

# Computers

## Spies, Lies, and Staying Safe Online

by Joe Stoddard

If you've ever wondered why you're bombarded with pop-up ads every time you go online, no matter what website you visit; or why you're suddenly getting dozens of unsolicited e-mails about things you wouldn't want your kids to even *know* about, let alone see on your computer; or why your brand-new computer is running slower than the old one you handed down to Junior, the answer could be "spyware," or in more polite circles, "adware."

Spyware makes use of an existing "back door" (or "backchannel") on your computer, allowing marketers, software companies, and hackers to look over your shoulder whenever you're connected to the Internet. That's bad enough, but think about the sensitive project data you have stored on that computer. Names, addresses, credit card numbers, mortgage qualifications, private correspondence. You owe it to your clients, subs, and suppliers to do what you can to protect their privacy and security, as well as your own.

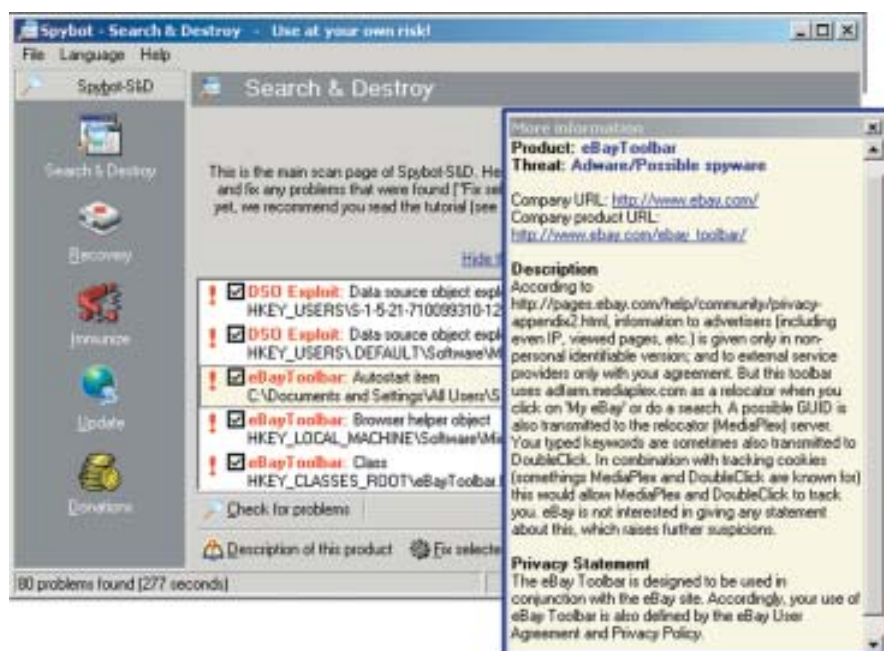
Internet security guru Steve Gibson at Gibson Research Corporation ([www.grc.com](http://www.grc.com)) defines spyware as "*any software...*" (scripts, web pages, programs, text messages, e-mail, etc.) "...that employs a user's Internet connection in the background (the so-called backchannel) without their knowledge or explicit permission. Silent background use of an Internet backchannel connection *must be preceded* by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed, consent for such use. *Any software* communicating across the Internet absent these elements is guilty of information theft and is properly and rightfully termed spyware."

So whether we're talking about a

teenage hacker in Thailand trying to steal credit card numbers from your accounting system, or a well-respected power tool retailer here in the states serving pop-up ads to your web

browser, there is a common theme: Someone is messing with your computer behind your back, probably without your knowledge.

I'd say without your knowledge or



Spy-Bot Search and Destroy (top) is arguably the most effective way to control spyware, but use it with caution. If you're not comfortable manipulating system files, Ad-aware (bottom) might be the better choice.

consent, but in many cases you have probably unknowingly given the thumbs-up. Spyware, and what a company is going to do with the information gathered from spyware, is often spelled out in the license agreement or terms of service that nobody reads before clicking “I Agree.”

### Spy vs. Spy

**S**pyware exists in many forms, some more dangerous than others. Here are a few of the more common categories.

**Ad trackers.** A common feature of banner-supported “freeware” and a common part of “interactive” websites, ad trackers try to track how often a given ad has been viewed or “clicked on” and by whom. They can be simple counters registering that you’ve visited a site, or complex “e-pending” (e-mail appending) schemes, database programs that correlate your personal data (say from a web sign-up form) to exactly which ads you’ve viewed. That way, the ad agency can send you more of the same — maybe as annoying pop-ups that appear out of nowhere, no matter what website you’ve visited.

**Keyloggers.** Keyloggers are programs that download automatically from a rogue website you may happen across, or are installed from an e-mail worm. They run in the background, recording every keystroke and mouse-click to a log file. The log file is tucked away in a hidden directory on your computer where someone in a remote location can analyze it whenever you’re online. Evildoers use keyloggers to find credit card numbers, passwords, and other sensitive information. Service or salespeople gathering

### Spy-ers

You can pick up spyware from a website you visit. You can get it up from a link or attachment you click in an e-mail message, or it could be built into the regular applications you’re using. There are even holes in the Windows operating system that Internet mar-

credit card numbers and customer information on a hand-held or laptop should be especially careful of keyloggers. (Note that if you want to spy on your employees or kids, there is a “legitimate” class of keyloggers sold as commercial software to monitor how people use their computers.)

**Usage trackers.** Trackers are used to collect data on your use of a specific program or website function — for instance, which music files you’ve downloaded with a file-sharing program like KaZaa, or how many times you’ve fired up that shareware file compression utility on a particular computer. Aside from slowing down your Internet connection, usage trackers can be used maliciously to expose all the information on your hard drive.

**Hijackers.** If you’ve ever had “Bonzo Buddy” show up unannounced, tried to get rid of “Gator,” or had your home page changed to something you didn’t want and couldn’t change back, you’re familiar with Hijackers. These programs take control of different aspects of your computer and can actually make changes to your Windows system files, making it impossible for you to put things back the way they were without reinstalling software from scratch. If you used to have a feature that worked a certain way, but now it doesn’t — suspect a Hijacker.

keters are now exploiting to send you pop-ups. And, if you’ve ever downloaded a piece of “free” software that displayed an ad banner, you’ve probably installed some spyware, which often remains on your computer even after you upgrade to the “paid” version.

And it doesn’t end with “freeware.” Demo versions of commercial software often have a spyware component so the developer can bug you to register. And many programs popular with contractors, including QuickBooks Pro and Adobe Acrobat, come with an Internet-connected “auto update” service that could potentially be abused as spyware as well.

### Liars

Software developers will always point to their “privacy statements” to protect you, but don’t count on it. History has proven that if a software company is forced to sell its assets (a common occurrence), there is no guarantee the new owner will be able or willing to honor the old agreements. Remember the Internet bust a couple of years ago? Some online project management products were forced by the bankruptcy court to liquidate their client lists to raise cash — a direct violation of their stated privacy policy. As a result, thousands of names in contractors’ associations along with their lists of subcontractors and suppliers were up for grabs.

Another growing problem is that legitimate software products and web services are increasingly becoming the target of organized attacks. A legit feature — say the harmless pop-up that lets you know there’s a new version of your software available — could conceivably be transformed into credit-card stealing spyware if it fell into the wrong hands. High-end security at data centers is expensive. Developing security updates is expensive. Well-established software companies like

Intuit spend a king's ransom every year to respond to security threats and keep their users' data safe, but what about smaller companies? Many of the web-based applications contractors would be interested in are poorly funded upstarts with tiny user bases. You can't always count on them to have the necessary resources available, which is why it's up to you to protect yourself.

### Fighting Back


Today, the only way to completely prevent an encounter with spyware and other security breaches would be to permanently unplug your computer from the Internet. Since that's not an option for most of us, taking control of your privacy and security when online requires a multi-pronged approach.

**Routers and firewalls.** Even if you have only one computer, a NAT router

(see *Computers*, 2/03) will keep you hidden from prying eyes on the Internet and should be part of every contractor's office. But a router by itself won't do much to control spyware because it isn't smart enough to manage outgoing connections and can't alert you when something bad is happening. For that, you need a true firewall. While a dedicated hardware firewall like the SonicWall SOHO 3 ([www.sonicwall.com](http://www.sonicwall.com)) is arguably the best fix, at around \$500, it's not cheap. Personal firewall software like the free version of ZoneAlarm ([www.zonealarm.com](http://www.zonealarm.com)) is just as effective, and the price is right.

**Anti-virus programs.** Computer worms and viruses aren't spyware per se, but they're related. A "Trojan horse" delivered by e-mail could be the mechanism that hijacks a legitimate Internet service. For swatting these bugs, I like AVG Anti-Virus ([www.grisoft.com](http://www.grisoft.com)) because it's free for

personal use, updates itself automatically in the background, and, unlike some of the commercial products on the market (Norton, McAfee), always seems to play nice with other programs you may have installed.

**Anti-spyware.** I recommend two anti-spyware products: Ad-aware ([www.lavasoftusa.com](http://www.lavasoftusa.com)) is the easiest to use and is free, but it won't always eliminate the most devious spyware. SpyBot Search and Destroy ([www.safer-net-working.org](http://www.safer-net-working.org)) — free, donations welcomed — will root out just about everything Ad-aware misses, but requires more in-depth knowledge of your computer to avoid zapping things you might want to keep. 

---

**Joe Stoddard** is a technology consultant to the building industry and a contributing editor at The Journal of Light Construction. You can reach him at [jstoddard@mountainconsulting.com](mailto:jstoddard@mountainconsulting.com).