How's this for a one-two punch -- software that secretly alters your Google search results, then tries to drop nasty programs on your computer by luring you to a bogus eBay link?

That appears to be what is happening with a new program documented by security software vendor Webroot Software Inc. Called 2search, the program secretly hijacks some Google searches by presenting fake results in the midst of legitimate ones. Because the pages shown look identical to regular Google results, most victims would have no clue anything is amiss.

As if that weren't enough, one of the fake results Webroot researchers recently saw seemed to be leading to product auctions on eBay. Webroot researchers could not say who was behind the eBay links, but they suspected what they were offering was more "spyware" -- a general term for software installed on computers without the owner's knowledge.

So why would the creators of spy software be lurking in the shadows of Google and eBay?

"If you had a Web site that said, "'Hey, get your spyware here,' no one would go to it," said Paul Piccard, Webroot's director of threat research. "So they look for ways to confuse or fool the user and make sure they are willing to download the spyware."

Spy software is going mainstream as it becomes big business, generating about $2.4 billion in annual revenue, according to a report issued last week by Webroot. Eager to make money by installing advertising and spy programs on more computers, the purveyors are using clever new tactics, such as pretending to be a Yahoo page or a music file from iTunes.

Webroot said spy programs are growing more sophisticated, harder to detect and more financially motivated. Since the start of the year, the number of Internet sites pushing unwanted software onto computers has quadrupled to 300,000. Webroot also found a sharp increase in such programs on corporate computers -- up 19 percent in the second quarter. The United States is still the leading host; nearly half of all spy software originates here, the report said. Yet the rest of the world combined now provides more, with Poland the second biggest host and the Netherlands third.

Often visitors get infected by what's known as a "drive-by download" -- the act of calling up a particular Web site secretly drops a program on their computer.

The programs range widely on the danger scale, starting with simple "cookie" files used by commercial Web sites to recognize repeat visitors and tailor ads and pages. More annoying are programs dubbed "adware" because they pop up unwanted ads and sometimes secretly track a user's Web surfing to decide which ads to show. More sinister are "system monitors" that track everything a computer user does and secretly send
reports over the Internet. Often those are used for crimes ranging from financial theft to extortion and espionage.

Webroot chief executive C. David Moll dropped by my office last week and offered a chilling account of a particularly nefarious variant -- "keyloggers," so-called because they invisibly log every keystroke a user makes and transmit that information back to their authors.

They've been around for years but are more widespread now and easier to install from a distance.

"What's new is you don't have to be a sophisticated technician to remotely install it," Moll said as he described off-the-shelf programs offered for sale online, including one marketed by an outfit named NetHunter.

If such standardized programs aren't to your liking, a group of Russian programmers called Rat Systems will take your order at their site and write a custom spy program for about $600, Moll said. While spy software has legitimate uses such as defending a corporate network, Moll said it increasingly is being used for electronic robbery.

As he talked, I imagined bank robbers selling point-and-click heist tools, or professional embezzlers selling custom scripts that siphon money from employers -- "Embezzling for Dummies" Web sites.

After he left, I went online to visit the sites of companies he mentioned for a first-hand look at how point-and-click spy tools were advertised. The sites I visited stressed how hard their programs were to detect: "Totally stealth operation. Run invisibly & transparently," claimed one.

I was hoping the security software from Symantec Corp. that I run on my desktop computer -- both "firewall" and antivirus programs -- would protect me from getting any bad software dropped on my machine as I surfed.

Wrong.

The next morning, I used special scanning software to check my computer for hidden programs. I had run a similar scan the week before and found nothing malicious. But this time it not only found a bunch of uninvited ad programs, it also discovered a "Trojan horse," so-called because it looks benign but actually opens your computer for installation of other bad software.

There was no telling what that "Trojan" planned to do with the back door it had opened on my machine.

Trojans increasingly are being used in industrial espionage, as demonstrated in a case that grabbed headlines in May when Israeli police arrested more than 20 people, including private investigators and chief executives of large European companies. The executives are charged with hiring investigators to pilfer private documents from business rivals by sending Trojan files disguised as e-mails from trusted sources.

There is no solution on the horizon to this escalating threat of spy software. At least 10 states have passed anti-spyware legislation, and two federal bills have passed the House and are pending in the Senate. But laws alone cannot stop electronic thieves who increasingly operate from overseas and alter their files daily to elude detection.

As the magnitude of cyber-crime sinks in, some folks may start disconnecting from the Net. But I think
there are saner strategies, such as learning more about the latest threats and taking all precautions recommended by experts. For example, I not only run multiple security programs on my home computer and regularly scan it with spyware-detection programs from Webroot and other companies, I also no longer keep any sensitive files on computers connected to the Internet. It's more expensive to keep a separate offline computer, for sure, but I just don't believe there is such a thing as safe surfing.

Leslie Walker's e-mail address is walkerl@washpost.com.