

Anti-Phishing Efforts

Make sure you're not taking a thief's bait to disclose your personal information online



Brannan Heywood

[Libby Carty McNamee](#)

Richmond.com

Friday, September 24, 2004

With the rise of cyber-crimes around the world, watch out for latest hoax — “phishing” scams which are running rampant and on the sharp increase in the past year, duping many unsuspecting consumers. The FBI recently dubbed these scams the “hottest and most troubling new scam on the Internet.” The Federal Trade Commission has issued a consumer warning about the fraud at www.ftc.gov. For those of you unfamiliar with the term, phishing (also known as “carding” or “brand spoofing”) is a thief’s fraudulent attempt to “fish” for your personal information such as passwords, user ids, credit card numbers, bank account numbers, social security numbers, and bank PIN numbers.

The goal of these thieves, or “phishers” as they are called, is to fool the sea of Internet users in order to obtain free access your financial accounts. Armed with that information, they can then dip into them, illicitly withdrawing your money to purchase costly products. In addition, phishers often attempt to steal your personal identity by opening credit cards in your name while having the bills sent to their own address, allowing them to run up purchases in your name without your knowledge, commonly known as identity theft. The “bait” is an innocent looking e-mail that you receive looking completely legitimate as if it has come from your bank or financial institution, complete with your bank’s familiar logo. Phishers are also known to send out computer viruses and worms that will send the original phishing e-mail to countless other potential victims. Identity theft alone affects between seven and 10 million US citizens every year, costing the US

economy an estimated \$50 billion a year.

The “bait” is a seemingly official e-mail that you receive looking as if it has come from your bank, financial institution, or company with whom you regularly conduct business -- complete with that company’s familiar logo. In the body of the e-mail, the phisher poses as your bank and informs you that the bank has a new security system. Next the phisher requires you to “re-enter” or “validate” your personal account information in order to access their updated system – or run the risk of having your account terminated. In reality, the e-mail is fraudulent, originating from the phisher’s phony separate Web site which is often a pirated “look-alike” of the real site with the same trusted trademarked graphic images. Normally five percent of customers respond to these fake e-mails providing the information requested with costly repercussions. The average impact per person is \$92,000 with hundreds of victims per incident. The victimized companies usually end up bearing the loss, not the consumer.

A common scheme is that in the body of the e-mail, the phisher may pose as your bank and inform you that the bank has a new security system due to recent threats to the bank - - from phishers. Next the phisher may ask you to provide your personal account information immediately so you can access the newly updated system. In reality, the e-mail is a spoof, created by phishers and originating from the phisher’s separate fake Web site. Other scenarios deal with similar upsetting or exciting false statements -- such as claiming that someone has used your Visa card without your knowledge or fabricated notification that you have won a prize. Although not common knowledge, it is remarkably easy for phishers to copy information from the legitimate business website and transfer it to their own fraudulent one. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince at least five percent of recipients to respond to these spoofed e-mails and divulge personal data who mistakenly believe that they came from a trusted source.

There have been rampant phishing attacks on the Federal Deposit Insurance Corporation (FDIC), the Department of Homeland Security, AOL, eBay, PayPal, Fleet Bank, Citibank, Barclays and Lloyds TSB, to name just a few. Unfortunately Richmond has not been immune from this accelerating cyber-crime. Capital One’s Web site has posted a warning to its customers about potential phishing attacks. Sun Trust, one of the largest banks in Richmond, currently receives up to 40 phishing attacks per month on average. As recently as Friday, August 20, 2004, SunTrust, phishers sent fake e-mails to SunTrust customers from three fraudulent sources. If you are a SunTrust customer and have received any suspicious e-mails, you can call 1-800-382-3232. Be careful not to call any of the numbers listed on these e-mails because they may be a hoax as well. If in doubt, get the number yourself off of the official website or from the phone book.

Recognizing the need to eliminate the rapidly escalating phishing problem, local Richmond entrepreneurs have created a revolutionary new technology called [Message Level](#) on which patents are currently pending. In its simplest form, this proactive software creates origination records for ALL outgoing e-mails from an organization. On

the receiving end, Message Level temporarily holds each e-mail, quickly authenticating whether it originated from that purported legitimate company. Once Message Level receives confirmation, it automatically allows delivery. Likewise, if there is a discrepancy, Message Level blocks delivery. This process would spare you, the potential recipient, of the aggravation of receiving any spoofed messages with no danger of false positives, previously seen as impossible. Architect **Brian Cunningham** noted the unique strength of Message Level, explaining, “We don’t rely on IP addresses like our competitors because thieves fake them all the time.” Product Manager **Bob Shaffer** said, “This technology will dramatically reduce operational costs, reduce spam by as much as 80 percent, provide brand security, as well as invaluable peace of mind.”

Visitors can download a free trial through the [Message Level website](#).

Although it is extremely difficult to apprehend phishers because of Internet anonymity and that many perpetrators are overseas, federal laws and some state laws criminalize phishing with substantial penalties. President Bush has also recently signed legislation to increase penalties after a person has been victimized. Senator Leahy recently introduced a bill targeting the entire scam before victimization, from sending fake e-mails to the creation of fraudulent Web sites. Concerned parties of the industry formed the Anti-Phishing Working Group, www.antiphishing.org, an organization dedicated to eliminating Internet fraud and scams. Recognizing the dangerous nature of this crime, the Department of Justice has issued a Special Report to inform Internet users about phishing and the various Federal laws that it potentially violates with substantial penalties.

Report suspected phishing schemes to the Internet Crime Complaint Center which is a joint effort of the FBI and the National White Collar Crime Center as well as the Federal Trade Commission’s identity theft Web site soon as you can. In addition, please forward any suspected phishing e-mails to which you have not responded to reportphishing@antiphishing.org. If you believe that you have disclosed confidential personal information, contact the fraud departments of the three major credit bureaus, report it, and request that they place a “fraud alert” on your file with no new credit granted without your prior approval. Also contact your local police and make sure to get a copy of the report. Close the accounts that have been compromised by contact the company’s fraud department. Lastly, do not use your mother’s maiden name as your password on any new accounts.

The bottom line is you should never under any circumstances provide any of your personal information in response to unsolicited e-mails or even phone calls that seem as if they came from your bank, including the link provided on the e-mail. The only time when it is wise to disclose such information is when you initiate contact with the bank by logging onto its official website or calling them yourself — but avoid sending any financial information by e-mail if possible. Make sure that there is a “lock” icon on the browser to be sure that your information is secure before sending it. Remember, your bank should already have your account information in their records. Also check your credit card and bank statements carefully each month.

Libby Carty McNamee is a lawyer and freelance writer living in the Richmond area. She can be contacted at libbymcneee@yahoo.com and 804-378-8218. This article does not constitute legal advice. If you need legal assistance, please contact a lawyer.

Ed. note: Message Level and Richmond.com are affiliated through parent company, Whitlock Portals.