

GONE PHISHING

The information for this article has, in part, been taken from a white paper entitled Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, which was authored by Aaron Emigh of Radex Labs.

What is Phishing?

Phishing, in very simple terms, is an on-line attempt at identity theft. The term phishing is the computer age variation of the word fishing; the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will ultimately be used for identity theft. The e-mail typically directs the user to visit a website where they are asked to update personal information.

The website is bogus and in many instances closely if not perfectly copies the format of a legitimate company or business such as Citibank or EBay. The sole purpose of the website is to steal the user's personal and confidential information. The prime targets of the phishing expedition are confidential personal information such as dates of birth, bank account numbers, Social Security numbers, credit card account numbers, and mother's maiden names.

Why is Phishing a Concern?

It has been estimated that phishing related losses to US banks and credit card issuers exceeds \$1 billion annually. Indirect losses such as a decreased use of on-line services in the face of widespread fear about the security of online financial transactions are much higher. Phishing also causes substantial hardship for victimized consumers when they try to repair or reverse the damage done to their personal credit. Phishing is a global criminal activity commonly committed by organized crime groups. Phishing marries the worst intentions of the criminal mind with modern computer technology.

How does Phishing Occur?

Phishing is a by product of the age of the internet. The most common vehicle for phishing today is e-mail. Typically, a phisher sends a descriptive mass e-mailing with some type of attention grabbing heading that demands the recipient click on a link. Some examples of these attention grabbing headlines are:

- A statement that there is a problem with the recipient's account at a financial institution or other business. The e-mail asks the recipient to visit a website to correct the problem, providing the necessary link.
- A statement that the recipient's account is at risk and offering to enroll the recipient in an anti-fraud program.
- A fictitious invoice for merchandise, often offensive merchandise, that the recipient did not order, with a link to "cancel" the fake order.
- A fraudulent notice of an undesirable change made to the user's account, with a link to dispute the charge.
- A claim that the attachment has something to do with pornography, salacious celebrity photos or gossip
- An offer for a free coupon or cash card.

In each case, the web site to which the user is directed collects the user's confidential information. If a recipient enters confidential information into the fraudulent website, the phisher can subsequently impersonate the victim to transfer funds from the victim's account, purchase merchandise, take out a second mortgage on the victim's house, file for unemployment benefits in the victim's name, or inflict other economic damage.

In many cases, the phisher does not directly cause economic damage, but resells the illicitly obtained information on a secondary market. Criminals participate in a variety of online brokering forums and chat rooms where such information is bought and sold.

Another approach taken by phishers is to create web pages for fake products, get the pages indexed by search engines, and wait for users to enter their confidential information as part of an order, sign-up or balance transfer. Such pages offer products at a price slightly too good to be true.

Scams involving fraudulent banks or lending institutions have been particularly successful. A phisher creates a web page advertising an interest rate slightly higher than any real bank. Victims find the online bank via a search engine and enter their bank account information for a "balance transfer" to the new account. Greed is a powerful motivator that can cloud judgment.

During 2003 there was a proliferation of a phishing scam in which users received e-mails supposedly from EBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated his credit card information already on file with the legitimate EBay. To lend an air of authenticity to the e-mail, it contained a copy of the legitimate EBay's website. The scam relied on people being tricked into

thinking they were actually being contacted by EBay and that they were being connected to the legitimate EBay site to “update” their credit card information.

There are many more variations of the previously described examples which can be read in their full context in the white paper.

Phishing Do's and Don'ts:

- Do not provide personal data in response to an e-mail notice without contacting the sender independently to confirm the request.
- Do not open e-mails or click on links within e-mails from unrecognized or suspicious sources.
- Do not reveal your password during any e-mail communications.
- Do not be deceived into opening an e-mail or clicking on a link simply because the subject line is offering something that sounds “too good to be true”.
- Do not be tricked into opening an e-mail or clicking on a link because the subject line suggests you or your account have been victimized by fraud.
- Do carefully read and review your e-mails before taking any suggested actions.
- Do protect your password and personal information
- Do immediately report any attacks or suspicious activity on your credit card or financial accounts to your credit card issuer or financial institution.
- Do immediately report any phishing attacks to the police.

Additional Sources of Information

If you believe you have been victimized by phishing or identity theft or if you simply would like to learn more about these topics, you may refer to these additional sources of information:

- www.antiphishing.org
- www.consumer.gov/idtheft
- www.ifccfbi.gov/index.asp
- www.ussstreas.gov/fieldoffices.shtml