Bugging Out

Virus Protection Is Serious Business

Michael R. Arkfeld is an Assistant United States Attorney in Phoenix. He is the author of *The Digital Practice of Law* (5th edition) and a frequent speaker and columnist on law practice. He can be reached at Michael@Arkfeld.com.

Before the information technology revolution, security amounted to preventing access to a firm's physical office building and paper files. Now, with high-speed modems and portable storage running into the gigabytes, security is much more of a threat to the protection of client confidences.

Nothing is 100 percent secure; you can only minimize your exposure to the risk of security breaches. And you must determine the value of the information you seek to protect: Is it cash or marketable securities, or is it word processing documents? In each case, what price do you pay for security? You must decide how much security is enough.

A virus can have a swift and devastating impact on your digital data. A computer virus has been described as a computer program that infects other programs by replicating itself.

A virus consists of two parts: a replication code, which spreads the virus, and the payload, which is the prank or destructive part. One new virus is created each day; there are more than 8,000 signature viruses. They can be distributed on a floppy, e-mail attachment, file download off the Internet, shrink-wrapped software, from another computer on your network or even via CD-ROM. You can pick up a virus from your home computer after your kids have played on it.

Once you open the infected file program, the replication code is activated and will spread by copying itself to other drives on your computer or hard drive. A virus may lie dormant for months and become triggered by a specific coded date.

Viruses can easily bring down a firm's computer system. They come in all sizes and shapes. Some are harmless, and others replicate on their own, destroying valuable data, affecting your law firm and your client files. They attach themselves to healthy files and can affect programs like Word or Microsoft Outlook.

> One new virus is created each day; there are more than 8,000 signature viruses.

There are different kinds of viruses. File infectors attach themselves to .com or .exe programs, commonly referred to as executable files. They can live on your computer for some time before doing inadvertent or deliberate damage to your system.

Other viruses, called worms, replicate and spread quickly. Melissa, or the Love Bug, was an attachment to an innocent-looking e-mail message. Opening the attachment activated the macro, and copies got delivered to other e-mail addresses, boot sectors or files.

There are warning signs that you have a virus on your system:

- Changes in file size, especially in .com and .exe files
- Unexplained changes in available RAM for your programs
- Unusual behaviors, such as not being able to load a program, a program not functioning properly or unusual messages flashing across the screen

Antivirus programs can locate and destroy viruses. Always run a virus program to check floppy disks before transferring files into your computer. Some antivirus programs to consider are Symantec's Norton Anti-Virus (**www.norton.com**) and McAfee's VirusScan (**www.nai.com** and **www.mcafee.com**). Norton Anti-Virus also will check for viruses on files you download from the Internet and provide the latest virus signatures.

You can take precautions:

- Assume every floppy disk and CD-ROM disk is infected—Trust no one.
- Set up the automatic features of your antivirus software.
- Update the antivirus signatures in a timely manner.
- Issue firm guidelines to ensure a virus-free computing environment.

If a virus strikes, consider using Ontrack (**www.ontrack.com**). They specialize in recovering data lost or corrupted as a result of computer crime, a hardware or system malfunction, human error, computer virus or natural disaster.

Viruses pose a risk to firm documents and client confidences. But perhaps the greatest possible damage inflicted is the significant amount of lost time in trying to recover infected files. When it comes to viruses, caution and vigilance are investments that pay dividends.

Be aware of hoaxes about computer viruses, but always err on the side of safety. To check out virus myths or rumors, go to www.kumite.com