TRAINING 2 · HANDS-ON TRAINING

Secure Your Devices



Updates, antivirus, encryption and screen locks on Windows, Mac, iPhone and Android

Cybersecurity Basics: Hands-On Training

By the end of this training you will have



Automatic updates
Security fixes installed as soon as they arrive



Working antivirus
Built-in protection switched on and current



Encrypted devices
Data unreadable if a device is lost or stolen



Strong screen locks
No one can simply pick up and use your device

02

Training 2 of 8
Secure Your Devices

About 30 minutes

The four device basics



Update

Most attacks use flaws that already have a fix



Protect

Built-in antivirus blocks known malware



Encrypt

Protects your data on a lost or stolen device



Lock

A PIN, password or biometric on every device

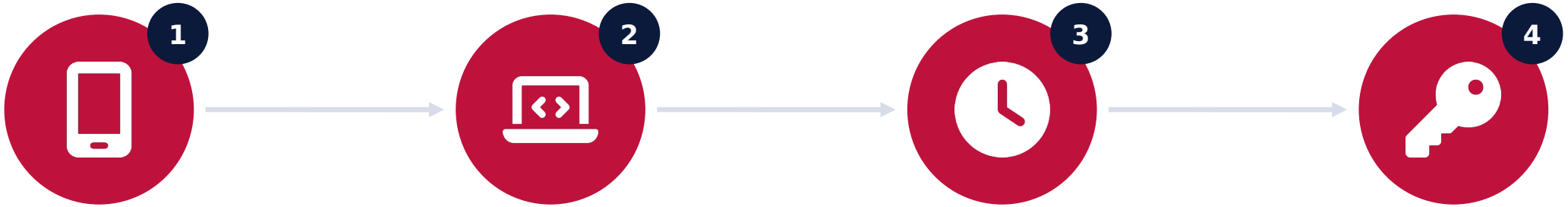
Step 1: Turn on automatic updates

Device	Where to find it	Set to
Windows 11	Settings › Windows Update	Install updates automatically
Mac	System Settings › General › Software Update	Automatic updates on
iPhone	Settings › General › Software Update	Automatic updates on
Android	Settings › System or Security › Software update	Auto-download on
Apps and browsers	App Store, Google Play, browser settings	Auto-update on

Steps 2 and 3: Antivirus and encryption

Device	Antivirus	Encryption
Windows 11	Windows Security › Virus & threat protection: green	Privacy & security › Device encryption, or BitLocker
Mac	Built-in protection, kept current by updates	Privacy & Security › FileVault: on
iPhone	Built-in protection; install apps only from the App Store	On automatically when a passcode is set
Android	Google Play Protect: on	On by default on modern phones with a screen lock

Step 4: Set strong screen locks



Phones

6-digit PIN or longer, plus biometrics

Computers

Password or PIN, plus Windows Hello or Touch ID

Auto-lock

After 1–5 minutes of inactivity

Lock when you leave

Windows + L, or Control + Command + Q

Avoid simple patterns and birthdays. Biometrics are convenient, but a strong PIN is the real protection.

Find your device if it is lost

Apple: Find My

Settings › your name › Find My. Locate, lock or erase iPhones and Macs

Android: Find Hub

Google’s Find My Device service, built into Android

Windows: Find my device

Settings › Privacy & security › Find my device

If it is stolen

Lock or erase it remotely, then change key passwords

Your checklist

- [ ] Automatic updates on for every computer and phone
- [ ] Apps and browsers set to update automatically
- [ ] Antivirus on and showing no problems
- [ ] Encryption on (Device encryption, BitLocker or FileVault)
- [ ] Phone PIN of 6 digits or more
- [ ] Auto-lock set to 5 minutes or less
- [ ] Find My or Find Hub switched on
- [ ] Old, unused apps removed

Restart your devices after updating: many security fixes only apply after a restart.

Check your work

1. Why are automatic updates the single most important device setting?

2. What does encryption protect against?

3. What should you do first if your phone is stolen?

Answers are in the training guide.

Well done

- Your devices install security fixes automatically.
- Your data stays protected even if a device is lost.
- No one can simply pick up and use your devices.

Next: Training 3 · Spot and Report Phishing