

iS3 News Articles:

The Mississippi Banker





'Phishing' threatens large and small banks

By Jessica S. Kalish

Director of Technical and Corporate Communications, iS3, Inc.

The same computer technologies that provide the financial industry with unprecedented opportunities also bring phishing, pharming, keyloggers, spyware, and new deceptions that emerge daily. Phishing is an immediate threat to financial institutions because it makes customers wary of using their banks' Web sites for online transactions. In the long term, it can undermine the general public's confidence in online commerce.

Phishing and other scams that use social engineering and technical deception to perpetrate ID theft are now the Internet's biggest scams. Between March 2005 and March 2006, some 2,370 separate phishing scams affecting millions of users were reported. In January 2006, 92 percent of all web sites counterfeited were those of financial institutions, according to the Anti-Phishing Working Group. The Federal Trade Commission predicts that in 2006, approximately 9 million people will report being victimized – at a cost of about \$56.6 billion. To make matters worse, many phishing sites host spyware. While the user's identity is being stolen, his or her computer is being set up for future malicious activities.

The success rate for phishers is staggering. Phishers can replicate web sites so well that an estimated 3 to 5 percent of recipients unknowingly furnish Phishers with personal data.

Spear-phishing, a newer, more efficient means of online identity theft, is personal and targeted. Criminals infer institutional affiliations from users' search histories and then send e-mails that appear to come from these institutions. Criminals can also present pop-up windows requesting "information updates" or "validation" when users go to the legitimate institutional Web site. In these cases, loyalty to one's bank or credit union works against both the customer and the institution. The user is deceived into providing criminals with personal identifiers because he or

she thinks that the pop-up is connected to the legitimate web site. This information is then transmitted to unauthorized third parties and used for fraudulent activities. Recipients are much more likely to be fooled by fraudulent sites if they have an affiliation with the institution whose site is being "spoofed." Approximately 19 percent of recipients respond to spear-phishing, one of the most insidious threats to Internet users.

These are disruptive technologies; innovations that have changed the fundamental way in which banks must do business. To be effective, the response must be equally innovative. Yet, the financial industry's responses have been based in sustaining technologies; traditional methods of alerting customers. E-mails, notices, brochures, and infor-

mation on institutional web sites all seek either to educate customers about the nature of online fraud or notify customers after an attack has taken place.

Among law enforcement, the judiciary, business, consumer groups and researchers who are engaged in the fight against malicious software, there is disagreement over how to approach this problem. However, all sectors agree that the weak link in the chain is the end-user; the customer. Even experienced Internet users are often unable to determine if a web site is fraudulent or legitimate.

Why are users fooled by phishing scams? Three common reasons:

Security Cues: Most users do not understand, and therefore do not look

(continued on page 26)

New types of Internet scams defined

What follows are some definitions of common internet scams, including 'phishing.'

Phishing: (From Password Harvest Fishing) A kind of e-mail fraud wherein the perpetrator sends out legitimate-looking e-mails, typically with links to fraudulent Web sites that appear to come from well known and trustworthy sources. Phishers attempt to gather personal and financial information from the recipient for purposes of identity theft.

Pharming: (From Password Harvest Farming) A rogue practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. In pharming, large numbers of computer users can be victimized because it is not necessary to target individuals one by one and no conscious action is required on the part of the victim. A particularly hostile pharming tactic is known as Domain Name System Poisoning (DNS poisoning)

Keylogger: A hardware device or software program that records each keystroke typed on a particular keyboard, for report back to another party. Often used to record personal data for identity theft.

Spyware: Programming that is installed in a computer to gather information about the user secretly and relay it to advertisers or other unauthorized parties; generally, any potentially unwanted software that could disrupt computer usage, installed without the user's knowledge. Spyware can get into a computer as a software virus or as the result of installing a new program.

Spear Phishing: Targeted Phishing attacks against known members or customers of a particular enterprise, typically those that are small to mid-sized. Spear-phishing yields far higher returns than phishing, and relies on the membership/customer database being compromised.

SSL (Secure Socket Layer): A security protocol that provides communication privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

TypeJacking or Typosquatting: Purchasing a domain name that is a variation on a popular domain name with the expectation that the site will get traffic from the original site due to the misspelling of the name. For example, a typosquatter would register the domain names goog1e.com or yaho0.com anticipating that users would navigate to that site by accident.

—definitions provided by iS3



Phishing

(continued from page 24)

for indicators of authenticity. These include indicators of a secure site, the proper protocol in the address window and a closed padlock in the browser window indicating that the Web page being viewed was delivered by SSL.

Typejacking or Typesquatting: Phishers often substitute letters or non-printing characters in legitimate addresses to deceive readers who “see what they want to see.” For example, in a common technique an “i” or a “1” is substituted for the “l” in “www.paypal.com”. The casual reader sees “www.paypal.com” when presented with “www.paypa1.com”.

Lack of security focus: When the user is attempting to perform a key task such as a making a bank transaction, a purchase or attending to job-oriented duty, security is often overlooked. This is especially true in a culture that encourages multi-tasking. Perhaps the price of multi-tasking is the inability to focus completely on any one thing at a time. The user who is receiving text messages, paying a bill online and engaged in a chat session is not likely to detect a fraudulent Web site.

One software maker, iS3, Inc., has introduced phishing prevention software aimed at customers called ZILLAbar, which works with Microsoft® Internet Explorer to block phishing attacks and other online identity theft scams. ZILLAbar’s downloads the URLs of the latest known phishing sites as often as every thirty minutes, to protect customers. In addition, the ZILLAbar uses heuristics –analysis of behavior and content- to determine the likelihood that a particular site is UNSAFE. Its unique Anti-Phishing Scoring Engine is a mathematical rules engine that subjects the Web content in the user’s browser to a set of sequential evaluations intended to identify fraudulent sites. If the score reaches the threshold level, a phishing Alert indicates that the site is potentially malicious. With the ZILLAbar, customers become empowered in the war against online fraud.

The future of computer security lies in smart technology, taking a predictive

rather than reactive approach. Rather than relying upon scanning, examining each file and attempting to match it with a known malicious signature, new software products now look for programs that monitor keystrokes, connect to unusual ports, or try to hide and make registry changes. Malicious attacks are detected and stopped in real time, before they can do any damage to the user’s computer or capture sensitive information.

The disturbing trend in online fraud is toward exfiltration; more targeted attacks of increasing sophistication aimed heavily at smaller local

banks and credit unions. Bankers must be prepared to block and counter these attacks with increasingly aggressive strategies. The question is no longer whether you will be a target of online fraud, but when and how you will respond to the attack.

Jessica S. Kalish’s background includes more than 25 years as an engineer, quality consultant and communications manager. At iS3, she has overall responsibility for ensuring that technical development documentation conforms to the highest industry standards.