Federal Bureau of Investigation—Washington Field Office

Personal Computer Security

It's within your control

Computer Security Tips for Students and Travelers

In the 21st Century, Internet connectivity is not an option, it is a necessity. Information. Collaboration. Knowledge. Communication. Entertainment. Life. All of these require some level of connectivity. Whether on campus in the US, studying abroad, or traveling for fun, there are some simple steps you can take to protect your information, your identity, your work product, your money, and your privacy.

Email Safety

A common way to exploit your computer and account information is through Phishing. These emails are designed to look like official communications from employers, school, friends or co-workers. To exploit your system, the hacker includes an attachment with a malware payload or a link to a malicious website. When you open the attachment or click the link you help the hacker infect your system. Spear-phishing is the same but directed at specifically identified recipients.

Top 10 Internet Safety Tips

- Use Antivirus and set it to update daily.
- Ensure your system's personal firewall is active.
- Use sophisticated passwords (see insert).
- Patch your Operating System.
- Think about what is on your Social Networking Site. (see insert other side)
- Use caution when trusting public WiFi.
- Think before clicking a link, such as from a bank, in an email. Type it in your browser.
- NEVER send personal information (SSAN, Credit Card Info, etc.) in an email. It is sent un-encrypted.
- Report suspicious emails or activity to your Information Technology department.

It's a different world out there

In the United States we live with the protection of the U.S. Constitution and an expectation of privacy. That is not the case in many other countries. Some citizens, in some foreign countries are not afforded Internet privacy and their access to Internet based information and their Internet postings are censored. Even worse, their Internet traffic is monitored and assessed for threats to their country, opinions and views counter to the ruling government and for information that their country's intelligence services could use. Be cautious about connecting your computer or mobile device to foreign Internet access points.

Password Guidance

- ***Do NOT use dictionary based words***
- ***Do NOT use common phrases***
- ***Do NOT repeat passwords for websites or accounts***
- ***Strong password. Mix $ymb0l5, numbers, CAPS***
- ***Change them on a regular basis***

Firewalls, Browsers, and WiFi, Oh My!

- Ensure your computer based firewall is secure and active.
- Ensure your router/WiFi router firewall is active.
- CHANGE the default administrator password on your router.
- Use WiFi encryption and closed network. (i.e. WPA2)
- Disable remote administration on your router.
- Turn off your router when away for long periods of time, i.e. vacation.
- Unplug your computer from the network or disable WiFi when not in use.
- Disable the Wake On LAN feature in your computers BIOS. (Check your computer manual)
- Check for router firmware updates.
- Use a personal WiFi router when traveling, if possible or use a personal WiFi hotspot.
- Disable 3rd Party cookies in your browser.
- Set cookies to expire at end of session.
- Clean House Often
  - Clear browser cache
  - Clear cookies
  - Clear browser history
- Set Flash security features.
- Use private browsing when needed.
- Do not do private work (banking) from public WiFi spots.
- If accessing accounts through public shared networks (hotels, etc.) change your passwords after returning home.

Smart Phone Smarts

- Password protect your device.
- Understand what applications are using location services and disable that feature as appropriate/needed.
- Your Smart Phone is a computer. All of the guidance in this publication applies to Smart Phones too.
- Install phone software updates when issued. They often contain security fixes.
- Use common sense and good judgment when purchasing apps for phones. Some malicious apps communicate personal information.

Social Networking Safety

- What type of information are you sharing? Too personal? GPS data from your photos?
- Is your site set to public or private viewing?
- Photos about you, your family and life are on the Internet? What is it telling people?
- Are location services enabled on your Smart-Phone?
- Use HTTPS (secure connection) for accessing your social network sites when possible.
- Are your Tweets or "status" telling people that your home is empty?

My FBI Cyber Point of Contact is:

WHERE TO GO FOR HELP

WWW.FBI.GOV WWW.IC3.GOV WWW.INFRAGARD.NET