Connect Safely
FBI Cyber Security Basics

In the 21st Century, Internet connectivity isn’t an option, it’s a necessity.—Real time communication and information sharing online have become a requirement for work collaboration, learning, entertainment, networking, travel, and so many other aspects of life. To keep the experience positive and productive, there are some simple steps we all need to take to protect our personal information, identity, finances, and corporate intellectual capital from cyber-criminal predators.

How do your Internet safety habits stack up to our cyber experts’ list of basics? Check and see below.

**Top 10 Internet Safety Tips**

- Use reputable antivirus software and set it to update daily.
- Ensure your system’s personal firewall is active.
- Use complex passwords.
- Install updated patches to your operating system.
- Think carefully about what information you offer on your Social Networking Sites.
- Avoid forwarding chain emails, as links and attachments may contain viruses.
- Think before downloading files and clicking emailed links, especially from a bank. Instead type the link manually into your browser.
- Beware the pop-up Antivirus alert. Be sure it’s from the company you use.
- Never send personal information (Social Security, Credit Card Info, etc.) in an email. This sensitive information needs to be encrypted.
- Report suspicious emails or activity at work to your IT department.

**Passwords Galore**

- Do not use simple words that may be guessed, common phrases, or easy-to-discover personal information (like your dog’s name).
- Do not reuse passwords for more than one website or account.
- Use long and strong passwords. Mix $ymb0!5, numbers, CAPS.
- Be sure your password hints don’t correspond to information that can be discovered on your social networking page.
- Change passwords on a regular basis.
- Always log out of accounts when you aren’t using them.

**Social Networking Considerations**

- Most sites should not be set to public viewing, but rather should be private access only.
- Use caution about what type of information you’re sharing and with whom. Is it too personal?
- Consider what photos reveal about you, your family, names, or addresses. Photos become a permanent record online.
- Use HTTPS (secure connection) rather than HTTP for accessing your social network sites whenever possible.

**Email Phishing**

A common means of exploiting computer and account information is through Phishing. Often preying on connections gained through social networking sites, these emails are designed to look like official communications from employers, school, friends or co-workers.

To exploit your system, hackers include an attachment with a malware payload or a link to a malicious website. When you open the attachment or click the link, your system is infected. Spear-phishing is similar but targets specific recipients.
Smart Phone Smarts

Your Smart Phone and Electronic Tablet are computers too! All of the guidance in this publication also applies to handheld devices.

- Password protect your handheld device with the same care you would any other computer.
- Understand what applications are using location services and disable that feature as appropriate/needed.
- Install phone and tablet software updates when issued. They often contain security fixes.
- Use common sense and good judgment when purchasing apps for phones and tablets. Some malicious apps communicate personal information.

Firewalls, Browsers, and WiFi, Oh My!

At Home WIFI:
- 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.
- Disable the Wake On LAN feature in your computers BIOS. (Check your computer manual)
- Check for router firmware updates regularly.

Public WIFI:
- Take precautions when trusting public WiFi.
- Use a personal WiFi router when traveling, if possible or use a personal WiFi hotspot.
- 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.

Both:
- Ensure your computer-based firewall is secure and active.
- Set cookies to expire at the end of a browsing session.
- Clean house often: Clear browser cache, cookies, and browser history.
- Disable 3rd Party cookies in your browser.
- Always open a fresh browser window when banking and purchasing online.
- Use private browsing when needed.
- Set Flash security features.
- Unplug your computer from the network or disable WiFi when not in use.

Travel Abroad: It’s a different world out there

Be extremely cautious about connecting your computer or mobile device to foreign Internet access points.

In the U.S. we’re protected by the Constitution and have an expectation of privacy. That’s not the case in some countries, where citizens are not afforded Internet privacy, and access to Internet-based information and web postings are censored.

Internet traffic may be monitored and assessed for threats, and opinions and views counter to the ruling government may provide information that their intelligence services could use.

To learn more about staying safe online contact us at www.FBI.gov, and visit www.IC3.gov and www.InfraGard.net.