TRAINING 1 · HANDS-ON TRAINING

Secure Your Accounts



Strong passwords, a password manager, multi-factor authentication and a breach check

Cybersecurity Basics: Hands-On Training

By the end of this training you will have



Checked your exposure
Found out if your email appears in known breaches



A password manager
Unique, strong passwords without memorising them



Multi-factor authentication
A second lock on your most important accounts



A completed checklist
Your key accounts secured, one by one

01

Training 1 of 8
Secure Your Accounts

About 30 minutes

Before you start



30–45 minutes
Do it in one sitting if you can



A computer
Windows or Mac, with a web browser

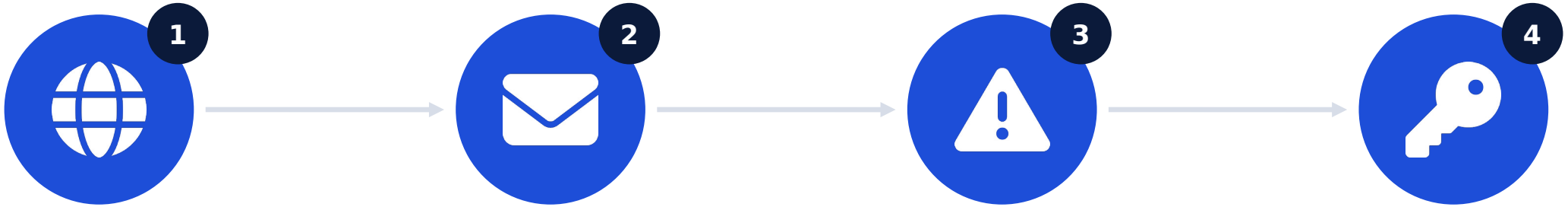


Your smartphone
For the authenticator app



Your account list
Email, bank, social media, work

Step 1: Check if your email was in a breach



Open the site

haveibeenpwned.com

Enter your email

Each address you use

Read the results

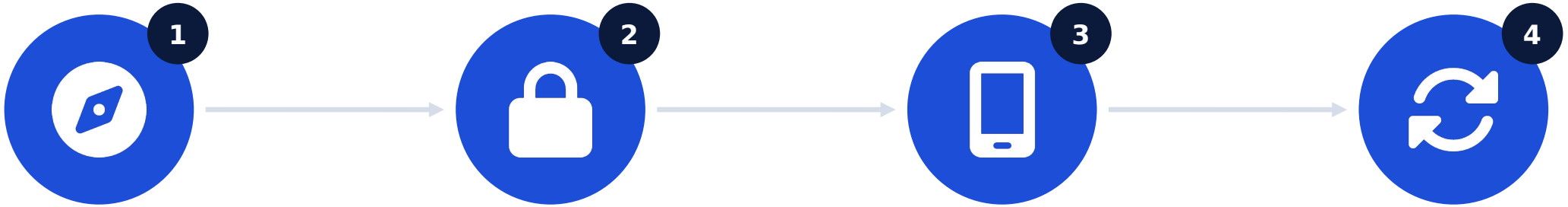
Which services leaked it

Change passwords

Start with those services

A result means your email appeared in a leak, not that you were hacked. Change any reused passwords now.

Step 2: Set up a password manager



Choose one

Built-in or Bitwarden, 1Password

Create a master password

A long passphrase you never reuse

Install everywhere

Computer, phone, browser

Replace weak passwords

Generate unique ones

Built-in options: Apple Passwords (iPhone and Mac) and Google Password Manager (Android and Chrome).

Weak versus strong passwords

Weak		Strong
Same password on many sites	→	A different password for every account
Short words and names: tanaka1985	→	Long and random, created by your password manager
Changing one character each time	→	A passphrase for your master password: river-lantern-mango-87
Saved in a notes app or on paper at your desk	→	Stored only in your password manager

Step 3: Turn on multi-factor authentication

Account	Where to find it	Best option
Google	Google Account › Security › 2-Step Verification	Passkey or authenticator app
Microsoft	Microsoft account › Security › Advanced security options	Authenticator app
Facebook and Instagram	Accounts Center › Password and security › Two-factor	Authenticator app
Apple ID	Settings › your name › Sign-In & Security	Two-factor (on by default)
Bank and work accounts	Security or login settings	Follow the provider’s method

Which second factor is safest?



Best: passkeys and security keys

Resist phishing because they only work on the real website



Good: authenticator app

Six-digit codes from an app such as Microsoft or Google Authenticator



Basic: SMS codes

Better than nothing, but texts can be intercepted or redirected

Your checklist

- [ ] Checked every email address on haveibeenpwned.com
- [ ] Installed a password manager on computer and phone
- [ ] Created a strong, unique master password
- [ ] Changed reused passwords, starting with email
- [ ] Turned on MFA for email accounts
- [ ] Turned on MFA for bank and payment accounts
- [ ] Turned on MFA for social media
- [ ] Saved backup codes somewhere safe and offline

Secure your email first: whoever controls your email can reset almost every other password.

Check your work

1. Why should your email account be the first one you secure?

2. Which second factor is the most resistant to phishing?

3. What should you do with MFA backup codes?

Answers are in the training guide.

Well done

- Every account now has its own strong password.
- Your most important accounts have a second lock.
- You know which accounts appeared in breaches.

Next: Training 2 · Secure Your Devices