McAfee

One Phish, Two Phish, Old Phish, New Phish

Phishing (fĭsh'ĭng) n. *A method of fraudulently obtaining personal information by sending spoofed emails that look like they come from trusted sources.*

Pharming (färm'ing) n. *A method of redirecting Internet traffic to a fake web site through domain spoofing.*

Whether you're a casual web surfer or immersed in a cyber lifestyle, all Internet users are under assault by phishing emails, pharming sites, and crimeware. Because cyber criminals use botnets—groups of hijacked PCs—to launch untraceable spam-based phishing attacks, the number of phishing and pharming schemes has grown immeasurably. Criminals are using blended or multifaceted attacks—which combine multiple crimeware techniques—to steal identities and hijack systems, often fooling even savvy users.

Financial services are by far the most targeted industry. Indeed, cyber prowlers frequently build fraudulent web sites that closely mimic legitimate banking and Wall Street sites, tricking users to turn over their online account names, passwords, Social Security numbers, and other personal information.

Phishing Tricks

When they set up a fake web site, phishers attract users through spam or targeted emails, hoping to get lucky and find real customers of the hijacked bank, e-retailer, or credit card company. The emails can be extremely convincing, such as a message from eBay saying that your credit card has been declined, or from Citibank saying that they have detected unauthorized activity on your account. The messages frequently feature logos, coloring schemes, and company mottos ("Avis: We Try Harder") that seem legitimate.

One example is a spam email that claimed to be from BBC News. It introduced a news story of interest, with a "Read more…" link to lead users to a fake BBC News site. The fraudulent site looked exactly like the real BBC News site's pages and carried real news stories copied from the BBC site. These fake web pages exploited the unpatched "Create Text Range" vulnerability in order to download and install a keylogger, which monitored users' activity on various financial web sites and sent the captured information back to the hacker.

Pharming Techniques

Pharming uses DNS (Domain Name Service) hijacking to misdirect users to a fake site by altering the DNS for the target web site. Or, the system redirects users to authentic web sites through phisher-controlled proxies that can be used to monitor and intercept keystrokes.

The spoofed sites collect credit card numbers, account names, passwords, and Social Security numbers. They do this by either displaying a popup to steal the information before sending the user to the real site, by using a self-signed certificate to fake authentication and get the user to trust it enough to enter personal data on the spoofed site, or by painting over the address and status bar of the browser to trick the user into thinking they are on the legitimate site so that they enter their information.

Crimeware—Deceptive Downloads

Phishers use tricks to install crimeware on consumers' computers to steal information directly. In most cases, you don't know you are infected, and only see a slight slowdown in computer performance, or notice blips in operation that they attribute to normal software glitches. Computer security software is a necessary tool to prevent crimeware from installing if you get caught in an attack.

In a deceptive download ploy, Trojan keyloggers and other spyware piggyback onto legitimate software, or the hacker can corrupt a legitimate site using bad scripts so that the software downloads secretly in the background when the user visits a site they trust. Phishers also use social engineering to persuade users to download the software from their site directly by convincing them that the software is something that they want, such as a screensaver or music download program.

Once the crimeware is installed, you are in trouble. It can cause the browser to launch spoofed sites, it can hijack the PC's host file to redirect the computer to spoofed sites, and it can use keystroke loggers and screen scrapers to record and send stolen data back to the hacker. Crimeware also installs rootkits that execute under the radar and hide the presence of the spyware, or can turn the PC into a remote-controlled bot ready to launch a massive spam campaign or Denial of Service (DoS) attack.

Phishing Trends

By all accounts, phishing attacks are on a steep rise. Tens of thousands of unique phishing cases surface each year, and these numbers are growing exponentially. New phishing sites are also seeing a similar growth trend, as well as password-stealing malicious code URLs. The United States hosts the most phishing sites, followed by China and the Republic of Korea.

Phishers are narrowing their focus and targeting attacks against large financial and e-commerce firms; for example, out of every hundred brands that are hijacked, approximately five account for 80 percent of all phishing campaigns. Also, as eBay and large financial institutions take more proactive measures to combat phishing, criminals are moving downstream to credit unions and other companies that might not be as technologically savvy. As people become smarter about phishing, attacks will be less like spam and, instead, take more advantage of targeted weaknesses.

Top 10 Ways to Defend Against Phishing

1. **Keep your operating system patched to avoid known software vulnerabilities from being exploited.** Install patches from software manufacturers as soon as they are distributed, since hackers can quickly assemble malware using pre-made components to exploit the vulnerability before the majority of people download the fix. A fully patched computer behind a firewall is the best defense against Trojan and spyware installation.

2. **Download the latest version of your browser to ensure that it is also fully updated and utilizes the latest technologies.** Internet Explorer 7 and other browsers include an anti-phishing toolbar to add another layer of protection.

3. **Check the domain name of the site as an indicator of whether the site is legitimate**. The origin of an email, the location of a page, and the use of SSL encryption can all be spoofed. Browser lock icons can also be spoofed. You should ensure SSL is being used (look for "https:" in the URL). Because of hacker tricks, though, you can't rely on these checks as an absolute indicator that the communication or site is safe.

4. **Never click on links in an unsolicited email, and ignore call-to-action emails such as "Your account will be terminated."** Call the company on the phone instead, using a phone number that you verify outside of the email.

5. **Be very careful when downloading any software from the web.** Spyware can piggyback onto legitimate software, or the software may contain keyloggers or screen scrapers that steal your information. You should completely avoid free screen savers and other freebies. Also be wary of opening an email attachment—a video, graphic, or PDF—even from someone you know. Virus-scanning software protects you by determining if viruses are hiding inside before you open the attachment.

6. **Use software that automatically checks to see whether a URL is legitimate before you are taken to the site.** Check out AccountGuard from eBay and ScamBlocker from EarthLink. You can also check the validity of individual web addresses (URLs) with a WHOIS search such as *www.DNSstuff.com*, which has a search tool that displays the contact information for a domain/IP based in almost any country.

7. **Use an Internet service provider (ISP) that implements strong anti-spam and anti-phishing technologies and policies.** For example, AOL blocks known phishing sites so that customers can't reach them. The SpamHaus organization (*www.spamhaus.org*) lists the current top-10 worst ISPs in this category—consider this when making your choice.

8. **Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.** If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

9. **Be an early adopter of new technologies.** New validation techniques are being used by banks and credit card companies to make online transactions more secure, so make sure to take advantage of them. The computer industry is also working on authentication technologies such as Sender ID, Domain Name, and S/MIME, which will greatly reduce the effectiveness of phishing attacks.

10. **Protect your computer with strong security software and make sure to keep it up to date.** Hackers have databases containing millions of email addresses. They target vulnerabilities in email applications and web browsers, and abuse design vulnerabilities in targeted web site programs. You can defend against phishing, though, because it blends existing techniques of spam and software exploitation.

    McAfee® Internet Security Suite guarantees trusted PC protection from viruses, hackers, and spyware. Its cutting-edge features include X-Ray for Windows®, which detects and kills rootkits and other malicious applications that hide from Windows and other anti-virus programs. Its integrated anti-virus, anti-spyware, firewall, anti-spam, anti-phishing, and backup technologies work together to combat today's sophisticated, blended attacks.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com