

# 3. Your Devices

- [3.1 Software and App Safety](#)
- [3.2 Mobile Device Hardening](#)
- [3.3 Operating System Hardening](#)
- [3.4 Physical Security](#)
- [3.5 Data Lifecycle and Disposal](#)

# 3.1 Software and App Safety

*Core Concepts: Minimize Your Exposure, Protect Your Data*

Malware often disguises itself as legitimate software. A free game, a helpful utility, even a security tool can hide viruses, spyware, or ransomware. The software you install is one of the largest parts of your attack surface. Knowing what's safe to install, and what to avoid, is critical.

## 3.1.1 Understanding Software Risks

Every piece of software you install increases your attack surface; the number of ways someone could compromise your system. Even legitimate software can have security vulnerabilities that attackers exploit.

### **Common ways malicious software spreads:**

- Fake versions of popular software on download sites
- "Free" versions of paid software (pirated/cracked)
- Browser extensions that promise useful features
- Mobile apps that look legitimate but aren't
- Software bundled with other installations
- Attachments in phishing emails

**Think before you install.** Every piece of software is a potential security risk. Ask yourself:

- Do I really need this?
- Is this from a trustworthy source?
- Have I checked reviews and permissions?
- What's the worst that could happen if this is malicious?

When in doubt, don't install it.

## 3.1.2 The Basics

- Never use pirated software

- Use official app stores
- Verify download sources
- Watch out for bundles
- Understand app permissions

# Never Use Pirated Software

**This cannot be emphasized enough: Pirated or "cracked" software is one of the most common ways to get infected with malware.**

## **Why pirated software is dangerous:**

- The crack/keygen itself is often malware
- No way to verify what's been modified in the software
- Can't receive security updates
- Often bundled with adware, spyware, or ransomware
- You have no recourse if something goes wrong

## **Alternatives to piracy:**

- Use free, open-source alternatives (LibreOffice instead of Microsoft Office, GIMP instead of Photoshop)
- Use free versions or trials to see if you actually need the paid version
- Look for student discounts or educational licenses
- Use subscription services when available (often cheaper than buying outright)
- Wait for sales and discounts

# Use Official App Stores Only

App stores vet software before allowing it in their store. While not perfect, this dramatically reduces your risk.

## **Mobile devices:**

- iPhone/iPad: Apple App Store only
- Android: Google Play Store (avoid "sideloading" APK files unless you really know what you're doing)

## **Desktop computers:**

- Windows: Microsoft Store or directly from the software maker's website
- Mac: Mac App Store or directly from the software maker's website
- Linux: Official repositories for your distribution (apt, yum, pacman, etc.) or directly from the software maker's website

## **Avoid:**

- Download sites like download.com, softonic.com, or similar aggregators
- Torrent sites
- Warez or "cracked software" sites
- Pop-up ads claiming you need to download something
- Email attachments claiming to be software updates

## **Other potentially useful software sites (use these with caution):**

- Homebrew: Package manager for Mac and Linux - <https://brew.sh/>
- Open Source Initiative: Non-profit org dedicated to open source collaboration - <https://opensource.org/>
- Github: Open source software repo - <https://github.com>

# Verify Download Sources

When downloading directly from a website instead of an app store, make sure you're downloading from the official publisher

## **Steps to verify:**

- Go directly to the software maker's website, don't use download buttons from search results or ads
- Check the URL carefully, is it the real company website?
- Look for HTTPS (padlock icon) in the address bar
- Avoid third-party download mirrors unless they're official (like SourceForge for open source)

*Example:* You want VLC media player. Search "VLC official download" and go to videolan.org (the real site), not vlc-player-download.com (fake).

# Watch for Bundled Software

Some legitimate software tries to install additional programs during installation, toolbars, antivirus trials, browser plug-ins.

## **How to avoid unwanted software:**

- Always choose "Custom" or "Advanced" installation, never "Express" or "Recommended"
- Read every screen during installation
- Uncheck boxes for additional software you don't want

- Watch for pre-checked boxes that make the default "Install toolbar" or "Change homepage"
- When in doubt, decline everything except the main program

# Understand App Permissions

Permissions tell you what an app can access on your device. Always check permissions before installing.

## **Ask yourself: Does this make sense?**

- Photo editing app wants camera access? Makes sense.
- Flashlight app wants contacts and location? Suspicious.
- Weather app wants location? Makes sense.
- Calculator app wants microphone access? Suspicious.

## **Permissions to be extra careful about:**

- Contacts - access to everyone in your address book
- Location - where you are at all times
- Camera/Microphone - can record you without indication
- SMS/Phone - can read messages or make calls
- Storage - access to all your files
- Install other apps - can install malware

If permissions don't make sense for what the app does, don't install it.

## 3.1.3 Better Protection

- Review app permissions regularly
- Uninstall unused applications and software
- Keep software updated
- Be careful with browser extensions

# Review App Permissions Regularly

Apps can request additional permissions after installation. Review these periodically:

## **On iPhone:**

- Settings > Privacy & Security
- Check each category (Location, Contacts, Camera, etc.)

- Revoke access for apps that don't need it

### **On Android:**

- Settings > Privacy > Permission manager
- Review each permission type
- Remove permissions from apps that don't need them

### **On Windows:**

- Settings > Privacy & security
- Review Camera, Microphone, Location, and other permissions

### **On Mac:**

- System Settings > Privacy & Security
- Review each category and remove unnecessary access

Do this review quarterly.

## Uninstall Unused Apps and Software

Software you don't use is a security risk for no benefit. Every unused app is a potential vulnerability.

### **Monthly cleanup routine:**

- Look through your installed apps
- If you haven't used it in 3 months, uninstall it
- You can always reinstall later if you need it
- Don't keep trial software after the trial expires

### **How to properly uninstall:**

- Windows: Settings > Apps > Installed apps > Select app > Uninstall
- Mac: Open Applications folder, drag app to Trash, empty Trash
- Mobile: Press and hold app icon, select "Remove" or "Uninstall"

**Don't just delete the icon or folder:** Use the proper uninstall process to remove all components.

## Keep Software Updated

Software updates fix security vulnerabilities. Delaying updates leaves you exposed to known exploits.

### **Enable automatic updates for:**

- Operating system
- Web browsers
- Antivirus software
- Mobile apps
- Any software that handles sensitive data

**For software without auto-update:** Check for updates monthly. Most programs have a "Check for updates" option in their menu.

## Be Careful with Browser Extensions

Browser extensions have access to everything you do in your browser, every website you visit, everything you type, all your passwords.

### **Extension safety rules:**

- Install from the official browser store only (Chrome Web Store, Firefox Add-ons, etc.)
- Check the number of users - thousands or millions is better than dozens
- Read reviews, especially recent ones
- Only install extensions you truly need
- Review installed extensions quarterly and remove ones you don't use
- Be suspicious of extensions that were recently sold or changed developers

### **Red flags for extensions:**

- Requests excessive permissions
- Very few users or reviews
- Recent reviews mention ads or changed behavior
- Poor grammar in description

## 3.1.4. Extra Credit

- Use a sandbox for unknown software

## Use a Sandbox for Unknown Software

A sandbox is an isolated environment where you can run software without it affecting your main system. If the software is malicious, it's contained.

### **Sandbox options:**

- Windows Sandbox (Windows 10/11 Pro): Built-in, creates a temporary isolated environment
- Virtual machines (VirtualBox, VMware): Run a complete separate OS
- Online sandboxes <https://hybrid-analysis.com> upload files for automated analysis

This is advanced but very effective for testing questionable software safely.

# 3.2 Mobile Device Hardening

*Core Concepts: Protect Your Data, Minimize Your Exposure*

Your phone carries more personal data than your computer ever did, photos, messages, contacts, emails, banking apps, location history, health data, and more. It goes everywhere with you, making it vulnerable to loss, theft, and unauthorized access. It's also constantly connected to the internet, making it a target for remote attacks.

Mobile operating systems (iOS and Android) are designed with security in mind and include excellent built-in protections. The challenge is ensuring these features are enabled and properly configured.

## 3.2.1 Understanding Mobile Security

Mobile devices face unique security challenges:

- **Physical security:** Phones are easily lost or stolen
- **Always connected:** Constant internet access means constant exposure
- **App permissions:** Apps can access cameras, microphones, location, contacts
- **Public networks:** Frequently connect to unsecured WiFi
- **Personal data concentration:** Everything in one device

This section covers both iPhone (iOS) and Android. Follow the instructions for your device, or both if you use multiple phones or tablets.

## Mobile Security Habits

Beyond settings, develop these habits:

- **Lock your phone every time you put it down:** Press the power button to lock manually
- **Don't leave your phone unattended:** Even for "just a second"
- **Be careful what you connect to:** Public charging stations can compromise phones (use your own charger with a power adapter)

- **Avoid public WiFi for sensitive activities:** Use cellular data or a VPN for banking, shopping
- **Review installed apps monthly:** Uninstall apps you don't use
- **Don't jailbreak (iPhone) or root (Android):** This removes built-in security protections

Your phone is your most personal computer. It knows where you go, who you talk to, what you buy, what you search for, and holds keys to your digital life. Protecting it isn't paranoia, it's common sense.

Mobile platforms are pretty secure by default. You just need to enable the right settings, review permissions regularly, and develop good habits. Start with The Basics, add Better Protection over time, and remember, the most important security feature is the lock screen. Use it every time.

## 3.2.2 The Basics

- Set a strong passcode
- Enable Find My Device
- Enable automatic updates
- Review app permissions
- Disable lock screen notifications for sensitive apps
- Enable automatic backup

## Set a Strong Passcode and Enable Biometrics

Your lock screen is your first line of defense.

### **iPhone:**

- Settings > Face ID & Passcode (or Touch ID & Passcode)
- Set up Face ID or Touch ID if you haven't already
- Tap "Change Passcode"
- Tap "Passcode Options"
- Choose "Custom Alphanumeric Code" for strongest security
- Or at minimum, choose "Custom Numeric Code" with 6+ digits
- Avoid simple patterns like 123456 or repeating digits

### **Android:**

- Settings > Security > Screen lock
- Choose "Password" or "PIN" (6+ digits)
- Avoid "Pattern" as these are easier to observe and guess

- Set up fingerprint in Settings > Security > Fingerprint
- Or face unlock (varies by device manufacturer)

Biometrics are convenient for daily use, but the passcode is more secure against certain attacks (can't be compelled in court, can't be used while you're unconscious). See Understanding Biometrics in the Authentication topic.

## Enable Find My Device

If you lose your phone, you need to be able to locate it, lock it remotely, and erase it if necessary.

### **iPhone (Find My):**

- Settings > [Your Name] > Find My
- Turn on "Find My iPhone"
- Turn on "Find My network" (works even when offline)
- Turn on "Send Last Location" (sends location before battery dies)
- Test it: Open iCloud.com on a computer, sign in, click Find My iPhone

### **Android (Find My Device):**

- Settings > Security > Find My Device
- Turn it on
- Make sure Location is enabled: Settings > Location > On
- Test it: Visit [android.com/find](https://android.com/find) on a computer, sign in with your Google account

## Enable Automatic Updates

Mobile OS updates fix security vulnerabilities. Enable automatic updates so you're always protected.

### **iPhone:**

- Settings > General > Software Update
- Tap "Automatic Updates"
- Turn on "Download iOS Updates"
- Turn on "Install iOS Updates"
- Turn on "Security Responses & System Files"

### **Android:**

- Settings > System > System update (location may vary by manufacturer)
- Enable automatic downloads and installation

- For Google Play apps: Open Play Store > Profile icon > Settings > Network preferences > Auto-update apps > Over any network

# Review App Permissions

Apps request access to your camera, microphone, location, contacts, and more. Review what you've granted and revoke unnecessary permissions.

## **iPhone:**

- Settings > Privacy & Security
- Go through each category (Location Services, Camera, Microphone, Contacts, etc.)
- Review which apps have access
- Remove access from apps that don't need it
- For Location: Use "While Using the App" instead of "Always" when possible

## **Android:**

- Settings > Privacy > Permission manager
- Review each permission type (Camera, Location, Microphone, etc.)
- Tap each to see which apps have access
- Change to "Don't allow" or "Ask every time" for apps that don't need constant access

Do this review quarterly; apps update and request new permissions over time.

# Disable Lock Screen Notifications for Sensitive Apps

Notifications on your lock screen can reveal sensitive information to anyone who glances at your phone.

## **iPhone:**

- Settings > Notifications
- Tap each sensitive app (banking, email, messaging, dating apps)
- Turn off "Show on Lock Screen"
- Or change "Show Previews" to "When Unlocked"

## **Android:**

- Settings > Apps & notifications > Notifications
- Tap each sensitive app
- Turn off "Show on lock screen"

- Or choose "Don't show notification content"

## Enable Automatic Backup

If you lose your phone, you need your data backed up. Enable automatic cloud backup.

### **iPhone (iCloud Backup):**

- Settings > [Your Name] > iCloud > iCloud Backup
- Turn on "iCloud Backup"
- Backs up automatically when plugged in, locked, and on WiFi
- Free tier: 5GB (may need to purchase more storage for photos)

### **Android (Google Backup):**

- Settings > Google > Backup
- Turn on "Back up to Google Drive"
- Select what to back up (app data, call history, contacts, etc.)
- For photos: Open Google Photos app > Profile > Photos settings > Back up & sync > Turn on

## 3.2.3 Better Protection

- Enable remote wipe capability
- Use encrypted backups
- Disable USB accessories when locked
- Use one-time passwords for apps
- Review location services settings
- Turn off unused wireless features
- Review privacy and tracking settings

## Enable Remote Wipe Capability

If your phone is stolen and you can't recover it, you should be able to erase all data remotely.

### **iPhone:**

- Already enabled with Find My iPhone (see Basics section)
- To erase remotely: iCloud.com > Find My iPhone > Select device > Erase iPhone

Note: After erasing, you can't track it anymore

**Android:**

- Already enabled with Find My Device (see Basics section)
- To erase remotely: [android.com/find](https://android.com/find) > Select device > Erase device

Note: After erasing, you can't track it anymore

## Use Encrypted Backups

Cloud backups can be encrypted so even the backup provider can't access your data.

**iPhone (Advanced Data Protection):**

- Settings > [Your Name] > iCloud > Advanced Data Protection
- Turn on Advanced Data Protection
- This end-to-end encrypts most iCloud data (even Apple can't access it)
- Important: Save your recovery key; if you lose it and your devices, your data is unrecoverable

**Android:**

- Google backups are encrypted in transit and at rest
- For additional security, use third-party encrypted backup apps

## Disable USB Accessories When Locked

USB accessories can be used to attack locked phones. Disable them when locked.

**iPhone:**

- Settings > Face ID & Passcode (or Touch ID & Passcode)
- Scroll down to "Allow Access When Locked"
- Turn off "USB Accessories" (requires unlocking to connect)

**Android:**

- Some phones have "Block USB connections while locked" under Settings > Security and Privacy > More Security Settings

## Use One-Time Passwords for Apps

For email and other accounts accessed through apps, use app passwords instead of your main password.

- Gmail, iCloud, and other services offer app-specific passwords
- These passwords only work for that specific app
- If your phone is compromised, revoke the app password without changing your main password
- See the Use One-Time Passwords for Apps in the Authentication topic for more details

## Review Location Services Settings

Location tracking is convenient but invasive. Review what's tracking you and when.

### **iPhone:**

- Settings > Privacy & Security > Location Services
- Review each app
- Change apps to "While Using the App" instead of "Always" where possible
- Turn off "Precise Location" for apps that don't need exact coordinates

### **Android:**

- Settings > Location
- Tap "App location permissions"
- Review each app
- Change to "Allow only while using the app" instead of "Allow all the time"

## Turn Off Unused Wireless Features

Bluetooth, WiFi, and NFC create additional attack surfaces when not in use.

- Turn off Bluetooth when not using wireless headphones or accessories
- Turn off WiFi when out and about (prevents auto-connecting to malicious networks)
- Turn off NFC (contactless payments) when not actively using it

Use Control Center/Quick Settings for easy toggling.

## Review Privacy & Tracking Settings

Apps and advertisers track your activity across apps and websites. Limit this tracking.

### **iPhone:**

- Settings > Privacy & Security > Tracking
- Turn off "Allow Apps to Request to Track"
- Settings > Privacy & Security > Apple Advertising

- Turn off "Personalized Ads"

#### **Android:**

- Settings > Privacy > Ads
- Turn on "Opt out of Ads Personalization"
- Settings > Google > Manage your Google Account > Data & privacy
- Review "Activity controls" and turn off tracking you don't want

## 3.2.4 Extra Credit

- Use separate work and personal profiles
- Use secure folder / private space features
- Enable advanced privacy features
- Set up a SIM PIN
- Use lockdown mode (iPhone) for high-risk situations

## Use Separate Work/Personal Profiles (Android)

Android allows multiple user profiles or work profiles to keep personal and work data separated. This may already be a requirements and set up automatically depending on where you work and how you access work data on your phone. Contact your local IT center with any questions.

- Settings > System > Multiple users
- Add a user or work profile
- Each profile has separate apps, data, and settings
- Useful for: Separating work/personal, creating a "clean" profile for sensitive activities

## Use Secure Folder / Private Space Features

Some phones offer encrypted, hidden spaces for sensitive apps and files.

#### **Samsung Secure Folder:**

- Settings > Security and privacy > Secure Folder
- Encrypted space for apps, photos, files
- Separate authentication from main phone

### **Google Private Space (Android 15+):**

- Settings > Security & privacy > Private space
- Hidden apps and data with separate authentication

### **iPhone:**

- No built-in secure folder, but you can:
- Use the Hidden album for photos (Settings > Photos > scroll down, turn on "Use Face ID" for Hidden album)
- Use Notes app with password-protected notes

## Enable Advanced Privacy Features

### **iPhone (iOS 15+):**

- Mail Privacy Protection: Settings > Mail > Privacy Protection (hides IP address and prevents tracking pixels)
- Hide My Email: Settings > iCloud > Hide My Email (generate random email addresses for signups)
- Private Relay: Settings > iCloud > Private Relay (Safari browsing privacy, requires iCloud+)

### **Android:**

- Privacy Dashboard: Settings > Privacy > Privacy dashboard (see which apps accessed permissions recently)
- Microphone/Camera indicators: Green dot appears when apps use camera/mic
- Permission auto-reset: Settings > Privacy > Permission manager > (gear icon) > Remove permissions if app unused

## Set Up a SIM PIN

A SIM PIN prevents someone from using your SIM card in another phone (protects against SIM-swap attacks).

### **iPhone:**

- Settings > Cellular > SIM PIN
- Turn on SIM PIN
- Default is often 1234 - change it immediately

### **Android:**

- Settings > Security > SIM card lock
- Turn on "Lock SIM card"
- Change from default PIN

**Warning:** If you enter the wrong SIM PIN 3 times, you'll need a PUK code from your carrier to unlock it. Keep your carrier's customer service number handy.

# Use Lockdown Mode (iPhone) for High-Risk Situations

Lockdown Mode is an extreme security mode for people facing serious targeted threats (journalists, activists, executives).

- Settings > Privacy & Security > Lockdown Mode
- Severely restricts functionality to protect against sophisticated attacks
- Most people don't need this, only use if you're at genuine risk of targeted attacks

# 3.3 Operating System Hardening

*Core Concepts: Minimize Your Exposure, Protect Your Data*

Your operating system is the foundation of your computer's security. Everything else, your applications, your files, your passwords, sits on top of it. A properly configured OS blocks most attacks before they can start. A poorly configured one leaves the door wide open.

Modern operating systems have excellent security features built in. The challenge is that many of these features aren't enabled by default, or the default settings prioritize convenience over security. This section shows you how to configure your OS for better protection without making it unusable.

## 3.3.1. Understanding OS Security

Operating system hardening means configuring your system to be more resistant to attacks. This involves:

- Closing unnecessary entry points for attackers
- Enabling built-in security features
- Reducing what information your computer shares
- Making it harder for malware to run or spread
- Protecting your data even if your computer is stolen

We'll cover Windows, macOS, and Linux. Skip to the section for your operating system, or read them all if you use multiple systems.

## Maintaining Your Hardened System

OS hardening isn't a one-time task. Maintain your security:

- **Monthly:** Verify updates are installing, review privacy settings, check firewall status
- **Quarterly:** Review app permissions, startup programs, installed software
- **After major OS updates:** Re-check privacy settings (they sometimes reset)
- **When something breaks:** Document what you changed recently so you can undo it

**Remember:** Security is about balance. If a setting makes your computer too difficult to use, you'll disable it or work around it, defeating the purpose. Find the right balance between security and usability for your needs.

## 3.3.2. The Basics

- Enable automatic updates
- Use an antivirus
- Enable the built-in firewall
- Enable full-disk encryption
- Create separate accounts for each person
- Lock your screen when not in use
- Disable autoplay

## Enable Automatic Updates

**This is the single most important thing you can do.** Unpatched vulnerabilities are responsible for roughly half of all data breaches. Software vendors release updates to fix security holes; if you don't install them, you're leaving known vulnerabilities exposed.

### Windows:

- Settings > Windows Update > Advanced options
- Turn on "Receive updates for other Microsoft products"
- Under "Additional options" enable "Get the latest updates as soon as they're available"
- Let Windows restart when needed - yes, it's annoying, but necessary

### Mac:

- System Settings > General > Software Update
- Click the info button (i) next to "Automatic updates"
- Enable all update options: Check for updates, Download new updates, Install macOS updates, Install app updates, Install security responses

### Linux:

- Ubuntu: Software & Updates > Updates tab > Check for updates: Daily
- Enable "Install security updates automatically"
- Other distributions: Configure your package manager for automatic security updates

## Use an Antivirus

Modern operating systems come with built-in antivirus that's quite good. Make sure it's enabled and updating.

Part of a defense in depth strategy.

### **Windows Defender:**

- Settings > Privacy & security > Windows Security > Virus & threat protection
- Verify "Real-time protection" is On
- Verify "Cloud-delivered protection" is On
- Verify "Automatic sample submission" is On
- Run a quick scan occasionally

There is some debate as to whether these are necessary for Mac and Linux. While Unix-based and Linux operating systems are generally more secure (Mac is Unix-based), they are not immune to viruses. There is also a rise in development of malware for Linux-based operating systems as their use becomes more common. Also, there is more to malware than just viruses, and most modern antivirus solutions are able to detect and block access to websites known to be infected, monitor system processes for evidence of ransomware, and detect malicious web traffic. Make a risk-based decision for yourself: Is the risk of dealing with leaked personal information and ransomware worth the tiny amount of system resources protection requires? Personally, I recommend Sophos as part of a defense-in-depth strategy.

### **Mac XProtect:**

- Built-in and automatic, no configuration needed
- Updates automatically with system updates

### **Linux:**

- Linux malware is rare but not nonexistent
- ClamAV is the most popular open-source antivirus for Linux
  - Install: `sudo apt install clamav`
  - Update: `sudo freshclam`

## **Enable Built-In Firewall**

A firewall blocks unauthorized network connections to and from your computer. Every modern OS has one built in, make sure it's on.

### **Windows:**

- Settings > Privacy & security > Windows Security > Firewall & network protection
- Verify the firewall is "On" for all three network types: Domain, Private, and Public
- If any show "Off," click them and turn the firewall on

## Mac:

- System Settings > Network > Firewall
- Turn on the firewall
- Click "Options" and enable "Block all incoming connections" for maximum protection (note: this may interfere with file sharing and screen sharing, but you can add exceptions as needed)

## Linux:

- Ubuntu: Use UFW (Uncomplicated Firewall)
- Open Terminal and type: `sudo ufw enable`
- Check status with: `sudo ufw status`

# Enable Full-Disk Encryption

Encryption scrambles your entire drive so no one can access your files without your password. If your laptop is stolen, your data is protected. This is especially important for laptops and any computer with sensitive information.

**Important:** Back up your data before enabling encryption. While rare, problems during encryption can result in data loss.

## Windows (BitLocker - Windows Pro or higher):

- Type "BitLocker" in the search bar
- Click "Manage BitLocker"
- Click "Turn on BitLocker" for your system drive (usually C:)
- Choose how to unlock: password or USB key (password is more convenient)
- Save your recovery key in a safe place (password manager, printed and stored in a safe)
- Let the encryption process complete (can take hours, but you can use your computer)

Note: Windows Home edition doesn't include BitLocker. Consider upgrading to Pro or using VeraCrypt (free, open-source alternative).

## Mac (FileVault):

- System Settings > Privacy & Security > FileVault
- Click "Turn On FileVault"
- Choose whether to allow iCloud account to unlock the disk (convenient) or create a recovery key (more secure)
- Save the recovery key if you create one (a password manager is a good place)
- Restart when prompted

## Linux (LUKS):

- Easiest to enable during installation
- Most distributions offer "Encrypt this installation" option during setup
- If already installed, encrypting requires backing up, reformatting, and restoring

# Create Separate Accounts for Each Person

**Never share user accounts.** Each person should have their own account to provide security and privacy for everyone.

## On computers:

- Create standard (non-administrator) accounts for children
- Give each child their own username and password
- Keep at least one admin account for parents only
- Children will need parent approval to install software

## Windows:

- Settings > Accounts > Other users > Add a user
  - If they are not going to sign into their Microsoft account (for OneDrive and O365 access) select "I don't know this person's sign-in information"
  - Then "add a user without a Microsoft account"
  - This creates a standard account, to provide admin rights select "change account type" once the account has been fully created
- To add a child, Settings > Accounts > Family
  - Follow instructions to add a child to your Microsoft account
  - This automatically creates a standard account with parental controls

## Mac:

- System Settings > Users & Groups > Add Account
- Select "Standard" account type
- For children, enable "Parental Controls" after creating the account

# Lock Your Screen When Not In Use

Your screen should lock when you step away. This prevents someone from accessing your computer if you forget to lock it manually. On Windows use windows key + L; on Mac use command + control + Q; on Linux, use windows key + L (dependent on keyboard).

You should also set your screen to automatically lock in case you step away and forget.

## Windows:

- Settings > Personalization > Lock screen > Screen timeout settings
- Set "On battery power, turn off after" and "When plugged in, turn off after" to 15 minutes or less
- Settings > Accounts > Sign-in options > Require sign-in: Select "When PC wakes up from sleep"

#### **Mac:**

- System Settings > Lock Screen
- Set "Start Screen Saver when inactive" to 15 minutes or less
- Enable "Require password after screen saver begins or display is turned off": Immediately

#### **Linux (Ubuntu):**

- Settings > Privacy > Screen Lock
- Enable "Automatic Screen Lock"
- Set delay to 15 minutes or less

## Disable AutoPlay/AutoRun

When you connect a USB drive or CD, your computer can automatically run files. This is dangerous as malware often spreads via USB drives. Turn off AutoPlay.

#### **Windows:**

- Settings > Bluetooth & devices > AutoPlay
- Turn off "Use AutoPlay for all media and devices"
- Or set all device types to "Take no action"

#### **Mac:**

- Finder > Settings > General
- Uncheck boxes for external disks, CDs, DVDs showing on desktop or opening automatically

#### **Linux:**

- Ubuntu: Settings > Removable Media
- Set all media types to "Ask what to do" or "Do nothing"

## 3.3.3. Better Protection

- Review and minimize privacy settings

- Configure user account control (Windows)
- Enable antivirus and keep it updated
- Disable unnecessary services (Windows)
- Disable legacy network protocols (Windows)
- Review startup programs

## Review and Minimize Privacy Settings

Modern operating systems collect data about how you use your computer. Some of this is for diagnostics, some for targeted advertising. Review these settings and turn off what you don't need.

### Windows:

- Settings > Privacy & security
- Go through each category on the left and turn off what you don't need:
  - General: Turn off advertising ID, website language access, Start menu suggestions
  - Diagnostics & feedback: Choose "Required diagnostic data" (minimum)
  - Activity history: Turn off "Store my activity history"
  - Location: Turn off unless needed
  - Camera/Microphone: Review which apps have access, remove unnecessary ones
- Review these periodically as Windows updates sometimes reset them or add more

### Mac:

- System Settings > Privacy & Security
- Review each category (Location Services, Analytics, etc.)
- Turn off what you don't need
- Review app permissions for Camera, Microphone, Contacts, etc.

### Linux:

- Privacy concerns are generally less with Linux as most distributions don't collect telemetry data by default
- Ubuntu: Settings > Privacy

## Configure User Account Control (Windows)

User Account Control (UAC) prompts you when programs try to make system changes. Make sure it is configured to always notify you.

- Type "UAC" in the search bar
- Click "Change User Account Control settings"
- Move the slider to the top: "Always notify"

- Yes, this is slightly annoying, but it's also what stops malware from making unauthorized changes.

# Disable Unnecessary Services (Windows)

Windows runs many background services. Some are necessary, others aren't. Disabling unused services reduces attack surface.

## Safe services to disable for most users:

- Remote Registry - unless you manage computers remotely
- Remote Desktop Services - unless you use Remote Desktop

## How to disable:

- Type "services" in search bar
- Find the service, right-click, select Properties
- Change Startup type to "Disabled"
- Click "Stop" to stop it now, then Apply/OK

**Warning:** Only disable services you understand. When in doubt, leave it alone.

# Disable Legacy Network Protocols (Windows)

Windows keeps old networking features for compatibility. You probably don't need them, and they're security risks.

- Settings > Network & Internet > Advanced network settings > More network adapter options
- Right-click your network adapter, choose Properties
- Uncheck these if present:
  - Client for Microsoft Networks (unless on corporate network)
  - File and Printer Sharing (unless you share files on your network)
  - QoS Packet Scheduler
  - Link-Layer Topology Discovery items
- Click OK
- Repeat for each network adapter (WiFi and Ethernet)

# Review Startup Programs

Programs that start automatically when you boot slow down your computer and can be security risks. Review and disable unnecessary startup items.

#### **Windows:**

- Press Ctrl+Shift+Esc to open Task Manager
- Click "Startup" tab
- Review the list - disable items you don't need running at startup
- Keep: Antivirus, system utilities you use daily
- Disable: Programs you rarely use, updaters, helper applications

#### **Mac:**

- System Settings > General > Login Items
- Review the list and remove items you don't want to start

#### **Linux:**

- Varies by distribution and desktop environment
- Ubuntu: Search for "Startup Applications"

## 3.3.4 Extra Credit

- Create a guest account
- Enable secure boot (Windows)
- Encrypt external drives
- Disabled SMB1 protocol (Windows)

## Create a Guest Account

If friends or family need to use your computer, create a guest account with limited access. This protects your files and prevents accidental system changes.

#### **Windows:**

- Settings > Accounts > Family & other users > Add account
- Choose "I don't have this person's sign-in information"
- Choose "Add a user without a Microsoft account"
- Create a "Guest" account as Standard User

#### **Mac:**

- System Settings > Users & Groups

- Click + to add user
- Select "Standard" account type
- Name it "Guest" with no password (or simple password)

## Enable Secure Boot (Windows/Linux)

Secure Boot prevents unauthorized operating systems and bootloaders from starting. It protects against bootkits and rootkits that load before Windows.

- This is configured in your computer's UEFI/BIOS settings
- Restart your computer and press F2, F10, Delete, or Esc during boot (varies by manufacturer)
- Look for "Secure Boot" option in Security or Boot menu
- Enable it
- Save and exit

Note: Some Linux distributions and dual-boot setups may have compatibility issues with Secure Boot. Verify that your distribution and hardware are compatible with secure boot before enabling.

## Encrypt External Drives

If you store sensitive data on external drives or USB sticks, encrypt them too.

### **Windows (BitLocker To Go):**

- Connect the external drive
- Right-click the drive in File Explorer
- Select "Turn on BitLocker"
- Follow the wizard, save recovery key (and save in your password manager)

### **Mac:**

- Connect the external drive
- Right-click in Finder, select "Encrypt [drive name]"
- Set a password

### **Linux:**

- Use LUKS with cryptsetup
- Or use VeraCrypt for cross-platform encrypted drives

## Disable SMBv1 Protocol (Windows)

SMBv1 is an old file sharing protocol with known security vulnerabilities (like WannaCry ransomware). Disable it unless you need to connect to very old network devices.

- Search for "PowerShell"
- Right-click, select "Run as Administrator"
- Type: `Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol`
- Press Enter
- Restart when prompted

# 3.4 Physical Security

*Core Concepts: Minimize Your Exposure, Protect Your Data*

All the passwords, encryption, and firewalls in the world won't help if someone can simply walk away with your laptop or peek over your shoulder to see your password. Physical security is often overlooked because we focus on digital threats, but physical access defeats almost all security measures.

If someone steals your laptop, they have unlimited time to try to break your encryption or find vulnerabilities. If they watch you type your password once, they don't need to hack anything. Physical security is where digital security starts.

## 3.4.1. Understanding Physical Security

Physical security covers protecting your devices and data from:

- **Theft:** Devices stolen for resale or data access
- **Loss:** Leaving devices behind or losing them
- **Observation:** Shoulder surfing, hidden cameras
- **Unauthorized access:** Someone using your unlocked device
- **Physical tampering:** Hardware keyloggers, evil maid attacks
- **Physical damage:** Accidents, water damage
- **Improper disposal:** Data recovered from discarded devices

The good news is most physical security measures are simple, inexpensive, and about habits more than technology. You don't need expensive equipment, you need to lock your screen every time, keep devices with you, and stay aware of your surroundings.

## 3.4.2. The Basics

- Lock your screen every time
- Be aware of your surroundings
- Use device tracking features
- Be cautious with public charging

- Mark your devices

# Lock Your Screen Every Time

**This is the single most important physical security habit.** Lock your screen whenever you step away from your device, even for a moment. Also, never leave devices unattended in public. It only takes a second for someone to pick it up.

## Quick lock shortcuts:

- Windows: Windows key + L
- Mac: Control + Command + Q (or close the lid)
- Linux: Usually Ctrl + Alt + L (varies by desktop environment)
- Phone: Press the power button

# Be Aware of Your Surroundings

Shoulder surfing is when someone watches your screen or keyboard to see what you're typing. They could observe passwords, PINs, sensitive emails, etc. They do not have to be directly over your shoulder either, across the room with a cellphone camera is enough. To that point, even security cameras could inadvertently capture sensitive information.

## How to protect yourself:

- Position your screen away from foot traffic
- Sit with your back to a wall when possible
- Be aware of people standing too close or paying too much attention
- Shield your keyboard or phone when entering passwords or PINs
- Reduce screen brightness in public
- Don't do sensitive work (banking, confidential documents) on planes or in crowded spaces

# Use Device Tracking Features

Enable Find My Device features on all your devices (covered in Mobile Device Hardening and OS Hardening sections).

## What this enables:

- Locate lost devices
- Lock devices remotely
- Display a message on the lock screen with contact info
- Wipe devices remotely if stolen

**Test it now:** Make sure you can actually locate your devices before you need to.

# Be Cautious with Public Charging Stations

Public USB charging stations (airports, hotels, conference centers) can be compromised with "juice jacking" attacks that install malware or steal data.

## How to protect yourself:

- Use AC power outlets with your own charger (safest)
- Carry a portable battery pack
- Use a "USB condom," a device that blocks data transfer, only allows charging (~\$10)
- Use charge-only USB cables (no data wires)
- If you must use public USB, turn off your device while charging

# Mark Your Devices

Visibly marking your devices makes them less attractive to thieves (harder to resell) and easier to identify if recovered. Just don't use anything which could make it a bigger target, such as your name or a company logo.

## Marking options:

- Engraving (most permanent)
- Distinctive stickers or decals
- UV marker with your contact info (invisible unless checked with UV light)
- Asset tags (if company-issued, check with local IT for rules about additional marking)

## What to mark:

- Bottom of laptop
- Inside battery compartment (if removable)
- Phone case
- External hard drives

**Document:** Keep a record of serial numbers and device identifiers. Take photos. Store this in your password manager or secure cloud storage.

## 3.4.3. Better Protection

- Secure webcam and microphone
- Use a cable lock for laptops

- Use privacy screens

# Secure Webcam and Microphone

Your webcam and microphone can be accessed by malware or accidentally left on during video calls.

## Simple protection:

- Use a webcam cover (sliding covers cost a few dollars)
- Or use a small piece of opaque tape
- For microphones, consider a hardware mute button or unplug external microphones when not in use
- Position your webcam to not show sensitive information in the background
- Use a background filter for calls

# Use a Cable Lock for Laptops

Cable locks (Kensington locks) physically secure your laptop to a desk or other fixed object.

## When to use:

- In offices with foot traffic
- Hotel rooms (lock to furniture or plumbing)
- Dorm rooms
- Anywhere you can't take the laptop with you

## What to buy:

- Kensington lock cable (~\$20-50)
- Check that your laptop has a lock slot (most do)
- Combination locks are more convenient than key locks (no key to lose)

Note: Cable locks are deterrents, not absolute security. Determined thieves can cut cables or remove the lock slot, but they do reduce opportunistic theft.

# Use Privacy Screens

Privacy screens are physical filters that narrow the usable field of view of your monitor. Some laptops have this feature integrated. HP has a feature called the Sure View integrated privacy screen which can be turned on and off using a keyboard shortcut. If your laptop does not have a built-in privacy screen, consider purchasing one if you frequently access sensitive data in public.

**When to use:**

- On planes or trains
- In coffee shops
- In open offices
- Anywhere you work with sensitive information in public

**What to buy:**

- Laptop privacy screens: ~\$30-60, measured to your screen size
- Removable vs. permanent adhesive: removable is more flexible
- Phone privacy screen protectors: ~\$10-20

**Tradeoff:** Privacy screens reduce screen brightness and can make it harder to see in certain lighting. Worth it for sensitive work.

# 3.5 Data Lifecycle and Disposal

*Core Concept: Protect Your Data*

Data doesn't just disappear when you delete it. When you click "delete" or throw a device in the trash, your personal information often remains completely recoverable. This section covers how to properly manage data throughout its entire lifecycle, from creation to destruction.

Whether you're selling an old phone, donating a computer, recycling a hard drive, or just trying to clean up years of accumulated digital clutter, you need to know how to truly delete data so it can't come back to haunt you.

## 3.5.1 Understanding Data Lifecycle and Deletion

Delete doesn't mean "gone." When you delete a file, your computer doesn't actually erase it, it just marks that space as "available for reuse." The data sits there, completely intact, until something else overwrites it. This might take days, months, or never happen at all.

### **Where your data lives:**

- **Active files:** Documents, photos, videos you're currently using
- **Trash/Recycle Bin:** Deleted files waiting to be permanently removed
- **Free space:** Deleted files not yet overwritten, recoverable with tools
- **Backups:** Local and cloud backups (Time Machine, iCloud, Google Drive)
- **Cloud services:** Email, cloud storage, social media
- **Device caches:** Temporary files, thumbnails, previews
- **Other devices:** Printers, copiers, phones, tablets

### **Real-world consequences of improper disposal:**

- Identity theft from recovered tax returns and financial documents
- Private photos recovered from donated computers
- Medical records from hospital equipment
- Passwords and login credentials from old phones

## 3.5.2. The Basics

- Factory reset devices before selling or donating
- Delete old online accounts
- Delete cloud data you don't need

# Factory Reset Before Selling or Donating Devices

Never sell, donate, or recycle a device without factory resetting it.

### **Before factory reset:**

- Back up any data you want to keep (see Backups section)
- Sign out of all accounts (iCloud, Google Drive, Microsoft OneDrive, etc.)
  - Right click icon on system tray (the icons around your clock)
  - Go to settings, or open and from the main window look for a way to log out (exit only closes the program on your computer, it does not sign you out)
- Deauthorize device from all services (iTunes, Adobe, etc.)
  - Log into account through their website and view authorized devices; remove the device from the list
- Remove active logins from all accounts (social media, email, etc.)
  - Log into each service and view active devices; remove the device from the list
- Remove device from Find My Device (see Mobile Device Hardening topic)
- Remove SIM card and memory cards

### **How to factory reset:**

#### **iPhone/iPad:**

- Settings > General > Transfer or Reset iPhone > Erase All Content and Settings
- Enter passcode and Apple ID password
- Confirm erasure

#### **Android:**

- Settings > System > Reset > Factory data reset
- Confirm and enter PIN/password

#### **Windows:**

- Settings > System > Recovery > Reset this PC

- Choose "Remove everything"
- Choose "Local reinstall" or "Cloud download"
- Additional settings > "Clean data" (more secure but slower)

#### **Mac:**

- Sign out of iCloud: System Settings > Apple ID > Sign Out
- Restart and hold Command+R to enter Recovery Mode
- Disk Utility > Erase main drive (choose APFS or Mac OS Extended)
- Reinstall macOS

## Delete Old Online Accounts

Old accounts you no longer use still contain your personal data.

Some accounts to review include:

- Old social media profiles
- Shopping sites you no longer use
- Gaming services
- Forums and community sites
- Old email accounts

#### **Before deleting account:**

- Download any data you want to keep
- Cancel any subscriptions or payment methods

If you're not sure how to delete an account (service provider instructions are not always clear) you can look up the site here: <https://justdeleteme.xyz/>

## Delete Cloud Data You Don't Need

Data in the cloud doesn't necessarily automatically delete when you delete it locally. Review your cloud data storage occasionally and remove any sensitive information to limit its exposure. Don't forget to empty the trash, as cloud services often retain deleted items for 30+ days.

### 3.5.3. Better Protection

- Use secure deletion tools
- Check printers and copiers

# Use Secure Deletion Tools

When disposing of a computer, if you have used it to store sensitive files, normal deletion isn't enough. Secure deletion tools overwrite the data multiple times.

## Recommended tools:

- **DBAN:** <https://dban.org/> - Free, boots from USB, wipes entire drive (DBAN only works with traditional hard drives (HDDs), not SSDs)
- **Parted Magic:** <https://partedmagic.com/> - Paid, includes secure erase for SSDs
- **Manufacturer tools:** Many SSD makers provide secure erase tools

**DoD 5220.22-M standard:** Overwrites data 7 times (for HDDs). Once considered necessary, now overkill; 1-3 passes is sufficient for HDDs. For SSDs, multiple overwrites are ineffective due to wear-leveling; use manufacturer's Secure Erase utility or ensure the drive was encrypted from the beginning.

# Check Printers and Copiers

Many printers and copiers have internal storage that keeps copies of things you printed or scanned.

## Before disposing:

- Check manual for how to clear memory/storage
- Many have "Clear All Settings" or "Factory Reset" option
- For office copiers with hard drives, remove and destroy the drive

## 3.5.4. Extra Credit

# Plan for Digital Legacy

What happens to your data when you die? Plan for it.

## Digital legacy planning:

- List all important accounts and where passwords are stored
- Designate trusted person to handle digital affairs
- Use your password manager's emergency access feature
- Set up legacy contacts on Google, Apple accounts

- Include digital assets in will

**Services:**

- Google Inactive Account Manager - Auto-delete or share after inactivity
- Apple Legacy Contact - Designate someone to access your Apple account
- Facebook Legacy Contact - Memorialize or delete account