Tips from the National Counterintelligence Executive

Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices

YOU SHOULD KNOW

- In most countries you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.
- All information you send electronically – by fax machine, personal digital assistant (PDA), computer, or telephone – can be intercepted. Wireless devices are especially vulnerable.
- Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this, remove the battery.
- Security services and criminals can also insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to your home server, the "malware" can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.
- Malware can also be transferred to your device through thumb drives (USB sticks), computer disks, and other "gifts."
- Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.
- Corporate and government officials are most at risk, but don't assume you're too insignificant to be targeted.
- Foreign security services and criminals are adept at "phishing" – that is, pretending to be someone you trust in order to obtain personal or sensitive information.
- If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, you should assume the device's hard drive has been copied.

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 government or competitor.
- Back up all information you take; leave the backed-up data at home.

- If feasible, use a different mobile phone or PDA from your usual one and remove the battery when not in use. In any case, have the device examined by your agency or company when you return.

- Seek official cyber security alerts from: www.onguardonline.gov and www.us-cert.gov/cas/tips

Prepare your device:

- Create a strong password (numbers, upper and lower case letters, special characters – at least 8 characters long). Never store passwords, phone numbers, or sign-on sequences on any device or in its case.

- Change passwords at regular intervals (and as soon as you return).

- Download current, up-to-date antivirus protection, spyware protection, OS security patches, and a personal firewall.

- Encrypt all sensitive information on the device. (But be warned: In some countries, customs officials may not permit you to enter with encrypted information.)

- Update your web browser with strict security settings.

- Disable infrared ports and features you don't need.

WHILE YOU'RE AWAY

- Avoid transporting devices in checked baggage.

- Use digital signature and encryption capabilities when possible.

- Don't leave electronic devices unattended. If you have to stow them, remove the battery and SIM card and keep them with you.

- Don't use thumb drives given to you – they may be compromised. Don't use your own thumb drive in a foreign computer for the same reason. If you're required to do it anyway, assume you've been compromised; have your device cleaned as soon as you can.

- Shield passwords from view. Don't use the "remember me" feature on many websites; re type the password every time.

- Be aware of who's looking at your screen, especially in public areas.

- Terminate connections when you're not using them.

- Clear your browser after each use: delete history files, caches, cookies, URL, and temporary internet files.

- Don't open emails or attachments from unknown sources. Don't click on links in emails. Empty your "trash" and "recent" folders after every use.

- Avoid Wi-Fi networks if you can. In some countries they're controlled by security services; in all cases they're insecure.

- If your device or information is stolen, report it immediately to your home organization and the local US embassy or consulate.

WHEN YOU RETURN

- Change your password.

- Have your company or agency examine the device for the presence of malicious software.