

Computer Security

Privacy and SPAM

Computer security is defined as the protection of computer systems and the data stored on them from unauthorized access.

Access can be either in person or electronic, via network connection (telephone or broadband cable). Physical access can be limited by locking the computer in a safe place. Requiring a password or fingerprint in order to use the computer affords further protection. Hackers will try to access your computer electronically via your Internet connection. You need to protect against this type of intrusion with a software or hardware firewall.

Data stored on a computer warrants special protection when it is either private or difficult to replace. Private data would include your medical, banking, income tax, credit card, and investment information. Unless this data is available in another form outside the computer, it could also be difficult to replace. Documents, such as recipes, may not be private but they, too, might be difficult to replace. Your software can always be reinstalled if it is corrupted, but the effort involved is huge, so you need to protect the software even though it is replaceable. The most common way data on a computer is lost or damaged is by a virus arriving via E-mail. You need anti virus software, with up-to-date virus definition files, to protect against virus attacks.

Data in transit between your computer and other computers is also subject to compromise. It is possible to tap into public networks and "listen" to your Internet conversations. Also, if you use wireless networking adapters to connect your computer to other computers at home or on the Internet, the transmissions can be intercepted several hundred feet away without your knowledge. The only way to protect data in transit is by encrypting it. This is not very easy or convenient for most of us.

Your computer keeps a list of the web sites that you have visited. If you prefer not to let others see what the list of URLs contains, you should purge the cache and history files. This can be done manually, or by using automatic software utility programs.

SPAM is defined as unwanted commercial E-mail. We all receive many of these “junk” messages each day, which clog up our inbox and waste resources as they travel in the network to reach us. Your Internet Service Provider may have an option, like the Earthlink Spaminator, that will block over 90% of the SPAM before it reaches your inbox. You can also turn on the filters in your own E-mail software such as Outlook Express to block SPAM that repeatedly comes from the same sender. Another approach is to set up the filters so they only allow incoming mail from the senders that you have listed in advance. If you establish a new E-mail address with a free service such as Hotmail, you will be free from SPAM for a period of time. When the SPAM begins to bother you, just change your address again.

R. Kent McDonald
rkmcdonald@earthlink.net
345-2931