

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.

Revision #1

Created 2026-07-12 21:38:51 UTC by Chris Landis

Updated 2026-07-12 21:41:12 UTC by Chris Landis