Understanding—and Protecting Yourself from——Viruses and Spyware

When spyware and viruses frolic about your PC, performance grinds to a halt, and annoying pop-ups make attempts at working impossible. This phenomenon affects mostly Microsoft Windows users—Linux and MacOS are relatively safe from these attacks, mostly because the desktop share favors Windows making it a more satisfying target for hackers.

Understanding the Culprits

First, a few lessons are in order about the differences between these maladies. They do different things to your PC, they arrive differently, and their removal requires different actions on your part.

Viruses are malignant computer programs that tend to have destructive behavior. They may delete files, create files, or cause the system to crash. Usually these are downloaded as attachments to email with innocent looking names, such as a greeting card or holiday screensaver, and are often supposedly sent by a friend. Viruses tend to propagate themselves to other systems by email (they like to send themselves to everyone in your address book) but put someone else's name in the "From:" slot, usually a random name from your address book.

For instance, if you get a virus on your PC, and list Don and Sandy in your address book, the virus might mail itself from your PC to Don but say it is from Sandy. (This is perfectly legal in email protocols which don't care about the authenticity of the sender information.) So Don gets the virus and calls up Sandy to complain when it actually came from you! Don't bother looking in your outbox for clues either—viruses of this type usually include their own mailing engine embedded in the program.

Spyware is less destructive, but very annoying. Downloaded to your PC by clicking somewhere on a webpage, spyware attempts to "spy" on you and collect information such as the sites you go to. It sends this marketing information to the mothership, which then instructs the spyware to cause pop-ups of that advertising genre to fill your screen. The worst class of spyware includes browser "hijackers." These take you to their own malicious site first, take note of where you wanted to go, then forward you on. In the meantime, you get lots of pop-ups.

More proactive spyware attracts more of its own ilk, as if to broadcast, "Hey, we've got an open PC here!" and suddenly more and more spyware gets downloaded—often by itself.

Best Defense

First and foremost, make sure you are up-to-date on your Windows Update downloads. As holes in the operating system are found, they are plugged. It is especially important to keep Internet Explorer up to the latest revision (which keeps Outlook Express updated) and Outlook too, if you use that instead. Internet Explorer now has its own pop-up blocker that works well. If the Windows operating system is equally updated, many of the holes will be plugged that allowed spyware and viruses to propagate to systems always connected to the internet (take note all you DSL and cable modem customers).

Since most of the nasty stuff comes in through email, just watch what you open. Don't use the Preview Pane in Outlook and Outlook Express because that automatically opens the email for you. Using an email virus scanner that comes with part of Norton, McAfee, or Grisoft's free AVG offering is a good way to catch those you don't see.

As for spyware downloaded from web pages, some feel that using Mozilla's Firefox browser is a better and safer alternative to Internet Explorer. But here again, watch what you click on. Many spoof pop-ups look like Microsoft Windows messages. They may look authoritative and warn "Spyware has been located on your system—click here to remove!" but if you look very closely, in the corner in almost the same color as the background it says "Advertisement." And if you click on it, you've just told Windows, "Yes—ignore the security I've set up. I want to download whatever it is they are offering!"

Best Offense

Once spyware and viruses get onto your system, you have to go on the offensive and root them out. Running a complete virus scan in Windows Safe Mode (a minimal version of Windows before any viruses or other programs start up) will usually clean them out, so long as your virus database is updated. But really tough ones, like weeds, need to be pulled out manually with virus removal tools, sometimes by editing the System Registry. Virus Removal tools that are downloaded from the major anti-virus vendor websites are meant for specific, hard-to-clean viruses. These are especially useful for viruses which actively prevent anti-virus programs from running!

Spyware removal is done with free tools such as Ad-Aware (which concentrates on removing things that cause pop-ups) and Spy-Bot. Microsoft has just released Microsoft Anti-Spy which also does a great job of removing spyware. I personally run all three when needed because they each catch something slightly different. Beware: while it is safe to run multiple spyware removal tools in sequence, they may report each other as spyware. Also, never run multiple anti-virus programs at the same time, or even have them simultaneously installed because all kinds of problems can occur!

One last bit of advice we'll discuss in more detail in a future article: use a firewall, especially if you're directly connected to the internet at all times. You can either use the Windows Firewall that came with Service Pack 2, or one of the ones from the anti-virus vendors. Best is a hardware firewall that is incorporated in many of the routers you buy today from Netgear, D-Link, Linksys, Microsoft and Belkin to gain wireless network connectivity. These help screen out attacks while you're sleeping. And with today's aggressive spyware and virus activity, you can use every bit of help you can get.

Daniel K. Kehoe is president of Bigfoot Labs in Connecticut. He has over 27 years experience in the computer industry in technical and marketing roles, most recently with Compaq Computer Corporation.