Department of the Interior
Office of the Chief Information Officer &
Office of Law Enforcement and Security
Joint Foreign Travel Threat Assessment:
Electronic Communications Vulnerabilities

September 03, 2013

Foreign governments routinely target the computers and other electronic devices and media carried by U.S. government and corporate personnel traveling abroad to gather economic, military, and political information. Theft of sensitive information can occur in a foreign country at any point between a traveler's arrival and departure and can continue after returning home without the victim being aware.

Use of cell phones, smartphones, BlackBerry's, laptops, and iPads in foreign countries exposes these devices to unauthorized access and theft of data by criminal and foreign government elements. Travelers should assume that they cannot protect electronically stored data and should not transmit sensitive government, personal, or proprietary information on the Internet or through telecommunications equipment. Malicious software surreptitiously installed abroad can become a continuing threat after the traveler returns home and connects an unwittingly compromised electronic device to government or personal information systems. Hackers can gain access to sensitive data networks more directly by attacking personal devices than through attacks mounted over the Internet.

Portable electronic devices (PEDs) carried abroad are vulnerable to installation of malicious software that can steal or manipulate data well after the traveler returns home.

Risks associated with use of electronic media overseas can be reduced through proper handling techniques. The simplest of these is to leave such devices at home. Barring that, protective measures may include using designated "travel" computers, single-use cell phones, and temporary e-mail addresses as well as refraining from communicating with a home organization's information technology systems.

Information Theft

Any U.S. citizen traveling abroad is a potential foreign intelligence collection target, but government and corporate leaders are most at risk because of the potentially useful information that they carry. Foreign intelligence services target the full range of U.S. economic, industrial, military, and political interests and emphasize private sector, state and local, and U.S. Government officials as potential sources of information. Many foreign governments control infrastructure to facilitate their intelligence collection efforts. Foreign government-owned telecommunications companies are particularly well postured to collect information from foreign travelers communicating within the country.

—The U.S. Department of State cautions that in certain countries, U.S. citizens should have no reasonable expectation of privacy in private or public locations.

— Intelligence collection activities and information theft likely will be conducted in a nonthreatening and unobtrusive manner. Victims may not realize they have been targeted until after their information is compromised.

— Hotel rooms, Internet cafes, offices, and public places may be subject to on-site or remote technical monitoring.

— Travelers should assume that all information processed and transmitted on fax machines, foreign computers, or telephones is subject to interception. This vulnerability extends to personal cell phones, smartphones, BlackBerry's, laptops, and iPads brought from the United States that transmit over a foreign country's networks.

— Spy software, which intercepts and transmits information without a user's knowledge, can be implanted in both wired and wireless Internet portals in cafes, hotels, transportation depots, and elsewhere.

— Universal Serial Bus (USB) memory sticks and similar storage devices may become infected with malicious software if used on devices in a foreign country or loaded with malicious software when they are not in the owner's possession. Such storage devices given out as advertising tokens at conferences already may be loaded with malicious software.

— Customs officials in some foreign countries regularly inspect laptops and luggage—often without the owners being present—to copy sensitive information.

— Malicious software can hijack and control thousands of personal computers at a time through robot networks (botnets). Custom-made viruses can attack government and corporate databases to corrupt or steal data.

Protective Measures

The best strategy to protect electronic devices when traveling is to leave them at home. If this is not feasible, alternatives include buying a single-use cell phone locally, using a designated "travel" laptop that contains minimal sensitive information. Even with these strategies, however, travelers should assume that all communications may be monitored.

When in transit or separated from a computer or cell phone, travelers should keep sensitive and proprietary information on removable storage media such as CD–ROMs, floppy disks, removable hard drives, and USB memory sticks continuously in their possession. Hardware-based, encrypted USB memory sticks should be used, where possible, if sensitive information will be stored on the device. Whole disk encryption software should be used to protect sensitive information on the other media listed if sensitive information will be stored on such media.

Travelers should use strong passwords on devices and encryption programs for electronic files and e-mails.

If you have any questions regarding these activities or would like additional information, please review the OCIO Memorandum entitled *Updated: Department of the Interior Policy for Use of DOI-Provided Portable Electronics Devices While on International Travel* found here: https://sites.google.com/a/ios.doi.gov/international-travel-advisory/ or Chris Riemer, Office of Law Enforcement and Security, at (202) 208-6206.

The information contained herein was derived from the Department of Homeland Security, Office of Intelligence and Analysis, Homeland Security Assessment, and the Office of the Counterintelligence Executive, Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices.