IT Defender

From the OIM Information Security Program

July 2011

Issue 5

Inside this issue:

Report an Incident

If you suspect lost, misplaced or stolen equipment or a breach of Personally Identifiable Information (PII), notify your equipment manager **AND** contact the FDA IT Security Operations Center (SOC) at:

- **Email:** [redacted]
- **Toll Free Number:** [redacted]

Traveling Outside of the United States

When you travel internationally for either business or pleasure there are several things to consider, such as what to take or not take, knowing the laws in the other country, if there is a current travel warning, etc. Before you travel out of the United States on behalf of the FDA with technology assets, please adhere to the following:

- Submit a travel request via GovTrip - *https://govtrip.com/govtrip/site/index.jsp*
- If you do not need a laptop or Blackberry, don't take it. This also applies to personal travel.
- Carrying portable devices is discouraged, but not prohibited. Consult with your Center Information System Security Officer (ISSO) if you plan to take portable devices.
- Do not leave IT equipment unattended.
- Do not connect unauthorized IT equipment to your laptop or Blackberry (i.e. thumb drives, hard drives, etc). USB thumb drives are prone to

Traveling Outside of the United States continued...

malware infections. Rewritable discs (i.e. CD-RW, DVD-RW) and IronKeys are an excellent substitute to thumb drives.

- Computers and Blackberries issued solely for international travel should NEVER be connected to the FDA network upon return. Users are encouraged not to travel with their VPN/RSA Token.
- Return all FDA loaner IT equipment within five business days upon coming back to the office.

In preparation for and while traveling overseas, it is important to be aware of the following whether traveling for business or pleasure:

- Expect that transmission of information is being intercepted and read at any location where networks are controlled by another government. Foreign network providers can disable mobile device encryption and then turn it back on after information is intercepted.

□ **How to protect the data:** Do not process or transmit sensitive information. Do not take technology assets (laptop, Blackberry, cell phone, etc) if you do not need them.

- When overseas, foreign communication networks can intercept wireless device signals. Assume that all forms of communication with wireless devices are monitored and subject to compromise. Hacker software can be used to locate and connect to vulnerable Bluetooth-enabled cell phones, allowing address book information, photos, calendars, and SIM card details to be downloaded, and long-distance phone calls to be made using the hacked device.

□ **How to protect the data:** Power off mobile devices when not in use and only use the Bluetooth function if absolutely necessary (Do not use the Bluetooth function if traveling for business). Remove the battery from your mobile device and store it separately from the device.

- Anywhere facilities (i.e. hotel) are controlled by another government, you should expect tampering with unattended electronic devices. Rooms are accessible by hotel staff, as are hotel safes. In many instances, local authorities can quickly gain access to an unoccupied hotel room.

QUICK TIPS

- Treat your laptop like a pile of cash and never let it out of your sight, not even "for just a few seconds".
- Keep your laptop off the floor while on public transportation, such as subways or buses.
- Pay close attention to your laptop while passing though airport security.

DID YOU KNOW?

- In third world countries, a laptop computer is a sign of wealth and carrying one may place you at risk.
- Hotel business centers and phone networks are regularly monitored in many countries.
- Encryption software is illegal in some countries. Violate the laws and you could be fined or even risk having your electronics confiscated. A good place to find information on a countries laws is at your library, your travel agent, and the embassies, consulates or tourist bureaus of the country you will visit.

Traveling Outside of the United States continued...

□ **How to protect the data:** Avoid leaving electronic devices unattended in a hotel room. If that is not possible, remove the hard drive and store it separately from the device.

- Be aware that public Internet kiosks and cafes are breeding grounds for malicious software that can capture private information (passwords, bank account or credit card number, phone numbers, names, etc).

□ **How to protect the data:** Never use them for official or confidential personal business.

- When passing through an airport, never send your laptop through the scanner until reaching the front of the line in order to keep it under observation.
- Do not check a laptop with your baggage.
- Immediately report any suspected tampering, unauthorized use, loss or theft of any FDA asset to the IT Security Operations Center (SOC) at soc@fda.gov or 855-533-2762 (24x7).

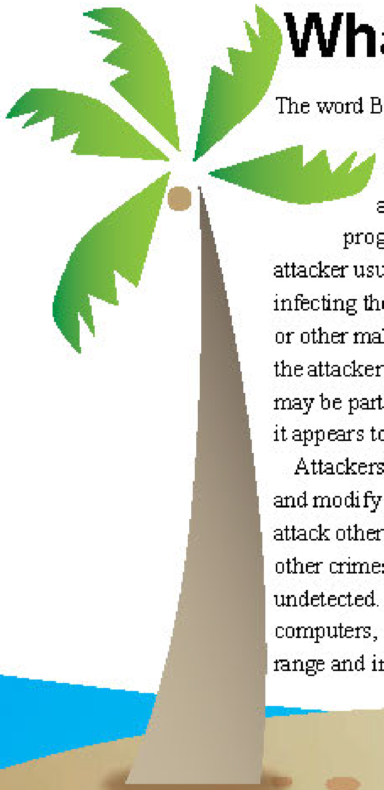
Remember if you do not need electronic devices leave them at home!!!

Below are a few links that will aid you in a safe trip overseas:

- *http://travel.state.gov/travel/tips/safety/safety_1747.html*
- *http://travel.state.gov/travel/tips/tips_1232.html*

TRAVEL TIPS & HELPFUL LINKS

- **Traveling Overseas with Electronic Devices -** *http://www.ncix.gov/publications/reports/traveltips.pdf*
- **FDA Travel Guide -** *http://inside.fda.gov:9003/Administrative/Travel/TravelInformation/ucm203232.htm*
- **Office of International Programs Homepage -** *http://inside.fda.gov:9003/OC/OfficeofInternationalPrograms/ucm135257.htm*
- **Travel Presentation -** *http://inside.fda.gov:9003/Administrative/Travel/InternationalTravel/ucm224159.htm*



What are Botnets?

The word Botnet is derived from the idea of bot networks. A bot is an automated computer program, or robot. An attacker usually gains control by infecting the computers with a virus or other malicious code that gives the attacker access. The computer may be part of a botnet even though it appears to be operating normally.

Attackers use botnets to access and modify personal information, attack other computers, and commit other crimes, all while remaining undetected. By using multiple computers, attackers increase the range and impact of their crimes.

How can you reduce the risk of your computer being compromised?

- Use and maintain anti-virus software
- Install a firewall
- Use good passwords
- Keep software up to date
- Take precautions opening emails and browsing the Internet

If you believe that your computer is infected, consider contacting a trained system administrator.

To learn more about Botnets and what they do visit these sites.

Here are some links:

- http://www.answers.com/topic/botnet
- http://singularityhub.com/2010/03/04/beware-the-bot-nets-zombie-cyber-attacks/

Note: The botnet content was provided/produced by US-CERT, a government organization.

HOT SUMMER SECURITY READING

1. **The Cuckoo's Egg**
   By Clifford Stoll

2. **Cyber Within: A Security Awareness Story and Guide for Employees** (Cyber Crime & Fraud Prevention)
   By Marcos Christodonte II

3. **Catch Me If You Can:** The True Story of a Real Fake
   By Stan Redding and Frank W. Abagnale

4. **Kingpin:** How One Hacker Took Over the Billion-Dollar Cybercrime Underground
   By Kevin Poulsen

5. **The Lure:** The True Story of How the Department of Justice Brought Down Two of The World's Most Dangerous Cyber Criminals
   By Steve Schroeder

6. **Stealing Your Life:** The Ultimate Identity Theft Prevention Plan
   By Frank W. Abagnale

7. **The Art of the Steal:** How to Protect Yourself and Your Business from Fraud, America's #1 Crime
   By Frank W. Abagnale

Celebration of National Cybersecurity Awareness Month

This year the Policy & Awareness (P&A) team will host several events at White Oak in celebration of October's National Cybersecurity Awareness Month. Throughout the year, P&A hosts ongoing educational activities to provide security awareness to FDA users. Join us for this year's annual celebration to hear interesting speakers, pick up educational materials to share with your peers, and enter for a chance to win great prizes.

Policy & Awareness Oktoberfest

National Cybersecurity Awareness Month Agenda

Oct. 4 11am-12pm
"Securing the weakest Link"
Presented by Jayson Ferron
White Oak Bldg 2 Room 2047 E

1pm-3pm
Awareness booth
Building 2 Atrium

Oct. 26 1pm-2pm
Cyber Awareness Demo
Presented by Robert Young (Rocky)
White Oak Bldg 32 Room 1243

Nov. 3 1pm-3pm
"Making the Internet Safer for Children & Families"
Presented by Donna Rice Hughes
White Oak Bldg 32 Room 1243

If you have any questions, comments or suggestions on topics to include in future newsletters, please contact...

ITSecurityAwareness@fda.hhs.gov