Cyber Safety Checklist for Beginners

Simple steps to protect your phone, computer, and accounts - without being a tech expert.

Who this is for	Newbies, families, seniors, and small-business owners who want practical protection.
How to use it	Print it or open it on your phone. Check items off. Start with the 10-minute quick start.
Writer	IM Secure
Version date	December 31, 2025

Important: This is general guidance, not legal advice or a guarantee. If you believe money or identity was stolen, act quickly (see the Incident Checklist).

Table of Contents

1) The 10-minute quick start (do this first)

If you only do one section, do this one. These steps stop most common attacks: account takeovers, password guessing, and many scams.

You do not need to understand hacking. You just need a few habits and settings.

> **Tip** Start with email. If someone controls your email, they can reset passwords everywhere.

Checklist

[ ]	Turn on automatic updates on your phone and computer.
[ ]	Turn on 2-step verification (2FA) for your email first, then your banking, then your social accounts.
[ ]	Use a password manager (or at least stop reusing passwords).
[ ]	Check your main email account for suspicious forwarding rules and unknown devices.
[ ]	Back up your phone (cloud backup) and your computer (external drive or cloud).
[ ]	Put a screen lock on every device (PIN or passcode).
[ ]	If you get a scary message: do not click. Pause. Verify using a known number or official website.

2) Passwords and logins (the biggest win)

Most people get hacked because of weak or reused passwords. A password manager is the easiest solution: it creates strong passwords and remembers them for you.

2-step verification (2FA) means you need a second proof (like an app code) to log in. It stops many takeovers even if your password leaks.

> **Tip** If you must write passwords down, keep them in a safe place like a locked drawer - not on a sticky note on the monitor.

Checklist

[ ]	Use a password manager (1Password, Bitwarden, iCloud Keychain, Google Password Manager, etc.).
[ ]	Change any password that is reused across sites. Reuse is the #1 problem.
[ ]	Make important passwords long (12+ characters). Longer beats complicated.
[ ]	Turn on 2FA for email, banking, Apple ID / Google account, and social media.
[ ]	Prefer authenticator app codes or security keys over SMS when possible.
[ ]	Do not share verification codes with anyone. Real support will not ask for them.
[ ]	Set account recovery options: recovery email, recovery phone, and save backup codes.

3) Your phone (iPhone/Android)

Your phone is your wallet, your mail, and your identity. Treat it like keys to your house.

Good news: phones are secure by default. Most risk comes from risky links, unknown apps, and weak account settings.

Tip	If your phone ever asks you to install a 'profile' or 'management certificate' and you are not in IT at work, stop and ask for help.

Checklist

[ ]	Use a 6-digit (or longer) passcode. Do not use 000000, 123456, or birthdays.
[ ]	Turn on Face ID / fingerprint if you like, but keep a strong passcode.
[ ]	Turn on device encryption (usually on by default) and keep the screen lock on.
[ ]	Turn on Find My iPhone / Find My Device so you can locate or erase a lost phone.
[ ]	Only install apps from the official store. Avoid random app download sites.
[ ]	Remove apps you do not recognize or do not use.
[ ]	Review app permissions (Location, Microphone, Photos). Turn off what is not needed.
[ ]	Turn on automatic system updates and app updates.
[ ]	Use a VPN only if you trust the provider. A bad VPN can be worse than no VPN.

4) Your computer (Windows/Mac)

Keep your computer updated and do not disable built-in security. Most infections happen through old software or fake downloads.

Tip	If a pop-up says your computer is infected and asks you to call a number, it is almost always a scam.

Checklist

[ ]	Turn on automatic updates for the operating system.
[ ]	Update your browser (Chrome/Edge/Firefox/Safari) and remove unused extensions.
[ ]	Use antivirus: Windows Security (built-in) is fine for most people. On Mac, built-in protections are strong; still keep updates on.
[ ]	Turn on a firewall (Windows: on by default; Mac: consider enabling in settings).
[ ]	Create a separate 'daily' account that is not an admin (best practice).
[ ]	Do not download cracked software. It is a common infection source.
[ ]	If you must install software, download only from the official site (not ads).

5) Email safety

Email is the master key. Hackers want your email because it can reset other passwords.

Many scams are simply fake emails that pressure you to click fast.

Tip	If an email claims to be from your bank, do not click the link. Open your bank app or type the website yourself.

Checklist

[ ]	Turn on 2FA for your email account.
[ ]	Check 'security' page: remove unknown devices and sign out of others.
[ ]	Check forwarding rules: remove any rule you did not create.
[ ]	Disable auto-forwarding to unknown addresses.

[ ]	Be suspicious of urgent requests: 'invoice overdue', 'account locked', 'verify now'.
[ ]	Hover over links on a computer to see where they really go.
[ ]	Do not open unexpected attachments, especially .zip, .exe, or macro-enabled Office files.

6) Web browsing and downloads

Your browser is where most tricks happen: fake 'update' popups, fake support pages, and dangerous downloads.

Tip	If you see a pop-up that looks like a system message inside the browser, it is usually just a webpage pretending.

Checklist

[ ]	Use a modern browser and keep it updated.
[ ]	Install updates only from the browser itself or the official app store - never from a random pop-up.
[ ]	Block pop-ups and reduce notifications. Do not allow unknown sites to send notifications.
[ ]	Avoid browser extensions unless you really need them.
[ ]	When downloading, verify the site is correct (spelling matters).
[ ]	Use an ad blocker if you can (it reduces malicious ads).

7) Home Wi-Fi and router basics

Your router is the front door to your home internet. A few changes make a big difference.

Tip	The router admin password and the Wi-Fi password are two different things. Change both.

Checklist

[ ]	Change the router admin password (not the Wi-Fi password).
[ ]	Use WPA2 or WPA3 security for Wi-Fi (avoid WEP).

[ ]	Use a strong Wi-Fi password and do not share it publicly.
[ ]	Create a guest Wi-Fi for visitors and smart devices if available.
[ ]	Keep router firmware updated (many routers can auto-update).
[ ]	Place the router in a safe spot at home (avoid easy physical access).

8) Backups (so you never panic)

Backups protect you from ransomware, broken devices, and accidental deletion. Backups are peace of mind.

Tip	A backup is only real if you can restore from it.

Checklist

[ ]	Turn on phone backups (iCloud backup or Google backup).
[ ]	Back up photos to a trusted cloud (or export to an external drive monthly).
[ ]	Back up your computer: external drive + automatic backup (Time Machine, File History, or a backup tool).
[ ]	Keep at least one backup that is not always connected (protects against ransomware).
[ ]	Test a restore once (open a backed-up file to confirm it works).

9) Scams, fraud, and social engineering

Most 'hacks' are actually scams. Scammers use fear, urgency, and authority to make you act fast.

Rules: slow down, verify, and never pay with gift cards or crypto because someone told you to.

Tip	The best scam defense is a pause: take 60 seconds and ask, 'How would I verify this without using their link or their number?'

Checklist

[ ]	If someone pressures you to act fast, slow down. Urgency is a scam tool.

[ ]	Never share one-time codes or passwords, even with someone claiming to be support.
[ ]	Do not move money because of a phone call. Hang up and call the official number yourself.
[ ]	Ignore 'romance' or 'investment' messages from strangers, especially if they mention crypto.
[ ]	Be careful with QR codes in public. Use official sources.
[ ]	Use a credit card for online purchases when possible (better protections than debit).

10) Social media privacy

Social accounts get targeted because they can spread scams to your friends and family.

Tip If your account sends strange messages to friends, assume it is compromised and change password + enable 2FA immediately.

Checklist

[ ]	Turn on 2FA for social accounts.
[ ]	Review privacy settings: who can see posts, phone number, email, friends list.
[ ]	Remove unknown friends/followers and suspicious messages.
[ ]	Limit what you share publicly: birthdate, address, travel plans, ID photos.
[ ]	Beware of quizzes and 'fun' apps that ask for account access.

11) Kids and family settings

Families are often targeted through kids' devices, shared tablets, and shared passwords.

Tip Simple family rule: no one installs apps without asking first.

Checklist

[ ]	Create separate user profiles for each person on shared devices.
[ ]	Use parental controls for app installs and screen time.

[ ]	Teach kids: never share passwords, never meet strangers from apps, and ask before clicking links.
[ ]	Review device location sharing and who can see it.
[ ]	Use a family password manager plan if possible.

12) Small business essentials (simple but important)

Small businesses get hit with fake invoices, hacked email, and ransomware. You do not need expensive tools to improve security quickly.

Tip The most common business loss is a fake wire or invoice. Always verify bank changes using a known phone number.

Checklist

[ ]	Use business email with 2FA for every user (no exceptions).
[ ]	Use separate accounts for each employee (no shared logins).
[ ]	Use a password manager for the team.
[ ]	Set up backups for critical files and test restore monthly.
[ ]	Use a reputable endpoint protection tool if you can (or at least keep updates on).
[ ]	Enable multi-factor on bank, payroll, and accounting platforms.
[ ]	Use a 'two-person check' for wire transfers and bank detail changes.
[ ]	Have an incident plan: who to call, what to shut down, where backups are.

13) If something goes wrong (incident checklist)

If you suspect your account or device is compromised, do not panic. Do these steps in order.

If money is involved, time matters. Act the same day.

Tip Do not keep using a device you think is infected for banking or password changes.

Checklist

[ ]	Disconnect the device from the internet (Wi-Fi off, unplug ethernet) if malware is suspected.
[ ]	From a safe device, change your email password and turn on 2FA if not already on.
[ ]	Change passwords for bank and important accounts. Log out of all sessions where possible.
[ ]	Check your email forwarding rules and account recovery settings.
[ ]	Run antivirus / security scan and remove suspicious apps/extensions.
[ ]	Contact your bank/card provider if payments were made. Ask about fraud process.
[ ]	If identity theft is suspected, place a fraud alert or credit freeze (country dependent).
[ ]	Tell close contacts if your social account was used to message them.
[ ]	Write down what happened: dates, messages, phone numbers, transaction IDs.
[ ]	If you need help, contact a trusted local IT professional or incident response service.

14) Weekly / monthly checklist pages

Print this page and keep it somewhere easy. The goal is simple habits, not perfection.

Weekly	Monthly
[ ] Check for device updates (phone and computer). [ ] Look at your email inbox for suspicious 'security' messages you did not request. [ ] Delete or unsubscribe from junk mail that looks risky. [ ] Check bank/credit card transactions quickly (spot fraud early).	[ ] Review your important accounts: change reused passwords and keep 2FA on. [ ] Check your router for updates and confirm Wi-Fi password is still private. [ ] Confirm backups are running (open a backed-up file). [ ] Review installed apps and browser extensions - remove what you do not need.

Personal notes

15) Glossary (plain English)

2FA / MFA	Extra login step after your password (like a code from an app).
Authenticator app	An app that makes login codes (more secure than SMS).
Backup	A safe copy of your files in case your device breaks or gets infected.
Data breach	When a company leaks user data (emails, passwords, etc.).
Malware	Bad software that steals data or damages your device.
Phishing	A fake message that tricks you into clicking or giving info.
Ransomware	Malware that locks your files and demands money.
VPN	A service that routes your internet traffic through another company. Useful sometimes, but choose carefully.

Need help building a safer setup for your home or small business? IM Secure can help you prioritize what matters and keep it simple.