

A New Security Threat – Pharming

©2005 US Netizen

What is Pharming?

Pharming (pronounced farming) is a technique used by unsavory individuals and companies to obtain important personal and financial information without your knowledge. It is similar to Phishing, except the information is collected without you needing to click a link in an email. Even the most savvy are subject to pharming because it does not require you to make a mistake.

As with Phishing, the ultimate purpose is to separate you from your money.

How does Pharming Work?

Pharmers have two main ways of operating: directly on users' computers or on domain name servers that resolve Web site addresses for users.

Similar to phishing, Pharmers send e-mails to users requesting that account information needs to be updated. The difference from phishing is that the email contains a virus that installs small software programs on users' computers. When a user tries to go to the bank's real Web site, the program redirects the browser to the pharmer's fake site. It then asks a user to update information such as logons, PIN codes or other sensitive information. Savvy users that do not click on the links in the email are still subject to this attack because it uses a virus to direct the browser to the scammer's website.



The pharmers' second method takes advantage of the fact that Web sites have alphanumeric names but reside at numeric addresses on the Internet. When users type a Web site's name into their browsers, Domain Name System, or DNS, servers read the name, look up its numeric address and take users to the site.


Pharmers interfere with that process by changing the real site's numeric address to the fake site's numeric address within the DNS server.

This technique can only be stopped at the server and there is little that the end-user can do. Pharming is like planting seeds of malicious viruses. As users are later directed to the fake site, the pharmers harvest the sensitive information.

How to Avoid Pharming

The virus-based method of pharming is stopped by maintaining up-to-date antivirus, antispyware, and firewalls on your computer. This will greatly reduce the possibility that a virus will redirect you to the malicious web site.

Additionally, be careful when entering sensitive information on a website. Look for the lock  or key icon  at the bottom of the browser. If the site has changed since your last visit, be suspicious. When in doubt, do not use the website.

A list of popular financial sites that use a secure page for logins is maintained on pharming.org. They also have a shocking list of financial sites that use an unsecure login page. To use this type of site, do not enter your username and password on the unsecure login page. Instead, just click login and you should get an error on a secure page telling you that you forgot your username or password. Verify that the error page is secure  and log in from there.

Threat Assessment

It appears that the server-based portion of pharming affects only Windows servers at this point. The main method of altering the DNS records is through "DNS Poisoning" that is a known vulnerability on Windows servers. A patch is available for Windows NT4 and Windows 2000 servers. Windows 2003 servers are not vulnerable.