Online Security Tips

Most of us are familiar with the internet to some degree. However, more businesses are providing products and services online and cyber-criminals are using this electronic medium to prey on victims.

Internet fraud and white collar crime is the fastest growing crime to date, which costs consumers billions of dollars a year. Although anyone can become a victim of crime, these useful tips can help prevent you from being the next target of Internet fraud.

1. **Creating and Protecting Your Passwords**
    - Use passwords that have at least eight characters and include numbers or symbols. The longer the password, the tougher it is to crack. A 10-character password is stronger than one with eight characters.
    - Don't use passwords that are based on personal information that can be easily accessed or guessed.
    - Use a combination of lowercase letters, capital letters, numbers, and special characters.
    - Avoid common words: some hackers use programs that can try every word in the dictionary.
    - Change your passwords regularly (at a minimum, every 90 days).
    - Don't use the same password for each online account you access.
    - Never use the "remember password" for online banking or transactional Web sites.
    - The strongest password is useless if you share it with others so guard yours closely.

2. **Security Software**

    Firewalls, antivirus, anti-spyware and other protection devices help keep a computer properly monitored and provide peace of mind. These tools are important in order to protect your computer and data. A good firewall is critical if you commonly access the Internet via a wireless connection. It is also important to keep your computer up-to-date with patches to security tools as well as to the operating system and other programs on your computer.

    Security software that comes pre-installed on a computer generally works for a short time unless you pay a subscription fee to keep it in effect. Resist buying software in response to unexpected pop-up messages or emails – especially ads that claim to have scanned your computer and detect malware. That's a tactic scammers have used to spread malware. Many new viruses are discovered everyday. To make sure your software offers the highest level of protection, you must update your anti-virus regularly. Most commercial anti-virus software include a feature which allows you to download updates automatically when you are on the Internet.

    Be sure you purchase your security software from a reputable company. You can always visit the Federal Trade Commission's website for more information (www.ftc.gov).

3. **Public Access Computers**

    Read these tips to help keep your work, personal, or financial information private when using public computers in libraries, Internet cafes, airports, copy stores, etc. Since you cannot validate the computer's integrity, there's a higher risk of fraud when you log in from a public computer.
    - Don't save your logon information. Always logout out of Web sites by clicking "log out" on the site. It's not enough to simply close the browser window or type in another address.

Many programs (especially social networking Web sites, Web mail, and instant messenger programs) include automatic login in features that will save your user name and password. Disable this option so no one can log in as you.

- Don't leave the computer unattended with sensitive information on the screen. If you have to leave the public computer, log out of all programs and close all windows that might display sensitive information.
- Erase your tracks. Internet Explorer also keeps a record of your passwords and every page you visit, even after you've closed them and logged out. Disable the feature that stores passwords. In Internet Explorer, click *Tools*, and then click *Internet Options*, click the *Content* tab, and then click *Settings*, next to AutoComplete. Click to clear both check boxes having to do with passwords.
- When you finish your use of a public computer, you can help protect your private information by deleting your temporary Internet files. Click *Start*, click *Control Panel*, and then double click *Internet Options*. On the *General* tab, click *Delete* under *Browsing history*. Click *Delete all*, click *Yes* to confirm that you want to delete this information, and then click *OK*.
- Watch for over-the-shoulder snoops. When you use a public computer, be on the look out for thieves who look over your shoulder or watch as you enter sensitive passwords to collect your information.
- Don't enter sensitive information into a public computer. These measures provide some protection against casual hackers who use a public computer after you have. But keep in mind that an industrious thief might have installed sophisticated software on the public computer that records every keystroke and then e-mails that information back to the thief. If you really want to be safe, avoid typing any financial sensitive information into any public computer.