ProcessGuy

CYBERSECURITY BEGINNER'S HANDBOOK

YOUR FIRST STEP TO UNDERSTANDING, PROTECTING AND THRIVING IN THE DIGITAL WORLD

AROWOLO ABIODUN M

ProcessGuy

CyberSecurity

Beginner's Handbook

A practical guide to Building a strong foundation in Cybersecurity

Written by

Arowolo Abiodun M

Empowering beginners with the knowledge and practical skills needed to confidently begin their journey into the world of cybersecurity

First Edition

Copyright

ProcessGuy CyberSecurity Beginner's Handbook

This book is intended for educational purposes only. While every effort has been made to ensure the accuracy of the information contained in this publication, the author and publisher assume no responsibility for errors or omissions or for any damages resulting from the use of the information presented. Cybersecurity techniques discussed in this book should only be practiced in authorized environments.

Never attempt to access, test, or interfere with systems, networks, or data without explicit permission from the owner. The author encourages ethical behavior and responsible use of cybersecurity knowledge at all times.

First Edition - 2026 Written by Arowolo Abiodun M

Acknowledgements

Writing this book has been a rewarding journey, and I would like to express my sincere gratitude to everyone who has supported me along the way.

To my students, thank you for your curiosity, your questions, and your willingness to learn. Many of the lessons in this handbook were shaped by the real challenges and discussions we've had together. Your enthusiasm continues to inspire me to teach and create better learning resources.

To the global cybersecurity community, thank you for sharing knowledge, developing open-source tools, publishing research, and encouraging collaboration. This field grows stronger because professionals are willing to teach others.

I also appreciate my family, friends, and colleagues for their encouragement, patience, and support throughout the writing process.

Finally, thank you to every reader who chose this book. Whether you are a student, career changer, IT professional, or simply someone curious about cybersecurity, I appreciate the opportunity to be part of your learning journey. I hope this handbook becomes a valuable resource that you return to throughout your career.

Preface

Technology has become an essential part of our daily lives. We use computers, smartphones, cloud services, online banking, social media, and countless digital platforms every day. As our dependence on technology grows, so does the need to protect the systems and information we rely on.

Unfortunately, many people are introduced to cybersecurity through complex jargon, advanced concepts, and overwhelming technical details. This often discourages beginners before they have the chance to build a solid foundation.

As someone who works in technology and spends a significant amount of time teaching others, I have seen this challenge firsthand. Many students are eager to learn cybersecurity but struggle because they don't know where to begin or because learning materials assume too much prior knowledge.

That experience inspired me to write this handbook.

The goal of this book is simple: to explain cybersecurity in a way that is practical, easy to understand, and accessible to complete beginners. Rather than focusing only on theory, this handbook combines explanations, real-world examples, practical exercises, and hands-on activities that reinforce learning.

Cybersecurity is not about memorizing commands or tools. It is about understanding how technology works, thinking critically, solving problems, and developing a mindset focused on protecting information and systems.

I encourage you to take your time with each chapter. Practice the exercises, experiment in safe environments, and remain curious. Every expert in this field started by learning the fundamentals.

Welcome to your cybersecurity journey. 🥳

Introduction

Welcome 🤗 to ProcessGuy CyberSecurity Beginner's Handbook.

If you're reading this, chances are you've decided to explore one of the fastest-growing and most exciting fields in technology. Whether you're a student, an IT professional looking to expand your skills, or someone completely new to technology, you've taken an important first step.

Cybersecurity is much more than hacking, as it is often portrayed in movies. At its core, cybersecurity is about protecting people, businesses, governments, and communities from digital threats. Every website you visit, every online payment you make, every email you send, and every file stored in the cloud relies on security measures working behind the scenes.

Throughout this book, you'll discover how computers communicate, how networks function, how attackers identify vulnerabilities, and how security professionals defend systems against those attacks. You'll also gain practical experience through exercises designed to help you apply what you learn. Inside this handbook, you will learn about:

- ➔ The foundations of cybersecurity
- ➔ Networking fundamentals
- ➔ Linux for cybersecurity
- ➔ Essential cybersecurity tools
- ➔ Web security basics
- ➔ Passwords and authentication
- ➔ Defensive security concepts
- ➔ Practical exercises and mini projects
- ➔ Best practices for ethical and responsible cybersecurity

No previous cybersecurity experience is required. The only things you need are curiosity, consistency, and a willingness to practice. As your knowledge grows, remember that cybersecurity is a field built on ethics and responsibility. The skills you develop should always be used to protect, educate, and improve the security of systems, not to cause harm or gain unauthorized access 😈.

My hope is that this handbook becomes more than just another book on your shelf. I hope it becomes your companion as you build knowledge, develop practical skills, and take your first confident steps toward a rewarding career in cybersecurity.

Let's begin

Table of Content

Acknowledgements....4
Preface.... 5
Introduction....6
1. Protecting Your Digital Castle.... 11
Your Digital Life Is Worth Protecting....12
Understanding Your Digital Castle.... 13
Watch Out for Digital Tricksters (Phishing Attacks)....14
Beware of Malware....17
Supercharge Your Passwords.... 18
Speak the Language: Know the meaning....20
Hands-On Challenge....22
2. Networking Fundamentals for Cybersecurity....23
Why Networking Matters....24
Locating Devices on a Network.... 25
How Data Travel: TCP vs UDP.... 28
Ports: The Doors to Network Services....31
Speak the Language: Know the Meaning.... 33
Hands-On Exercise.... 35
Review Questions....35
3. Linux Fundamentals for Cybersecurity....36
Why Learn Linux?....37
Why Do Cybersecurity Professionals Prefer Linux?....38
Linux Distributions (Distros).... 40
Understanding the Linux File System.... 41
The Terminal.... 43
Understanding File Permissions....46
Sudo & Privilege Escalation.... 48

Speak the Language: Know the Meaning..... 49
Hands-On Exercise..... 50
4. CyberSecurity Tools..... 51
From Theory to Practice..... 52
The Command-Line Advantage..... 53
The Big Three..... 55
Nmpa: The Network Mapper..... 56
Tcpdump: Watching Network Traffic..... 60
Nikto: The Web Server Inspector..... 63
Ethical and Legal Boundaries..... 67
Hands-On Lab..... 68
Speak the Language: Know the Meaning..... 71
5. Web Security Basics..... 73
How the Web Works..... 75
Understanding HTTP Response Codes..... 78
Introducing Web Application Security..... 80
SQL Injection..... 82
Cross-Site Scripting (XSS)..... 84
Cross-Site Request Forgery..... 86
Broken Access Control..... 87
Your Beginner Web Security Toolkit..... 90
Speak the Language: Know the Meaning..... 92
Hands-On Challenge: Explore Your Browser..... 95
Chapter Review Question..... 97
6. Password & Authentication Security..... 99
Introduction..... 100
Identity, Authentication & Authorization..... 101
The Password: Your First Digital Lock..... 104
How Should Websites Store Passwords?..... 108
Password Security Checklist..... 111
The Three Pillars of Multi-Factor Authentication (MFA)..... 112
The MFA Effectiveness Spectrum..... 113
Enterprise Access Protocols..... 114
Speak the Language: Know the Meaning..... 117
Hands-On Challenge: Strengthen Your Own Accounts..... 119
7. Defensive Security..... 122

Introduction..... 123
What Is Defensive Security?..... 123
The Three Goals of Security..... 124
Firewalls: The Security Gatekeeper..... 128
Logging: The Security Camera..... 133
What Is an Incident?..... 135
Backups: Your Digital Safety Net..... 139
Security Awareness..... 141
Speak the Language: Know the Meaning..... 144
Hands-On Challenge: Build a Defensive Plan..... 148
Appendix A: References and Further Reading..... 153
About This Reference List..... 153
A.1 Cybersecurity Standards and Frameworks..... 153
A.2 Web Application Security..... 154
A.3 Network Security and Nmap..... 154
A.4 Linux and Command-Line Security..... 155
A.5 TCP/IP and Networking..... 156
A.6 Authentication and Multi-Factor Authentication..... 157
A.7 Cybersecurity Tools..... 157
A.8 Defensive Security..... 157
A.9 Additional Recommended Resources..... 158
A.10 Responsible Use of Cybersecurity Knowledge..... 159
A.11 AI-Assisted Content and Illustration Disclosure..... 159
A.12 Note to the Reader..... 159
About the Author..... 161

Chapter 01

1. Protecting Your Digital Castle

By the end of this chapter, you will be able to:

- ➔ Understand what cybersecurity is and why it matters.
- ➔ Recognize the different layers that protect your digital life.
- ➔ Identify common phishing attacks.
- ➔ Understand the most common types of malware.
- ➔ Create stronger passwords and passphrases.
- ➔ Apply simple security practices to protect yourself online.

Your Digital Life Is Worth Protecting.

Think about everything stored on your phone or laptop.

Your photos.
Your emails.
Your bank account.
Your school or work documents.
Your social media accounts.
Your passwords.

Every one of these contains information that is valuable, not only to you, but also to cybercriminals. In cybersecurity, you can think of all these devices, accounts, and personal information as your Digital Castle. Just as a real castle has walls, gates, guards, and locks to keep intruders out, your digital life also needs multiple layers of protection.

No computer connected to a network is completely immune to attack.

People often joke that the safest computer is one that is turned off, and even that isn't perfectly safe if someone has physical access to it.

Since we rely on our computers and smartphones every day, the goal of cybersecurity is not to achieve perfect security.

Instead, it is to make it as difficult as possible for attackers to steal your information or damage your devices.

Cybersecurity is all about building strong layers of defense.

Understanding Your Digital Castle

Imagine your digital life as a modern house protected by several security systems. Each security feature has a cybersecurity equivalent.

Your Real House	Your Digital Castle	What It Does For You
Front Door Lock	Passwords or Passphrases	Monitors incoming and outgoing network traffic and blocks suspicious connections.
Security Guard	Firewall	Monitors incoming and outgoing network traffic and blocks suspicious connections.
Guard Dogs / Alarm System	Antivirus Software	Detects and removes malicious software before it causes damage
Windows & Doors	Wi-Fi & Internet Connections	Connects you to the outside world, and must be properly secured
Safe	Data Backup	Protects your important files if your computer is lost, damaged, or infected.

Watch Out for Digital Tricksters (Phishing Attacks)

Many people imagine hackers writing complicated code to break into computers.

In reality, one of the easiest ways for attackers to succeed is simply by tricking people into giving away their information.

This technique is known as Phishing.

Instead of hacking your computer, attackers try to hack your trust.

Common Types of Phishing

Email Phishing

Fake emails pretending to come from trusted organizations such as banks, Netflix, Amazon, or Microsoft.

These emails often claim:

- Your account has been suspended.
- Someone logged into your account.
- You have won a prize.
- You need to verify your payment details.
- Smishing (SMS Phishing)

Attackers send fake text messages containing malicious links.

Examples include:

- Fake parcel delivery notifications
- Job offers
- Banking alerts
- Mobile network promotions

Vishing (Voice Phishing)

Attackers call pretending to be customer support, your bank, or even law enforcement.

They may ask for:

- Your PIN
- Your password
- One-Time Passwords (OTP)
- Banking details

Legitimate organizations will not ask for your password or PIN over the phone

How to Spot a Phishing Attempt

Look for these warning signs:

1. Urgency

Messages like:

> "*Your account will be deleted in 10 minutes!*"

are designed to make you panic.

Always slow down before clicking.

2. Suspicious Email Addresses or Links

Attackers often use addresses that look almost correct.

Example:

❌ *support@paypal-security.com*

Notice the capital I replacing the lowercase l.

Always check carefully before clicking.

3. Requests for Sensitive Information

No legitimate bank or trusted online service will ask you to send your:

- Password
- PIN
- CVV
- One-Time Password (OTP)

If someone asks for these, it is almost certainly a scam.

Beware of Malware

Malware is short for Malicious Software.

It refers to software designed to damage devices, steal information, spy on users, or disrupt normal operations.

Some common examples include:

Malware	What it Does	How to Protect Yourself
Virus	Attaches itself to legitimate files and spreads when those files are opened.	Avoid opening unknown attachments and keep antivirus software updated.
Worm	Spreads automatically across vulnerable computers and networks without user interaction.	Install operating system updates and use a firewall.
Ransomware	Encrypts your files and demands payment to restore access.	Maintain regular backups and avoid suspicious downloads.
Spyware / Keylogger	Secretly monitors your activity and records sensitive information such as passwords.	Download software only from trusted sources and keep your device updated.

Many ransomware victims never recover their files, even after paying the ransom. This is why regular backups are one of the most effective defenses.

Supercharge Your Passwords

Your password is often the first line of defense protecting your online accounts.

Cybercriminals use automated tools to try millions or even billions of password combinations.

This type of attack is called a **Brute Force Attack**.

Long Passwords Are Stronger

Many people believe a complicated eight-character password is enough.

For example:

> ❌ *P@ss12!*

Although it contains symbols, it is still relatively short.

A better approach is to create a passphrase. Example:

> ✅ *I have a blue monkey as a child*

Long passphrases are generally much harder to crack while also being easier to remember.

Even better, consider using a password manager to generate and store unique passwords for every account.

Remember: Long is Strong and Short is Weak!

Two Simple Steps That Greatly Improve Your Security

1. Enable Two-Factor Authentication (2FA)

Two-Factor Authentication adds another layer of protection.

Even if someone discovers your password, they still need your second verification method, such as:

- Authentication app
- Fingerprint
- Security key
- One-time verification code

2. Keep Your Software Updated

Software updates do more than add new features.

They also fix security vulnerabilities that attackers actively search for.

Whenever your device notifies you about an important security update, install it as soon as possible.

Speak the Language: Know the meaning

Antivirus Software: Detects and removes malicious software before it causes damage to your devices.

Brute Force Attack: An attack method where cybercriminals use automated tools to try millions or billions of password combinations to gain unauthorized access.

Cybersecurity: The practice of building layers of defense to make it as difficult as possible for attackers to steal information or damage devices.

Data Backup: Copies of important files saved separately to protect against loss, hardware damage, or ransomware infections.

Digital Castle: A security metaphor representing all your devices, accounts, and personal data as a fortress requiring multiple layers of protection.

Email Phishing: Fake emails sent by attackers posing as trusted organizations to trick recipients into revealing personal or account details.

Firewall: A security system that monitors incoming and outgoing network traffic and blocks suspicious connections.

Keylogger: A type of spyware that secretly monitors device activity and records sensitive information like typed passwords.

Malware: Short for malicious software; programs designed to damage devices, steal information, spy on users, or disrupt normal operations.

Passphrase: A long sequence of words used as a password that is significantly harder for automated tools to crack while being easy for humans to remember.

Password Manager: A tool used to generate, manage, and securely store unique passwords for every online account.

Phishing: A social engineering technique where attackers trick individuals into giving away sensitive information by exploiting their trust.

Ransomware: A type of malware that encrypts files on a device and demands payment to restore access.

Smishing (SMS Phishing): Fraudulent text messages containing malicious links

or fake alerts designed to steal sensitive data.

Software Updates: System patches released by developers to fix security vulnerabilities that attackers actively look to exploit.

Spyware: Software that secretly monitors user activity on a device and records sensitive personal information.

Two-Factor Authentication (2FA): An added security layer requiring two separate verification methods (like a password plus an authenticator code or biometric) before granting access.

Virus: A type of malware that attaches itself to legitimate files and spreads when those files are opened.

Vishing (Voice Phishing): Fraudulent phone calls where attackers pretend to be trusted entities (like banks or support) to trick individuals into sharing sensitive details over the phone.

Worm: A standalone type of malware that automatically spreads across vulnerable computers and networks without requiring user interaction.

Hands-On Challenge

Choose one of these real-world cybersecurity incidents and research it.

Suggested case studies:

- ★ Sony Pictures Cyberattack (2014)
- ★ Colonial Pipeline Ransomware Attack (2021)
- ★ Ashley Madison Data Breach (2015)

Write down:

- What happened?
- How did the attackers gain access?
- What were the consequences?
- What lessons can we learn?

Daily Cybersecurity Checklist

Now that we have come to the end of this chapter, ask yourself the following tick appropriately:

- ☐ I use long, unique passphrases.
- ☐ I have enabled Two-Factor Authentication on important accounts.
- ☐ I avoid clicking suspicious links.
- ☐ I download software only from trusted sources.
- ☐ My phone and computer are updated regularly.
- ☐ I regularly back up my important files.

Chapter Questions

1. Why is cybersecurity described as a layered defense?
2. What is the difference between phishing, smishing, and vishing?
3. How does ransomware differ from a computer virus?
4. Why are passphrases generally stronger than short passwords?
5. What are two benefits of enabling Two-Factor Authentication?