International travel: technology and security

Last Modified on 03/20/2025 9:00 am EDT

This article reviews LITS's recommendations when **traveling internationally** with computers and mobile devices.

See also:

- Password Managers
- Two-Factor: Get started with Duo
- Two-Factor: Methods of Authentication

College and personal accounts

Using Duo

Set up Duo Mobile to access **College accounts** without an international phone or data plan!

- get push notifications when **connected** to the internet
- generate a one-time code when disconnected from the internet

Consider requesting a Duo security token as a secondary authentication method, which works **completely offline**!

Attention: Some high-risk countries **restrict access** to specific websites, providers, or security tokens.

Privacy and security

- Use a password manager to store and access your passwords securely and hide accounts while travelling.
- Use a consumer VPN in countries where it is legal to secure your connection.
- **Avoid** logging into any **personal** or **financial** accounts.

International calling

Use the **MiCollab mobile app**'s softphone to place and receive calls from your College phone number. **Charges may apply** if you use cellular data instead of Wi-Fi; check with your provider to prevent this!

Encrypted devices

> **Attention:** All College computers are, and must be, **encrypted** per College and LITS policy.

Some countries heavily regulate or ban the import, export, and use of encrypted devices (e.g., **Computers**, **phones**, and **tablets**). Travelling without proper authorization could result in **fines, confiscation, or other penalties**.

Preparing for travel

> **Note:** What is the **Wassenaar Arrangement**?

1. Check if your destination **restricts** encrypted devices.
   - **GP Digital**: World map of encryption
   - **Wassenaar Arrangement**: Participating states
2. If they do, please contact the Help Desk to arrange for a temporary **unencrypted loaner**.

Exceptions: high-risk countries

> **Attention:** The U.S. designates some countries, such as **China** and **Russia**, as "high-risk" for information security. Always check the U.S. Department of State before travelling!

Why it matters

When travelling to a high-risk country, assume that **any device or account used while abroad is compromised**. Electronic devices are vulnerable to physical or otherwise undetectable tampering.

- Compromised accounts affect **your data** and the College's.
- Security software is **not guaranteed** to prevent targeted attacks.
- U.S. travelers, particularly STEM faculty, are **priority targets** for cyberattack(s).

Guiding principles

1. Don't travel with electronic devices.
2. If electronic devices are needed, use burner devices.
3. Don't log in to any College or personal accounts.
4. If you must log in to an account:
    - only use those protected by two-factor authentication
    - change your password when you return

How to prepare

Before you leave

- Make a backup of any devices you plan to bring.
- Contact the Help Desk to request an unencrypted loaner and visitor account.
- Download data in advance to use it offline.
- Enable two-factor authentication for any accounts you must use.
- Purchase an RFID-blocking wallet.
- Update all electronic devices.

What to leave in the US

- One-time password tokens/fobs (such as those for Duo)
- Your College and personal computers
- USB security keys (e.g., YubiKey)

While you're there

- Avoid making calls or sending SMS messages.
- Don't access any sites or services that require a VPN.
- Don't use a VPN, including the College's VPN.
- Don't leave your device(s) unattended.
- Don't log in to any College or personal accounts.
- Don't use public charging stations, computers, or Wi-Fi.

When you return

- **Change any passwords you used.**
- Don't approve any unexpected Duo push notifications.
- Return your unencrypted loaner.
    - If you brought your primary College computer, contact the Help Desk to have it reimaged.

Further reading and references

- **1Password**: Travel Mode
- **Columbia University**: Data security guidelines for international travel
- **Comparitech**: Where are VPNs legal?
- **FBI**: Business travel tips
- **Freedom House**: Countries by internet freedom score
- **Princeton University**: Travel guidelines
- **Stanford University**: Risk ratings
- **University of Colorado**: International travel with encrypted mobile devices
- **University of Pittsburgh**: Technology guidelines for international travel
- **University of Rhode Island**: Travel to China or Russia
- **U.S. Department of State**: Travel advisories
- **U.S. Embassies**
- **Wassenaar Arrangement**: Participating states
- **Wikipedia**: List of websites blocked in mainland China

Questions?

If you have any additional questions or problems, don't hesitate to reach out to the **Help Desk**!

Phone: 610-526-7440 | Library and Help Desk hours
Email: help@brynmawr.edu | Service catalog
Location: Canaday Library 1st floor