Travel and Border Crossing Data Security Considerations

HCS TECHNOLOGY GROUP

Rev. 20250521

Contents

Preface

This document is designed to inform you of the technology and data protection measures available to enhance security for yourself, your devices, and the data contained within them. These protections can be utilized when traveling, crossing borders, or in everyday activities.

Historically, Information Security (infosec) focused on strategies to adopt when interacting with potentially hostile environments. The current approach emphasizes Zero Trust Networking: treating every network and connection as potentially hostile and maintaining an active security stance during all interactions. HCS Technology Group advises our clients to transition to Zero Trust Networking actively, and numerous recent updates have aimed at bolstering security.

Please use this document to stay informed and make well-informed decisions for yourself, your business, and your family.

Destinations outside the United States

When traveling, your devices and data are subject to the laws of the jurisdiction you travel to. In certain countries, there is an assumption of hostile intent and active hacking attempts may be made. There may be firewalls that restrict or actively block Virtual Private Network (VPN) or Zero Trust Network Access (ZTNA) usage. Internet traffic may be monitored and logged.

Anything you carry into these countries is subject to search or seizure. You can be required to provide access to your devices, accounts, and social media.

If you feel any data on your device, or any service you use that you may be forced to provide access to, might cause damage to you, your business or your clients; you can take steps, before you leave, to minimize these risks.

Even after arriving at your destination, extreme caution is advised There have been reported cases of hotel maids using USB devices to compromise computers The user is unaware, and the compromised computer may return and spread an infection or malware to its home network. Hotel room safes are not reliable security. There are YouTube videos showing how quickly and easily these safes can be compromised.

Unattended devices in cars are vulnerable. Many cheap and widely available scanning tools are available that can show the presence of devices, even when off, even when hidden, in a vehicle.

Returning to the United States or traveling near US borders

Reports of incidents in the United States of travelers' digital devices being searched, either in person, or after seizure, have increased concern. These same concerns may also apply during a law enforcement interaction.

Current accepted understanding of doctrine is that while a US citizen can be compelled by law enforcement or border agents to unlock biometric authentication methods, a US citizen can't be compelled to reveal or enter a password. Note that this is not a matter of settled law and may vary according to jurisdictions.

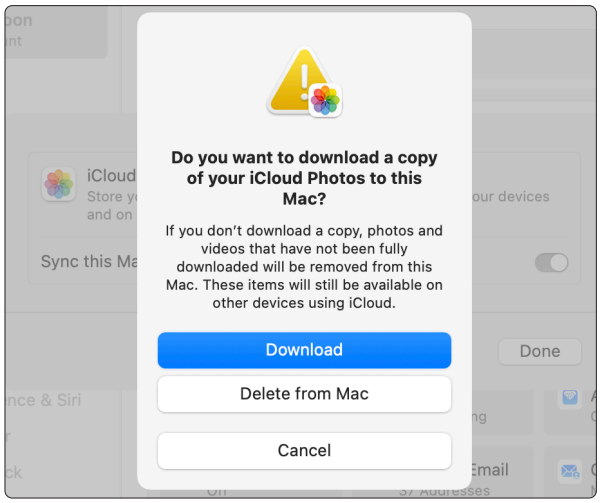
Even if you feel you have solid legal grounds to protect your privacy you may find that, in the tension of the moment, your comfort with refusing to provide access is compromised.

Customs and Border Protection agents are able to conduct warrantless searches without reasonable suspicion or probable cause at its 328* ports of entry, including border crossings and airports. Further, that ability extends to 100 miles surrounding those ports of entry.

*https://www.cbp.gov/locate-port-entry#:~:text=CBP provides security and facilitation,air%2C sea and land entries.

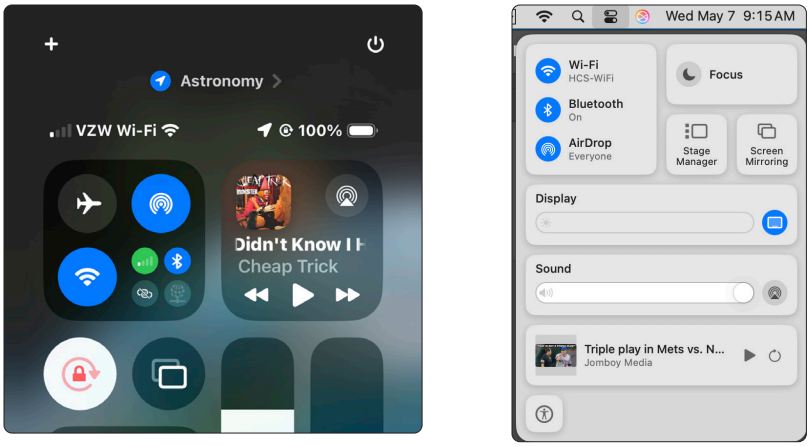
Section 1: What you can do to protect private data

1. Ensure you have a full, encrypted backup of your data to a local drive or cloud service. Leave that backup at home or in the office.
2. Critically evaluate your risk profile. Consider the current political climate of the destination, the work you do, your social media activity, your origin and your family's origin, as well as the profiles of the people you are closely associated with. These will help define the likelihood of being stopped, searched or detained. Consider people to whom you have privileged access. A contact in your address book can bring questions or further scrutiny.
3. Consider the data on your devices. Not just what is directly stored on the device, but also what services your devices connect to. You may decide to temporarily sign out of sensitive data sources such as Box, Dropbox, iCloud, SharePoint, OneDrive, Google Drive, etc. You may also decide to sign out of social media applications and even temporarily delete them from your devices.
4. Consider setting social media accounts to private or creating a fake account populated with uninteresting posts and followers prior to travel.
5. Evaluate the contents of your Photos library. Photos can contain detailed information about previous travel, images of people you know, and an astounding amount of metadata information. If you are using iCloud Photos. you can turn it off temporarily to remove the library.



6. Plan in advance how you will respond if asked to provide access to your devices. In some cases you can refuse, but that action may cause you to be denied entry or result in confiscation of your devices. Significant effort may be expended to crack protected devices over many months or years before they are returned to you.
7. Use strong passwords to secure your computer, phone and tablet. Use a minimum of 13 alphanumeric characters and symbols. A passphrase that is easy for you to remember is advised. **bUgsbUnnyLUVS14^^** is a great example of a password, that is both difficult to crack, and memorable.
8. Use biometric authentication to make the password more manageable but understand how to force your device to require a password to unlock.
9. To temporarily disable Face ID on iPhone and iPad, press and hold the power button and either of the volume buttons until you see the option to turn off the device You can tap cancel to leave the device on. To unlock the device and allow Face ID again requires entering your passcode.
10. To temporarily disable Touch ID on a Mac, either log out or shut down the Mac to require a password instead of Touch ID.

11. Introduced in iOS 18, iPhone will automatically restart after 3 days without being unlocked. Once restarted, the iPhone is hard locked and presents additional protections to being accessed until the passcode is entered. This can help protect a seized device. This automatic restart is not in iPadOS 18.
12. Actively ensure your software is up to date. New versions of operating systems incorporate additional security measures and are harder to access.
13. Reboot devices at least once a week to help maintain system integrity. Apple operating systems use a secure startup process based on a protected snapshot of system files. When a device reboots, this snapshot is verified using a checksum. If anything appears tampered with or corrupted, the system discards the snapshot and creates a clean one—effectively neutralizing and removing certain types of malware.
14. Rebooting regularly acts as a simple but powerful security measure. For users at higher risk, especially during travel, daily reboots are advised.
15. Store secrets, not just passwords, in a password manager such as Apple Passwords App, 1Password, or Dashlane. Know how to sign out and sign back in when needed. If you sign out of your password manager, the data may be removed from your device. These password managers can store lengthy notes, PDF files and other attachments and if you are signed out, they will not be with you to be searched.
16. Store work documents in secure cloud storage. Choose not to have files stored on your computer that should be in cloud storage.
17. For particularly sensitive travel, speak to your IT team about carrying a temporary, sanitized computer that does not have any data on it.
18. In a hostile environment consider whether your device use requires Cellular, Bluetooth and Wi-Fi, and if not, you can temporarily turn them off in Control Center.



Use Control Center to turn off Cellular, Bluetooth and Wi-Fi in hostile environments

Section 2: Apple Protections

Apple's platforms incorporate high-level protections, and when properly used, increase device and data security. Briefly, here are the major points:

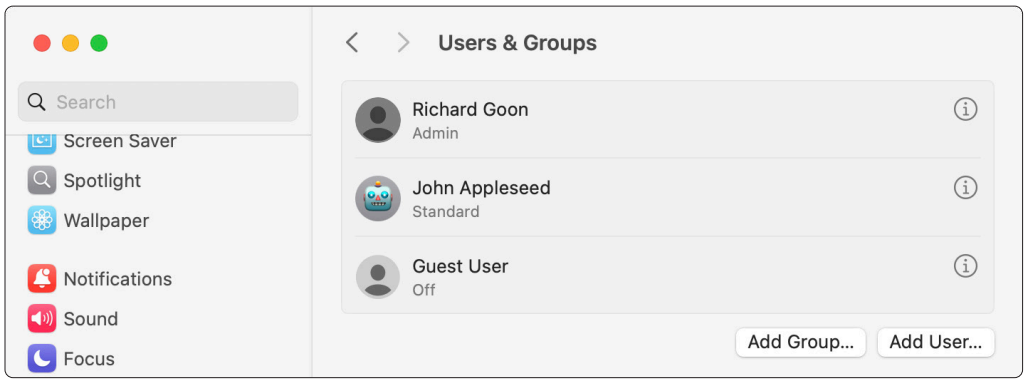
Account Type
Each user account created on a Mac has a standard set of capabilities assigned to it.

Root Root is traditionally a type of computer account with full permission to access and change any file on a computer. The root account is disabled in all current versions of macOS, and, even when enabled, has a reduced set of permissions to protect macOS.

Administrator The administrator account is powerful because it can install unsigned software, override certain protections, and affect other user accounts.

Standard A standard account has reduced permissions and can't affect other users' use of the computer. In some instances, this account type can present issues for traveling users because a standard user can't install or delete printers.

Guest The typical use for a guest account is to allow someone to temporarily use a computer on which they do not have an account. This type of account has limited permissions and is restricted to an environment that deletes itself each time the account is signed out. There is a second potential use for a Guest account, it can act as a "honeypot" account. Imagine a device is stolen and you want to remotely issue a wipe command to the computer. To receive that wipe command, the computer needs to connect to a network, and this honeypot account permits a thief to temporarily use the computer and to make that network connection that allows the remote wipe command to arrive.



Recovery Lock
macOS includes an alternate boot mode called macOS Recovery with powerful troubleshooting and maintenance options. A savvy hacker can leverage access to macOS Recovery to hijack a computer. While FileVault restricts macOS Recovery to administrator users, Recovery Lock secures macOS Recovery with a key stored in the MDM Server.

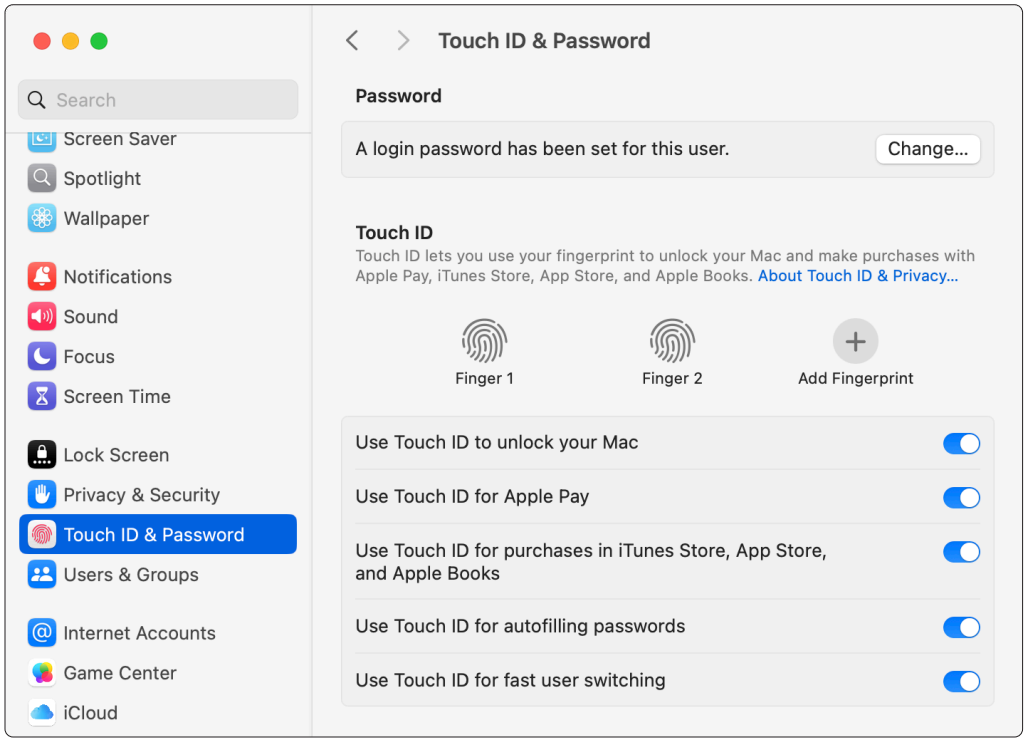
FileVault
Internal storage is always encrypted with macOS, however, when FileVault is turned on the encryption protects data further by requiring a FileVault enabled user to enter their password before any decryption of data is performed. This also enables a time lock where after a certain number of failed login attempts the Mac will prevent further attempts for an increasing amount of time, preventing brute force attacks.

Activation Lock
Activation Lock locks activation of a device to the owner of the device. When used in a consumer context, the user's personal Apple Account details need to be entered before the device will activate after being erased. For an organization-owned device, Activation Lock can be controlled by the MDM. This protection makes stealing a protected Apple device mostly pointless because the device can't be reused by anyone but the owner.

Biometric Authentication
Biometric authentication (Face ID and Touch ID) are protections because certain conveniences and features, are either limited or unavailable without a higher level of authentication for user actions. Third-party applications can utilize biometric authentication once Face ID or Touch ID has been set up by the user.

It's important to note that when using either Face ID or Touch ID, no actual fingerprint or faceprint is stored on the device. Instead, a mathematical representation of the fingertip or face is used to create a checksum that is compared to a similar checksum created when a user attempts to authenticate. If the stored and new checksums match, within a prescribed limit of variance, the user is authenticated. This representation is securely stored on the device it is created on in something called the Secure Enclave and is not available to be read, even by the device itself, and does not leave the device.

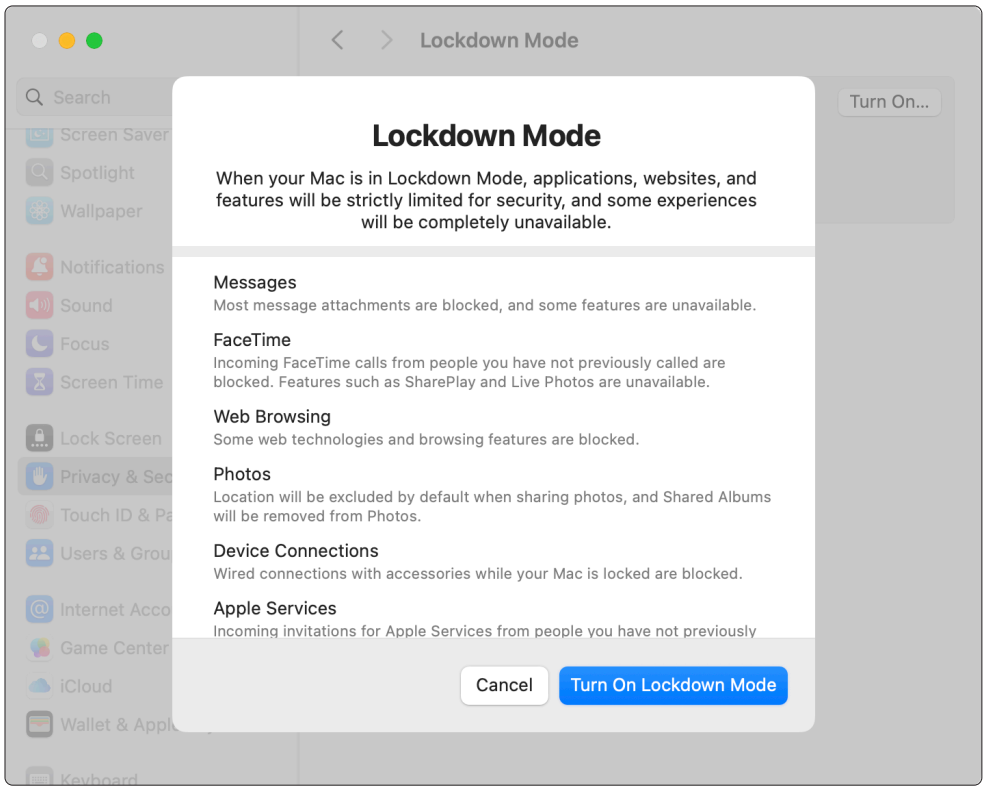
.



Lockdown Mode
Lockdown Mode is an optional, extreme protection, that's designed for the very few individuals who, because of who they are or what they do, might be personally targeted by some of the most sophisticated digital threats. Most people are never targeted by attacks of this nature.

When Lockdown Mode is enabled, your device won't function like it typically does. To reduce the attack surface that potentially could be exploited by highly targeted mercenary spyware, certain apps, websites, and features are strictly limited for security and some experiences might not be available at all.

About Lockdown Mode: https://support.apple.com/en-us/105120



Stolen Device Protection
Stolen Device Protection adds a layer of security when your iPhone is away from familiar locations, such as home or work, and helps protect your accounts and personal information in case your iPhone is ever lost or stolen.

Stolen Device Protection requires an Apple Account and Face ID. When enabled, Stolen Device Protection introduces a one hour delay to significant changes that impact security, like turning off Find My, changing passwords and resetting a device. This delay is intended to provide a window in which a user can mark a device as lost in Find My.

With Stolen Device Protection, some features and actions have additional security requirements when your iPhone is away from familiar locations such as home or work. These requirements help prevent someone who has stolen your device and knows your passcode from making critical changes to your account or device.

About Stolen Device Protection: https://support.apple.com/en-us/120340

Section 3: How are devices protected?

All users should be issued complex passwords for access to their computers, services like Active Directory and cloud storage. Single sign-on (SSO) will enable this login to be one and the same.

Any users with a password management app should be using that app. If you need help ensuring that passwords are recorded in the app, or in moving passwords into the app, please let your IT team know.

HCS Technology Group can assist you in migrating services to use SSO for user authentication.

- All HCS Technology Group supported computers should use Recovery Lock.
- All HCS Technology Group supported users should have FileVault turned on for their Mac computers.
- All HCS Technology Group supported users should have Activation Lock set.
- All HCS Technology Group supported users with Firewalls and utilizing VPN/ZTNA should be doing so with Multifactor Authentication (MFA).

.

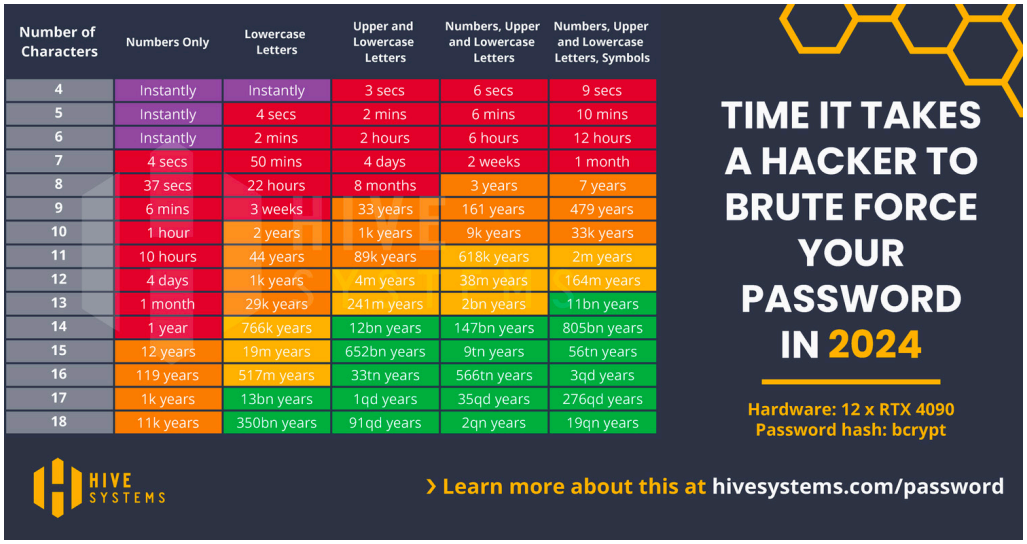
Traveler's Quick Checklist

- Back up and encrypt data (Time Machine, 1Password, DocMoto.)
- Sign out of sensitive services.
- Temporarily require passcode before border entry (e.g., Face ID cancellation).
- Turn off Wi-Fi/Bluetooth if unnecessary.
- Use VPN or ZTNA, if possible.
- Consider using a sanitized loaner device for high-risk destinations.

Section 4: References

- How to Enter the US With Your Digital Privacy Intact
  https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/
- How to lock down your phone if you're traveling to the U.S.
  https://www.washingtonpost.com/technology/2025/03/27/cbp-cell-phones-devices-traveling-us/
- How to prevent customs agents from copying your phone's content
  https://www.washingtonpost.com/technology/2022/09/18/phone-data-privacy-customs/
- Can police search your phone? Here are your legal rights.
  https://www.washingtonpost.com/technology/2024/10/08/can-police-search-your-phone
- Travel Screening
  https://www.eff.org/issues/travel-screening
- EFF Border Search Pocket Guide
  https://www.eff.org/document/eff-border-search-pocket-guide

Passcode Strength



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years