Cybersecurity Fundamentals — 2026 Complete Course

Cybersecurity Fundamentals — The Complete Beginner Course

TechSparking Free Course — 12 chapters · 28 lessons · 2 practical labs

---

How to use this course

This course teaches the fundamentals of digital self-defense and professional security thinking. Work through it in order — each chapter builds on the last. Do the labs for real (they take minutes), and test everything on your own devices only. Expect 15–35 hours total. Pair this PDF with our free article *The Complete Home Cybersecurity Check: 24 Steps* for a hands-on checklist.

Chapter 1 — The Threat Landscape

Lesson 1.1 — Who attacks, and why

Attackers are not all hoodie-wearing hackers. The 2026 threat landscape looks like this:

- **Cybercriminals with kits** — ransomware and phishing toolkits are sold like software; attackers buy, not build
- **Scammers at scale** — fake support calls, fake invoice emails, fake "you've won" texts
- **State-sponsored actors** — targeting infrastructure, supply chains and public figures
- **Insiders** — employees or partners with access, often accidental

In 2025, small and mid-size businesses accounted for 88% of ransomware breach incidents. You are a target — the question is how hard you are to hit.

Lesson 1.2 — The attack playbook

Almost every attack follows the same five steps:

1. **Reconnaissance** — learn about the target (public profiles, breached data, open ports)
2. **Initial access** — phishing, weak passwords, exposed RDP, unpatched software
3. **Lateral movement** — move from the first foothold to valuable systems
4. **Action** — exfiltrate data, encrypt systems, plant ransomware, abuse access
5. **Cover tracks** — delete logs, disable alerts, cash out

Defense is about breaking this chain at every step.

Lesson 1.3 — The security mindset

Security is not a product you install; it's a habit you practice. The core principle: **least privilege** — give every person, app and process only the access it needs, nothing more. The second principle: **assume breach** — design so that if one layer fails, the next still protects you.

Exercises — Chapter 1

1. List every account you own that you could NOT recover if you lost the password tomorrow.
2. Map your "attack surface": devices, accounts, cloud storage, home network devices, work logins.
3. Write down why an attacker might target you specifically (nothing is embarrassing here).

Chapter 2 — Passwords and Authentication

Lesson 2.1 — Why passwords fail

Humans reuse passwords. When one site leaks (and leaks happen constantly), attackers take that password and try it everywhere — this is called **credential stuffing**. The fix is not a "stronger" password; it's a **different** password everywhere.

Lesson 2.2 — The password manager solution

A password manager generates and stores a unique, strong password for every site, protected by one master password. Tools like Bitwarden, 1Password and KeePassXC work on all devices. Set one up this week — it is the single highest-impact change in this course.

Lesson 2.3 — Multi-factor authentication (MFA)

MFA requires a second proof of identity: a code, a hardware key, or biometrics. Even if your password leaks, MFA blocks the login. Use **app-based authenticators or hardware keys** (YubiKey) for critical accounts; SMS is better than nothing but weaker (SIM-swap attacks).

Exercises — Chapter 2

1. Move your 10 most important accounts into a password manager.
2. Enable MFA on your email (the master key to everything) and your financial accounts.
3. Do a password-reuse audit: find three sites where you use the same password and fix them now.

Chapter 3 — Phishing and Social Engineering

Lesson 3.1 — The anatomy of a phishing email

Phishing is the #1 entry method. Look for:

- **Urgency** — "your account will be closed in 24 hours"
- **Impersonation** — logos and names of real companies, spoofed sender names
- **Mismatched links** — hover before you click; the visible text masks the real URL
- **Attachment pressure** — invoices, "scanned documents", PDFs asking you to enable macros
- **Grammar oddities** — sometimes subtle, sometimes obvious

Lesson 3.2 — Smishing and vishing

- **Smishing** (SMS phishing) — fake delivery texts, fake bank alerts, "your package is held"
- **Vishing** (voice phishing) — fake tech support calling you, fake bank security calling "about unusual activity"

Rule: **never act on an inbound request for credentials, codes or payments**. Hang up, go to the official website or app yourself, and check there.

Lesson 3.3 — Red flags that actually work

- The message asks for a **one-time code** (legitimate services never do this)
- The sender address is wrong when expanded (not just the display name)
- The domain in the link is slightly misspelled (paypa1.com, amaz0n.com)

- It creates panic — panic is the shortcut around your judgment

Lab 1 — The phishing test

Create 5 sample scam messages (email, SMS, voice script) using real scenarios. For each: identify the psychological trigger, the technical red flag, and the safe response. This 20-minute exercise trains your instinct better than any course.

Chapter 4 — Network and Router Security

Lesson 4.1 — Your router is the front door

The router is the first device attackers touch. Defaults are dangerous: change the admin password, update firmware, and disable remote admin access.

Lesson 4.2 — Wi-Fi security settings

- Use **WPA3** (or WPA2 if devices are old); never use WEP or open networks
- Separate networks: main, guest, and IoT (smart devices) should not share one
- Hide nothing — hiding the SSID does not protect you and causes real problems

Lesson 4.3 — Firewall basics

A firewall examines traffic and blocks what you didn't ask for. Your router has one built in; your operating system has another. Learn to check both are on:

- Windows: Windows Defender Firewall, enabled by default
- macOS: Application Firewall, enable in System Settings
- Router: verify SPI/stateful filtering is on (usually default)

Exercises — Chapter 4

1. Change your router admin password today and update its firmware.
2. Enable WPA3 (or WPA2) and set up a guest network for visitors.
3. Check the firewall status on your phone, laptop and PC.

Chapter 5 — Malware and Ransomware

Lesson 5.1 — The malware family tree

- **Viruses** — attach to files and spread when you run them
- **Trojans** — look useful, do harm
- **Spyware** — watches you quietly
- **Ransomware** — encrypts your files and demands payment
- **Cryptominers** — steal your computing power

Lesson 5.2 — How ransomware enters

Ransomware arrives through phishing (the classic "invoice"), drive-by downloads, cracked software, pirated apps, and exposed remote services. The business model is now seamless: ransomware-as-a-service with support desks.

Lesson 5.3 — Ransomware defenses that work

1. **Offline/immutable backups** — the only reliable recovery; test them
2. **MFA everywhere** — blocks the credential foothold
3. **Patching** — automatic updates on everything
4. **Least privilege** — standard user accounts for daily work
5. **Email filtering** — catch the payload before it lands

Exercises — Chapter 5

1. Verify your backups are disconnected after the backup job (physically or logically).
2. Perform a test restore of one folder from backup — now, not in an emergency.
3. Find three "cracked"/pirated apps you have and remove them (they are malware delivery systems).

Chapter 6 — Backups and Recovery

Lesson 6.1 — The 3-2-1 rule

- **3** copies of your data
- **2** different media types (cloud + external drive)
- **1** copy off-site

Lesson 6.2 — What to back up

Photos, documents, financial records, 2FA recovery codes, password manager export, browser bookmarks, email archives. Inventory first; you can't back up what you haven't listed.

Lesson 6.3 — Testing restores

A backup you've never restored is a hope, not a plan. Quarterly: restore a random folder to a spare device and confirm it opens. Note the time it takes — that's your recovery-time goal during an incident.

Exercises — Chapter 6

1. Set up automatic daily backups of your main documents (cloud + local).
2. Export your 2FA recovery codes and store them offline (paper in a safe place).
3. Do a full test restore of your phone or laptop backup.

Chapter 7 — Safe Browsing and Privacy

Lesson 7.1 — The browser as an attack surface

Extensions are a leading infection vector. Only install extensions you need, from official stores, and audit them yearly — an extension can read everything you type.

Lesson 7.2 — Privacy tools that matter

- **Password manager** (not browser's built-in) — portable, encrypted
- **Ad/tracker blocker** — uBlock Origin — reduces malicious ad exposure
- **DNS filtering** — block known-bad domains at the router or device level
- **VPN** — honest use: prevent snooping on public Wi-Fi; it is not anonymity

Lesson 7.3 — Data minimization

Every registration form is a data leak waiting to happen. Use a dedicated email alias for newsletters and signups (e.g., Proton Mail aliases, SimpleLogin). Never give your real phone number to random sites.

Exercises — Chapter 7

1. Audit your browser extensions and remove anything unused or unverified.
2. Create an email alias and use it for the next 5 signups.
3. Check which sites you're logged into and log out of the ones you don't use weekly.

Chapter 8 — Email Security

Lesson 8.1 — Securing the inbox

Email is the master key to your digital life (password resets arrive there). Protect it as the crown jewel:

- Strong unique password + MFA (hardware key if possible)
- Avoid loading remote images from unknown senders
- Use spam filtering and report phishing

Lesson 8.2 — Recognizing spoofed mail

Spoofing fakes the "From". Look at the raw headers if it matters: the SPF/DKIM/DMARC results tell you if the domain authorized the sender. Most webmail clients show this under "Show original".

Lesson 8.3 — The reset-attack

Attackers who control your email can reset every password. Your defense: MFA on email, account-recovery questions that are not public facts, and a recovery code printed and stored offline.

Exercises — Chapter 8

1. Enable MFA on your primary email today.
2. Locate and print your account recovery codes; store them offline.
3. Check SPF/DKIM on one suspicious email you've received.

Chapter 9 — Social Media and Identity

Lesson 9.1 — OSINT and you

Open-source intelligence (OSINT) is the practice of collecting public info. Attackers use your social media to build targeted phishing. What you post is research material for them.

Lesson 9.2 — Locking down profiles

- Make friends-only what can be friends-only
- Remove location tags, exact birthdays, and access cards visible in photos (office badges, home keys)
- Keep your employer private if you handle sensitive work

Lesson 9.3 — Deepfakes and voice cloning

AI can now clone a voice from seconds of audio and generate realistic faces. Receive any unusual "family emergency" or "boss request" call? Verify through a second channel you initiated yourself.

Exercises — Chapter 9

1. Google yourself and note what an attacker learns in 10 minutes.
2. Lock down the top 3 social profiles (privacy settings, photos, birthdate).
3. Agree a family code word for "verify it's really me" with close relatives.

Chapter 10 — Home Lab and Testing Basics

Lesson 10.1 — Why a home lab

A safe sandbox to test security concepts without risk. Minimum: a virtual machine (VirtualBox or VMware) or Raspberry Pi on an isolated network.

Lesson 10.2 — First tools (run only in your lab)

- **Nmap** — scan your own network to see what's exposed
- **Wireshark** — inspect your own traffic
- **Hashcat** — test password strength on your own hashes (never others')
- **Burp Suite Community / OWASP ZAP** — web app testing on intentionally vulnerable apps (DVWA, Juice Shop)

Lesson 10.3 — The legal line

Test only systems you own or have written permission to test. Hacking other people's networks — even "just looking" — is a crime in nearly every country. Skill without permission is prison; skill with permission is a career.

Lab 2 — Network discovery (own network)

1. Install a VM or use your own machine
2. Run `nmap -sn 192.168.1.0/24` (adjust to your subnet) and list what's alive
3. Identify each device; flag any device you don't recognize (could be a compromise or a forgotten smart device)
4. Write a one-page report of what you found, like a real consultant would

---

Chapter 11 — Responding to an Incident

Lesson 11.1 — The incident response steps

1. **Isolate** — disconnect the affected machine from the network (do not turn it off; you may need forensic data)
2. **Assess** — what's the blast radius? Accounts, files, devices involved?
3. **Contain** — change passwords from a clean device, revoke sessions, rotate API keys
4. **Recover** — restore from known-good backups, verify integrity
5. **Learn** — write down what happened and what you'll change

Lesson 11.2 — Ransomware: to pay or not

In most cases, do not pay. Paying funds criminals, and a significant share of victims never recover data even after payment. Law enforcement consistently advises against it. Recovery comes from your backups and your incident plan, not the ransom.

Lesson 11.3 — Your one-page incident plan

Write it now: who to call (IT person, bank, insurer), what to unplug first, where the offline backups are, which accounts to lock first. A plan written in daylight beats a decision made at 2 a.m. in a panic.

Exercises — Chapter 11

1. Write your one-page incident response plan for home and (if you work) for the office.
2. Do a tabletop drill with family/colleagues: "the email just asked us to pay an invoice — what do we do?"
3. If you were hit today, list the first five actions you'd take in order.

Chapter 12 — Building Good Habits

Lesson 12.1 — The annual security review

Security decays as life changes. Once a year:

- Rotate critical passwords (email, banking, cloud)
- Audit connected devices and remove old ones
- Review app permissions on phone
- Check MFA is still on everywhere
- Test backups restoration

Lesson 12.2 — The monthly 10 minutes

- Update everything (OS, browsers, apps)
- Check your password manager health report
- Glance at login alerts on email + bank

Lesson 12.3 — The daily 30 seconds

- Never click links or attachments from unexpected messages
- Never share codes or passwords with anyone who asks
- Lock your screen when you step away

Course glossary

Term	Meaning
Attack surface	Everything an attacker could exploit
Least privilege	Minimum access needed, nothing more
MFA	Multi-factor authentication
Credential stuffing	Reusing leaked passwords across accounts
Phishing	Fraudulent messages to steal credentials
Smishing	Phishing by SMS
Ransomware	Malware that encrypts and demands payment
3-2-1 backup	3 copies, 2 media, 1 off-site
Firewall	Filter between your network and the world
Incident response	The steps to contain and recover from an attack
OSINT	Public information gathering

Course complete! You now understand the threat landscape, passwords, phishing, networks, malware, backups, privacy, email, social media, testing and incident response — and you've done real labs. Continue with our articles on ransomware defense, router security and the home security checklist for deeper dives. You are now harder to attack than 90% of people — that was the goal.