BEFORE YOU TRAVEL

Understand Local Laws and Customs | Know your destination's laws and customs, including restrictions on photography and internet use.

Device Preparation | Leave non-essential electronics; secure essential ones by removing sensitive data and updating security.

Social Media Caution | Tighten privacy settings and avoid sharing travel details to prevent targeting.

Document Safety | Digitally copy and securely store important documents like passports and visas.

Office of Information Security
Education & Awareness

Traveling abroad as a student is an exciting opportunity for growth and learning. However, it's crucial to stay vigilant about your digital security. This guide offers comprehensive advice to help you protect yourself and your digital footprint, contributing to your safety and the broader security of the UC community.

CYBERSECURITY DURING TRAVEL

Facts & Tips for UC Students Abroad

- ✓ **Surveillance Risks**: Your phone can be tracked abroad, and devices remotely activated for eavesdropping.
- ✓ **Phishing Threats**: Beware of impersonators seeking personal info. Always verify the source.
- ✓ **Passport Security**: American passports are targeted. Keep yours secure and watch for theft.
- ✓ **Civil Caution**: Avoid demonstrations and know local laws, especially regarding speech and photography.
- ✓ **Online Monitoring**: Your online activities can be tracked. Avoid sensitive discussions and sharing confidential info electronically.
- ✓ **Post-Travel Security:** Stay vigilant after returning, as cybercriminals often target travelers post-trip.

Travel Smart, Stay Secure.

Your Vigilance Abroad is Your Best Defense.

University of CINCINNATI

DURING YOUR STAY

Wi-Fi Caution | Avoid public Wi-Fi; use a VPN for security.

Device Security | Never leave devices unattended. Shield passwords and clear browser history.

Caution with Strangers | Don't share personal info or travel plans with strangers.

Passport Safety | Keep the original passport in a hotel safe or secure location. Carry a copy with you for identification.

RETURNING HOME

Security Check | Upon return, change your passwords and check your devices for any signs of tampering or malware.

Stay Alert | Continue to monitor your accounts for any unusual activity, indicating potential security breaches during your travel.

ADDITIONAL SAFETY TIPS

Avoid Flashy Displays
As Americans are often perceived as wealthy, avoid wearing expensive-looking jewelry or clothing that identifies you as an American tourist.

Emergency Contacts
Keep a list of important contacts, including the local US Embassy or Consulate, and establish emergency points of contact at home and abroad.

Support from Digital Technology Services

Pre-Travel Check: Contact DTS for a pre-travel equipment check and advice on data security.

Account Monitoring: DTS will monitor your university account for unusual activities during your travel period.

24/7 Assistance: Reach out to DTS anytime for support or if you suspect a security breach.

Resources & Contacts

U.S. Embassies & Consulates: Keep contact info handy.

FBI Office: Contact for reporting incidents or seeking advice (www.fbi.gov).

State Department Travel Website: For country-specific advisories

Overseas Security Advisory Council: For security news and reports (www.osac.gov).

State Department Travel Warnings

National Counterintelligence and Security Center Guidelines