STATUS: ARCHIVED (Depreciated)

Just a bit of caution will keep your PC and your personal data safe. Plus: How good is an anti-spyware tool marketed through spam?

Scott Spanbauer

From the August 2004 issue of PC World magazine

One phenomenon that has become quite obvious from the vast numbers of virus victims over the last year is that people click first and ask questions later. Maybe we're inspired by the false belief that firewalls, antivirus software, and anti-spyware programs protect us from all viruses, worms, and intrusive programs. But even the best of these shields can't always protect you from your biggest security threat: yourself.

Curiosity killed the cat, and sometimes it ropes us into launching viruses, gobbling spam, installing browser-disabling add-ons, or even forking over credit card numbers and passwords. You're probably smarter than that, but I'll bet you have a credulous friend or relative who needs a wake-up call. Here's what they--and you--can do to avoid the latest "social engineering" tricks.

Don't click e-mail attachments: Most viruses and worms arrive on your PC in the form of e-mail attachments. A few of them exploit security flaws in Windows or in your browser to launch automatically, but if you keep your programs updated, your chances of being infected via this route are slim to none.

Instead of exploiting software flaws, some of the worst recent viruses rely on recipients' tossing out common sense and launching a lethal e-mail attachment. Common executable--and therefore dangerous--file-name extensions include .bat, .com, .exe, .pif, .scr, and .vbs. To elude the dangerous-attachment filters built into most e-mail programs, virus authors may enclose their nasty code in a .zip or .rar archive file. The file may even be password-protected to foil antivirus programs that scan inside archives. And naturally, the author includes an image of the password in the message body for the convenience of the gullible.

Don't believe the return address: Though an e-mail message may claim it's from your bank, your ISP, or even your boss, that doesn't mean it is. Spammers and virus mailers generally spoof the from address field in their messages with a legitimate address that they've stolen. You may even have received spam from yourself as a result of this clever technique.

Of course, not all e-mail is bad. But if a message from a coworker or friend insists that you launch a file attachment, first confirm with the sender what the file is (make a call or send an e-mail asking whether the purported sender in fact e-mailed the file attachment, and whether it is indeed intended for you). If you have any doubts about the legitimacy of the message and its attachment, delete them.

Don't believe the message: To persuade you to launch a virus-laden mail attachment or provide your personal information, virus authors must earn your trust. They try to accomplish this by composing

convincing-looking messages that appear to be sent from Microsoft, your ISP, or some other entity you do business with. The message may even contain links to a counterfeit version of the company's Web site, complete with genuine-looking graphics and corporate logos.

Often the message laments that the company is experiencing technical problems, and that it needs you to click an executable attachment. You don't need to rely on your intuition to determine whether this message is truthful. If the message hasn't been verified by a company representative via phone or in person, it almost certainly contains a virus. Microsoft doesn't e-mail updates to its customers, and neither should your ISP.

Don't believe the link, either: A link in an e-mail message that claims to point to a Citibank Web site may not really go there. Devious phishing scams use the wonders of HTML to snooker you into uploading your Social Security number, PIN, credit card number, password, or other sensitive data to a scammer's Web site. A carefully crafted e-mail message purporting to be from your bank, PayPal, or some other institution (and often also containing links to the real company's Web site) warns that you must update your records there. The biggest tip-off should be this: Banks and ISPs don't lose your information and then send e-mail requests for you to reenter it online. Another tip-off is that the link text and the real underlying URL don't match. Always examine log-in Web pages and their URLs closely. If you do get hooked by creeps on a phishing expedition, notify your bank, ISP, or other institution immediately.

Don't download the browser code: You're browsing the Web via Microsoft's Internet Explorer when suddenly an official-looking dialog box pops up, asking if you want to download a browser plug-in. Why not? You do the same thing all the time when using Microsoft's Windows Update Web site. This one even has a digital. But if you want to avoid a flurry of pop-ups, undesirable toolbars, a home-page hijacking, or worse, don't do it. Certificates won't protect you from adware and other online annoyances borne by these ActiveX controls. If you're really unlucky, you could end up with the dreaded CoolWebSearch infestation.

Last September's *Internet Tips* column detailed how to avoid dangerous ActiveX controls. Here's the executive summary: Choose *Tools, Internet Options* , click the *Security* tab, select the *Internet* zone, and confirm that the 'Security level' slider is set to Medium or higher. At this setting, IE will ask you whether you want to accept ActiveX downloads, but it won't run them automatically. You should consider the controls as potentially hazardous as executable file attachments. Or switch to a Web browser such as Mozilla or Opera that doesn't support ActiveX controls. When you want to visit Windows Update, you can still launch IE manually.

Is Spammy Anti-Spyware Safe?

Among the deluge of spam messages pitching term life insurance, Viagra, and college degrees, you may have noticed another category--advertisements for free anti-spyware software.

If you're like me, you might wonder: Could an anti-spyware program hawked via spam be any good?

I decided to check out several programs whose names showed up either in my inbox's lunch-meat department or in a search engine's paid results section. All four--Noadware.net's Noadware 2, Enigma Software's SpyHunter, SwankSoft's SpyKiller, and ParetoLogic's XoftSpy--are widely available through dozens of Web sites, thanks to their makers' affiliate marketing programs.

Because these tools' creators rely on affiliate marketers (who in turn employ spam to sell products), I figured that some or all of these programs would contain adware. I tested all four, scanning the PC with the free Spybot Search & Destroy both before and after installation. To my surprise, Spybot found nothing objectionable in any of them.

That doesn't mean you should use them, however. All four downloads are time- and/or feature-limited trial versions of commercial anti-spyware tools, and a few of them employ scare tactics. For example, SpyKiller informed me that a cookie related to Microsoft's Passport log-in service was a severe danger. To remove this innocuous text file, I would have to pay SwankSoft a stiff $50 to register the product.

At least until *PC World* conducts more-extensive testing of these and other spyware catchers, I recommend that you stick with either Spybot Search & Destroy or Lavasoft's equally free Ad-aware 6.