Tip Sheet: Secure Web Navigation and Transactions

Tips for Securing Your Online Surfing and Transactions

Anti-virus and firewall programs protect computers from a host of potentially dangerous programs that can wreak havoc not only on their computer hosts, but can spread to any other computer connected to the same network. That's the bad news . . . .

The good news is there are things you can do to protect yourself and your kids from malicious software that may be downloaded to your computer without your knowledge when you are surfing the Internet.

1. **Make sure your anti-virus and firewall software are up-to-date.** Chances are that trial versions of anti-virus and firewall protection software were installed on your computer when it was purchased. These trial versions typically last for 30 to 60 days after the computer is first turned on by the user. After the trial period expires, the software is generally not as effective at keeping your computer safe from the latest germs. You need to keep anti-virus protection current to maximize the protection against malicious attacks.

2. **Check With Your Internet Service Provider to See if it Offers Anti-virus and Firewall Protection.** If you do not already have anti-virus or firewall software, your Internet service provider may offer it, perhaps even at little or no additional charge.

3. **Check Your Computer's Built-in Defenses and Use Them.** Some types of spyware can send keystrokes entered by a user to a hacker. The hacker can then use passwords entered by users to hack into online accounts. Anti-virus software can quite often detect these types of programs and remove them, particularly if you run your scanning software every week. Make it a habit.

   Recent versions of Windows support a spyware scanner called "Windows Defender" (www.microsoft.com/windows/products/winfamily/defender/default.mspx) that is built into the computer's operating system. It can check to see if software germs have been able to penetrate a computer's defenses and are sitting quietly in the background recording information about websites visited. Apple computers also come with software defenses, such as a built-in firewall (http://docs.info.apple.com/article.html?path=Mac/10.6/en/8154.html).

4. **Use Strong Passwords and Change Them Frequently.** When was the last time you changed your login passwords to your online accounts? How disciplined are the kids at changing their passwords? You should use inventive, long passwords that are hard for hackers to guess, and not any passwords with personally identifiable information. Passwords with a mix of letters, numbers, and punctuation are best. And, if the password has already been compromised via a key-stroke logger discussed above, frequently changing online passwords may minimize the risk of a hacker using a password they have uncovered.

5. **Secure Your Wireless Environment.** Most computers are enabled for wireless ("Wi-Fi") communication, which can introduce security vulnerabilities when information flows over open airwaves between the computer and the connection to the Internet. Fortunately, data-scrambling techniques, known as encryption algorithms, make it difficult for hackers to understand information that they might intercept over the air. Everyone with a Wi-Fi connection should encrypt their connection. For more information, check out our video and tip sheet on securing wireless networks (www.fcc.gov/encyclopedia/protecting-your-wireless-network).

If you keep your anti-virus and anti-spyware software up-to-date, use strong passwords, and secure your wireless network, you will substantially increase the security of your online surfing and transactions.

Consumer Help Center

For more information on consumer issues, visit the FCC's Consumer Help Center at www.fcc.gov/consumers.

Accessible formats

To request this article in an accessible format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed 11/01/16