

# Secure Your Devices

Simple, senior-friendly steps to lock down laptops, phones, and tablets — plus password managers & antivirus setup.

1

## First things first (do these on every device)

- Update everything: Turn on automatic updates for Windows/macOS, iOS/iPadOS, Android, browsers, and apps.
- Auto-lock: Lock after 1–3 minutes idle; require PIN/password/biometric to unlock.
- Backups:
  - Phones/Tablets: iCloud/Google One automatic backup daily.
  - Computers: External drive backup weekly (Windows File History / macOS Time Machine) or cloud (OneDrive/iCloud/Drive).
- Find-My: Enable Find My iPhone / Find My Device and keep location on for lost-device recovery.
- Remote-access rule: Do not give remote access until you verify the company's identity. If you're an existing Saffron Guru customer, never allow remote access without the official Saffron Guru password provided by our tech during the call.

2

## Passwords the right way (with a password manager)

- Pick one password manager (any reputable one). Install it on all devices.
- Create a strong master password (at least 4–5 random words). Write it on paper and store safely.
- Turn on 2-Step Verification for the password manager (authenticator app preferred).
- Store every login in the manager and let it generate 16+ character random passwords.
- Use unique passwords for: email, bank, shopping, social media, cloud storage.
- Emergency access: Add a trusted family member as the manager's emergency contact so they can help if needed.

# Antivirus & Device Protection

## Windows (11/10)

- Windows Security → Real-time protection ON.
- SmartScreen → ON (blocks dangerous downloads).
- Ransomware Protection → ON (Controlled Folder Access).
- Optional: a reputable paid suite is fine, but never run two AVs at once.

## macOS

- Keep macOS updated (includes XProtect/Gatekeeper).
- App Store only or identified developers; avoid random downloads.
- Consider a reputable security suite if you share files with Windows users.

## iPhone/iPad (iOS/iPadOS)

- Keep iOS updated; no need for "antivirus" apps.
- App Store only; disable profiles you don't recognize (Settings → General → VPN & Device Management).
- Use Screen Time → Content & Privacy to prevent accidental installs.

## Android

- Google Play Protect → ON. Play Store only (no APKs).
- Update system & apps; remove apps you don't use.
- Consider a reputable security app with anti-phishing for the browser.

## Phone safety (SIM, calls, messaging)

- SIM PIN: Turn on a SIM PIN to block SIM-swap abuse.
- Two-factor codes: Never share OTP with anyone.
- Unknown callers/texts: Don't tap links; add bank & doctor official numbers to Contacts now.
- Spam filters: Turn on Silence Unknown Callers (iPhone) or Spam protection (Android).

## Safer browsing & email

- One primary browser (Chrome, Edge, Safari, Firefox) kept updated.
- Extensions (optional): a reputable ad/tracker blocker to cut malicious pop-ups.
- Bookmarks for banks: type the address once, bookmark it, use the bookmark every time.
- Hover & inspect links in email. If unsure: don't click —open the site yourself.

# Home Network & Data Protection



## Home Wi-Fi & router

- Change the router admin password (not the Wi-Fi password—the admin one).
- Wi-Fi security: WPA2/WPA3, a long unique Wi-Fi password.
- Update router firmware twice a year.
- Guest network for visitors; no WPS; hide/disable remote admin.

## Lock down data if a device is lost

- Enable full-disk encryption (Windows BitLocker / macOS FileVault; most phones are encrypted by default).
- Know how to wipe remotely: Test "Find My" / "Find My Device."
- Carrier lock: If lost, call your carrier to suspend the SIM.

### ⚠ Red-flag refresher (device edition)

- Pop-ups yelling "VIRUS DETECTED" with a number to call → close the tab/app, do not call.
- Anyone asking to install remote software right away → stop and verify with the company directly.
- Requests for gift cards/crypto/wires → treat as scam.

# Monthly 5-minute checkup

Run updates (OS, browser, apps)

Open the password manager → fix any weak/reused passwords it flags

Check bank/email for unusual activity; ensure alerts are working

Verify backups completed (last backup date)

Skim your phone for new or suspicious apps; remove anything you don't recognize

---

**Saffron Guru LLC**

Toll-Free: 844-313-4987

Email: [info@saffronguru.com](mailto:info@saffronguru.com)

 [www.saffronguru.com](http://www.saffronguru.com)

Available 7 days a week to protect you with digital security, scam protection, anti-hacking, and IT support.