

Identity Theft and Pharming - A New Twist on an Old Theme

Article by: Michael Solomon

Identity theft is big business and, like it or not, the likelihood that you will become a victim is increasing. As the Internet and its popularity have grown, the number of unscrupulous operators out there has grown as well. There are so many scams and attack methods out there it is difficult to keep up with them.

One of the identity thief's more productive techniques is *phishing*. A phishing scam is one where an email message contains a link to a web site that asks for personal information. The scam uses *social engineering* to trick people to go to a web site they would not normally visit. A common scam is one in which an email that looks like it has come from a bank or credit card company asks you to "click on this link" to update your user information. There is generally a part of the email that tries to convey a sense of urgency to get you to "do it now". When you click on the link you are actually forwarded to a thief's web site that is designed to look like your bank or credit card company's web site. You are then asked to provide information, such as user id, password, and other identifying information. Identity thieves use this information to open or use credit accounts and steal money from unsuspecting consumers.

Phishing attacks are relatively easy to spot and avoid. Never follow links in email messages unless you know the link is valid. Compare the actual link address with the text you see. If you are expecting to go to PayPal.com, make sure the link really takes you there. You can view the hyperlink before you click on it by pointing your mouse cursor at the link. Most email clients and web browsers will show you what the actual address is before you click on it. If the address doesn't match the web site address you expected to see, don't click on the link. Likewise, NEVER provide any personal information from an unsolicited source. You will also see the address you are visiting in your web browser's address bar. Make sure you are visiting the site you expect.

There is a new trend in identity theft, called *pharming*. Well, it is actually a fairly old type of attack put to a new and alarming use. The basic attack generally relies on DNS poisoning or domain spoofing. The difference between phishing and pharming is that while phishing targets individuals, pharming targets large groups of people. Before we get into a discussion of a pharming attack, let's look at a short primer on how Internet addresses work.

Anytime you type in an address in your web browser, such as <http://www.somecompany.com>, your computer needs to find the Internet Protocol (IP) address before sending any information. There are two main methods for finding IP addresses for web site addresses. The legacy method consists of a file, called the 'hosts' file, that lists all of the host names you may want to visit, along with their IP addresses. The other method is to send a name resolution request to a Dynamic Name Server (DNS). The DNS server looks up the address in its database and returns the corresponding IP address. Once your computer looks up the IP address for <http://www.somecompany.com>, it then uses the IP address for all further communication.

A pharming attack is one where the host file or DNS entry is modified to send users to a counterfeit web site. The slightly simpler of the two attacks is the host file modification. This can be accomplished with a virus or worm. It is generally harder to compromise DNS servers. With the phishing attack, a careful view of your web browser's address bar will show that you are visiting a site you did not expect. Pharming attacks are more difficult to detect since your web browser tells you that you are at the right site even when you really aren't.

The effect of a pharming attack is that all users who want to go to a particular site end up being redirected to a thief's site. While this might sound similar to a phishing attack, it can be much worse. There is no indication to the end user that a redirect has occurred. The web browser still shows the original web address. This behavior makes pharming attacks more difficult to detect. Also, if the thief is able to change DNS entries on a commonly used DNS server, all users who request IP addresses from the compromised server will be sent to the counterfeit site.

So, how do you protect yourself from a pharming attack? Much of the work in stopping pharming attacks is up to the DNS administrators. They will be responsible for ensuring any DNS entry changes are authentic. But, there are some steps you can take. Following these guidelines will reduce your chances of becoming a pharming victim:

Install and update a good anti-virus program. Since many attacks start as malicious software, protecting your system from viruses and other malicious software will go a long way toward stopping an attack before any information is changed. Protect your 'hosts' file. On Windows operating systems, the hosts file resides at: (assuming C:\Windows is where your OS installed) C:\Windows\system32\drivers\etc\hosts. On Unix systems, it resides at /etc/hosts. You can manually check your hosts file to ensure no unusual entries have been put there or you can install software shields that watch the hosts file for you (along with anti-virus software). Know the sites you visit and carefully protect any information you give out. Never divulge any information for any reason unless you are absolutely certain the information is necessary and you are providing it to the correct organization. If your bank web site, or any other web site, asks you to provide confidential information, call their customer service department to get confirmation that the information is needed. Don't call the number on the web site (it may be compromised). Look up the number in the phone book or use directory assistance. As more and more web sites start using digital certificates to authenticate their identities, you will begin to see more popup windows asking you to accept these certificates the first time you visit the web site. Always read the certificate details and ensure the web site really is the one you wanted to visit. If you are unsure, reject the certificate.

We will all hear more about pharming in the coming months. Its use is growing. This is just another opportunity to remind as many people as possible to be careful with the sites you visit and the information you give out. Protect your personal information. Not doing so can be very expensive.

Want more tips and information on how to recognize, prevent, and repair the effects of identity theft? Go to <http://www.thesecurityguy.net> right now and you'll find eBooks and home study courses on identity theft and other security related topics.