Computer **Briefs**

Practicing Safe Computing

Michael J. Ackerman, Ph.D.[*]

Hardly a day goes by that we don't find ourselves reading or talking about computer security. This is not a new topic. Computer viruses have been with us for more than 16 years. I discussed the topic as an analogy to clinical disease viruses in this column back in 1988 (Ackerman, MJ. A New Category of Disease: Computer "Virus." Journal of Medical Practice Management 1988; Vol.4#1: 39-40). Since then the etiology of computer viruses has gotten much more complex and sophisticated but so has our ability to recognize them and protect our computers from them.

. . . the etiology of computer viruses has gotten much more complex . . . but so has our ability to recognize them and protect our computers . . .

Today, security includes not only protection against viruses, but also adware and spyware (Ackerman, MJ. Spyware and Adware. Journal of Medical Practice Management 2005; Vol.20#4: 183–184), data theft, and the use of your computer without your knowledge. The topic of computer security most recently fell into the public eye with the release of an update to Microsoft's latest operating system, Window XP. Every computer consultant that I know recommends that the update, known as Service Pack 2 (SP2), should be installed on every computer running Windows XP. It can be downloaded from the Microsoft Web site for free. It may take as much as 30 minutes to download using DSL or a cable modem and another 30 minutes to install. All that you need to do is to click on Yes and be patient.

Service Pack 2 (SP2) should be installed on every computer running Windows XP. It can be downloaded from the Microsoft Web site for free.

The main purpose for the SP2 update is to add computer security directly into the operating system instead of trying to add it on later. The update adds a security center that provides three types of security: a firewall, security updates, and a virus protection monitor.

It does not contain virus protection software or protection against adware and spyware, but it does monitor this software if installed and warns the user of possible security problems if it is not installed or not current.

Back in 1988, most people were unaware of the Internet. Computer viruses were generally spread through the use of floppy disks to exchange computer programs. The warnings were often presented as an analogy to health warnings, especially analogous to warning about venereal disease. These were typical messages to the public: "Practice safe computing." "Has your computer been vaccinated?" "Do you use protection?" Since viruses were spread through the exchange of floppy disks, you knew when you were putting your computer at risk and you should have known how to protect it.

One recent computer virus spread worldwide within 24 hours of first detection.

Today the Internet is the main vector for the spread of computer viruses. This means that viruses can be spread orders of magnitude faster than before. One recent computer virus spread worldwide within 24 hours of first detection. Viruses on the Internet are spread through more ways than the downloading of programs. Anything you receive through the Internet could potentially contain a virus. We have all heard of the stories of viruses being spread through music and video files. Viruses can also be spread through e-mail, document files, spreadsheet files, and presentation files. Every file you receive is open to suspicion.

Anything you receive through the Internet could potentially contain a virus.

The solution today is the same as it was 16 years ago: install a virus protection package. In this age of the Internet, where new viruses can be spread with almost lightning speed, you should also subscribe to a virus protection update service designed to work with the virus protection package you have installed. Think of a computer virus as a flu virus. A flu shot can protect against only the flu viruses that are included in the vaccine. Next year you need another flu shot because there are new viruses that were not included in previous shots. Your initial virus protection software is like your first flu shot. It contains protection

[*]Assistant director for high-performance computing and communications, National Library of Medicine, Building 38A, Room B1n-30, 8600 Rockville Pike, Bethesda, MD 20894; e-mail: ackerman@nlm.nih.gov. *This article was written by the author in his private capacity. No official support or endorsement by the National Library of Medicine is intended or should be inferred.*

against all viruses known up to that point. Your virus protection update service is like subsequent flu shots. It updates your protection to include all known viruses since the last update. Unlike flu shots, however, which are needed once a year, updates to computer anti-virus software are generally released once a week, sometimes more frequently, perhaps even daily.

. . . updates to computer anti-virus software are generally released once a week, sometimes more frequently, perhaps even daily.

Installing virus software and updates is painless (but that's what you tell your patients). Once the initial software is installed, it can be set up to automatically check the subscription site daily when you connect to the Internet for any new updates. The transaction happens in the background and is barely detectable if you are connected to the Internet by DSL or cable.

A firewall is different from anti-virus software, but the two of them work together to help protect your computer.

The other major feature of a modern computer security system is the firewall. To quote Microsoft:

> A firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network. A firewall is different from anti-virus software, but the two of them work together to help protect your computer. You might say that a firewall guards the windows and doors against strangers or unwanted programs trying to get in, while an anti-virus program protects against viruses or other security threats that can try to sneak in through the front door.

Basically a firewall is designed to block any incoming data that was not specifically requested by a computer on the internal network. This works in most situations. The most common exception is Internet videoconferencing using the H.323 protocol. The firewall will allow you to make videoconference calls, but will not allow others to call you. Methods have been developed to overcome this problem. The least desirable method involves adding exception rules to the firewall. These exceptions can be detected by hackers who soon exploit them to gain entry to the network.

Basically a firewall is designed to block any incoming data that was not specifically requested by a computer on the internal network . . . [and is needed] at home or in the office.

Firewalls were originally used by institutions to protect their internal networks from unauthorized entry through the institution's connection to the Internet. With the popularization of DSL and cable modems, as well as home and office networks, there is also a need for a firewall at home or in the office. Firewalls are often built into the home network router or wireless access point. A firewall is built into every copy of Microsoft XP with SP2 . Once set up and turned on, a firewall usually needs no further maintenance or update unless exception rules are implemented. ■