



www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

FACT SHEET

U.S. Army Cyber Command

The Nation's Army in Cyberspace

THE FACTS: CYBERSECURITY TIPS FOR INTERNATIONAL TRAVELERS

Before You Go

- Treat your information and communications and the devices that contain and transmit as valuables. The more you protect yourself, the more secure your information and devices will be.
- Remember that while in a foreign country, you are subject to its laws. Its statutes and policies regarding online security and privacy may be different than in America. [The U.S. State Department website](#) has helpful information for every country in the world.
- Don't take along any electronic equipment you won't need during your travel.
- Protect the devices you do take along. Back up your files, remove as much sensitive data as possible, make sure you have strong passwords, and make sure antivirus, operating system and browser software are up to date.



While Traveling

- Be vigilant about possession and use of your equipment and information. Don't assume that they're safe.
- Keep a close eye on your devices close in airports, hotels, restaurants, etc.
- Be aware of your surroundings. Can someone get your information by looking at your devices?
- Consider using a privacy screen on your laptop.
- Mobile phones and other electronic devices that connect with local networks abroad may be vulnerable to malware or give away your personal location information to others.
- Electronic communications, equipment and services in public places such as Internet cafés, coffee shops, book stores, travel agencies, clinics, libraries, airports and hotels may be

ABOUT US: United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 2 March 2016

vulnerable. Consider not using these services at all, or avoid using them for sensitive communications.

- Don't use the same passwords or PIN numbers abroad that you use at home. For example, if the hotel safety deposit box requires a PIN number, use a unique one.

When You Get Home

- Electronics and devices used or obtained abroad can be compromised. Consider safety measures such as changing passwords for laptops or smartphones.

Source: <https://www.fcc.gov/guides/cybersecurity-tips-international-travelers>



Follow ARCYBER on
(click the images to visit our pages)



ABOUT US: United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 2 March 2016