

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
-

Revision #1

Created 2026-07-12 21:35:18 UTC by Chris Landis

Updated 2026-07-12 21:37:30 UTC by Chris Landis