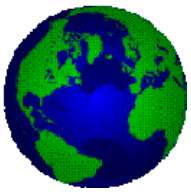

CYBERSECURITY
CONSUMER TIPS FOR INTERNATIONAL TRAVELERS

Be Aware

1. When traveling internationally, in addition to taking your passport, ***take responsibility for your cybersecurity.***

2. Your information and communications – and the devices that contain and transmit them – are as much a part of you as the valuables in your suitcase. The more you do to protect yourself, the more secure your information and devices likely will be.

3. While in a foreign country, you are subject to its laws. Laws and policies regarding online security and privacy may be different in other countries than in the United States. If you would like to become familiar with other laws, the State Department website contains safety information for every country in the world, including regarding communications.[1]

4. Protect yourself by leaving at home any electronic equipment you don't need during your travel.

Before You Go

5. If you take it, protect it:
   - Back up your electronic files
   - Remove sensitive data
   - Install strong passwords
   - Ensure antivirus software is up-to-date

While Traveling

6. Be vigilant about possession and use of your equipment and information. Don't assume it's safe. Culprits are visible and invisible.

---

[1] www.travel.state.gov/travel/cis_pa_tw/cis/cis_1765.html. For information regarding treaties, laws and policies, see: www.travel.state.gov/law/legal/legal_818.html. For general international travel tips, see: www.travel.state.gov/travel/tips/tips_1232.html.

- Keep *your* eyes on your electronics. Keep your devices with you in airports, hotels, and restaurants, etc.
- Be aware of your surroundings. *Other* eyes can take information from you by looking at your devices.
- Consider using a privacy screen on your laptop.

7. Your mobile phone and other electronic devices may be vulnerable to malware because they will connect with local networks abroad. They also may identify your personal location information to others.

8. Electronic communications, equipment and services (*e.g.*, phones, computers and fax machines) in public places such as Internet cafes, coffee shops, book stores, travel agencies, clinics, libraries, airports, and hotels may be vulnerable. You may choose not to use these services at all, or avoid using them for sensitive communications.

9. Don't use the same passwords or PIN numbers abroad that you use in the United States. For example, if the hotel safety deposit box requires a PIN number, use a unique one.

Upon Return Home

10. Electronics and devices used or obtained abroad can be compromised. Consider safety measures such as changing passwords for your laptop or smartphone.

Additional Cybersecurity Resources

- Department of Homeland Security, Computer Emergency Readiness Team Tips[2]
- FCC Privacy and Online Security Tips[3]

[2] www.us-cert.gov/cas/tips/

[3] reboot.fcc.gov/privacy-and-online-security