

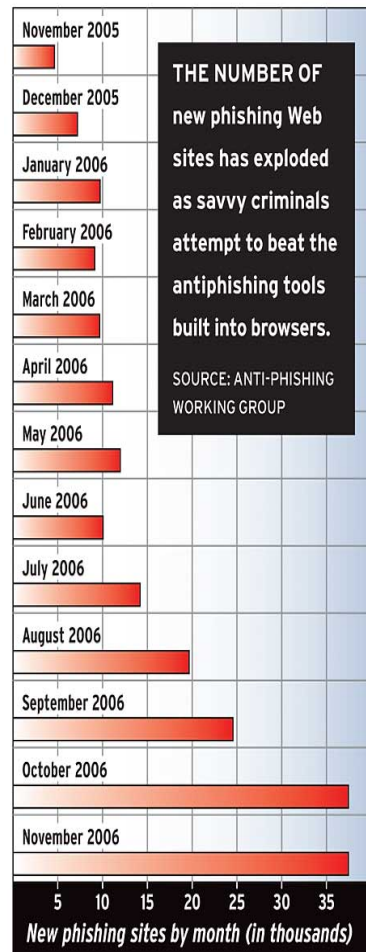
Phishing Sites Explode on the Web

PCWORLD

Online criminals are thriving even in the face of new automated defenses.

Robert McMillan, PC World

Think the new built-in phishing filters in Internet Explorer 7 and Firefox 2 will protect your private data? Think again. The number of sites devoted to phishing skyrocketed last year, and the number of Americans taken in by phishing schemes has nearly doubled. In November 2006, the last month for which data is available, the Anti-Phishing Working Group found 37,439 new sites, up an astounding 709 percent from the 4630 sites in November of 2005. (Click on the "Image Enlargement" icon 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 known phishing sites. In response, resourceful phishers are flooding new fake Web sites onto the Internet too quickly for them all 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 Group, "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 very convincing 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 account 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 single phishing 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 recent jump in phishing sites. And the image spam that hides its pitch from filters by embedding it in a picture was a Rock Phish invention, these experts say. On some days this one group, which specializes in spoofing U.S. and European financial institutions, may 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, it analyzes a site's behavior, looking for techniques commonly used by phishers. IE 7 uses heuristics, as does the free SiteAdvisor browser 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--may also help. To get this certificate, sites will have to be checked out by third parties like VeriSign or Entrust to make sure that 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 come on board as well.

But if the current surge in phishing sites demonstrates anything, it's that phishers can and do get around automated tools and procedures to protect their sizable profits. Recently they have been developing new technologies that could well thwart 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 deserve some of 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 these [online] 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 accounts. If, instead, you always use your own bookmark or type in the address, even when you're 100 percent certain that the e-mail is legitimate, you should be safe.

Monday, February 26, 2007 01:00 AM PST