10 Tips to Stay Safe Online

1. Keep Your Programs "Patched"

Security flaws are regularly found in operating systems and application software. Companies that make software release quick fixes called "patches" that you should install to correct the latest software flaw. It is a good idea to check for security updates on the publisher's website for all the software you own.

2. Watch for Unwanted Add-Ons

Some software companies will offer you additional programs when downloading updates or installing new applications. Read the text in the box before clicking "next". Watch for items that are checkmarked offering to change your default browser, install additional toolbars or install additional programs. Uncheck the options you do not want before proceeding.

3. Know to What You Are Agreeing

Every program comes with an end-user license agreement (also known as a EULA). Many online services, like gaming or video sites, also have user agreements. Read the agreement before continuing on. Many "free" sites pay for their services by offering you advertisements or sharing your information with third-party affiliates. You may be opening yourself up to pop-up ads or tracking software if you continue. Know what you are getting yourself into.

4. Know Where You Are Going

Before clicking on a link in an e-mail or a web browser, hover over it. You can see the address (URL) to which it leads in a bar at the bottom of the screen. If it looks suspicious, DO NOT CLICK it.

5. Don't Trust Any Pop-Ups

Many virus/malware authors write their programs to pop-up looking like a legitimate warning. Because of this, it is easy to get tricked into clicking on the box, starting an install routine for malware. Instead of clicking the pop-up, right click the title on the start bar to close the window. Then, go to your known good anti-virus on your computer and run a full scan to truly check for malware on your system.

10 Tips to Stay Safe Online

6. Use Anti-Virus Software

A computer virus is a program that can invade your computer and damage or destroy information. Anti-virus software is designed to protect you and your computer against known viruses. But with new viruses emerging daily, anti-virus programs need to be updated regularly. There is NO anti-virus program that keeps out 100% of the viruses and malware.

7. Increase Junk Mail Filters and Avoid Clicking Through on E-Mails (Even from Friends)

You may receive an e-mail letting you know that you have a new deposit pending and need to login and verify. Many phishing schemes start with something looking very innocent and official, but lead unassuming users to websites designed to collect the information direct from you. If you receive an e-mail from one of the account-holding websites, open a new tab in your web browser and go directly to the website instead of clicking the links provided. It adds only a few seconds to the access, but keeps you out of any legit-looking phishing websites. Most legitimate services will never ask you for your login credentials, so make sure to avoid giving out this information. Using a junk mail filter can also help you keep from seeing some of these.

THINK BEFORE YOU CLICK!

8. Use Hard to Guess Passwords and Keep Them Private

The safest passwords are ones that include a capital letter, lowercase letters, at least one number and a character (like *, % or #). Be creative like using a 3 as a backwards E or substitute an ! or a 1 for an I in a word you will remember.

9. Use a Firewall

Firewalls help prevent thieves from stealing and using private information including your phone number and credit card numbers, which may be stored on a family computer. Windows comes with a good firewall already built in. We recommend using the Windows firewall.

10. Do Not Share Access to Your Computer With Strangers

Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files". This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you do not pay close attention. Check your operating system and other program help files to learn how to disable file sharing. Do not share access to your computer with strangers, including people who may call you claiming to be from Microsoft or an anti-virus company. These companies will NEVER call you unsolicited and you should never allow them access to your computer.