10 ways to avoid viruses and spyware

By Erik Eckel

Oh, the deck is stacked. Don't think for a minute it's not. As a technology professional responsible for securing office networks, workstations, and servers from viruses, spyware, adware, Trojans, and other malware infections, I can tell you that the situation is only getting worse.

A Computer Economics report showed that annual worldwide malware expenses increased by $10 billion (to $13 billion) over a recent 10-year span. Google Research suggests that one in every 10 Web sites is infected with "drive-by" malware. In June 2009, the Windows Secrets e-newsletter reported that such seemingly safe Web sites as Coldwell Banker.com, Variety.com, and even Tennis.com were exposing Internet Explorer visitors to the Gumblar exploit, which threatens to compromise visitors' systems in order to propagate.

IT professionals must encourage their users to follow several security practices to minimize virus, spyware, and malware exposure. But many computer techs are too busy to spread the word, or they don't have the time to build an appropriate memo or handout.

With that in mind, here's a handy reference list of 10 steps end users can adopt to avoid infection (including when using home systems to read and send work e-mail, create, edit, and distribute documents and spreadsheets, access the corporate VPN, and perform other office tasks). Post this list on your Intranet, distribute it in an e-mail, or print it out and pass it along to end users. Just be sure the word gets out. Otherwise, you're likely to find yourself losing precious time cleaning and repairing infected systems or entire networks.

1 Install quality antivirus

Many computer users believe free antivirus applications, such as those included with an Internet service provider's bundled service offering, are sufficient to protect a computer from virus or spyware infection. However, such free anti-malware programs typically don't provide adequate protection from the ever-growing list of threats.

Instead, all Windows users should install professional, business-grade antivirus software on their PCs. Pro-grade antivirus programs update more frequently throughout the day (thereby providing timely protection against fast-emerging vulnerabilities), protect against a wider range of threats (such as rootkits), and enable additional protective features (such as custom scans).

2 Install real-time anti-spyware protection

Many computer users mistakenly believe that a single antivirus program with integrated spyware protection provides sufficient safeguards from adware and spyware. Others think free anti-spyware applications, combined with an antivirus utility, deliver capable protection from the skyrocketing number of spyware threats.

Unfortunately, that's just not the case. Most free anti-spyware programs do not provide real-time, or active, protection from adware, Trojan, and other spyware infections. While many free programs can detect spyware threats once they've infected a system, typically professional (or fully paid and licensed) anti-spyware programs are required to prevent infections and fully remove those infections already present.

3 Keep anti-malware applications current

Antivirus and anti-spyware programs require regular signature and database updates. Without these critical updates, anti-malware programs are unable to protect PCs from the latest threats.

In early 2009, antivirus provider AVG released statistics revealing that a lot of serious computer threats are secretive and fast-moving. Many of these infections are short-lived, but they're estimated to infect as many as 100,000 to 300,000 new Web sites a day.

Computer users must keep their antivirus and anti-spyware applications up to date. All Windows users must take measures to prevent license expiration, thereby ensuring that their anti-malware programs stay current and continue providing protection against the most recent threats. Those threats now spread with alarming speed, thanks to the popularity of such social media sites as Twitter, Facebook, and My Space.

4   Perform daily scans

Occasionally, virus and spyware threats escape a system's active protective engines and infect a system. The sheer number and volume of potential and new threats make it inevitable that particularly inventive infections will outsmart security software. In other cases, users may inadvertently instruct anti-malware software to allow a virus or spyware program to run.

Regardless of the infection source, enabling complete, daily scans of a system's entire hard drive adds another layer of protection. These daily scans can be invaluable in detecting, isolating, and removing infections that initially escape security software's attention.

5   Disable autorun

Many viruses work by attaching themselves to a drive and automatically installing themselves on any other media connected to the system. As a result, connecting any network drives, external hard disks, or even thumb drives to a system can result in the automatic propagation of such threats.

Computer users can disable the Windows autorun feature by following Microsoft's recommendations, which differ by operating system. Microsoft Knowledge Base articles 967715 and 967940 are frequently referenced for this purpose.

6   Disable image previews in Outlook

Simply receiving an infected Outlook e-mail message, one in which graphics code is used to enable the virus' execution, can result in a virus infection. Prevent against automatic infection by disabling image previews in Outlook.

By default, newer versions of Microsoft Outlook do not automatically display images. But if you or another user has changed the default security settings, you can switch them back (using Outlook 2007) by going to Tools | Trust Center, highlighting the Automatic Download option, and selecting Don't Download Pictures Automatically In HTML E-Mail Messages Or RSS.

7   Don't click on email links or attachments

It's a mantra most every Windows user has heard repeatedly: Don't click on email links or attachments. Yet users frequently fail to heed the warning.

Whether distracted, trustful of friends or colleagues they know, or simply fooled by a crafty email message, many users forget to be wary of links and attachments included within email messages, regardless of the source. Simply clicking on an email link or attachment can, within minutes, corrupt Windows, infect other machines, and destroy critical data.

Users should never click on email attachments without at least first scanning them for viruses using a business-class anti-malware application. As for clicking on links, users should access Web sites by opening a browser and manually navigating to the sites in question.

8   Surf smart

Many business-class anti-malware applications include browser plug-ins that help protect against drive-by infections, phishing attacks (in which pages purport to serve one function when in fact they try to steal personal, financial, or other sensitive information), and similar exploits. Still others provide "link protection," in which Web links are checked against databases of known-bad pages.

Whenever possible, these preventive features should be deployed and enabled. Unless the plug-ins interfere with normal Web browsing, users should leave them enabled. The same is true for automatic pop-up blockers, such as are included in Internet Explorer 8, Google's toolbar, and other popular browser toolbars.

Regardless, users should never enter user account, personal, financial, or other sensitive information on any Web page at which they haven't manually arrived. They should instead open a Web browser, enter the address of the page they need to reach, and enter their information that way, instead of clicking on a hyperlink and assuming the link has directed them to the proper URL. Hyperlinks contained within an e-mail message often redirect users to fraudulent, fake, or unauthorized Web sites. By entering Web addresses manually, users can help ensure that they arrive at the actual page they intend.

But even manual entry isn't foolproof. Hence the justification for step 10: Deploy DNS protection. More on that in a moment.

9 Use a hardware-based firewall

Technology professionals and others argue the benefits of software- versus hardware-based firewalls. Often, users encounter trouble trying to share printers, access network resources, and perform other tasks when deploying third-party software-based firewalls. As a result, I've seen many cases where firewalls have simply been disabled altogether.

But a reliable firewall is indispensable, as it protects computers from a wide variety of exploits, malicious network traffic, viruses, worms, and other vulnerabilities. Unfortunately, by itself, the software-based firewall included with Windows isn't sufficient to protect systems from the myriad robotic attacks affecting all Internet-connected systems. For this reason, all PCs connected to the Internet should be secured behind a capable hardware-based firewall.

10 Deploy DNS protection

Internet access introduces a wide variety of security risks. Among the most disconcerting may be drive-by infections, in which users only need to visit a compromised Web page to infect their own PCs (and potentially begin infecting those of customers, colleagues, and other staff).

Another worry is Web sites that distribute infected programs, applications, and Trojan files. Still another threat exists in the form of poisoned DNS attacks, whereby a compromised DNS server directs you to an unauthorized Web server. These compromised DNS servers are typically your ISP's systems, which usually translate friendly URLs such as yahoo.com to numeric IP addresses like 69.147.114.224.

Users can protect themselves from all these threats by changing the way their computers process DNS services. While a computer professional may be required to implement the switch, OpenDNS offers free DNS services to protect users against common phishing, spyware, and other Web-based hazards.

Additional resources

- TechRepublic's Downloads RSS Feed **XML**
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our IT Leadership Newsletter
- Check out all of TechRepublic's free newsletters
- 10 Faces of Computer Malware
- 10 things to look for in an anti-spyware application
- 10+ things you should know about rootkits

Version history

Version: 1.0
Published: June 19, 2009

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Content Team