MS-ISAC

MS-ISAC Security Primer

Cybersecurity While Traveling

March 2017, SP2017-0817

OVERVIEW: Whether traveling for business or leisure, travelers face increased cyber targeting and exposure during their trips. Key threats include accidental loss and exposure, financially-motivated crime, espionage, and different laws. Key vulnerabilities include the information carried with the traveler; the use of insecure devices and data; oversharing information; the greater exposure travelers are subject to; the traveler's coworkers, friends, and family; and the lack of due diligence. The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends assessing travel risk based on the threats and vulnerabilities posed by the trip; host; traveler; the traveler's equipment and devices; the traveler's coworkers, friends, and family; and gaps in your knowledge.

TECHNICAL RECOMMENDATIONS:

- When possible, travel with a new or reimaged device so that no data is stored on it, and ensure that automatic logins, the push/pull of data, and auto-download features are disabled. Turn off all other device network connections and services when not in use.
- If traveling with a non-reimaged device, clear browsing histories and other stored information that could be abused by foreign actors. Delete unnecessary applications, plugins, and software.
- Ensure the device has the most recent patches, software updates, and anti-virus software installed.
- When not in use, devices should be powered off and where possible, have the batteries removed.
- If traveling with data, store it on a USB thumb drive or other removable media that can be destroyed after use, to prevent SLTT network compromises upon return.
- Encrypt data storage and conduct all activities over encrypted connections, where legal.
- Where possible use a one-time webmail account instead of SLTT email accounts.
- Do not connect a device or transfer data from a device to SLTT government networks until the device has been scanned, preferably reimaged.

USER RECOMMENDATIONS:

- Keep electronic devices with you at all times; hotel safes are not secure.
- Before traveling, change all passwords that you will use while traveling abroad, and upon return change the passwords of any accounts that were accessed while abroad.
- Use wired connections instead of Bluetooth or WiFi connections.
- Do not access sensitive accounts or conduct sensitive transactions over public networks, including hotel business centers and Internet cafés. If a connection to sensitive accounts or systems is required use a virtual private network (VPN) connection, if it is legal in the country to which you are traveling.
- Do not accept USB thumb drives or other removable media from any source.
- Do not plug USB powered devices into public charging stations. Only connect USB powered devices to the power adapter with which they were intended to be used.
- Know the local laws regarding online behavior and law enforcement authorities, as some online behaviors are illegal in certain countries. Consult the State Department website for information about particular destinations.
- Assume that all online activity is subject to government and/or other monitoring techniques.
- Report suspicious activity, including incidents in which your electronic device is handled or examined by anyone, to your Information Technology and Security departments.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.