

## **Thieves Go “Phishing” For Your Identity** **by Harry Erickson, Crime Prevention Unit Corporal**

Have you been *phished*, *spoofed*, *cloaked* or *cloned* lately? These are all the latest hi-tech terms associated with the current methods of Identity Theft.

A large number of our population utilizes e-mail on a daily basis. It is a fast, effective and convenient way of communicating with friends, family and business associates. If you have an e-mail account, chances are you have been the target of “phishing” in the recent past. The term ***phishing*** is a variation of the word fishing as in “fishing for information”, used by computer hackers. A phishing scam utilizes an e-mail message to trick victims into revealing their personal financial information, ultimately leading to identity theft.

***A phishing scam utilizes an e-mail message to trick victims into revealing their personal financial information, ultimately leading to identity theft.***

### **The Lure**

The perpetrator first sets up a “clone” of a reputable company’s website, utilizing actual graphics, font style, color scheme and logos to make a copy of that company’s website. They then pose as the reputable company and send out thousands or even hundreds of thousands of random e-mail messages to potential victims. The message appears to be from the legitimate company. One such actual case involved the use of the Visa Credit Card Company name. The email appeared to be from notification@visa.com.” This is a very simple technique called “spoofing,” which can be done from most computers, by someone with basic computer knowledge. Most of the people who receive the e-mail don’t even have an account with the company who it appears to be from. However, based on the large volume of e-mails sent out, and the large customer base of the spoofed company, there is likely a good number of people who do have an account with that company. Even if, out of the thousands of e-mails sent, only a few people fall for the scheme, the scam pays for the thief.

### **The Hook**

The unsuspecting victim thinks that they have received a legitimate notification from their bank or other company whom they do business with. The victim clicks on a link within the e-mail message, which appears to direct them to the real company’s website. Remember, the thief has already set up a clone of the real company’s website somewhere out in cyberspace. Even the address in the browser bar appears to be that of the legitimate company. This is called “cloaking.” The link is disguised something like “www.visa.com,” but really directs the victim to the thief’s cloned copy website. Once the victim is at the cloned website, there is a form for him/her to fill out, asking to verify or update their account information. Some phishing scams simply integrate graphics and a form into the e-mail message, eliminating the need to set up a cloned website.

### **The Catch**

After the victim fills out the form and clicks “send,” the information is sent to the thief. The thief then uses the information to open bank and credit card accounts and makes purchases under the victim’s name. The thief may also sell the victim’s information to other thieves. The thieves and computers used to commit these crimes can be stationed anywhere in the world, making apprehension and prosecution very difficult.

### **Protecting Yourself**

- If you receive an e-mail asking you for personal or financial information, do not click on any links or fill out any forms within that email. Legitimate companies will not request this information via e-mail.
- If you get an e-mail which appears to be phishing for information, forward a copy to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov).
- Be cautious of opening any attachments within emails, regardless of who they appear to be from. These attachments can contain spyware or viruses which can monitor your computer activity without your knowledge.
- Use firewall and anti-virus software to protect your computer. They will not protect you from phishing scams, however, they are good at protecting you against virus and spyware intrusion.
- If you wish to make a purchase online, make sure you are buying from a reputable company through a secure website. Secure web pages begin with "https" and there will be a security lock icon near the lower right area of your browser. Unfortunately, this can be forged as well, however, if you initiate the transaction with a known reputable company on their secure website, your information should be safe.
- Finally, if you think you have been the victim of a phishing scam, notify your bank and credit card companies right away and check your credit report for suspicious activity.

### **Neighborhood Watch Success Stories**

This month's success story arrived with perfect timing to go along with our article on Internet "Phishing." It's a crime that can affect anyone with an e-mail account. Read on to see how Neighborhood Watch takes a bite out of Internet schemes!

Block Captain Sharman Wallace keeps her Neighborhood Watch Group current on the latest in crime prevention by scheduling regular meetings with her neighbors. Recently, this training prevented a neighbor, Mr. Spencer Leister, from becoming yet another victim of Internet fraud. When he received a suspicious e-mail on April 6<sup>th</sup>, he put his training to use and thwarted a possible identity theft attempt.

The subject line of the e-mail read, "Unauthorized Access to Your Washington Mutual Internet Banking Account." The message stated the bank had recently reviewed Mr. Leister's account and suspected the account may have been accessed by a third party. Mr. Leister was directed to restore his account access by clicking on a provided Internet link. He was instructed to enter his social security number in both the personal identification and account number.

Mr. Leister immediately became suspicious. He knew he should not provide his personal information because he had just attended one of Sharman's Neighborhood Watch meetings with a presentation on Identity Theft and Fraud. Instead of following the instructions to click on the provided links, he called the bank. The bank advised him that the message was fraudulent and provided a phone number to report the incident. After following through with the report, Mr. Leister notified his Block Captain, who passed the alert to others in their Neighborhood Watch Group.

Violent crimes usually make the biggest headlines, but Internet crimes occur much more frequently and within the safety of our own homes. Education is the most effective tool to prevent us from falling victim to these crimes.

*Reprinted with permission of the Crime Watch News. For more information, please call (562) 570-7215 or visit [www.longbeachpd.gov/police](http://www.longbeachpd.gov/police).*