CITADEL
INFORMATION GROUP, INC.

Cyber Security – Don’t leave home without it

Don’t neglect cyber security when you’re traveling. Traveling exposes you to higher than normal cyber risk. This is true whether you’re planning to surf the web, do email, or Skype with family and friends. It’s particularly true if you plan to conduct sensitive corporate business online, especially in certain Asian and Eastern European countries with a reputation for cybercrime. Any device used to store or process information is at risk: laptops, netbooks, tablets, iPads, iPhones, smartphones, USB-drives.

Here’s a baker’s dozen of basic travel tips. They apply whether you’re traveling to China or just going down the street to your neighborhood Starbucks.

1. **Minimize sensitive information.** If it’s sensitive and you don’t need to carry it with you, then don’t.

2. **Password protect devices.** A not-to-be-neglected basic line of defense. Citadel recommends a minimum of 12 characters, including three of the four basic character groups: upper-case, lower-case, numbers and special characters.

3. **Encrypt drives.** Both Windows and Mac OS X have encryption built into the Operating System. Truecrypt is free disk encryption tool. Axcrypt is a free file encryption tool. Be sure to set a very long passphrase: 15 or more characters, including upper-case, lower-case, numbers and special characters. When you can, set the encryption to erase all data after 10 failed attempts at entering the passphrase.

4. **Set *User Type* in the Windows Control Panel to Standard.** This will add a layer of protection against rogue programs.

5. **Keep all programs updated to the most recent versions.** Use our *Weekend Patch and Vulnerability Report* to stay current with updates for common programs.

6. **Install and use antivirus programs.** Antivirus programs are far from sufficient but they do add a necessary layer of protection.

7. **Be wary of connecting into unknown networks.** That internet café in a hip part of downtown may not only be compromised, it could be actively distributing malware. So could the “supposedly secure” hotel network. Unknown *Wireless Access Points* are particularly dangerous.

8. **Keep WiFi turned off except when you want to use it.** Don’t let your WiFi automatically connect. If you connect to an access point, set your WiFi to forget the access point when you leave.

9. **Keep Bluetooth turned off except when needed.** Too few people are aware that cellphones and even laptops can be compromised by exploiting Bluetooth vulnerabilities.

10. **Turn on "Remote Wipe" for mobile devices.** This lets you erase all the data off of a device if it is lost or stolen. iPads, iPhones and Macs use a program called *Find iPhone* to do this. They can even help you find your lost device.

11. **Be careful using public computers.** I wouldn't use a computer in an Internet café for anything but checking the news. I'll print my boarding pass on the hotel's computers. Online banking, eCommerce, checking my email — places where I have to enter a password — no way!!

12. **Use a VPN for sensitive connections.** Use a virtual private network (VPN) to connect to your office network, cloud storage, your bank or potentially sensitive email.

13. **Physically protect devices.** Don't leave computing devices in cars or hotel rooms. And don't leave your laptop on a restaurant table while you take that quick trip to the restroom.

China Travel: If you are traveling to China and not just to your neighborhood Starbucks (or Canada or France), there are other precautions the wary traveler will want to take.

Travelers to China need to operate from the assumption that the State has an active interest in

- Accessing the information on your computing devices
- Monitoring your telecommunications
- Eavesdropping on your conversations
- Installing a back door on your computer to provide access to your computer (and any network you connect to) when you get home

A recent article in The New York Times — Traveling Light in a Time of Digital Thievery — describes the steps one must be prepared to take in visiting China. The article describes the precautions a China expert at the Brookings Institute, Kenneth G. Lieberthal, takes when he travels to China.

According to the story, Lieberthal "follows a routine that seems straight from a spy film … He leaves his cellphone and laptop at home and instead brings 'loaner' devices, which he erases before he leaves the United States and wipes clean the minute he returns. In China, he disables Bluetooth and Wi-Fi, never lets his phone out of his sight and, in meetings, not only turns off his phone but also removes the battery, for fear his microphone could be turned on remotely. He connects to the Internet only through an encrypted, password-protected channel, and copies and pastes his password from a USB thumb drive. He never types in a password directly, because, he said, 'the Chinese are very good at installing key-logging software on your laptop.'"

Whether you feel the need to be as careful as Lieberthal — it's not paranoia if they are trying to get you — or you're willing to tolerate a greater degree of risk, all travelers should assume

- Their conversations are being eavesdropped on
- Their telephones are tapped
- Their Internet usage is monitored and logged
- If they give their computing device to anyone, it will come back with a key-logger and other malware on it.

China has import restrictions on encrypted devices that adds yet another element to the information security challenge. Before an encrypted device can be brought into the country, China requires the traveler to get a permit issued by the *Beijing Office of State Encryption Administrative Bureau*. Information on how to get a permit can be found in the "Casting a wide net: China's encryption restrictions."

Several countries besides China also have import controls on encryption. These include:

- Burma (you must apply for a license)
- Belarus (import and export of cryptography is restricted; you must apply for a license from the Ministry of Foreign Affairs or the State Centre for Information Security or the State Security Agency before entry)
- Hungary (import controls)
- Iran (strict domestic controls)
- Israel (personal-use exemption – must present the password when requested to prove the encrypted data is personal)
- Morocco (stringent import, export and domestic controls enacted)
- Russia (you must apply for a license)
- Saudi Arabia (encryption is generally banned)
- Tunisia (import of cryptography is restricted)
- Ukraine (stringent import, export and domestic controls)

Travelers should check the U.S. State Department website before traveling to verify that the above information is current. Travelers should also check the U.S. Department of State's country-specific information before traveling with an encrypted laptop. Another useful reference is the *Crypto Law Survey* maintained by Prof.dr. Bert-Jaap Koops of Tilburg University.

U.S. federal regulations control the export of “encryption commodities, software and technology” (see Code of Federal Regulations, Title 15, Section 740.17). There are, however, license exceptions that allow travelers to take encrypted devices with them, provided that they return within the year and “retain effective control and ownership.” Travel with encrypted devices is allowed except for travel to the following five countries designated by U.S. government as supporting terrorism.

- Cuba
- Iran
- North Korea
- Sudan
- Syria.

Travel to any of these countries requires removal of any encryption technology before entering it.

Below are a few additional web sites with information on securing sensitive information while traveling abroad:

1. New Import License Requirement for Encryption Products and Equipment Containing Encryption Technology, Baker & McKenzie, 2010
2. Casting a wide net: China’s encryption restrictions, Christopher Cloutier, Jane Y. Cohen, WorldECR, November 2011
3. The Regulation of Encryption Products in China, Xia Yu, Matthew Murphy, Bloomberg Law Reports, MMLC Law Group, 2011
4. Advisory for Travelers, Harvard University
5. Important information When traveling internationally, Princeton University
6. Travel Restrictions on Encryption Software, Wright State University

Reprinted from our blog: www.Citadel-information.com/blog

© Copyright 2012. Citadel Information Group, Inc. All Rights Reserved.