

# Online Safety Checklist

*Checklist · The Non-Negotiable Basics Every Internet User Should Run Through Yearly.*

**If you do nothing else this year for your digital safety, do these. 25 actions across five layers of defence — accounts, devices, network, family, awareness.**

## Accounts (5 Min)

- Email account uses a long unique password and authenticator-app MFA (not SMS).
- Bank and brokerage accounts have transaction alerts enabled.
- Password manager installed and in active daily use.
- Have I Been Pwned alerts enabled for every email I use.
- MFA enabled on social media (Facebook, Instagram, X, LinkedIn).

## Devices (10 Min)

- Phone auto-locks within 60 seconds, requires biometric or passcode to unlock.
- Phone OS up to date (Settings → General → Software Update).
- Laptop has full-disk encryption (FileVault on Mac, BitLocker on Windows).
- Laptop OS up to date.
- Antivirus running on Windows (Defender is fine for most users).
- Find My iPhone / Find My Device enabled for remote-wipe capability.

## Network (5 Min)

- Wi-Fi router is using WPA3 or WPA2-AES (NOT WEP, NOT 'mixed mode').
- Default router admin password has been changed.
- Router firmware auto-update is enabled.
- Guest Wi-Fi network is set up for IoT devices and visitors.
- WPS, UPnP, and remote management are turned OFF in router settings.

## Family (5 Min)

- Spouse / partner has their own password manager and MFA on email.
- Kids' devices have parental controls (Apple Screen Time / Google Family Link) active.
- Elderly parents have fraud alerts and login alerts on their bank.
- Family has a verify-word system for any urgent money request.

## Awareness (5 Min)

- I never click links in 'bank,' 'IRS,' or 'shipping' texts — I open the app directly.

- I never send gift cards, wire transfers, or Zelle to anyone I don't know in person.
- I check Have I Been Pwned (haveibeenpwned.com) at least once a year.
- I have my credit frozen at all 3 bureaus (Equifax, Experian, TransUnion).
- I have a free identity-theft monitoring tool set up (HIBP, Mozilla Monitor, or paid IDP).

**TRY THE TOOL**

**Is That Email A Scam? Find Out In 10 Seconds.**

Run any suspicious email through our free Scam Detector. It checks the link, sender, and language patterns instantly.

**Visit Making Sense Of Security →**