

Phishing Sites Explode on the Web



Robert McMillan, PC World

Mon Feb 26, 4:00 AM ET

Think the new built-in phishing filters in Internet Explorer 7 and Firefox 2 will protect your private data? Think a number of sites devoted to phishing skyrocketed last year, and the number of Americans taken in by phishing nearly doubled. In November 2006, the last month for which data is available, the Anti-Phishing Working Group reported 1,463 new sites, up an astounding 709 percent from the 4630 sites in November of 2005. (Click on the "Image Enlarge" link above to see the chart showing this trend.)

Last October, both Mozilla and Microsoft released new versions of their browsers that use blacklists to block access to phishing sites. In response, resourceful phishers are flooding new fake Web sites onto the Internet too quickly to be shut down or blacklisted.

The alarming ease with which the fraudsters changed course, plus other new phishing tactics, makes some security experts say that phishers have the upper hand in the war against online fraud.

"Ultimately," warns Zulfikar Ramzan, who is a senior principal researcher with Symantec's Security Response Center, "technologies that rely heavily on blacklists are going to be useless."

Easy Phishing

According to RSA, a security vendor, hackers in January started selling a phishing kit that lets criminals set up fake Web sites with little effort. The fake site pulls images and layouts from the real site, usually a bank or other financial institution, and passes the user's information back to the real site to mimic a regular log-in--while keeping a copy of the data for the criminals.

The draw, of course, is ever-increasing profits. Research firm Gartner estimates that 3.5 million Americans gave up sensitive information to phishers in 2006, an 84 percent jump from the previous year--for a total loss of \$2.8 billion. One gang, called Rock Phish, is estimated to have taken in more than \$100 million.

According to security experts, Rock Phish has pioneered many of the techniques that have contributed to the rise of phishing sites. And the image spam that hides its pitch from filters by embedding it in a picture was a Rock Phish specialty, these experts say. On some days this one group, which specializes in spoofing U.S. and European financial institutions, account for as many as one-half of all the phishing sites in operation, according to researchers.

Heuristic scanning may help combat the scourge. Instead of depending on a blacklist of known phishing sites, security software can monitor a site's behavior, looking for techniques commonly used by phishers. IE 7 uses heuristics, as does the free SiteAdvisor add-on for IE and Firefox.

An emerging standard for a new type of site certification--called Extended Validation Secure Sockets Layer, or EV SSL, can also help. To get this certificate, sites will have to be checked out by third parties like VeriSign or Entrust to make sure they at least appear to be legitimate. On such sites, the browser address bar will turn green.

Microsoft supports EV SSL in its IE 7 browser, and major online-commerce sites such as PayPal have now started to display the EV SSL logo on their boards as well.

But if the current surge in phishing sites demonstrates anything, it's that phishers can and do get around automatic security procedures to protect their sizable profits. Recently they have been developing new technologies that could weaken current protection measures like EV SSL, according to Avivah Litan, a Gartner analyst.

Litan, who doubts EV SSL certificates will have much impact on phishing, believes security technology firms do the blame for the growing phishing threat.

"The security industry has been a little arrogant," she explains. "I don't think that people realize how sophisticated criminals are."

Best Defense

Although no magic bullet may exist now (or ever) to safeguard us all, there is one simple way to protect yourself from the majority of phishing attempts: Never click a link in an e-mail or on a third-party site to go to any of your financial institutions. Instead, you always use your own bookmark or type in the address, even when you're 100 percent certain that the site is legitimate, you should be safe.

Automated tools, such as the free Password Safe and PwdHashutilities can still provide help. But to combat even the most sophisticated phishers, your best protection remains...you.

Copyright © 2007 [PC World Communications, Inc.](#)

Copyright © 2007 Yahoo! Inc. All rights reserved.

[Questions or Comments](#)

[Privacy Policy](#) - [Terms of Service](#) - [Copyright/IP Policy](#) - [Ad Feedback](#)