

Inoculating Your Computer

BY LAURA R. ARONSON

The flu isn't the only virus you should be worried about. While people may fastidiously wash their hands, glom on hand sanitizer and cough into their arm to guard against the flu, many aren't as proactive in guarding their computers against infections. Your Internet-connected computers operate in a rapidly changing, hazardous environment with new viruses and other risks cropping up every day. In fact, IT security groups scramble to identify "day zero" infections and issue protection within hours. (To see current listings, go to Sunbelt Security or Symantec on the Web.)

Viruses and other computer infections—or malware—are a vehicle for organized Internet crime. You can assume that a sizable percentage of your customers' computers are infected and should take precautions to protect your computers and data with systems designed to spot fraudulent activities associated with advanced malware operating on customers' computers. In March 2010, Symantec Corporation named Shaoxing, China, as the world's malware capital though other virus hubs include Europe, Russia, and elsewhere in Asia.

Securing Your Data

No computer network can be 100 percent protected from threats, but with a multi-layered approach, you can reduce your company's risk of attack. This is like placing a defense barricade at every possible entry point onto your network.

- Filter all incoming e-mail through a cloud-based (Internet) anti-spam service that detects and quarantines infected messages outside your network. More than 10 percent of spam is infected.

- Protect the network with a firewall appliance to keep out hackers, filter incoming traffic, and control user access to the Internet, blocking access to Web sites that are sources of infection.

- Install antivirus software on all servers, PCs, and networked laptops. Always pay the renewal fee promptly and make sure the software is updated every night because it cannot detect new viruses without an update. There are many software options, with widely varying reputations. Ask your IT consultant for their recommendation.

A complete multi-layered security approach includes offsite backup, complex passwords, encrypted laptops, security for your wireless network, and a virtual private network (VPN) for connections from offsite employees or branch offices. While these measures don't directly prevent viruses, you need them to protect your data. If your anti-



virus software predates 2008, replace it with a new program. Never run two antivirus programs at the same time, because this causes more problems than it solves. Always buy antivirus software from a trusted IT consultant or directly from the vendor, and never succumb to pop-up ads on the Web. These are not legitimate and will part you from your money while doing no good.

Educating Your Staff

Your staff can do a lot to prevent computer infections. Enact an acceptable user policy (AUP) that clearly states rules for employees using your computers and data. You may reinforce it with employee training and enact penalties for infractions. You do not want employees copying company data to USBs or downloading infected files. Among the rules your company should consider are:

- Do not open e-mail attachments you aren't expecting. Verify with the sender. This includes Grandma's jokes.

- Update your PDF reader (from Adobe) and your Java reader. If you have any doubt about the validity of a notice that pops up telling you to update your software, close it and go directly to the manufacturer's Web site for your update.

- Be cautious about inserting CDs, DVDs, or USB drives. Always know their source.

- Only perform file transfers from trusted sources.

- Do not download or install software that isn't authorized by management or your IT administrator. It may be a "Trojan horse" carrying a dangerous payload.

- Be selective about attaching your laptop to a public Wi-Fi. Files you transfer or keywords you type may be intercepted.

Cleaning Up an Infected System

If, despite your best efforts, something unusual happens, disconnect the computer from the network and consider it infected. Signs of an infected system include erratic or slow performance, pop-up ads, notices saying your computer is infected and asking you to buy antivirus software, and other odd behavior. Always restart your system to see if that clears up the problem. If not, then you may be able to clear up the infection by running a program, such as VIPRE PC Rescue in safe mode, which is available on the Web from Sunbelt Software under the Support tab.

If you receive and open a suspicious message from someone you know, it may be caused by a worm in their e-mail software that can make your e-mail broadcast to all the people in your address book. Call them and tell them not to open the messages or attachments, as that is the only effective way to stop the spread. The next step is to have a professional IT consultant remove the infection. The longer you wait to clean up an infected computer, the worse it gets. ■

Laura R. Aronson is principal of MLANS, an IT consultancy firm based in Londonderry. For more information on this topic, visit www.mlans.com. or call 877-287-0081.

