

## Beyond Phishing is Pharming

Most financial institutions today understand what a phishing attack is, and many have even experienced them first hand. Although more difficult to execute, “pharming” is a more cunning method of stealing member information, and when it works, its broad impact can be devastating.

Phishing and pharming tactics direct people to fraudulent websites where they are likely to disclose important information such as names, social security numbers, PIN numbers, and passwords. Phishing uses a lure, most-often an email, to get victims to go to the website and give information, while pharming can use a variety of methods to compromise systems without a lure.



One method is to “poison” a domain name server (DNS). This effectively re-routes all of a Financial Institution’s (FI’s) customers to a false website that looks identical to the real one. Another method is to use a worm or spyware to modify a “hosts” file on the PC. When the user attempts to login to the FI’s website, they are forced to the false site. A third method is a man-in-the-middle attack using fraudulent SSL certificates. A last method is compromising the FI’s website, and modifying it to redirect traffic to a false site. This is similar to a traditional website defacement attack, but the attackers hide the fact that the FI’s website has been modified.

Many people are taught not to click on links in email, but rather type the website directly into the address bar of the browser. This is quite an effective method to avoid phishing scams, but will not prevent a pharming attack.

The good news is that pharming attacks can be prevented through the use of specific monitoring tools. These include website defacement monitoring to ensure only authorized modification to the FI’s website. Also a SSL certificate monitor will prevent a man-in-the-middle attack from occurring. Lastly a DNS monitoring tool will ensure your traffic is correctly routed to your website and avoid re-routing traffic to a false website. Up-to-date patch management, anti-virus, and spyware detection and removal software can also reduce the chance of host file modification.

Remember to have a phishing and pharming incident response program developed because even if you detect a pharming attack, steps should be taken to get the false website shut down as quickly as possible.

Kevin Prince  
CSO  
Perimeter Internetworking (formerly Red Cliff Solutions)  
kprince@perimeterusa.com