

Information Technology

Viruses, Worms, and other Computer Wildlife

Caught the Melissa virus? Bitten by the “I love you!” bug? Where do these irritants come from? Who devises them, and how can you protect your computers from them?

In the age of computer innocence, 15 years or so ago, there were few personal computers, and programmers were all professionals. Faced with a technical challenge, a true geek might spend three days coming up with an elegant solution, then show it to his or her peers as “just a hack”, implying that “if I only had time I could come up with something much better than that”. Hence the term “hacker” – someone who hacks out computer code. Later the term was used to describe someone who “hacks” (breaks into) a computer without authorization.

By the mid 1980s social misfits were devising small programs to cause mischief. Since computer users would not willingly install such programs, they were written to attach themselves to legitimate programs and spread like viruses when users exchanged diskettes. The first “worms”, named for how they worm their way through a network, appeared about 1987. To increase the power and flexibility of products like Word and Excel, Microsoft provided ways of writing programs, called macros, and inserting them into Word and Excel files. “I love you” and similar bugs are the inevitable result. What’s surprising about “I love you” is how unsophisticated it is – no talent was required to create it. Still, one Rockland business lost over 4000 files to it.

Sophisticated or not, what should you do to protect your computers from viruses, worms and network hackers? There are two kinds of threat, requiring two different defenses.

To defend against worms and viruses you’ll need to install an antivirus program like Norton, McAfee or Trend Micro and keep it updated. Alas, the nature of an antivirus program requires it to monitor the computer closely, possibly causing conflicts with other programs. If your computer gets indigestion, try a different antivirus product.

Fast, always-on Internet connections like DSL and cable unfortunately create openings through which hackers anywhere in the world can penetrate unprotected computers and steal or damage data. To defend against such attacks you’ll need a firewall, hardware or software that detects and stops unauthorized access to your network.

Ah, the wonders of technology!

This column by Denis Williamson of MacLamor Computer Consulting aims to help readers maximize the value of information technology. You can reach Denis at 845-357-1877 or denis@maclamor.com

