Cybersecurity

Traveler Summary

Introduction

Use the following practices to reduce vulnerability to malicious cyber actors: data leaks and cyberattacks can occur regardless of destination and local cybersecurity standards.

Communications

- Use a virtual private network (VPN) on internet-connected devices when traveling: without use of a VPN, unencrypted data can be intercepted and exploited, and geo-restricted services may be inaccessible.
- Do not connect to unsecure public Wi-Fi networks such as those in airports or hotels: these networks are vulnerable to malicious actors.
    - Strictly avoid networks that do not require passwords: open networks allow unrestricted interception.
    - If essential to connect to a public network:
        - Verify VPN activation before connecting: unencrypted data may be intercepted and exploited.
- Beware of “evil twin” networks, which are set up by malicious actors and have the same (or similar) names as legitimate networks: these spoofed networks are designed to lure users into connecting to them to capture credentials and data.
- Limit activity on untrusted networks to HTTPS-enabled websites: data transmitted over HTTP can be intercepted.
- Use a VPN on mobile networks when handling sensitive data: cellular infrastructure may be compromised despite default encryption.
- Use secure messaging applications with end-to-end encryption, such as Signal or WhatsApp: unencrypted messages can be intercepted.
    - Avoid SMS messaging: these messages are not encrypted.
- Use encrypted voice-call applications when available: standard cellular calls are not encrypted.
- Use multi-factor authentication for all accounts: single-factor credentials are easily compromised.

Devices

- Create secure backups of device files and settings before travel: device loss, theft, or cyber incidents may cause permanent data loss.
- Update device software to latest versions before travel: outdated software may have unpatched vulnerabilities cyberattacks seek to exploit.
- Protect devices with strong passwords: unsecured devices can be accessed if lost or stolen.
- Lock or power off devices when not in use: unattended devices are vulnerable to tampering.
- Disable Bluetooth when not in use: active Bluetooth connections increase unauthorized device-access risk.
- Avoid leaving devices or chargers unattended: theft or data compromise may occur.
    - Use a hotel safe when available: unsecured storage increases risk of theft.
    - Recognize that hotel safes may have override access: stored devices remain vulnerable.
- Avoid leaving USB chargers unattended: USB chargers can be modified to implant malware or steal data.
- Use USB data blockers when charging via USB ports: exposed data pins allow hidden scripts, data theft, or malware.
    - Use standard power outlets for charging: electrical outlets do not transmit data.
- Store devices, credit cards, and passports in Faraday bags (shielded containers that block electromagnetic signals) when appropriate: electromagnetic signals can be used to hack or steal data.
- Perform a daily hard shutdown/force shutdown of mobile devices: persistent malware, temporary spyware, and unauthorized background processes may remain active or in memory without full shutdown. Note that this is not the same as turning off the phone.

Operational Security (OPSEC)

OPSEC is the risk management process of protecting sensitive information that could be used by malicious actors.

Take the following OPSEC measures while traveling:

- Avoid announcing travel plans in advance, whether it’s leaving home or the hotel room: public disclosures increase theft and targeting risk.
- Delay sharing location information until after travel: real-time location data reveals traveler movement and absence from home.
  - Delay posting photos or videos until after travel: geotagged* media reveals current location.

*Geotagging is the process where geographic information is added to photos, videos, or other social media. This can happen manually, by taking and sharing photos or videos of well-known monuments or locations, or passively, such as when latitude and longitude coordinates are added to media by photo or video applications.

- Disable geotagging functions in camera and social media applications: embedded location data exposes traveler whereabouts.
- Arrange for mail or newspaper collection while away: visible accumulation signals absence.
- Delay sending sensitive personal (social security number, personal address, etc.) or financial data (online banking) until after travel or at least until on a known secure network: intercepted transmissions expose confidential information.
- Avoid clicking unknown or suspicious links or attachments: malicious files can install malware on devices.
- Use ad-blocking software when possible: some ads can install malware.
- Be aware of shoulder surfing or eavesdropping when transmitting sensitive data: nearby individuals may observe and exploit this information.
- Consider screen blockers when working in public with sensitive data: visual access to screens increases exposure.

Returning Home

- Remember to reenable any desired functions disabled for travel: disabled protections may reduce normal device functionality.
- Perform a hard shutdown of mobile devices before connecting to home networks: compromised devices may spread malware to trusted systems.
- If a device is compromised by a cyberattack:
  - Do not connect to home Wi-Fi networks: infected devices can spread malware to other devices on the same network.
  - Perform factory resets of the device: this may wipe any malware.
  - Consult a cybersecurity professional if compromise persists after reset: advanced malware may survive standard remediation.