Tips for Secure Web Navigation and Transactions

Computers, laptops, tablets and other connected devices are always at risk of being compromised by hackers that use spyware, malware and other programs to access files, track web usage and financial transactions, and steal passwords and other personally identifiable information. Some malware is even designed to spread to other devices connected to the same network.

Installing anti-virus and firewall programs – and being vigilant in personal web security practices – are strongly urged to help thwart hacking attempts.

Make sure your security software is up-to-date

Make sure your firewall software is maintained and updated regularly for maximum effectiveness**.** Trial versions of both anti-virus and firewall protection software may have been installed on your computer when it was purchased, but trial periods typically expire 30 to 60 days after a computer is first powered on by the user. If protection software expires, your computer is at a much higher risk of attack. Keep security software current to maximize the protection against malicious attacks.

If you do not already have security software, check with your internet service provider to see if it offers such protection.

Set up software to auto-update and run security scans

Some types of spyware can send keystrokes entered by a user to hackers who use it to pick off passwords and hack into online accounts. Anti-virus software is designed to detect these types of programs and remove them. Schedule routine security scans and software updates to run automatically.

Use strong passwords and change them frequently

When was the last time you changed your 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. Passwords with a mix of letters, numbers and special characters are best. Never use passwords that include or allude to personally identifiable information. Frequently changing your passwords minimizes your risk of being hacked.

Secure your wireless environment

Almost all computers and connected devices today are enabled for wireless and Wi-Fi communication, which can introduce security vulnerabilities as information flows over open frequencies to wireless connections to the Internet. Encryption algorithms scramble data and make it difficult for hackers to understand information that they might intercept. Be extremely cautious when using public Wi-Fi and encrypt wireless connections whenever possible. For more information, check out our consumer guide (www.fcc.gov/consumers/guides/how-protect-yourself-online).

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.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau

Consumer Help Center

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

Alternate formats

To request this article in an alternate 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 02/23/18

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau