

Phishing Attacks

Don't Let Them Reel You In!

By Tracey Losco
tracey.losco@nyu.edu

This year, the ITS Technology Security Group has seen an enormous increase in the number of phishing scams that have been sent out by e-mail to members of the NYU community. Phishing is a type of e-mail attack, in which a criminal claims to be representing a legitimate company or organization in an attempt to trick the recipient into providing their private information so that it can be used for fraud and identity theft. This type of scam has been relatively successful and is becoming a major problem.

ANATOMY OF A PHISHING ATTACK

The typical phishing attack starts with an e-mail in your inbox that appears to be from a company you know and trust. When you click on the link in the e-mail message, you are directed to a “spoofed” (fake) website designed by the criminal that sent the e-mail message (the “phisher”). Once there, you are asked to provide confidential information about yourself (e.g., your credit card number, bank account information, social security number, etc.). After you have entered this information, the phisher can use it to try to gain access to your online

bank accounts and steal money, to charge purchases to your credit card(s), and/or to use your identity for illegal activities. In addition, your credit rating may be damaged, which can be difficult and time-consuming to repair.

WHY PHISHING WORKS

In a survey conducted by the Gartner group in April 2004 (published in the webcast “Go Phish: Protecting Your Enterprise from E-mail Based Fraud Attacks”¹), 1.78 million people recalled having given out their personal information when they received a message of this type. This is a staggeringly high number.

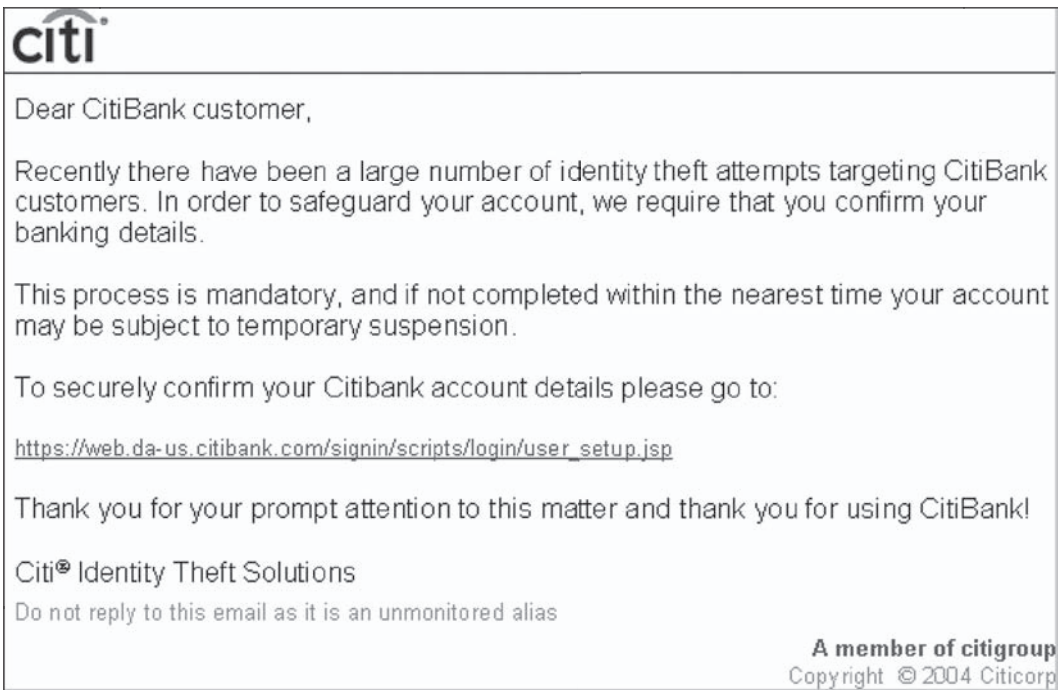
There are several reasons why this type of scam is so successful. The criminals who perpetrate phishing scams use certain tactics to help ensure that the messages end up in the inboxes of a large number of their intended victims. They often use a “dictionary attack” against a company to obtain the e-mail addresses of their existing customers. (A dictionary attack is a method of breaking into a password-protected computer system using software that systematically tries every possible password until it

discovers the right one.) Once they have the addresses of people who are likely to trust the company they are targeting, the phisher will usually distribute the message as an image file rather than as plain text. This allows the message to slip by many people’s e-mail spam filters, since the filters cannot decipher individual words within the message.

Once the first goal of getting the message into the inbox of a likely victim is achieved, the phisher needs to convince recipients to respond to the message. The primary tactic for achieving this, as you can see from the example in the figure on p. 26, is to use logos and/or the recognizable look and feel of a company or organization in order to gain the recipient’s trust. In the past year, there were phishing scams targeted at the customers of PayPal, AOL, Citibank, Citizens Bank, eBay, and the US Bank; all used the look and feel of the real organization.

The secondary tactic for eliciting a response is to instill fear. In the example in the figure, you will notice that there is a sense of urgency in the statements “this process is mandatory” and “your account may be subject to tem-

1. http://searchsecurity.techtarget.com/webcastRegister/0,295011,sid14_gci999879,00.html



An example of a phishing scam message.

porary suspension.” This is a form of “social engineering” (a general term for tricks intended to get people to reveal passwords and other personal information), and an attempt to create a situation in which you will feel the need to comply with the phisher’s request for fear that you might lose your account or break the rules of the institution.

WHAT YOU CAN DO TO PROTECT YOURSELF

The most important thing to remember is that no reputable company will ever ask you for confidential information through an e-mail message. If you receive a message that you are not sure about, the first thing that you should do is call the organization. Use a confirmed telephone number that you find on the back of your bank or credit card or on any paperwork from that company. You can also log into the company’s website the way

you normally do (not by clicking on the link in the e-mail), to see if there are any alerts or messages which confirm the content of the message. When in doubt, always err on the side of caution.

If you think that you might be a victim of identity theft, you should immediately request copies of your credit report from the three major credit bureaus. This is something that should also be done on a routine basis once each year. You can contact the bureaus at:

Equifax

<http://www.equifax.com>
1-800-685-1111

Experian

<http://www.experian.com>
1-888-397-3742

TransUnion

<http://www.transunion.com>
1-800-916-8800

If you see any activity on your report that does not look familiar and you believe may be fraudulent, contact the credit bureau immediately to file a fraud alert.

You should also know your rights and stay informed about the scams that are currently circulating. We encourage you to review the following resources:

- <http://www.antiphishing.org>: Phishing news, help, and a list of recent attacks.
- <http://privacyrights.org/fs/fs17a.htm>: Helpful information for victims of identity theft.
- <http://www.consumer.gov/idtheft/>: Federal Trade Commission (FTC) online resource regarding identity theft.
- <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>: Tips from the FTC on how to avoid getting taken by a phishing scam.
- <http://www.citibank.com/domain/spoof/learn.htm>: Information from Citibank regarding phishing of their user’s data.

Tracey Losco is a Network Security Analyst in ITS Communications & Computing Services.