Cybersecurity Tips for International Travelers

When traveling internationally, remember that your mobile phone and other personal communications devices transmit and store your personal information, which is as valuable as the contents of your suitcase, possibly moreso.

Before you go

Take proactive steps to secure your devices and your personally identifiable information before you travel. Leave at home any electronic equipment you don't need during your travel, and if you take it, protect it. Be sure you:

- Back up your electronic files.
- Remove sensitive data.
- Install strong passwords.
- Ensure antivirus software is up-to-date.

While traveling

Be vigilant about where and how you use your devices, and don't be lulled into a false sense of security. Make sure you:

- Keep your devices secure in public places such as airports, hotels and restaurants.
- Be aware of your surroundings and take care that nobody is trying to steal information from you by looking at your device screen when you use it.
- Consider using a privacy screen on your laptop.

Be cautious while using public Wi-Fi

Some threats – device theft, for example – are obvious, but others will be invisible, such as data thieves trying to pick off passwords to compromise your personally identifiable information or access your accounts. You may be especially vulnerable in locations with public Wi-Fi, including internet cafes, coffee shops, book stores, travel agencies, clinics, libraries, airports and hotels.

Some helpful tips:

- Don't use the same passwords or PIN numbers abroad that you use in the United States.
- Do not use the public Wi-Fi to make online purchases or access bank accounts.
- When logging into any public network, shut off your phone's auto-join function.
- While using a pubic Wi-Fi network, periodically adjust your phone settings to forget the network, then log back in again.
- Try purposely logging onto the public Wi-Fi using the wrong password. If you can get on anyway, that's a sign that the network is not secure.

Remember also to avoid using public equipment – such as phones, computers and fax machines – for sensitive communication.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/consumer-governmental-affairs-bureau

When you get home

Electronics and devices used or obtained abroad can be compromised. Your mobile phone and other electronic devices may be vulnerable to malware if you connect with local networks abroad. Update your security software and change your passwords on all devices on your return home.

Additional resources

For more tips, check the Department of Homeland Security, Computer Emergency Readiness Team webpage: http://www.us-cert.gov/cas/tips.

Laws and policies regarding online security and privacy differ in other countries. While in a foreign country, you are subject to local laws. The State Department website has travel safety information for every country in the world: http://travel.state.gov/content/passports/english/country.html.

Consumer Help Center

For more information on consumer issues, visit the FCC's Consumer Help Center at www.fcc.gov/consumers.

Alternate formats

To request this article in an alternate format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last reviewed: 3/28/18

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/consumer-governmental-affairs-bureau