TRAVEL CHECKLIST | HIGH CYBERSECURITY RISK

BEFORE DEPARTURE

When traveling to your destination country, assume that any and all information on your devices will be compromised.

Travel light! Take a **clean device** (e.g., loaner laptop, burner phone) or **clean your own devices** (e.g., personal or institutional).

CLEAN YOUR DEVICES

Back up your data on an institutional cloud environment and/or external hard drive; leave the backup at home
Consider wiping devices to reduce compromise risk

Install **the latest software** and **security updates** on all devices because outdated software increases security risks

Forget all saved Wi-Fi networks and **Bluetooth devices**

Learn to boot your devices in **safe mode** to help with remote tech support

SET UP YOUR LAPTOP

Remove any research data and **IP** (e.g., export controlled, sensitive data) from local hard drive and store them in institutional cloud storage

Use **encryption*** to protect your files

Install **institutional VPN*** software

SET UP YOUR MOBILE DEVICES

Turn on **security/PIN codes** (6+ characters) for your device's lock screen

Install end-to-end **encrypted messaging applications*** (e.g., Signal, WhatsApp)

Uninstall nonessential applications (e.g., social media)

**Encryption and VPN are illegal and/or unavailable in some countries*

PROTECT YOUR ACCOUNTS AND PRIVACY

Use **complex passwords** and set up **two-factor authentication (2FA)**
Use tokens or authentication apps instead of SMS when possible

Do not access personal accounts on clean devices (e.g., bank accounts)

Turn off
- Camera and microphone access for all applications
- Background application refresh
- Notifications for all applications not in use
- "Join automatically" for Wi-Fi connection
- AirDrop

These steps help increase privacy and reduce hacking risks

Install **privacy screens** on your devices to prevent others from viewing

Bring your **own cables, chargers** and **plug adapters**; avoid purchasing or borrowing them

WHILE TRAVELING

Assume you have no privacy and that all your messages and connections may be monitored or intercepted.

PROTECT YOUR DEVICES

Never leave your devices unattended
Assume even hotel rooms and safes are not secure

Do not use **public charging stations** or **USB ports**
Use your own cables, chargers and block adapters only to prevent data theft

Do not let others connect to your devices (e.g., via USB sticks)

SECURE YOUR DATA AND CONNECTIONS

Use **institutional VPN** and **cloud storage*** to securely access the internet and your files
Do not access/download controlled or sensitive data (e.g., CUI, PII, human subjects data)

Use **encrypted messaging applications*** to communicate

Manage your connections
- Disable Wi-Fi, Bluetooth, GPS and NFC when not in use
- Use private browsing whenever possible
- Avoid scanning QR codes; type website URLs directly
- Avoid downloading new applications unless required or necessary

Power cycle devices daily

These steps prevent devices from being discoverable, minimize unauthorized connections and malicious redirects, and disrupt temporary malware

REPORT IMMEDIATELY IF YOUR DEVICE IS ...

Lost, stolen or **temporarily taken** away

Showing signs of **tampering** or **compromise** (e.g., unusual battery drain, performance issues, suspicious software behavior, unexpected data usage)

UPON YOUR RETURN

Power cycle devices by turning them completely off and on

Properly wipe or **restore devices from** a clean backup before connecting to any network because compromised devices can spread malware

Change passwords you used on travel

Contact your IT team for additional guidance on setting up, wiping, and restoring your devices

NSF SECURE Center

This material is based upon work supported by the U.S. National Science Foundation under Cooperative Agreement No. 2403771. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. National Science Foundation and other U.S. government agencies.

Last updated: 02/17/2026