Internet Security Tips For Seniors

The number of senior citizens getting connected to the Internet is increasing daily. As per the latest studies, almost 54% of American seniors (over 65 years of age) use the Internet and are capable of communicating through emails. Although a senior can handle the fundamentals, they are specifically targeted by criminals and fall victim to the latest scams just as others do.

This article is focused on providing some important guidance for seniors to stay away from such cyber scams and identity theft.

1. Install a security software

Gone are the days that anti-virus software provided all the security you needed. This is one of the most important factors to consider for senior citizens when using Internet. Be sure to install a paid suite that includes anti-virus **and** anti-malware that will protect you from the latest threats.

2. Update everything

Your operating system (Windows or Mac) that runs your computer needs to be periodically updated. Your web browser, anti-virus and anti-malware program, VOIP (like Skype) programs and anything else should be updated with the latest patches. Updating allows your programs to operate in a more secure manner.

3. Strengthen the security of home Wi-Fi

If you use Wi-Fi to access the Internet, make sure to use a strong encryption like WPA2. If you are not familiar with setting up Wi-Fi, ask someone in the family to do it for you.

4. Different passwords for every website

You need to create different passwords for every website. Why? When a hacker gains access to one of the websites, they don't also gain access to all your accounts across the Internet.

5. Avoid suspicious banners

Sometimes, you might see animating banners asking you to click on them. They will display messages like "your computer is infected, call ###-###-####" or "scan your computer for viruses" or "click here to claim your prize $$$". Never click them or call. They are fake advertisements to mislead you and gather your sensitive information. Just by clicking on such banner, you can become a victim of a scam.

6. Avoid emails from the "bank"

If you receive an urgent email asking for you to login to the "bank" website or to provide information like bank account information, social security number or anything personal, avoid these emails. These emails, most probably, are from a third party that wish to steal your information. Instead, call your bank.

7. Always use secured sites for online transactions

When you make a payment online, be sure to use sites that have secure encryption. They have a small padlock mark on the address bar and an extra "S" on the URL (instead of HTTP, they have HTTPS).

After all, it is about your own security. Do not believe everything you see in on the Internet or email. If you suspect something, just verify it from a family member who is familiar with computers.

Call **1-888-576-2578** for help with virus and spyware infections and computer tune up.

See http://RockStarVirusRemoval.com for details.

ROCKSTAR VIRUS REMOVAL