Hardware Security

- FileVault Encryption for Mac Computers (macOS)
- Securing Your Mobile Device

FileVault Encryption for Mac Computers (macOS)

Mac computers include FileVault, a built-in encryption system that secures all data at rest using AES-XTS encryption.

How It Works

On Apple Silicon and T2 Macs:

- FileVault uses Data Protection Class C with a volume key
- Encryption leverages the Secure Enclave and AES engine hardware
- User credentials required at boot after enabling FileVault

Important: On older Macs (pre-T2), non-original internal storage, or external drives: Files created before enabling FileVault aren't encrypted and may be recoverable with forensic tools.

Internal Storage Security

FileVault Enabled

When FileVault is on, volumes remain encrypted even if the physical drive is removed. Without valid credentials or a recovery key, the data is inaccessible.

Encryption covers:

- macOS 10.15: Both system and data volumes
- macOS 11+: Data volume (system volume protected by signed system volume feature)

Key Management Apple Silicon and T2 Macs use a hierarchical key system that:

- Requires user password for decryption
- Protects against brute-force attacks on removed storage
- Enables instant secure data wiping
- Allows password changes without full reencryption

All key operations occur within the Secure Enclave—encryption keys never reach the CPU. Each APFS volume has a volume encryption key (VEK) that encrypts contents and metadata. The VEK is wrapped by a key encryption key (KEK), which is protected by both the user password and hardware UID.

FileVault Disabled

Even without FileVault, Apple Silicon and T2 Macs still encrypt volumes—but the VEK is protected only by the hardware UID. Enabling FileVault later is instant (data already encrypted) and adds an anti-replay mechanism to prevent the old hardware-only key from being used.

Secure Deletion

Deleting a volume triggers the Secure Enclave to securely erase its VEK, preventing future access. Additionally, all VEKs are wrapped with a media key. Erasing the media key (via MDM commands, for example) makes the volume cryptographically inaccessible.

External Storage

Removable drives don't use Secure Enclave capabilities—they're encrypted the same way as Intel Macs without T2 chips.

Securing Your Mobile Device

Most of us use our personal phones for work, and that's okay. But it creates real security questions: What happens if your phone is lost or stolen? Who can see your work data? What if your org needs to manage your device? **There's no single right answer**, and the right approach depends on your role, your organization, and the sensitivity of what you're working with.

> If you work with confidential data like client records, legal documents, source information, immigration files, or donor details, the stakes are higher and some of these steps move from "good idea" to "essential."

---

1. Lock Your Device

A strong lock screen is your first line of defense if your phone is lost, stolen, or handed to someone else.

- Use a **PIN of at least 6 digits** or a strong alphanumeric passcode. Avoid patterns and 4-digit PINs.
- Face ID and fingerprint unlock are **convenient and secure but not sufficient on their own**. Always require a passcode as the fallback.
- Set your screen to lock automatically after no more than 1–2 minutes of inactivity.
- Enable "Erase data after failed attempts" if you carry particularly sensitive information.

> **Higher-sensitivity roles:** Consider disabling biometric unlock entirely and using a strong passcode only, particularly especially for border crossings or high-risk situations. Border agents can legally compel biometric unlock in ways they cannot compel a passcode.

---

2. Review App Permissions

Apps routinely request access to your location, contacts, camera, and microphone, often more than they need.

- Go through your app permissions periodically: Settings → Privacy (iPhone) or Settings → Apps (Android).

- Revoke location access for apps that don't need it. Choose "While Using" rather than "Always" where possible.
- Disable microphone and camera access for apps that have no clear need for it.
- **Uninstall apps you no longer use**. Dormant apps can still collect data.

> **Work accounts specifically:** Be thoughtful about which apps have access to your work email or calendar. A personal productivity app like Asana or Trello connected to your work Google account could expose more than you intend.

---

3. Keep a Boundary Between Work and Personal Data

When your personal phone is also your work phone, **data can mix in ways that are hard to untangle**. A few strategies help keep things separate:

- Use your work email account (e.g., Google Workspace) through a dedicated app (like the the Gmail app) rather than the Mail app, which combines personal and work inboxes.
- **Android work profiles:** Some organizations use MDM tools (see section 4) to set up a dedicated work profile — a separate section on your phone for work apps. This keeps work data isolated even if your personal apps are compromised.
- **Avoid storing work documents in personal cloud storage** (personal Google Drive, iCloud, Dropbox). Use your organization's designated storage (Google Workspace, Tresorit, or another approved service).
- **Use a dedicated secure messaging app** like Signal for sensitive conversations, rather than SMS or personal messaging platforms.

---

4. Mobile Device Management (MDM)

MDM software allows an organization to remotely manage devices, enforcing security policies, pushing updates, and wiping a lost or stolen device. If your organization uses MDM (such as Jamf, Microsoft Intune, or Google Endpoint), they may ask to install a profile on your personal device.

What MDM can do on your device:

- Enforce passcode requirements and encryption
- Remotely wipe the device if it's lost or stolen
- Require software updates
- Limit or monitor work-related apps and data

>

> MDM profiles give your organization visibility into and control over the portions of your device covered by the profile. Before installing, ask your IT contact exactly what the profile can see and do.

If installing MDM on a personal device feels like too much of an intrusion, it's worth discussing with your organization whether they can provide a dedicated work device instead.

---

5. Keep Your Phone Updated

Software updates patch security vulnerabilities. An unpatched phone, even one with a good passcode, can be compromised through known holes in the device's software.

- Enable automatic OS updates on your phone.
- Update your apps regularly, or enable automatic app updates.
- **Don't ignore "your software is out of date" warnings**! These often address active vulnerabilities.