Internet Safety Tips

Ten Simple Steps To Internet Safety

(NAPSA)—It's an unfortunate reality that the Internet is simply not always a safe place. The Internet is a shared space, a virtual world of incredible beauty. However, just as in the real world, on the Internet, there are threats to your security. It is vital that you take steps to protect yourself, your family, your information and your technology. Just as you lock your doors at night, if you consider the facts about online security, you'll recognize that you should take a few precautions.

You should take the time to secure your computing system from online threats such as hackers, viruses and worms. If there are children in your home, consider setting filters so that they can visit only sites that are educational or entertaining in an age-appropriate way. If you're the type who hates pop-up ads and who would prefer not to have spyware reporting on your online activities, find out what measures you can take to shield yourself.

Your Internet service provider can be a great source of information about online security. Some ISPs also provide their customers with security software and tools that users can implement to enhance their security when connected to the Web.

To most people, Internet security is daunting. If you're like most people, you just want to be able to do simple things on the Web quickly and easily—you don't want to become a tech scholar just to make sure your PC and your family are not violated via their connection to the Internet. Fortunately, it's really not as difficult as you think. Basic Internet security can be had if you follow 10 simple steps.

Cox Communications, for example, has made it easy for Cox High Speed Internet subscribers to protect themselves, their families and their PC systems from malice by offering integrated security software that includes firewall, anti-virus, pop-up blocker, anti-spyware and parental controls, all conveniently managed from an easy-to-use toolbar. Launched just before the holidays, the new feature is offered to customers free of additional charge. The company also endeavors to keep their broadband subscribers and other Internet users in the community informed on the issues of Internet security. Cox.net includes links to information on online security and timely warnings about rampaging viruses, worms and even phishing schemes (online scams).

If you commit to only these 10 practices, your PC system will be a virtual fortress from which you can enjoy a fantastic view of the Internet. You'll be protected by a moat and control data access via a convenient drawbridge and portcullis. To learn more, go to www.cox.com/takecharge.

Top 10 Tips for Staying Safe Online

1. If there are children in the home, protect them by utilizing parental control software. The Internet is fraught with content that parents may find objectionable for youngsters. What's worse is that online chat rooms can provide fertile ground for child predators.
2. Routinely update your operating system to get the latest security patches. If you're using Microsoft Windows, turn on "automatic updates."
3. Utilize anti-virus software, routinely update your virus definitions and run a full system scan at least once a month.
4. Use a firewall.
5. Use safe practices when using e-mail. In particular, refrain from opening attachments from senders who are unknown to you.
6. Do not download program software via peer-to-peer file-sharing networks such as Kazaa.
7. Disable unnecessary services such as Web server, mail server and/or FTP (file transfer protocol) servers that can present an open door to hackers. If you don't know what these services are, you likely don't need them to be on!
8. Be smart when buying anything online. Only use reputable vendors and take care to protect your personal account information by choosing only vendors who offer a secure payment process based on encryption.
9. Install a home router that includes NAT (Network Address Translation). Using NAT between your cable modem connection and your PCs will stop incoming data packets from entering your network, unless one of your PCs has specifically requested the information. This complements firewall protection.
10. If you have a wireless network, secure it by enabling WEP or WPA encryption. With encryption, a user must have the key in order to access your wireless network. This helps keep hackers away from your network and personal information and also keeps neighbors from stealing your Internet service and possibly using it for illegal purposes (e.g., trading copyrighted material).