

The Everyday **Security** Checklist

25 simple things you can do to lock down your digital life — no jargon, no fear, just a clear list to work through at your own pace.

You do not need to be a tech expert to be safe online. Most break-ins happen through a handful of small, fixable gaps. Work down this list whenever you have a few spare minutes and tick each box as you go. Start at the top — the first five matter most.

START HERE

The five that protect you the most

- ☐ **Lock down your email first.** Give it a long, unique passphrase. It is the master key that can reset every other account.
- ☐ **Turn on two-factor authentication.** Start with email, banking, and your main social accounts.
- ☐ **Set up a password manager.** Let it create and remember a different password for every site.
- ☐ **Replace every reused password.** If one site is breached, reused passwords hand over all the others.
- ☐ **Switch on automatic updates.** Phone, computer, and apps. Most updates quietly close security holes.

SPOT THE EVERYDAY THREATS

Scams and phishing

- ☐ **Learn the phishing tell-tales.** Urgency, a link to click, and a request for personal info. Two or three together is a red flag.
- ☐ **Never click links in unexpected messages.** Go to the website yourself by typing the address instead.
- ☐ **Verify "your account is locked" warnings.** Log in directly, never through the link in the message.
- ☐ **Hang up on surprise "support" calls.** Your bank and tech companies will not cold-call asking for codes or remote access.
- ☐ **Slow down when something feels urgent.** Panic is the scammer's main tool. A 30-second pause defeats most of them.

PROTECT YOUR DEVICES AND DATA

Phones, computers, Wi-Fi

- 🔒 **Put a screen lock on every device.** A PIN, fingerprint, or face unlock stops a lost phone becoming a disaster.
- 🔒 **Turn on full-disk encryption.** FileVault on a Mac, BitLocker on Windows. It is free and built in.
- 🔒 **Back up your important files automatically.** Follow 3-2-1: three copies, two types of storage, one off-site.
- 🔒 **Use a VPN on public Wi-Fi.** Airports, cafes, and hotels are the easy places to get snooped on.
- 🔒 **Rename your home Wi-Fi and give it a strong password.** Avoid using your name or address in the network name.
- 🔒 **Change your router's default admin login.** The factory username and password are public knowledge.
- 🔒 **Review app permissions.** Turn off camera, microphone, and location access that an app does not need.
- 🔒 **Sign out of old devices.** Remove your accounts from phones and laptops you no longer use.

PEOPLE AND RECOVERY

Family, identity, and bouncing back

- 🔒 **Set recovery options on key accounts.** A backup email and phone number so you can get back in if locked out.
- 🔒 **Save your two-factor backup codes offline.** Print them or store them somewhere safe away from your phone.
- 🔒 **Talk to your kids about what not to share.** Names, schools, locations, and photos that give too much away.
- 🔒 **Freeze your credit.** It is free, and you can lift it temporarily when you actually need credit.
- 🔒 **Switch on bank and card alerts.** Real-time notifications catch fraud far faster than a monthly statement.
- 🔒 **Have a simple "if I get hacked" plan.** Know which account to secure first and who to contact.

One habit beats this whole list: when anything online makes you feel rushed or scared, stop and slow down. **Urgency is the scammer's favourite weapon.** Almost every attack falls apart the moment you pause and check.

Want a steady stream of plain-English security tips?

Get one short, useful email a week — a scam alert, a quick fix, or a new guide. No fear-mongering, no jargon. asecuritygeek.com