffective, and the developers of Tor, who keep bringing out new ways to keep Tor as effective as possible.

The second major weakness of Tor is that it is complicated. There is a massive difference between just using Tor and actually using Tor effectively. In order to use Tor effectively, you need to have a deep understanding of how the internet and networks work.

Also, you need to have the necessary software to use Tor effectively. It is always recommended that if you are going to use Tor on a regular basis, do not install Tor on Windows or Mac, especially Windows, because the Windows operating system has a lot of loopholes. If you plan to use Tor constantly, install it on a Linux operating system, preferably **Debian Linux**. This is much more effective for you than using Windows.

Another major disadvantage of using Tor is that your accounts can be suspended, especially if your ISP has an agreement that allows them to suspend your account if you use Tor. They can do this if they detect Tor traffic. In addition, many websites simply block Tor users. If a website detects that your connection is coming from the Tor network, it will block your access. Examples of such sites include Craigslist, Nike, Hilton, Fox News, ShopClues, and Best Buy.

A news article from Naked Security by Sophos titled "Tor users being actively blocked on some websites," discusses how many sites now block Tor connections.

Tor attacks

Tor is also susceptible to attacks because whoever controls the exit node can see your request. If they also have access to your initial request to the entry node, they can figure out your identity. All these relays and nodes are managed by volunteers, so for Tor to work effectively, the volunteers who manage these nodes must be trustworthy.

The node that your request passes through before reaching the internet is called the **exit node**. The connection inside the Tor network is encrypted, but the final communication between the exit node and the internet is unencrypted.

If a hacker is able to access that unencrypted information at the exit node, they can potentially see your request. If they can also access the initial communication between your computer and the entry node, they can establish who you are by correlating the volume of transmitted data

or by comparing the timing of packet transmissions. This is known as an **end-to-end correlation attack**.

To protect yourself, you should always ensure your requests are encrypted. Always use **HTTPS** or **SSL** when making your initial request to the Tor entry node. This way, the entire communication is encrypted from start to finish, making it much harder for a hacker to figure out who you are, even if they control the exit node.

The developers have specifically addressed this kind of attack. According to the Tor blog, the Tor design does not try to protect against an attacker who can see or measure both traffic going into and coming out of the Tor network. Tor tries to protect against traffic analysis, where an attacker tries to learn whom to investigate, but it cannot protect against **traffic confirmation** (end-to-end correlation), where an attacker tries to confirm a hypothesis by monitoring the right locations in the network and doing the math. So, end-to-end correlation attacks are a known limitation.

Another type of attack is the **tagging attack**. In this attack, the attacker modifies the initial connection between your computer and the entry node and then checks if that modification appears at the other end, between the exit node and the internet. If the modification is present, the attacker knows the connection is from the original source they tagged, allowing them to establish your identity.

Anonymizers and the dark web

The **dark web** is a small, intentionally hidden part of the deep web. It generally requires specialized software such as Tor. The dark web can be used for legitimate purposes, such as avoiding censorship, protecting journalists and sources, or communicating privately, but it is also associated with illicit marketplaces and other criminal activity.

NOTE

The terms **deep web** and **dark web** are often confused. The deep web is simply any part of the internet that isn't indexed by ordinary search engines such as Google or Bing. Most of it is completely normal and something we use every day. Your email inbox, online banking account, private cloud storage, subscription content, and an organization's internal systems can all be part of the deep web because you cannot find their contents through a Google search.

Anonymizers such as Tor allow you to access hidden services on the dark web. You begin by navigating to a **Pastebin** page containing a list of deep web links. Some links, such as Kamagra for Bitcoins, are accessible, and display a page where you can buy Kamagra tablets in exchange

for Bitcoin. Bitcoin is often the only accepted payment method for services on the dark web, reinforcing the importance of cryptocurrency for anonymous transactions.

You also encounter links to Project Evil, Discounted Electronics Goods, UK Guns and Ammo, and the Hitman Network. Not all links are functional; some sites fail to load, which can happen for various reasons.

As you continue scrolling, you may find additional links such as an open letter to revolutionaries, anonymous forums, and Swiss email services. This demonstrates the diversity of content and services available through anonymizers on the deep web.

The following figure shows the Pastebin page listing various deep web links, including Bitcoin Laundry, Counterfeit US Dollars, and High-Quality Tutorials:

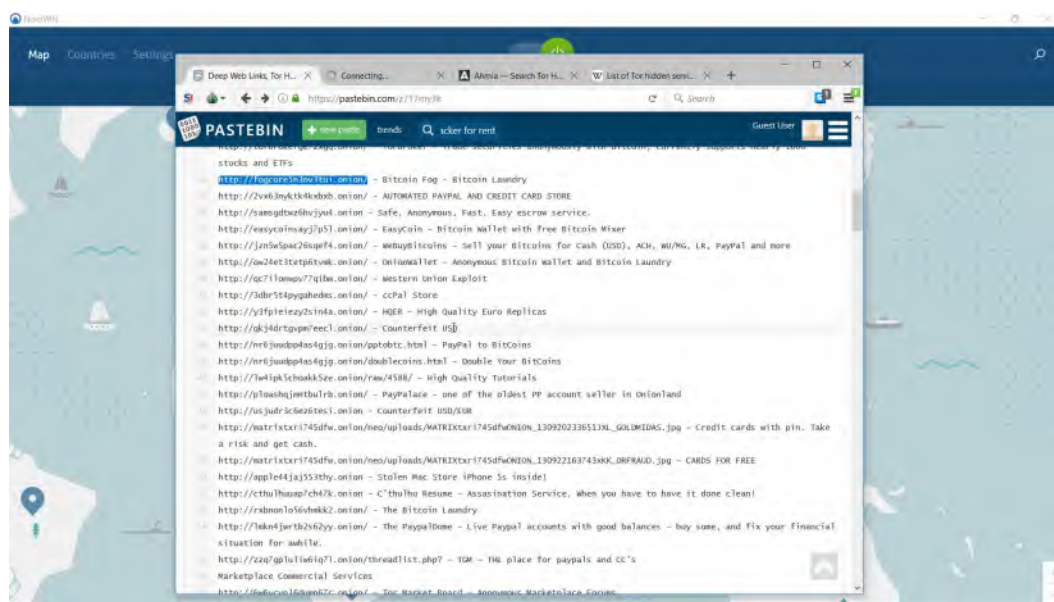


Figure 12.15: List of dark web links advertising illegal goods and services, such as counterfeit currency, hacking, and illicit marketplaces

Search tools such as ahmia.fi can also help you find dark web links to various services. Further, Wikipedia maintains a categorized list of Tor hidden services. These resources allow you to search for specific types of services, such as hacking, commerce, or whistleblowing, and access a wide range of dark web links. As a cybersecurity specialist or someone interested in online safety, you should be aware that these services exist and understand how people find and use them, even if you do not intend to participate yourself.

Other anonymizing services

There are websites that allow you to do various activities anonymously. The very first one here is FreeNet. **Freenet** is a decentralized, peer-to-peer network designed to let people publish and retrieve information with greater privacy and resistance to censorship.

Unlike the normal web, where you typically connect to a particular server that stores a website, Freenet distributes encrypted pieces of information across computers participating in its network. There is no single central server that authorities or other parties can simply shut down to remove the information. You can download and install FreeNet, which allows you to browse websites, post questions in forums, and you can do all of these anonymously.

The FreeNet homepage, highlights its features for censorship-resistant communication and publishing:

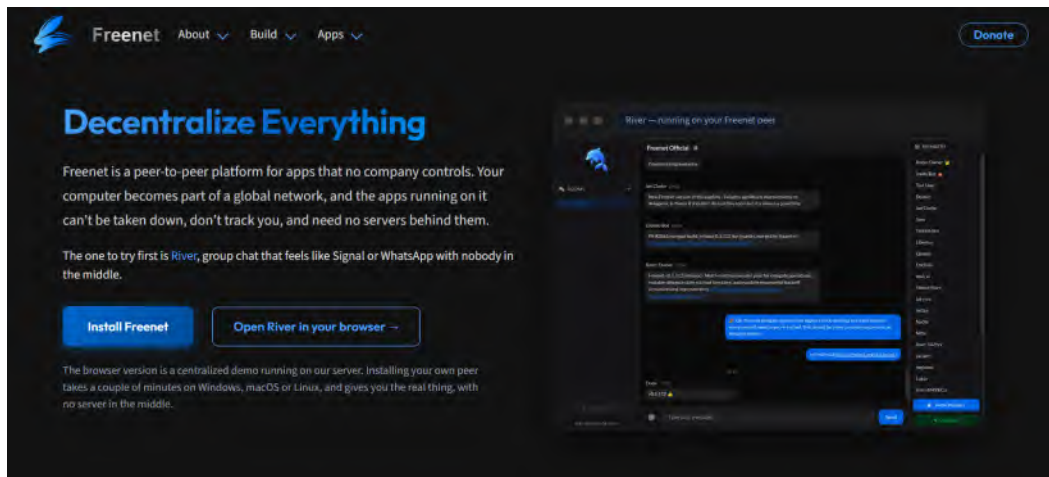


Figure 12.16: Freenet website explaining its features for anonymous and censorship-resistant communication and browsing

Next is I2P, also known as the Invisible Internet Project. It basically allows you to do everything online anonymously. I2P is a software that you can download and install, and it's available on Mac, Linux, Debian, and also on Android.

Here is the main page for the Invisible Internet Project, where you can download the latest version and read about its privacy features:

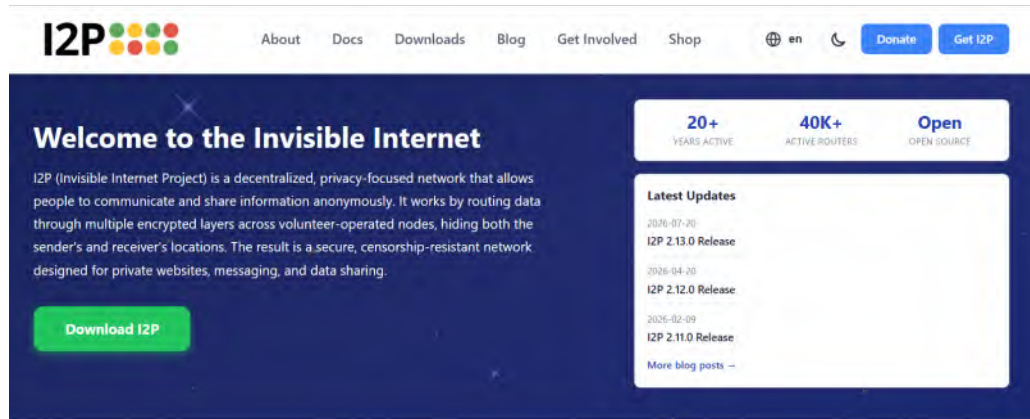


Figure 12.17: I2P homepage

One of the best services you can get with I2P is email. You can actually send and receive emails anonymously. It may take a while to load, but once it does, you can create an account with I2P mail and use it for anonymous communication. I2P also supports torrents. You can click on torrents, add torrents, create torrents, and download files as well.

I2P also has hidden services of interest, which you can browse. However, you can't just open them directly; you need to use a certain service to access these hidden services. If you have been following along, you should know which service you need to run to open these hidden services of interest.

Next is **OneSwarm**. It is a peer-to-peer (P2P) file-sharing system designed to provide more privacy than traditional BitTorrent-style sharing.

Instead of making files and participants openly visible to everyone in a swarm, OneSwarm allows users to create **friend-to-friend (F2F) networks**. You connect to trusted contacts, and content can be transferred through intermediate peers. This makes it harder for participants to determine the original source or final recipient of a file. The limitation is that if you are on Windows 10, you are out of luck because there is no version for Windows 10 or higher. However, it is available for Windows 7, Vista, XP, Mac OS X, and Linux (both 32-bit and 64-bit), so you might want to take a look at this software.

Last but not least is **RetroShare**, which is considered one of the very best of the bunch. Think of RetroShare as a kind of private Facebook, where you can share pictures, communicate with your friends and family, and not have to worry about third parties spying on your photos or invading your privacy. RetroShare is highly recommended if you want to quit Facebook and still have an encrypted, private social media platform for posting photographs and staying in touch with people you trust. You can chat, send email, share files, post links, participate in forums, and more, all within a secure environment. RetroShare stands out as one of the very best options among privacy-focused social platforms.

Summary

In this chapter, we explored how to protect your privacy and anonymity online. We distinguished between privacy, anonymity, and pseudonymity; examined identity compartmentalization and common tracking techniques such as cookies, browser fingerprinting, and cross-device tracking; and looked at ways to detect and limit tracking. We also explored the capabilities and limitations of incognito mode and anonymizing tools, including VPNs and Tor.

The key takeaway is that no single tool makes you anonymous or completely private online. Effective privacy comes from understanding what you are trying to protect, recognizing how your activities can be tracked or connected, and combining appropriate tools with careful online habits. With this foundation, you can make more informed decisions about what you expose online and how you protect your digital identity.

In the next chapter, we will shift from protecting your privacy online to protecting the devices, networks, and information you use every day. *Chapter 13* will take you through maintaining security at home and at work.

13

Cybersecurity at Home and Work

Cybersecurity at home and work is about more than just installing antivirus software or setting strong passwords, it requires a clear understanding of how organizations and individuals protect both virtual and physical assets from a wide range of threats.

By the end of this chapter, we will be able to identify the essential policies and plans, such as the **security policy**, **bring your own device (BYOD)** policy, **incident response plan**, and **disaster recovery plan**, which form the backbone of effective cybersecurity, and distinguish between device deployment models such as **BYOD**, **company-owned, business-only (COBO)**, **company-owned, personally enabled (COPE)**, and **choose-your-own-device (CYOD)**.

Along the way, we will explore the **security** versus **Ease of Access Paradox**, learning how organizations balance the need for strong protection of their systems, data, and other assets with the practical demands of daily work. Mastering these concepts matters because the right combination of policies and deployment models not only shields sensitive data from attackers but also ensures that employees can work efficiently without unnecessary barriers, ultimately supporting both productivity and security.

In this chapter, we will cover the following topics:

- **Organizational cybersecurity policies and plans**
- **The BYOD phenomenon in the modern workplace**
- **The security versus Ease of Access Paradox**

Organizational cybersecurity policies and plans

Cybersecurity at the workplace depends on clear policies and plans that define how you protect both data and physical assets from threats. In this section, you will explore the security policy and the questions it must address. Then, you will take a quick look at the **BYOD** policy, **incident response plan**, and **disaster recovery plan**.

A security policy is a general written document that describes how an organization protects its virtual and physical assets from threats. Cybersecurity is not just about protecting data; you also need to protect servers, hard disks, and other physical devices that may contain information. It lays out the ground rules for areas such as who can access data, how employees prove their identity, what constitutes acceptable use, and how the organization's assets are kept safe.

Your typical security policy will answer questions such as:

- **Assets:** What assets need to be protected?
- **Data access:** What kinds of data can employees access? For example, if you are in the marketing department, can you access data from the finance department?
- **Access methods:** How can employees access the data? Do they need to provide a password or a security key?
- **Data usage:** What can employees actually do with the data? Can they copy data to USB drives? Are they allowed to use USB drives at all?
- **Internet access:** Can employees access the internet freely? For example, are they allowed to go on YouTube or use social media while in the office?
- **Password policy:** How often must passwords be changed?

A security policy addresses just a sample of the questions listed above. A full security policy will go beyond these examples. Along with a general security policy, organizations also put more specific policies and plans in place to handle particular security needs.

A **BYOD policy** describes how employees are able to use their own personal devices to access company data in a safe and secure manner. You will look at BYOD policy in more detail in the next section.

An **incident response plan** is a set of policies and procedures used to identify, contain, and eliminate cyber attacks. The objective of an incident response plan is to allow an organization to quickly detect and stop cyber attacks, and also to prevent the same kinds of attacks from happening again in the future.

A **disaster recovery plan** focuses on the restoration of critical systems after a disaster.

A disaster can be anything from a fire to an earthquake, or even a very serious cyber attack. The purpose of a disaster recovery plan is to describe how your company can recover effectively and how quickly you will be able to resume work after such disasters. While there are additional policies and plans, such as a business continuity plan, the four policies and plans described in this section are among those you will commonly encounter in organizations.

Now that you understand the role of common cybersecurity policies and plans, let's take a closer look at the BYOD phenomenon.

The BYOD phenomenon in the modern workplace

The term **BYOD**, as we established in the introduction of this chapter, stands for "*bring your own device*." This refers to a phenomenon in the modern workplace where employees are able to perform work tasks on their personal devices. For example, you might send work emails from your mobile phone, or download sensitive documents to your laptop or tablet and take that work home. It is extremely common today, as most people use mobile phones, laptops, and tablets for both personal and work-related activities.

There are clear pros and cons to BYOD. The main advantage is improved efficiency: you can work from various locations, without needing to be physically present at your workplace or tied to a company-assigned computer. You might be at lunch, commuting on a bus, or at home, and still be able to send emails or complete tasks from your personal device. The main disadvantage, however, is that it opens up new security vulnerabilities.

If you are responsible for security in your company, you might have already secured your local network, installed antivirus software on all computers, set up firewalls, and implemented security policies. However, a major challenge arises when employees use their own personal devices for work. These devices do not belong to the company, so you need to create a security policy that restricts how employees use their personal devices for work purposes. In many organizations, this is often overlooked, and employees are simply allowed to download company documents to their phones or laptops and work from home. This is the main risk associated with the BYOD phenomenon and the BYOD policy: while it increases efficiency by allowing employees to work from anywhere, it also introduces a new gateway for security vulnerabilities.

Organizations can manage these security vulnerabilities in different ways depending on who owns the device and how it can be used. Before examining the structure and key elements of a BYOD policy, let's look at three other common device deployment models: COBO, COPE, and CYOD.

COBO, COPE, and CYOD

With the COBO (company-owned, business-only) model, the company provides you with a device, such as a laptop, which is strictly for business use. The device remains the property of the company, and you are only permitted to use it for official work activities. Access to personal sites such as Facebook or YouTube is not allowed, except when required for business-related tasks. This approach is extremely strict, with devices preconfigured by the IT security team to include anti-malware, encryption, and other necessary security tools. COBO generally provides

organizations with greater security control because the company maintains full control over the device and its configuration.

In the COPE (company-owned, personally enabled) model, the device is still owned by the company, but you are allowed some personal use. While the laptop or mobile device is primarily for business, you can check your social media account or do some personal web browsing. The idea behind COPE is to improve employee productivity by allowing some personal use of company-owned devices, such as checking Instagram or Facebook during short breaks, which can help you feel more comfortable and potentially improve your work performance.

CYOD (choose your own device) is by far the least common deployment model. Not many companies have the resources to let you choose your preferred device. In this model, the company typically offers several types of laptops or mobile devices running operating systems such as Windows, macOS, iOS, or Android. Because the devices are company-owned, the organization can configure and manage them according to its security requirements, such as by applying security updates, encryption, and access control. However, supporting multiple device types and operating systems can increase the complexity of device management and security. This approach is usually found in larger organizations that have the budget and resources to support multiple device options, allowing you to select the device with which you are most comfortable.

Of the four deployment models, BYOD, COBO, COPE, and CYOD, BYOD is the most popular, while CYOD is the least popular.

Now that you've seen how these device deployment models stack up, let's circle back to BYOD and look at how organizations can put together a policy to handle their security challenges.

Sample BYOD policy structure

A sample bring your own device (BYOD) policy helps you understand how organizations write policies and what elements they include. Even if you do not plan to become a security specialist, it is useful to see a real-life example and gain a basic understanding of the policy structure.

A BYOD policy must address both company and employee concerns. The company is primarily worried about new security vulnerabilities that may arise when employees take work home on personal devices. On the other hand, employees are concerned about how much control over their personal devices they must relinquish. The policy needs to strike a balance between security and ease so that security concerns are addressed while still allowing employees to work effectively with their mobile devices.

When writing a BYOD policy, it is essential to start with the basics before getting technical.

The first step is to determine what devices will be permitted and who will be allowed to use them. Decide whether you will allow only mobile phones, or if laptops and iPads are also included.

Once you have determined which devices are permitted and who is allowed to use them, you need to decide which employees or departments will have access. For example, will only senior executives be allowed to use personal devices, or will entry-level workers and specific departments such as accounting also be included? These foundational questions must be addressed at the outset.

Next, specify the types of company data that employees can access on their personal devices. Decide whether all company data will be accessible or whether only certain categories will be accessible. This step ensures that you are still covering the basics before moving into more technical requirements.

You must also clearly state the company's rights regarding access, monitoring, and deletion of information on employee-owned devices. Employees need to understand that the company will have some level of control over their personal devices, and there must be a mutual agreement about these rights.

The policy should then explain how the company will protect employees' personal data. A BYOD policy is not only about safeguarding company interests but also about protecting employees. Describe whether personal data will be backed up, encrypted, or otherwise secured so that, for example, if a device is stolen, personal information remains protected.

Once these basics are established, you can move on to technical measures such as deploying **mobile device management**. At this stage, you might require that hard drives or memory cards be partitioned into two sections: one for personal data (like photos and videos) and one for work data. This separation helps protect both company and personal information.

You should then enforce the use of strong passwords, require up-to-date anti-malware on all devices, and set up automatic lockout after periods of inactivity. These security measures apply to every permitted device, regardless of type.

Establish protocols for lost or stolen devices. Decide what actions will be taken if an employee's laptop or phone is stolen. For example, you might require encryption so that if a device is lost, you can remotely destroy company data to prevent unauthorized access.

Finally, develop the BYOD policy in partnership with IT, risk management, and legal counsel. Writing an effective policy is not a solo effort; it requires input from all relevant departments to ensure the policy is practical, enforceable, and legally sound.

You must ensure that any security policy you create is defensible in court, especially if an employee challenges it legally. Always revise your current policies and protocols regularly.

Security policies are not static; they may need updates as often as every week or month due to new technologies and evolving hacking methods. Continually update your policies to keep pace with changes in technology and workplace security needs.

As the BYOD policy demonstrates, keeping organizational data safe often means putting some limits on how employees can access and use that data. But at the same time, these limits shouldn't make it too hard for people to get their work done. This need to balance protection with usability leads to a broader cybersecurity challenge that we will look at next.

The security versus ease of access paradox

Security professionals must constantly weigh the balance between strong security and convenient access to work files.

Imagine you arrive at your desk and need to access important files. Before you can start work, you must log in to your computer using your username and password.

After entering your credentials, you are prompted to provide a four-digit **PIN (Personal Identification Number)** sent to your mobile device, adding a second layer of security through two-factor authentication. Once you have logged in, you navigate to the folder containing your work files, but before opening it, you must enter yet another password because the folder is password protected. This third defense makes unauthorized access extremely difficult. However, as an employee who needs to access those files, you might find it frustrating if you have to wait several minutes for an SMS (short message service) to arrive or enter yet another password before you can finally open your work documents.

The security versus Ease of Access Paradox is a challenge you will encounter whenever you try to protect sensitive data while still allowing people to do their work efficiently. From a security perspective, multiple layers of protection are excellent for keeping unauthorized users out. However, these same controls can make it more difficult for legitimate users to access the resources they need.

Additional restrictions, such as preventing employees from sharing files or copying them to USB drives to work from home, can further strengthen security but may also make the employees' jobs more difficult. This is the essence of the security versus Ease of Access Paradox: increasing security can make access more difficult for legitimate users, while reducing security can make resources more accessible to potential attackers.

When your company's cybersecurity team creates security policies or deploys new controls, they must balance these competing needs. You do not want to make access so difficult that employees spend five or ten minutes just trying to open a file, but you also cannot make it so easy that a hacker only needs a username to get in. Finding the right balance between security and usability is therefore an ongoing challenge for cybersecurity professionals.

You might find yourself asking, *"Why do I have to provide this? I just want to do my work."* This happens frequently because you generally want convenient access to the resources you need, while security specialists need to ensure that those resources remain protected.

Summary

In this chapter, you learned about the key policies and plans that organizations use to protect their data and physical assets, including security policies, BYOD policies, incident response plans, and disaster recovery plans. You also explored the kinds of questions a security policy should answer and why allowing employees to use personal devices for work can introduce additional security risks.

Next, you looked at the COBO, COPE, and CYOD deployment models and how each gives organizations a different level of control over the devices employees use. You also walked through a sample BYOD policy and learned what organizations need to consider when allowing employees to access company data from their personal devices.

Finally, you explored the security versus ease-of-access paradox and saw why adding more security is not always as simple as it sounds. Strong security controls can help keep attackers out, but they can also make it harder for employees to do their jobs. Finding the right balance between security and usability is an important part of protecting an organization while still allowing people to work efficiently.

In Chapter 14, you will look ahead at how AI is changing cybersecurity, including the opportunities, risks, and ethical challenges it brings.

14

Looking Ahead

As **artificial intelligence (AI)** becomes increasingly prominent in cybersecurity, we face new questions about how these technologies will shape the future of digital defense and risk. In this chapter, we will explore and identify the emerging challenges and opportunities that AI brings to cybersecurity. We will discuss the risks of bias in AI cybersecurity systems, the promise and pitfalls of automated incident response, and the ethical considerations around privacy and AI model training. We will also learn how tools and techniques such as ethical hacking, regulations and AI in cybersecurity, and the evolving roles of security analysts interact with longstanding applications such as threat detection, malware analysis, and behavior analysis, as well as newer developments such as ChatGPT and DeepSeek.

Understanding these distinctions and the practical implications of AI's dual use, both defending against and enabling cyber threats, will prepare us to navigate a future where the boundaries between human expertise and machine intelligence are continually redrawn.

In this chapter, we will cover the following topics:

- Applications of AI in cybersecurity
- Malicious uses of AI by cybercriminals
- Ethical and responsible use of AI in cybersecurity
- Future trends in AI and cybersecurity

Applications of AI in cybersecurity

AI is now a very prominent topic, and you see it everywhere, from ChatGPT to DeepSeek and other AI tools. It is important to understand the relationship between AI and cybersecurity, especially as AI becomes more integrated into daily technology conversations. It is used in cybersecurity, including threat detection, malware analysis, behavior analysis, and the newer area of automated incident response.

In **threat detection**, using AI allows you to identify threats in real time. AI-powered tools are also used for **malware analysis**, helping you analyze different types of malware efficiently. With **behavior analysis**, AI helps you detect unusual activity, such as fraud detection, by identifying patterns that deviate from the norm. These applications are not new; cybersecurity professionals have used AI for these purposes for almost two decades.

While AI these have been around for a long time, **automated incident response** is a newer development. Automated incident response means that when a company experiences a cyber-attack or data breach, you can now use AI to speed up your reaction and combat such threats more quickly. This represents one of the newer ways professionals are applying AI in cybersecurity.

You encounter artificial intelligence in cybersecurity through several familiar tools and services. For example, AI is used in spam filtering, which has been around for a very long time. You also see AI in fraud detection systems, such as those used by banks to spot suspicious transactions. AI-powered antivirus software, like Kaspersky and Bitdefender or Windows Defender, uses machine learning to identify and block threats. Additionally, chatbots are now being used to provide security support, helping users resolve issues and answer questions about cybersecurity.

Malicious uses of AI by cybercriminals

Cybercriminals are also taking advantage of AI to generate more convincing phishing emails that are personalized and smarter, making them harder to detect. Deepfakes and misinformation campaigns are another growing concern, with AI being used to create realistic fake videos and audio. Automated hacking tools now use AI to drive brute-force and password-cracking attacks, increasing their effectiveness.

AI-powered malware is particularly concerning because it can adapt to a computer system's defenses. These advanced malware programs infect a computer, analyze how the anti-malware product reacts, and learn to evade detection by adapting their behavior. For example, an AI-powered malware might notice when a particular antivirus program tries to quarantine it, then automatically change its code or behavior to avoid being recognized the next time.

This ability to learn and adapt makes it much harder for traditional security tools to keep up. Moreover, it's not just theoretical. Let's look at some real-world case studies that have already shown how AI can be used for malicious purposes.

Arup Deepfake financial scam

A high-profile case from 2024 involved a company called Arup, which specializes in architectural design. One of their employees in Hong Kong transferred \$25 million to fraudsters after being deceived by a sophisticated scam.

The employee received a suspicious email from the **chief financial officer (CFO)** requesting participation in a secret transaction, which immediately raised doubts. Despite his suspicions, he joined an online video call where he saw what appeared to be the CFO and other employees. The meeting felt authentic, with everyone behaving as expected, which convinced him to proceed. In reality, the CFO and the other attendees were deepfakes, artificially generated by cybercriminals who had clearly studied the real individuals and orchestrated a convincing, well-planned attack.

The important details worth noting in the Arup case are the suspicious email address initially used to contact the employee, a convincing video call, and the ultimate deception using deepfakes. The fraudsters did not use the real CFO's email address, but instead an address that looked similar, much like what you see in typical phishing emails. If the employee had paid closer attention to the sender's email, they might have realized the invitation was fake. However, the deepfakes used in the video call were so convincing that the deception succeeded. This indicates that scrutinizing suspicious email addresses as early as possible is important in detecting deepfake-driven scams.

The Brad Pitt romance scam

Another real-world example involves a case from January 2025, where a French woman was deceived by a scammer impersonating the well-known Hollywood star, Brad Pitt. The scam began when the victim was contacted on Instagram by someone claiming to be Brad Pitt's mother. The story presented was that Brad Pitt was in the hospital and needed money for medical bills. The scammer claimed that, due to a divorce case with Angelina Jolie, Brad Pitt's phones were frozen, and he could not access his funds, so he needed help. This supposed relationship between the victim and the scammer lasted about 18 months and the victim sent about \$850,000 to the scammer over this period.

Deepfakes can be extremely convincing to the point that it's clear and alarming how AI-driven technologies such as deepfakes can be used to manipulate and exploit individuals, and are difficult to detect. As these tools become more sophisticated, it becomes increasingly important to consider how AI can be used both ethically and responsibly in the field of cybersecurity.

Ethical and responsible use of AI in cybersecurity

While AI is extremely powerful, there are significant challenges and ethical responsibilities that AI companies must address. One of these is the risk of **bias** in AI cybersecurity systems. If the data that an AI model is being trained with is biased, the model itself will produce biased responses and answers.

For example, if an AI system is trained mostly on network traffic from large financial institutions, it might fail to recognize phishing techniques that target small businesses simply because it differs from the data it knows. This can cause the system to miss real attacks or generate unnecessary alerts, both of which are consequences of bias in the training data. This can lead to a significant risk of generating false positives or false negatives in your cybersecurity systems, simply because of the bias present in the AI model.

Ethical hacking and responsible AI deployment

AI should be used responsibly for **ethical hacking**, meaning you use AI to test and improve security in a way that is ethical and does not cause harm. For instance, as an ethical hacker, you might use AI tools to scan your company's network for vulnerabilities and help fixing security gaps before attackers can exploit them. This kind of testing is done with permission and aims to strengthen defenses rather than cause harm.

Meanwhile, it is important for you to be aware that cybercriminals use AI for malicious purposes. This makes it important for communities and countries to have clear rules about the same. Hence, there is a strong need for **regulations and ethical guidelines** regarding the use of AI in cybersecurity. The European Union has the **General Data Protection Regulation (GDPR)**, which requires companies to explain how their AI systems make decisions and protect personal data when using AI for cybersecurity. In the United States, the **National Institute of Standards and Technology (NIST)** has published guidelines that set standards for transparency and fairness in how AI is used to detect and respond to cyber threats.

Another important point is **privacy**. Many AI models require large amounts of user data for training, which can include sensitive information such as addresses and bank accounts. When AI companies use real user data to train their models, there is a risk that this information could be exposed or misused. To address this, many organizations use techniques like data anonymization, where identifying details are removed before the data is used for training. Some also use synthetic data or limit access to sensitive information to reduce the risk of exposure.

Balancing the benefits of AI with ethical considerations is an ongoing challenge in cybersecurity. As technology continues to evolve, it is important to adapt your practices to protect privacy and maintain trust. With these ethical and practical concerns in mind, let's look ahead to understand how AI is shaping the future of cybersecurity.

Future trends in AI and cybersecurity

The future of artificial intelligence in cybersecurity is a very exciting topic. And you are likely wondering whether AI will eventually replace human cybersecurity experts and what the future of AI-driven security will look like. Let's explore these questions and consider how AI's influence is expanding not just in cybersecurity, but across many industries.

Certain job roles in cybersecurity, such as junior level security analysts, are likely to be obsolete in the near future because AI tools can now do the exact same job quickly and efficiently. However, there are still many cases where human expertise will be needed for specific jobs, tasks, or roles within cybersecurity, such as interpreting ambiguous security incidents, making judgment calls in complex ethical situations, or designing creative security strategies. These areas depend on the logic, rationality, and decision-making qualities of humans that AI cannot replace.

Remember that you are advancing your career in cybersecurity, which is rapidly evolving with the integration of artificial intelligence. You are going to see AI-driven security not just in cybersecurity, but in almost every area including entertainment, communication, transportation, medical care, and more.

Summary

In this chapter, we established how artificial intelligence, through tools, is transforming cybersecurity by enabling advanced threat detection, malware analysis, and automated incident response. Starting from foundational applications such as behavior analysis and spam filtering, we examined malicious uses such as phishing, deepfakes, automated hacking tools, and adaptive AI-powered malware. We also discussed real-world case studies of the Arup deepfake financial scam and the Brad Pitt romance scam. This chapter equipped us with a comprehensive understanding of both the protective and malicious roles of AI in cybersecurity, as well as the ethical, regulatory, and privacy challenges that must be navigated as these technologies continue to evolve.

15

Unlock Your Exclusive Benefits

Your copy of this book includes the following exclusive benefits:



DRM-Free PDF Version

Download DRM-free PDF and ePub copies of this book.



7-Day Packt Library Access

Get 7-day unlimited access to 8,000+ books and videos. No credit card required.

Available for first-time Packt+ trial users only.



Next-Gen Reader Access

Read this book on Packt Reader with progress sync, dark mode and note-taking.

Follow the guide below to unlock them. The process takes only a few minutes and needs to be completed once.

Unlock this Book's Free Benefits in 3 Easy Steps

Step 1

Keep your purchase invoice ready for *Step 3*. If you have a physical copy, scan it using your phone and save it as a PDF, JPG, or PNG.

For more help on finding your invoice, visit <https://www.packtpub.com/en-us/unlock?step=1>.

Note: If you bought this book directly from Packt, no invoice is required. After *Step 2*, you can access your exclusive content right away.

Step 2

Scan the QR code or go to [packtpub.com/unlock](https://www.packtpub.com/unlock).



On the page that opens (similar to *Figure 15.1* on desktop), search for this book by name and select the correct edition.

Unlock Your Book's Free Benefits

Bought a Packt book from Amazon or one of our channel partners? Unlock your free benefits in 3 easy steps.

Find Your Book Sign Up or Sign In Upload Purchase Proof

Need Help?

✦ 1. Find Your Book

Search by title or ISBN

✧ 2. Sign up (Free) or Sign In

📎 3. Upload Purchase Proof

Search for your book here

Figure 15.1: Packt unlock landing page on desktop

Step 3

After selecting your book, sign in to your Packt account or create one for free. Then upload your invoice (PDF, PNG, or JPG, up to 10 MB). Follow the on-screen instructions to finish the process.

Need Help?

If you get stuck and need help, visit <https://www.packtpub.com/unlock-benefits/help> for a detailed FAQ on how to find your invoices and more. This QR code will take you to the help page.



Note: If you are still facing issues, reach out to customercare@packt.com.



packtpub.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

At www.packtpub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:



Cybersecurity Beginner's Guide

Joshua Mason

ISBN: 9781836207474

- Master the fundamentals of cybersecurity and why it's crucial
- Get acquainted with common cyber threats and how they are countered
- Discover how cybersecurity impacts everyday life and business
- Explore cybersecurity tools and techniques used by professionals
- See cybersecurity in action through real-world cyber defense examples
- Navigate Generative AI confidently and develop awareness of its security implications and opportunities
- Understand how people and technology work together to protect digital assets
- Implement simple steps to strengthen your personal online security



Hack the Cybersecurity Interview

Christophe Foulon, Ken Underhill, Tia Hopkins

ISBN: 9781835461297

- Identify common interview questions for different roles
- Answer questions from a problem-solving perspective
- Build a structured response for role-specific scenario questions
- Tap into your situational awareness when answering questions
- Showcase your ability to handle evolving cyber threats
- Grasp how to highlight relevant experience and transferable skills
- Learn basic negotiation skills
- Learn strategies to stay calm and perform your best under pressure

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit authors.packt.com and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Share your thoughts

Now you've finished *The Absolute Beginner's Guide to Cybersecurity 2026*, we'd love to hear your thoughts! Scan the QR code below to go straight to the Amazon review page for this book and share your feedback or leave a review on the site that you purchased it from.



<https://packt.link/r/1808493850>

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Index

Symbols

2014 Sony Pictures hack	98
2018 disinformation campaigns involving Qatar	96
3-2-1-1-0 rule	150

A

AAA principles	6
access control	130
access control models	
ABAC	132
DAC	130
MAC	131
RBAC	131
real-world application	132
access control system	128
access management	128
account hijacking	157
accounting	8, 129
Acecard banking Trojan	89
address identification	
practical demonstration	17
advanced cyber attacks	70
business email compromise	70
deepfakes	72
drive-by downloads	72
session hijacking	73
SIM swapping	71
Advanced Encryption Standard (AES)	116
adware	80
examples	80
ahmia.fi	233
AI behavioral tracking	212
AI security tools	
real-world examples	146
AI-driven security	148
AI-powered malware	246

Arup Deepfake financial scam	246
Brad Pitt romance scam	247
AI-powered security	146
alteration	8
Amazon Web Services (AWS)	152
amiunique.org	211
Android	172
Android device	
special access settings, reviewing	185
unknown applications, uninstalling	186
anonymity	204
anonymizers	215
networked anonymizer	225
advantages	215
networked anonymizer	217
single point anonymizer	217
topology	216
anonymous identity	207
API exploits	157
app permissions	
managing	184
reviewing	184
Apple App Store	173
application layer	21
application level rootkit	85
artificial intelligence (AI)	72
applications, in cybersecurity	245
malicious uses, by cybercriminals	246
artificial intelligence (AI), in cybersecurity	
future trends	249
Arup Deepfake financial scam	246
ASN	36
ASpotCat	184
asset	10
asymmetric encryption	116
attack execution	43
attribute-based access control (ABAC)	132

authentication	6, 117, 128
biometric authentication	117
factor authentication	118
authorization	6, 128
automated incident response	246
availability	5

B

backdoor Trojan	79
background check companies	214
backups	150
incremental backup	151
common mistakes to avoid	151
differential backup	151
full backup	150
recommended tools and services	152
security practices	151
baiting	45
banking Trojan	88
Acecard banking Trojan	89
six-step process	88
behavior analysis	246
behavioral biometric identifiers	117
bias	247
biometric authentication	117
behavioral identifier	117
physiological identifier	117
biometrics	5
Bitcoin	81, 233
black box problem	147
black hat hackers	41
bootkits	159
bot herder	63
bot master	63
botnets	65
bots	63
Brad Pitt romance scam	247
Brave	208
bring your own device (BYOD) policy	237
structure	240
browser fingerprinting	210
browser hijackers	86
brute force attack	54
defending against	55

dictionary attack	55
example	54
business continuity plan	238
business email compromise	70

C

ChatGPT	147, 245
for security analysis	147
checkbox security	145
checksums	5
chief financial officer (CFO)	247
choose-your-own-device (CYOD)	240
CIA triad	5
risks, connection	11
ciphertext	115, 157
CISA Zero Trust maturity model	137
cloud	152
cloud computing	152
cloud deployment models	155
hybrid cloud	155
multi-cloud approach	156
private cloud	155
public cloud	155
cloud environments	156
security risks	156
cloud networks	15
cloud ransomware	157
cloud services	154
best practices	154
cloud storage	152
advantages	153
limitations	154
Cloudflare	31
Cloudways	35
cold boot attacks	160
cold cyber warfare	94
Colonial Pipeline attack	83
command and control server	63
communication components	15
company-owned, business-only (COBO)	239
company-owned, personally enabled (COPE)	240
compromised employee	42

confidentiality	5	data	150
Controlled folder access	161	data access ransomware	81
cookies	209	data anonymization	248
Evercookies	210	data breaches	
first-party cookies	209	monitoring	125
super cookies	210	data brokers	214
third-party cookies	209	Data Encryption Standard (DES)	116
Cooperative Cyber Defense Center of Excellence	95	data link layer	20
cover-up and avoiding detection	44	data logging	29
credential stuffing	157	data sensitivity ransomware	81
cross-device tracking	212	data transmission	15
cross-site scripting (XSS) attack	67	Debian Linux	231
CrowdStrike Falcon	146	decryption	115, 157
cryptography	115	deep web	232
cyber attacks		deepfakes	70, 246
botnet	63	DeepSeek	245
bots	63	default allow	106
brute force attack	54	default deny	106
cross-site scripting (XSS) attack	67	defense in depth	138
Denial of service (DoS)	64	core principles	139
Distributed Denial-of-Service (DDoS)	64	layers	140
man-in-the-middle attack	66	demilitarized zones (DMZs)	119
phishing	56	deniability	8
SQL injection	67	Denial of service (DoS) attack	64
supply chain attack	68	dictionary attack	55
cyber espionage	94	differential backup	151
cyber incidents	51	DigitalOcean	36
cyber warfare	94	direct memory access (DMA)	159
debates	94	disaster recovery plan	237
2014 Sony Pictures hack	98	disclosure	8
2018 disinformation campaigns involving Qatar	96	discretionary access control (DAC)	130
Estonia cyber attack	97	disgruntled employee	42
legal frameworks	94	distributed denial of service attacks (DDoS)	64 - 97
Stuxnet attack	95	Distributed Denial-of-Service (DDoS) attack	63
CyberGhost	224	DNS (Domain Name System)	29
cybersecurity	3, 237	DNS spoofing	29
applications of AI	245	DNSSEC (Domain Name System Security Extensions)	29
D		domain profile	107
DAD principles	7	drive-by downloads	70, 83
daemon	21	dumpster diving	48
dark web	232		
Darktrace	146		

Dynamic Lock	165	firmware level rootkit	85
dynamic pricing	213	first-party cookies	209
E		footprinting	42
e-commerce and payment processors	213	FreeNet	234
email communications		friend-to-friend (F2F) networks	235
protocols	19	full backup	150
email hijacking	67	G	
email tracking	214	general data protection regulation (GDPR)	144, 248
emails		GhostBear	222
working	31	Google	31
encrypted systems		Google Chrome	111
attacks	159	Google Gmail	146
encryption	5, 115, 158	Google Play Protect	194
asymmetric encryption	115	Google Play Store	173
symmetric encryption	115	Google Voice	208
end-to-end correlation attack	232	gray hat hackers	41
endpoint detection and response (EDR)	138	Guardians of Peace (GOP)	98
Estonia cyber attack	97	Gulf diplomatic crisis	
ethical hacking	248	2017-2018	96
Evercookies	210	H	
exit node	231	hack attack vishing	46
exploitation	43	hackers	
F		misconceptions	39
factor authentication	118	hacking methodology	42
three-factor authentication	119	attack execution	43
methods	118	cover-up and avoiding detection	44
multi-factor authentication	119	exploitation	43
two-factor authentication	119	persistence	43
Federal Bureau of Investigation (FBI)	100	privilege escalation	43
File Transfer Protocol (FTP)	20	reconnaissance	42
Find My iPhone	198	hacktivists	41
Find My Mobile	194	hashing	5
Find My Phone	196	Havij	67
firewall configurations		Health Insurance Portability and Accountability Act (HIPAA)	145
default allow	106	Hidester	218
default deny	106	URL	218
firewall rules	105	honeypots	119
firewalls	104	research honeypot	119
filtering rules	105	production honeypot	120
host-based firewalls	105	host-based firewalls	105
network firewalls	105		

HTTPS Everywhere	226	Internet data transmission processes	27
hub	23	emails	31
hybrid cloud	155	return path of internet data	31
Hypertext Transfer Protocol (HTTP)	18	Internet Message Access Protocol (IMAP)	19
Hypertext Transfer Protocol Secure (HTTPS)	18, 193, 232	Internet of Things (IoT)	27, 146
example	22	Internet Protocol (IP)	20
hypervisor level rootkit	85	internet service providers (ISPs)	28, 214
I		Invisible Internet Project (I2P)	234
identification	128	iOS	172
identification, authentication, authorization, accounting (IAAA)	127	IP address	16, 43
identification, authentication, authorization, accounting (IAAA) processes	129	IP version 4 (IPv4)	16
identities		IP version 6 (IPv6)	16
browser profiles	207	ISO/IEC 27001	144
personal identity	206	ISP traffic filtering	29
anonymous identity	207	J	
professional identity	206	jailbreaking	181
pseudonymous identity	207	legal and safety considerations	181
identity	128	technical process	181
identity and access management (IAM)	137	JBS Meat Plant attack	83
identity compartmentalization	205	K	
benefit	207	Kamagra	232
core principles	207	Kaspersky	86
mistakes	207	kernel	181
tools	208	kernel level rootkit	85
inbound connections	109	L	
Inbound Rules	107	layer 3 switch	27
incident response plan	238	layered security	138
incognito mode	214	least-privilege access	137
incremental backup	151	Let's Encrypt.org	23
indicators of compromise (IOCs)	142	library level rootkit	85
Info Stealer Trojan	79	local area network (LAN)	14
information security	4	Lock Screen and Security	193
management systems (ISMS)	144	locker ransomware	87
insider threats	42	logical controls	104
integrity	5	lunchtime attack	47
Internet Control Message Protocol (ICMP) tunnels	44	M	
internet data		MAC address	15
return path	31	machine learning	145

Malvertising	72, 83	networked anonymizer	217
malware analysis	246	networking	
Malwarebytes	89	intelligence	23
using	90	networking commands	
man-in-the-middle attack	66	nslookup	35
email hijacking	67	ping	32
session hijacking	67	traceroute	33
Wi-Fi eavesdropping	67	networking devices	23
mandatory access control (MAC)	131	hub	23
memory remanence attack	160	routers	23
Microsoft Defender	146	switches	23
Microsoft Sentinel	146	networking layer	21
misconfiguration	156	networking tools	
MITRE ATT&CK framework	142	Reverse IP Lookup	35
mobile applications	172	Whois tool	36
best practices, for downloading	175	NIST cybersecurity framework (CSF)	144
install numbers, analyzing	177	NIST SP 800-207	137
red flags, analyzing	177	non-repudiation	6
reviews and ratings, evaluating	177	NordVPN	188, 209
security guidelines	187	specialty servers	227
mobile apps and permissions	214	North Atlantic Treaty Organization (NATO)	95
mobile device management	241	Notify Me feature	125
mobile malware	86	nslookup command	35
symptoms	89		
mobile ransomware	87	O	
removal techniques	87	OneSwarm	235
modern backup security practices		online tracking locations	
access controls	151	data brokers	214
encryption	151	background check companies	214
immutable storage	151	data brokers	214
monitoring and testing	151	e-commerce and payment processors	213
multi-cloud approach	156	email tracking	214
multi-factor authentication (MFA)	119 - 137	internet service providers (ISPs)	214
		mobile apps and permissions	214
		search engines	212
		social media platforms	213
N		open source intelligence (OSINT)	143
National Institute of Standards and Technology (NIST)	248	opt-out services	214
natural language processing	145	Orion	68
network	14	outbound connections	109
access controls	5	Outbound Rules	107
packets	33		
segmentation	26	P	
network segmentation	27	passive reconnaissance	43
reasons	26		

password attacks	159	best practices	133
password formula		privileged account security	
examples	125	threats	133
password management strategies	124	production honeypot	120
passwords	5, 124	professional identity	206
Pastebin page	232	protocols	15, 122
patches	181	for email communications	19
payment card industry data security standard (PCI DSS)	144	ProtonMail	205
permission management applications		proxy server	217
using	184	allowing cookies	220
permissions		hide.me	219
matching, to app objectives	183	removing scripts	220
persistence	43	Hidester	218
personal identity	206	proxy servers	217
phishing	45 - 83, 157	ProxySite.com	219
smishing	62	pseudonymity	204
spear phishing	61	pseudonymous identity	207
vishing	46 - 61	public cloud	155
high-profile invoice fraud cases	62	public profile	106
payment verification best practices	62	public Wi-Fi network	192
preventive methods	46	PureVPN	224
smishing	62		
whaling	61	Q	
phishing emails		Quad	31
examples	56	Quid pro quo	45
physiological biometric identifiers	117		
piggybacking	47	R	
PIN (Personal Identification Number)	48, 242	ransomware	81, 150
ping command	32	as a service	83
plaintext	115, 157	attacks	83
ports	15	methods	83
Post Office Protocol (POP)	19	attacks	83
PowerShell	144	data access ransomware	81
pretexting	45	data sensitivity ransomware	81
principle of least privilege	130	reconnaissance	42
privacy	6, 204 - 248	active reconnaissance	43
private cloud	155	passive reconnaissance	43
private profile	107	active reconnaissance	43
privilege creep	127	regulations and ethical guidelines	
privilege escalation	43	AI in cybersecurity	248
privileged access	132	relays	225
privileged access management (PAM)	132	research honeypot	119
		responsible AI deployment	248
		RetroShare	236

reverse IP lookup	36	session hijacking	74
risk	10	preventing	75
connection, to CIA triad	11	session prediction	75
rogue security software	86	session sniffing	75
role creep	131	shadow profiles	213
role-based access control (RBAC)	131	shared responsibility model	
rootkits	84, 159	division of responsibility	156
kernel level	85	in cloud security	156
application level rootkit	85	shoulder surfing	48
firmware level rootkit	85	SIM card lock settings	200
hypervisor level rootkit	85	SIM swapping	70
infection, symptoms	85	Simple Mail Transfer Protocol (SMTP)	19
library level rootkit	85	single point anonymizer	217
routers	23	SiteGround	36
RSA algorithm	116	smishing	62
S		SOC 2	145
saboteurs	42	social engineering	44
safe mode	87	baiting	45
script kiddies	41	dumpster diving	48
search engines	212	lunchtime attack	47
second streamer	42	phishing	46
Secure File Transfer Protocol (SFTP)	20	piggybacking	47
Secure Sockets Layer (SSL)	21, 232	pretexting	45
security		Quid pro quo	45
access methods	238	shoulder surfing	48
compliance frameworks	148	tailgating	47
data access	238	social media platforms	213
data usage	238	SolarWinds attack	68
password policy	238	spear phishing	61
policy	215	spies	42
security compliance frameworks	144	spyware	81
security controls	104	SQL injection	67
managerial	104	SSL certificate	
operational	104	free SSL certificate	23
technical	104	Structured Query Language (SQL)	67
security information and event management (SIEM)	138	Stuxnet attack	96
security policy	238	subnets	26
assets	238	super cookies	210
internet access	238	supply chain attack	68, 157
security versus Ease of Access Paradox	242	SolarWinds attack	68
segments	26	Target attack	69
server management	5	preventing	69
		switches	23
		symmetric encryption	116

T

tactics, techniques and procedures (TTPs)	142	tracking	209
tagging attack	232	AI tracking	212
tailgating	47	cross-device tracking	212
Tallinn manual	95	online tracking locations	212
Target attack	69	tracking methods	
TCP/IP protocol layers		browser fingerprinting	210
application layer	21	cookies	209
data link layer	20	traffic confirmation	232
networking layer	21	Transmission Control Protocol (TCP)	20
transport layer	21	transport layer	21
TCP/IP Protocols	20	Transport Layer Security (TLS)	21
TempMail.org	208	Trojan DDoS	80
third-party cookies	209	Trojan Downloader	80
threat	9	Trojan horse	79
threat actors	39	removal methods	89
black hat hackers	41	Trojans	78
gray hat hacker	41	banking Trojan	88
hacktivists	41	defensive measures	80
insider threats	42	Info Stealer Trojan	79
saboteurs	42	Trojan DDoS	80
script kiddies	41	TunnelBear	222
spies	42	two-factor authentication	118
threat detection	246	U	
threat hunting (TH)	141	unlocking	181
elements	143	Updates Checker	178
threat intelligence (TI)	141	user and entity behavior analytics (UEBA)	
combining, with threat hunting	143	entity	137
operational	142	V	
strategic	142	Verizon	221
tactical	142	VigilantBear	223
technical	142	virtual local area networks (VLANs)	27
threat intelligence platforms (TIPs)	144	communication between VLANs	27
Tor	225	virtual private network (VPN)	15, 188, 220
attacks	231	topology	220
considerations	225	virtual private networks (VPNs)	
through VPN	227	myths	224
URL	225	VirtualBox	208
weaknesses	230	viruses	78
working	229	objectives	78
traceroute command	33	variants	78
trackers		defending against	79
blocking	212	life cycle	78
deleting	212		

methods of spread	78	demonstration	113
vishing	46 - 61	Windows Update	161
vulnerability	10	Wired Equivalent Privacy (WEP)	122
W		wireless security	121
WannaCry ransomware	87	wireless security protocols	122
web communication protocols	21	worms	78
whaling	61	defending against	79
white hat hackers	41	methods of spread	78
Whois tool	36	WPA2	122
URL	36	WPA2-Personal	122
Wi-Fi eavesdropping	67	WPA3	122
Wi-Fi Protected Access (WPA)	122	Z	
wide area network (WAN)	14	Zero Trust	135
Windows 11		challenges	138
securing	161	components	137
Windows Defender	104	core principles	136
Windows Firewall		drivers	136
demonstration	106	zombie	63

