Salus

A PERSONAL SECURITY CHECKLIST

Short goals, grouped by area. Check each one off as you complete it.

01 Passwords

- ☐ Use one password manager for every login.
- ☐ Run its breach check (Watchtower in 1Password) and fix breached, reused, and weak passwords, starting with email, Apple or Google, bank, and brokerage.
- ☐ Give every site its own generated password, with no scheduled rotation.
- ☐ Save recovery codes, credit-freeze PINs, and disk-encryption recovery keys in the manager.
- ☐ Turn off the browser's built-in password saving after moving those logins into the manager.

02 Two-factor authentication (2FA)

- ☐ Buy two hardware security keys, one carried and one kept at home.
- ☐ Put security keys on these accounts first: Apple ID, Google, email, the password manager, banks, brokerages, social media accounts, and GitHub.
- ☐ Use security keys everywhere else they're offered. Where they aren't, use the next best option in this order: passkeys, authenticator-app codes stored in the password manager, then text-message codes as a last resort.
- ☐ Remove the phone number as a backup sign-in method where possible, and list any accounts still relying on text-message codes.
- ☐ Rotate old developer API tokens.

03 Old accounts

- ☐ Use the password manager as the master list of accounts you have.
- ☐ For any account you don't recognize or no longer use, sign in, delete your data, delete the account, and then delete its entry in the password manager.
- ☐ Review "Sign in with" and connected-app access on Google, Apple, Facebook, X, and GitHub.
- ☐ Delete accounts and apps for devices you no longer use.

04 Identity

- ☐ Freeze credit at Equifax, Experian, and TransUnion.
- ☐ Freeze ChexSystems and NCTUE. Innovis and Early Warning are optional.
- ☐ Review what you share on social media. Keep personal details to a minimum, like birthday, hometown, address, phone, family names, and where you are right now, and restrict who can see your posts and profile.
- ☐ Submit opt-outs to people-search sites (Spokeo, Whitepages, BeenVerified, That'sThem, Radaris, the PeopleConnect group, MyLife, Nuwber, TruePeopleSearch, FastPeopleSearch), and follow up until each one confirms.
- ☐ Re-check those sites regularly for new listings.
- ☐ Sign up for Have I Been Pwned breach alerts on every email address.

05 Phone

- ☐ Turn on your carrier's Number Lock and SIM protection.
- ☐ Turn on theft protection: Stolen Device Protection on iPhone, or Theft Protection and Identity Check on Android.
- ☐ Turn on the strongest cloud backup encryption available: Advanced Data Protection on iPhone, with a recovery contact and a paper recovery key. On Android, use the closest equivalent, such as Google's encrypted backups or Advanced Protection.
- ☐ Use a longer alphanumeric passcode.
- ☐ Delete apps you don't use, limit which apps can run in the background, and restrict each app's access to location, contacts, photos, camera, mic, and other app data.

06 Home network

- ☐ Review every device connected to the router.
- ☐ Reset smart devices you don't use and take them off Wi-Fi.
- ☐ Change the router's admin password from the default.
- ☐ Confirm remote management is off.
- ☐ Turn off UPnP, NAT-T, and WPS.
- ☐ Use WPA2 or WPA3 on the Wi-Fi.

07 Computers

- ☐ Check that the firewall, System Integrity Protection, and Gatekeeper are on.
- ☐ Turn on FileVault disk encryption.
- ☐ Turn on automatic OS and App Store updates.
- ☐ Delete apps you don't use, limit which apps run in the background or at login, and restrict each app's access to location, contacts, files, camera, mic, and other app data.
- ☐ Limit self-hosted services to the machine itself or a private network like Tailscale.
- ☐ Remove unused public routes, stale devices, and background services.
- ☐ Optionally, add DNS filtering such as NextDNS and confirm it's working.

08 Browser

- ☐ Keep the browser updated and run its Safety Check.
- ☐ Keep extensions to a minimum and restrict their site access.
- ☐ Turn on Enhanced Safe Browsing and secure DNS.
- ☐ Review camera, mic, location, and notification permissions.
- ☐ Install an ad blocker (uBlock Origin Lite) set up conservatively.
- ☐ Set up an automatic schedule for clearing browser data (monthly is recommended).

09 Finances

- ☐ Turn on login and transaction alerts at every bank, card, and brokerage.
- ☐ Review statements every month.
- ☐ Use virtual or single-use cards for everyday shopping.
- ☐ Lock cards you rarely use.

10 Family

- ☐ Agree on a family safe word.
- ☐ Set a rule to hang up and call back on a known number, and never act on urgency alone. If possible, check with another family member to gut-check the request.
- ☐ Agree on how, where, and when money gets sent in a real emergency.
- ☐ Walk older relatives and kids through passwords, two-factor sign-in, credit freezes, and phone protections.
- ☐ Run scam drills now and then so everyone gets practice spotting and handling a fake request.

Ongoing

- ☐ Hold a quarterly check-in: a clean breach check, keys on new accounts, freezes still on, extensions still minimal, nothing unfamiliar on the router, updates installed, people-search re-listings, and unused accounts and app access removed.
- ☐ Pull free credit reports once a year.