UNITED STATES DEPARTMENT OF STATE
OSAC
BUREAU OF DIPLOMATIC SECURITY

General Cyber Security Precautions While Traveling

Information Security

4/23/2012

While traveling abroad, OSAC constituents should practice good cyber security. Some suggested protocols are below.
Consider traveling with “clean” electronic devices – if you do not need the device, do not take it. Otherwise, essential devices should have all personal identifying information (PII) and sensitive files removed or “sanitized.” Devices with wireless connection capabilities should have the Wi-Fi turned off at all times. Bluetooth functions on Smartphones should be disabled at all times. Do not check business or personal electronic devices with your luggage at the airport. All electronic devices should remain in your control and on your person throughout your trip. Do not connect to local ISPs at cafes, coffee shops, hotels, airports, or other local venues. Only use trusted networks. Check the US CERT National Vulnerability Database before departure. Update your “clean” device with new patches and antivirus software. Change all your passwords before and after your trip. Be cognizant of spear-phishing campaigns through both SMS and email. Confirm all senders before clicking on links or attachments. Be sure to remove the battery from your Smartphone when not in use. Technology is widely available that can geo-track your location and activate the microphone on your phone. Review your company’s reporting policy on lost or stolen devices. Ensure that you have good points of contact for reporting any incident. Keep your desktop on your tablet, PC, or Mac “clean.” Once used delete unnecessary files, clear browser history, and empty “trash” and “recent” folders after each trip. Ensure your IT forensics department examines your devices upon your return.