TRAVEL CHECKLIST | BEST PRACTICES

BEFORE DEPARTURE

Prepare for international travel by securing your devices and data against theft, loss, and compromise.

PREPARE YOUR DEVICES

Travel light! Only bring the devices that you need

Back up your data on an institutional cloud environment and/or external hard drive; leave the backup at home

Install **the latest software** and **security updates** on all devices because outdated software increases security risks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

Bring only **essential data;** remove non-essential data/files from local hard drive and store them in institutional cloud storage

Use **encryption*** to protect sensitive 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

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

Be aware that your messages and connections may be intercepted, especially on public networks.

DAILY SECURITY PRACTICES

Never leave your devices unattended

Do not use **public charging stations** or **USB ports**

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

Use **institutional VPN*** and **cloud storage** to securely access the internet and your files

ENHANCED SECURITY PRACTICES

Use **encrypted messaging applications*** for sensitive communications

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

Contact IT before connecting to any network if you believe your device has been compromised because compromised devices can spread malware

Change passwords you used on travel

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