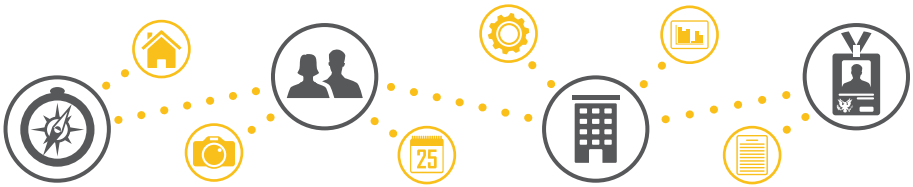
SAFE TRAVELS

International travel has become an essential part of government, business, and, for some, our personal lives. If you work for the government, or are employed in an industry active in the global marketplace, foreign adversaries or competitors may target you using various methods when traveling abroad, even to a friendly country.

Smartphones, laptops and tablets, or even digital cameras and external storage components, are vital to travelers but more susceptible than ever to security threats. If compromised, an adversary or competitor can learn exactly where you are, who your friends and families are, where you work, and what you do.



PROTECT SENSITIVE INFORMATION WHEN TRAVELING ABROAD

When traveling abroad, you should have no expectation of privacy. Wi-Fi networks overseas are regularly monitored by security services and others. Security services and criminals can insert malicious software into your device through any connection they control. They can also do it remotely if your device is enabled for wireless. The malicious software can then be migrated when you connect to networks at home or your place of employment upon your return, compromising such networks.

In addition to your electronic devices, you may also be targeted by persons around you. Travelers should be aware that hotel staff, drivers, guides, and others may be working on behalf of an adversary.

Before You Travel:

- If you can do without the device, don't take it.
- Don't take information you don't need, including sensitive contact information. Consider the consequences if your information were stolen by a foreign adversary or competitor.
- Back up all information you take; leave the backed-up data at home.
- Review your device passwords. Where possible, use strong passwords (i.e., a combination of numbers, upper and lower case letters, and special characters).

While You're Traveling:

- Foreign intelligence services and criminals are adept at "phishing" – pretending to be someone you trust to obtain personal or sensitive information.
- If a customs official demands to examine your device, or if you suspect your hotel room was searched while the device was in the room and you were not, assume the device has been compromised. Don't leave electronic devices or sensitive information unattended. A hotel safe is never "safe."
- Don't overshare personal information with new acquaintances.
- Use digital signature and encryption capabilities when possible.
- Remain cautious when browsing the web. Do not use the 'remember me' feature on websites (e.g., re-type your password every time). Where possible, limit web usage to general browsing and avoid online banking and other online transactions that could expose sensitive information or passwords.
- Avoid Wi-Fi networks, if you can. In some countries they're controlled by security services; in all cases, they're insecure.
- Avoid charging a mobile device in an international airport. Charging stations and data ports can also be used to extract data from your device or upload malware onto it.

When You Return:

- Modify passwords when you return. Remember, if your device is compromised, so are your passwords.
- Monitor your financial accounts and beware of suspicious emails and new contacts.
- If you believe your personal information may have been compromised, contact the appropriate banks, credit card companies, credit bureaus, etc.

INTERNET RESOURCES

OnGuardOnline.gov
Operated by the Federal Trade Commission (FTC), this site provides tips and technical guidance on cybersecurity issues, as well as a guide for talking to children about Internet use.

StaySafeOnline.org
This site offers resources on a variety of cybersecurity issues, including information on adjusting privacy settings on a number of popular platforms.