Cyber Security Tips and Recommendations for International Travelers

By: Bryan Ray

Global Incident Response Manager, Satcom Direct

When traveling internationally, you should be proactive and take preventive measures to protect your mobile devices and personal data. The SD Cyber Security team has put together the following guidelines to add to your travel checklist for before, during, and after your international trip.

Before you leave:

1. Leave your mobile devices and sensitive data at home. If you need connectivity, consult with your IT department to see if there's an option to borrow loaner devices for your trip. Also, pre-paid phones are an option for maintaining communications, but it is recommended to purchase them from your home country.
2. Whether you are traveling with loaner devices or your own, you should always back up your data just in case your devices are lost or stolen.
3. Install and configure encryption software. In the unfortunate scenario where your device is lost or stolen, encryption software can ensure the confidentiality of your data and is typically included with modern operating systems installed on laptops and mobile devices. Some countries restrict the use of imported encryption software; be sure to research the software import laws of your destination country.
4. Install and configure Virtual Private Network (VPN) software to protect against eavesdroppers on networks during your trip to create a secure and encrypted connection back to your home or corporate network. Consult your corporate IT department before installing VPN software on a company-issued device.
5. Update your operating system and application software to the latest versions possible. This prevents the potential exploit of vulnerabilities associated with outdated software.
6. Ensure your antivirus software is up to date.
7. Choose strong passphrases and passwords (including aircraft Wi-Fi passwords).
8. For laptops, set up and use an account that does not have administrator privileges.
9. Ensure device firewalls are turned on.
10. Disable autorun features.

While traveling:

1. Do not leave your devices unattended, even in your hotel room. Use room safes if available. Preventing physical access to your device will help protect your sensitive data. If you must leave your device unattended, power it off. Sleep or hibernation modes are not always secure.
2. Use passcodes on all devices. The more passcode digits, the better.
3. Consider using a privacy screen on laptops when in public places. Someone may be looking over your shoulder.
4. Do not plug devices into untrusted accessories or USB docked charging stations. They can be infected with malware.
5. Avoid plugging in any untrusted accessories, such as a flash drive or charging cable.
6. Do not enter your credentials into public computers, such as hotel business center workstations and internet cafes because they are often poorly managed and provide minimal security protection.
7. Only connect to known, trusted, and secured Wi-Fi networks. It is easy to create an "evil twin" or rogue access point and give the network a legitimate sounding name. Find out the correct network name from the staff prior to connecting.

   Additional Wi-Fi tips:

   - Do not use public Wi-Fi to make online purchases or access bank accounts.
   - If connecting to a public Wi-Fi hotspot, turn off your device's "auto join" feature.
   - Turn off your device's Bluetooth, Near Field Communications (NFC), and Wi-Fi when not in use.
8. Do not install applications while traveling internationally.
9. Practice safe web browsing. The websites you visit online hold valuable data about you that hackers can steal by infecting reputable or seemingly reputable websites with malware. Only connect to trusted websites, which are secured "https." Web pages you connect to using "http" exchange information unencrypted.
10. If your browser displays an error about the digital certificate used to encrypt the data, and cannot verify the identity of the seemingly secure website, you should assume the website is fake or compromised, or that the web traffic is being intercepted. Close your browser to exit the site.
11. Do not click on suspicious links or prompts. Malicious websites commonly craft attacks to exploit a user's curiosity or impatience, or to scare them with malware threats.
12. Clear browsing session information when using devices that do not belong to you. Some web applications do not log you out entirely, even when clicking the logout button or closing the browser.

After your trip:

1. On a trusted computer, change all credentials used during the trip because they may be compromised.
2. Update your device's security and antivirus software as well as the operating system and applications if newer versions are available.

To learn more about our business aviation cyber security solutions, email cybersecurity@satcomdirect.com

Satcom Direct

Satcom Direct's SD Data Center brings enterprise-level security audits to data transmissions on the ground and in the air. SD's compliance experts use a consultative approach to provide aircraft cyber security audits focusing on both the cabin and the ground network. The audit addresses cyber security issues, best practices in network design, and policies and procedures, all to ensure passenger data is classified and properly protected.
http://www.satcomdirect.com