

No. 87

CYBERSECURITY

Cybersecurity Basics

Protect yourself, your family and your small business from today's online threats, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 87

Cybersecurity Basics

Protect yourself, your family and your small business from today's online threats, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Cybersecurity Basics

Protect yourself, your family and your small business from today's online threats, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What cybersecurity is 4
2 The threat picture 6
3 How attackers think 8
4 The four basic steps 9
5 Phishing 11

PART II · PROTECTING YOURSELF

6 Passwords and password managers 14
7 Multi-factor sign-in and passkeys 16
8 Updates 18
9 Backups 19
10 Protecting your devices 21
11 Home networks and Wi-Fi 23
12 Safe browsing and shopping 24
13 Phones and messaging apps 25

PART III · MODERN THREATS

14 Scams and fraud 28
15 Ransomware 30
16 AI scams and deepfakes 32
17 Privacy and social media 34
18 Protecting children and older relatives 35

PART IV · BEYOND THE BASICS

19 If you've been hacked or scammed 37
20 Small business security 39
21 Security at work 41
22 Careers in cybersecurity 42

FREE SAMPLE · ojayo.com

23 Building good habits 44
Checklists 46
Glossary 48
Further reading 49

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Cybersecurity means protecting your accounts, devices, data and money from criminals and mistakes online. It remains one of the most searched technology topics, and for good reason: the FBI's Internet Crime Complaint Center received more than one million complaints in 2025 for the first time, with reported losses of $20.9 billion, up 26% on the year before.

The good news is that a handful of habits stop most attacks: strong, unique passwords stored in a password manager; multi-factor sign-in; recognizing scams; keeping software updated; and having backups. This book explains these and more in plain language, for individuals, families and small organizations.

What this book covers

- How online threats work, including AI-powered scams and deepfakes.
- Protecting accounts, devices, home networks and data.
- Safe habits for email, browsing, phones and social media.
- What to do if something goes wrong.
- Basics for small businesses, and an introduction to cybersecurity careers.

Who this book is for

- **Everyone** who uses the internet.
- **Parents and carers** protecting a family.
- **Small business owners and staff** without a security team.
- **Beginners** curious about a career in cybersecurity.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–5): what cybersecurity is, the threat picture, how attackers think, the four basic steps, and phishing.
- **Part II — Protecting yourself** (Chapters 6–13): passwords, multi-factor sign-in and passkeys, updates, backups, devices, home networks, safe browsing and shopping, and phones.
- **Part III — Modern threats** (Chapters 14–18): scams and fraud, ransomware, AI-powered scams and deepfakes, privacy and social media, and protecting children and older relatives.
- **Part IV — Beyond the basics** (Chapters 19–23): if you've been hacked, small business security, security at work, careers, and building habits.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How a protection looks in real apps and settings.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

A note on screens and examples

Screens are **simplified illustrations**, not copies of real apps. Names in examples are invented. Settings differ between devices and change over time.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what cybersecurity is, the scale of today's threats, how attackers think, the four basic protective steps, and how to spot phishing.

FREE SAMPLE · ojayo.com

CHAPTER 1

What cybersecurity is

Cybersecurity protects the information and systems we depend on.

Three goals

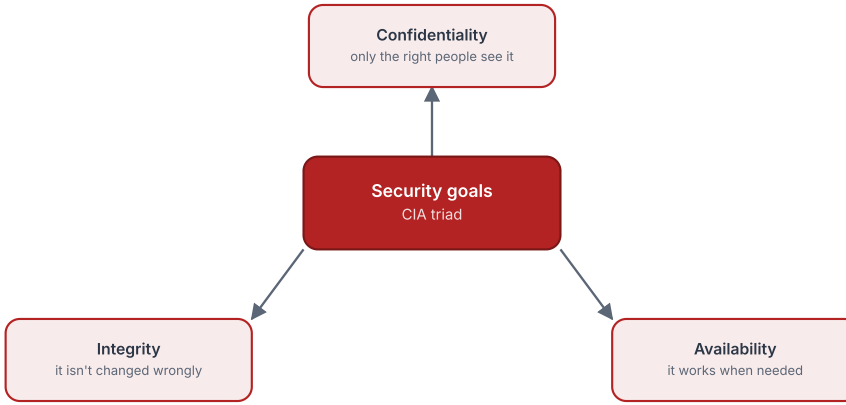


Figure 1.1 Confidentiality, integrity and availability

- **Confidentiality**: private things stay private.
- **Integrity**: information is not changed by the wrong people.
- **Availability**: your systems and data work when you need them.

It is about people as much as technology

Most attacks start by tricking a person: clicking a link, sharing a code, sending money. Technology helps, but habits matter most.

FREE SAMPLE · ojayo.com

Security is layers

No single protection is perfect. A strong password, multi-factor sign-in, updates and backups together make attacks much harder.

KEY IDEA

You do not need to be an expert. A few good habits put you ahead of most targets.

FREE SAMPLE · ojayo.com

CHAPTER 2

The threat picture

Understanding the threat picture helps you focus on what matters.

Finding	Figure
US cybercrime losses reported to FBI, 2025	$20.9 billion
Complaints to FBI IC3, 2025	over 1 million
Breaches involving the human element (Verizon 2026)	62%
Breaches with a third party involved (Verizon 2026)	48%
Breaches with ransomware present (Verizon 2026)	48%

Figure 2.1 Key numbers from 2025 and 2026 reports

What the reports say

- The **FBI's 2025 Internet Crime Report** recorded $20.877 billion in reported losses, a record. Cryptocurrency scams alone accounted for $11.36 billion. For the first time the report tracked AI: more than 22,000 complaints referenced AI, with about $893 million in losses.
- The **Verizon 2026 Data Breach Investigations Report** found that exploiting software vulnerabilities overtook stolen credentials as the top way attackers first got into organizations. People were involved in 62% of breaches, a third party in 48%, and ransomware appeared in 48%.

FREE SAMPLE · ojayo.com

The most common threats

Threat	What it is
Phishing	fake messages that steal logins or money
Malware	harmful software
Ransomware	locks files, demands payment
Scams and fraud	tricks to send money
Account takeover	criminals use your accounts
Deepfakes	fake voices and videos made with AI

Figure 2.2 Threats you will meet

Who is targeted

Everyone. Criminals use automation to attack millions of people and small businesses at once. You do not need to be important to be a target; you need only be reachable.

> **TIP**
> Most losses come from scams and stolen accounts, not from movie-style hacking. Focus your effort there.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics (you are reading this)
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Cybersecurity Basics

Enjoyed it? The full book has 54 pages and 23 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.