

Tips N' Techniques

5 tips for spurning spyware and browser hijackers

By Kim Komando

I regularly get e-mails from readers and listeners who have lost control of their browsers. They usually go something like this:

"My Internet browser has been taken over by something. When I try to do a search on Google or MSN, some other search program appears. I reset my home page, but somehow it always goes back to a pornography site. Please help me."

This person is the victim of a browser hijacker. The victim may have gone to a site that downloaded a program automatically. More likely, the victim downloaded a nasty program voluntarily.

These programs fall into the realm of "adware," or advertising-supported software, known more popularly as "spyware." At their most basic, spyware/adware programs feed you a bunch of ads. They often show up as pop-ups on your computer. Sometimes they are ads on Web pages.

Different companies use the terms "spyware" and "adware" differently. So, to avoid confusion, I use them synonymously. I consider any program that feeds you ads spyware/adware.

Some people use the term "spyware" to describe spying programs, such as keyloggers. They are a problem, but have nothing to do with advertising. So I am not including them in this column.

Here are five things to know and do when it comes to hassling with spyware/adware.

1. Watch what you download!

The absolute worst are the browser and search-engine hijackers. They're intrusive and often difficult to delete. Sometimes, people actually wipe their hard drives clean and start over again just to get rid of them. Some are aimed at children, who may be more credulous than their parents.

Occasionally, these programs arrive via a drive-by download. If you get one this way, you know two things: You're hanging out at the wrong places, and your copy of Windows needs to be updated.

A flaw was discovered in Internet Explorer in 2003 that allowed such hijackings. Microsoft has patched the flaw. But many people have failed to update their machines.

However, most of these programs are downloaded intentionally. When you're surfing, you may see a message asking if you would like to download a special search engine or other supposedly helpful program, or change your home page. Smart computer users always say *no*. If you are uncertain of the program, *do not* download it!

Typically, these programs are geared to feed you advertising. When you attempt to go to Google for a search, for instance, these programs will redirect your browser to another site. You might get a search function, but it will be lame. And you can count on getting plenty of advertising.

2. Beware of freeware programs; many come with a cost.

The Internet has a great tradition of free software. Over the years, there have been many wonderful free programs offered. However, the authors of such programs often find themselves making a living doing them. Therefore, they need an income. Big advertising services companies offer them a deal. Include our program with your download, and we'll pay you. Usually, the presence of the spyware/adware is included in the user agreement for the freeware. Unfortunately, few people read those agreements. Besides, sometimes it's not clear. And sometimes, it just isn't there. "A majority of the time, it gets on the system without the knowledge of the user," says Bryson Gordon, a senior manager at McAfee Security.

These piggybackers fall into two categories. Some arrive with advertising, which they feed to you. They may be pop-ups, or they may be ads that appear on Web pages.

The more nefarious programs track your surfing. For instance, if you visit kayaking sites, they will note that. Then they feed that information to a computer on the Internet. First thing you know, your Web pages have kayaking ads on them. Or you start getting pop-ups offering kayaking equipment.

KARABOWICZ & ASSOCIATES

1215 Paramount Pkwy
Batavia, IL 60510
630-879-1360
www.karanet.com

Tips N' Techniques

3. Know good cookies from bad cookies.

These little text files have a bad reputation. But much of that is based on ignorance. Cookies actually perform valuable services. For instance, they can shoot you right into a site so you don't have to enter your password.

Here's how cookies work: Say you visit the ABC Book Co. You buy a book. The company downloads a text file to your computer, which includes an ID number. That's a cookie.

Two weeks later, you go back to the ABC Books site. First thing, your browser checks for an ABC cookie. It finds it, and sends it to ABC's computer.

When the ABC site opens, it says "Welcome back, Joe!" How does it know? The ABC Book Co. has the information about the sale two weeks ago in its database. It matches the ID number in the cookie to the sale information, and customizes the page for you.

When you next make a purchase, you won't have to enter your credit-card number or address. That will already be filled in. Again, that came from the database, and was enabled by the cookie.

That is all very convenient. But there are less desirable cookies, too. They're called tracking cookies. Say you visit the XYZ Brain Surgery site. There's a banner ad there. It is linked to an advertising services company. It downloads a cookie. The cookie says, "This person visited XYZ Brain Surgery."

Next, you go to a heart transplant site. The banner ad there is associated with the same advertising company. The browser sends the cookie to the banner ad. The ad adds a notation that you visited the heart transplant site.

Over time, the tracking cookie builds a profile of your interests. The advertising services company sells this information. That's why you start getting advertising for medical equipment.

4. Warning: The Web bugs are watching.

When you visit a site, you may be watched by a Web bug. This is a tiny graphic, measuring one pixel by one pixel. It sends information to another computer.

Included will be your IP number and the main address of the Web site you visited. That Web site can use the Web bug to transmit other information ? your e-mail address, for instance ? to the Web bug's mother computer.

Why would that site send your e-mail address? Money.

"Everybody starts out with innocent intent, but it is all driven by the profit motive," says Roger Thompson, vice president of development at PestPatrol, which publishes computer security software.

As you surf, Web bugs from advertising companies pop up on other sites. Each advertising company uses this information to build a profile. The result? More advertising. Sigh.

5. Beef up your security.

What other actions can you take? First, use common sense. If a site offers to download a program, refuse. If it asks to be your home page, say no. And keep Windows updated. You can set more recent versions of Windows to do that automatically. Or open Internet Explorer. Click Tools and Windows Update. Follow the prompts.

If you do those things, you will avoid the hijackers. The tracking tools, though intrusive and irritating, are less dangerous. Much of this stuff can be stopped with security programs. McAfee and PestPatrol have well-regarded programs. I like SpywareBlaster, which is free.

If you block the spyware/adware programs that come with freeware, the program that you did want may not work. In that case, you may want to leave the spyware/adware running. At least, you'll know it is there.

You can remove spyware/adware that is already on your computer. Try Ad-aware or Spybot Search and Destroy. I have links to these and many other security software programs, most of them free, on my site (www.komando.com/bestshareware.asp).

Kim Komando is the host of the nation's largest talk-radio show about computers and the Internet. She also writes a weekly column for more than 100 newspapers and a Q&A column for USA Today.

Source:

http://www.microsoft.com/smallbusiness/issues/marketing/privacy_spam/5_tips_for_spurning_spyware_and_browser_hijackers.msp

KARABOWICZ & ASSOCIATES

1215 Paramount Pkwy
Batavia, IL 60510
630-879-1360
www.karanet.com