

Safety in Cyberspace

Personal computers (PCs) and the internet have been a boon to many, including a lot of seniors. We can stay in contact with friends and relatives around the world. It allows us to access information on any subject – news, medical, maps, weather, sports, etc. – from a wide variety of sources. Instead of being on hold at the Insurance Company, or Social Security, we can get to them online, do what is necessary and be finished in minutes. We can shop online, purchasing anything from needed medication to a gift for a grandchild. We can even pay bills online.

PCs and the internet can open many doors but they can leave those doors open for the “bad guys”. There are a number of actions you can take to safeguard your computer and all of the information it contains.

First, protect your computer by using:

- a. Antivirus software. Protects your computer from viruses –programs introduced by a hacker through emails or other programs– that destroy data, slow or crash your computer, or even allow an outsider to take over your computer to send emails or raid your personal information.

Anti-virus software scans your computer and incoming emails, find viruses and delete them. Since viruses are constantly changing, to be effective, anti-virus software must be updated regularly to catch the new viruses. So look for software that updates automatically and frequently so it catches the new viruses, and effectively reverses any damages. The most popular are Norton and MacAfee, but there are other brands that are effective as well. Stores such as Best Buy or Circuit City sell these products as well as the two mentioned below.

- b. Firewalls look for outside attempts to access your system and block them. At its best, a firewall prevents outside hackers from even “seeing” your computer. Firewalls can be either “hardware”, i.e. equipment, or “software”, i.e. programs. Hardware firewalls usually come with your cable modem. Software firewalls are often on the operating systems such as Windows XP or Macintosh OS X, or they can be obtained from suppliers such as Norton or MacAfee. In either case, hardware or software, you need to be sure they are set to “on”.
- c. Anti-Spyware As you surf the web, spyware monitors your activities and collects information about you. Anti-spyware periodically scans your computer, identifies the “threats”, notifies you and can clean them out. It is best to use more than one system to catch all threats. Trend Microsystems is a supplier of this type of software.

Second, protect yourself and your personal data.

- a. If asked for any personal information, your first reaction should be to refuse. Always ask why they need it, how it will be used, and how it will be protected. If you feel uncomfortable, do not give them the information. If the request seems to come from a company you deal with regularly, contact them via phone instead of

email to verify the request. Avoid sending personal data via email. It is not secure.

- b. Be extra careful if shopping online. Look for the lock icon or website urls that begin with “https:” which indicates that it is a secure site. For online shopping, my wife and I use an extra credit card, with a low limit, and not tied to any other card or account. It isolates any online purchases and makes it easier to track any activity on that card.
- c. Guard your email. Do not open unsolicited or unknown email messages. Turn off the “Preview Pane” function, and set default options to view open emails as plain text to avoid triggering an active link or pop-up. Never open an email attachment from someone you do not know, and never open an “.exe” file.
- d. Use email filters. Most email programs have filters. Learn to use the filters to limit the emails you receive.
- e. Secure your browser. Most Web browsers (Internet Explorer, Netscape, Firefox) and Operating Systems (Windows, Linux) are unsecured as the default option. However, the “Tools” or “Options” menus will allow you to access built-in security features. The “Help” function, or tech support, can provide some aid in understanding these options. The operating system’s own website also provides software patches to close some of the security holes, but you have to go find, download, and activate them.

Third, learn how to fix problems if things go wrong.

- a. If you get hacked or infected by a virus, unplug the machine from the phone or cable, then run a scan with anti-virus software, and reboot the machine. If that solves the problem, reconnect to the internet, and take steps to minimize future incidents by updating or installing a firewall. Contact your ISP (Internet Service Provider) and provide them with all of the information. Also contact the FBI at www.ifcfbi.gov. You will need to provide them with all the details.
- b. Fraud at an internet auction or when shopping online should be reported to the FTC at www.ftc.gov. They act as a clearing house to send the information to the “Consumer Sentinel” which publishes the information to law enforcement agencies across the country.
- c. Deceptive spam, especially “phishing” for personal data should be forwarded to spam@uce.gov. If the spam purports to come from a legitimate company, forward it to their security people as well. (Their website will tell how to do this.)

To protect yourself on the internet requires that you be knowledgeable, and stay up to date on all of the perils in cyberspace. One source for this information is the National Cyber Security Alliance, which provides free, non-technical cyber security and safety resources covering most, if not all, aspects of cyberspace. They can be accessed at www.staysafeonline.org.