GREENVIEW DATA Inc.

SPAM STOPS HERE
www.spamstopshere.com

White Paper

Phishing – Past, Present and Future

By Theodore Green, President, SpamStopsHere.com

Abstract

A particularly dangerous and now common type of spam known as "Phishing" attempts to trick recipients into revealing personal and sensitive data, such as passwords, login ID's, financial information or social security numbers. Recipients are directed to counterfeit and fraudulent websites that are exact duplicates of well known and respected companies such as eBay, PayPal or large banking institutions and prompted to enter account information.

This white paper addresses current issues associated with phishing scams and argues the most probable and likely direction phishing scams will follow in the future.

Recommended safe user guidelines are included to help protect users from both current and future phishing attacks.

58 Parkland Plaza, Suite 400, Ann Arbor, Mi. 48103
Tel: 800-458-3348 Fax: 734-996-1308

Table of Contents

Introduction

Spam has evolved from a minor annoyance into a new and dangerous form known as “phishing”. A typical phishing scam consists of an official-looking email, supposedly sent from institutions that are known to have personal sensitive data on file. Financial institutions, eBay and PayPal are often the target. Phishing scams typically state that an account belonging to the recipient has been locked and that he/she must click the provided link to log-in to the account to re-activate it. After the link is clicked, the user is directed to a website which looks EXACTLY like the supposed company’s website, but is actually a forgery.

If sensitive data such as account numbers, passwords, login ID, social security numbers or any other personal information is entered on the fraudulent site, cyber-criminals can access personal accounts, steal finances and the victim’s identity.

While anti-spam systems, such as SpamStopsHere.com, are constantly updated to block these dangerous phishing scams, it is impossible to block them all. There are reported to be more than 10,000 different phishing scams every month and the sophistication level is steadily increasing.

History and Myths

Previously, articles about phishing scams attempted to educate users on how to detect a scam. However, due to the sophistication of the latest scams, it is nearly impossible for even a moderately experienced user to detect the difference between a legitimate bank's website and a forgery.

Myths:

1. Phishing scams contain spelling errors and just don't quite look right.

>> This was true a year ago, but is now the exception.

2. Check the status line of the browser to see what website the email is taking you to.

>> Sophisticated code in the email can display any desired URL on the browser's status line.

3. Check the browser's URL when you are on the website.

>> Even legitimate banks often link to other domain names. For example, the domain "citibank-us.com" looks legitimate, but was actually a phishing site (forgery). Other recent phishing site domains were:

- deutshe-bank.net
- verifiedvisaonline.net
- eservice-paypal.com
- citibahnk.com

The forged URL is easily confused with the real URL.

4. Check that the website is secure; that the URL begins with https://.

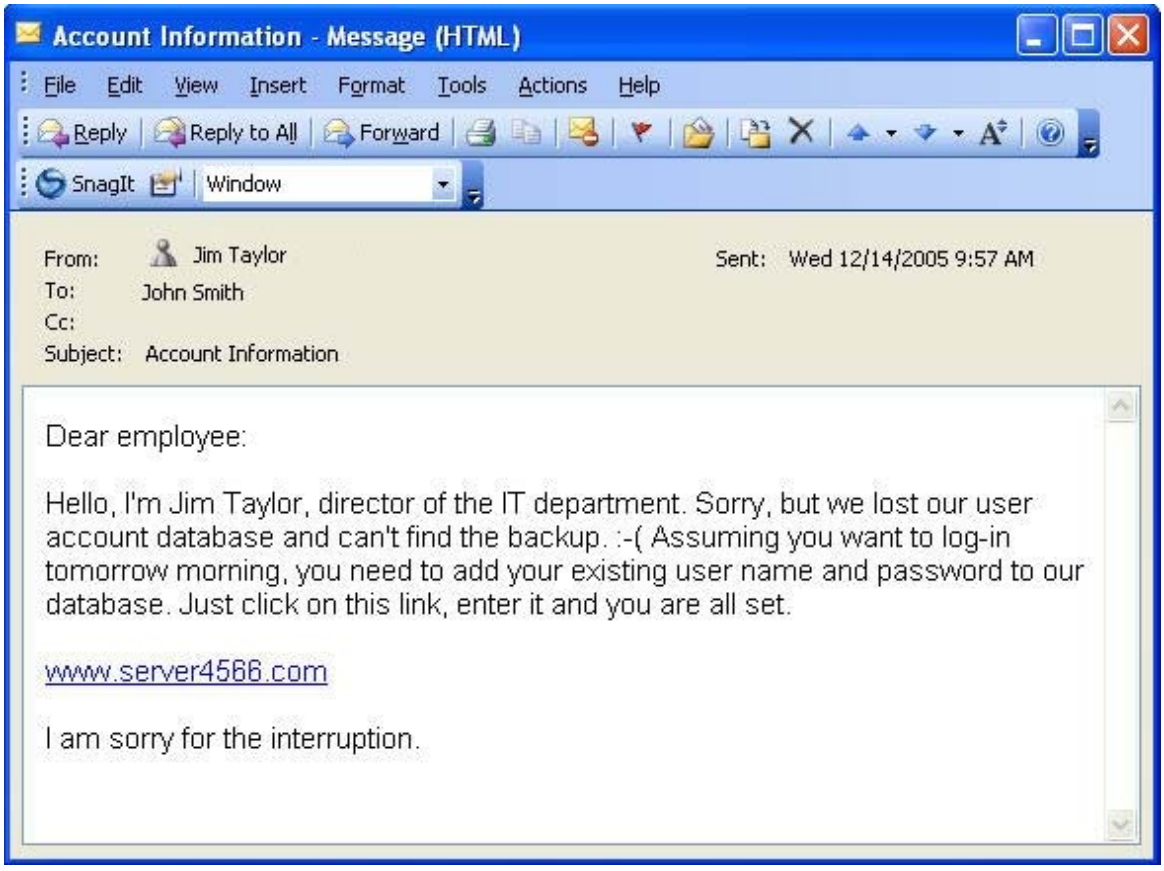
>> As secure certificates only cost $50 and can be run on servers in remote countries, some phishing scams already use "secure" websites.

While a spelling error, non-professional appearance, a dubious URL, or a non-secure website are sure signs of a fraudulent phishing site, the lack of these traits can no longer be used as a sure sign of a legitimate site.

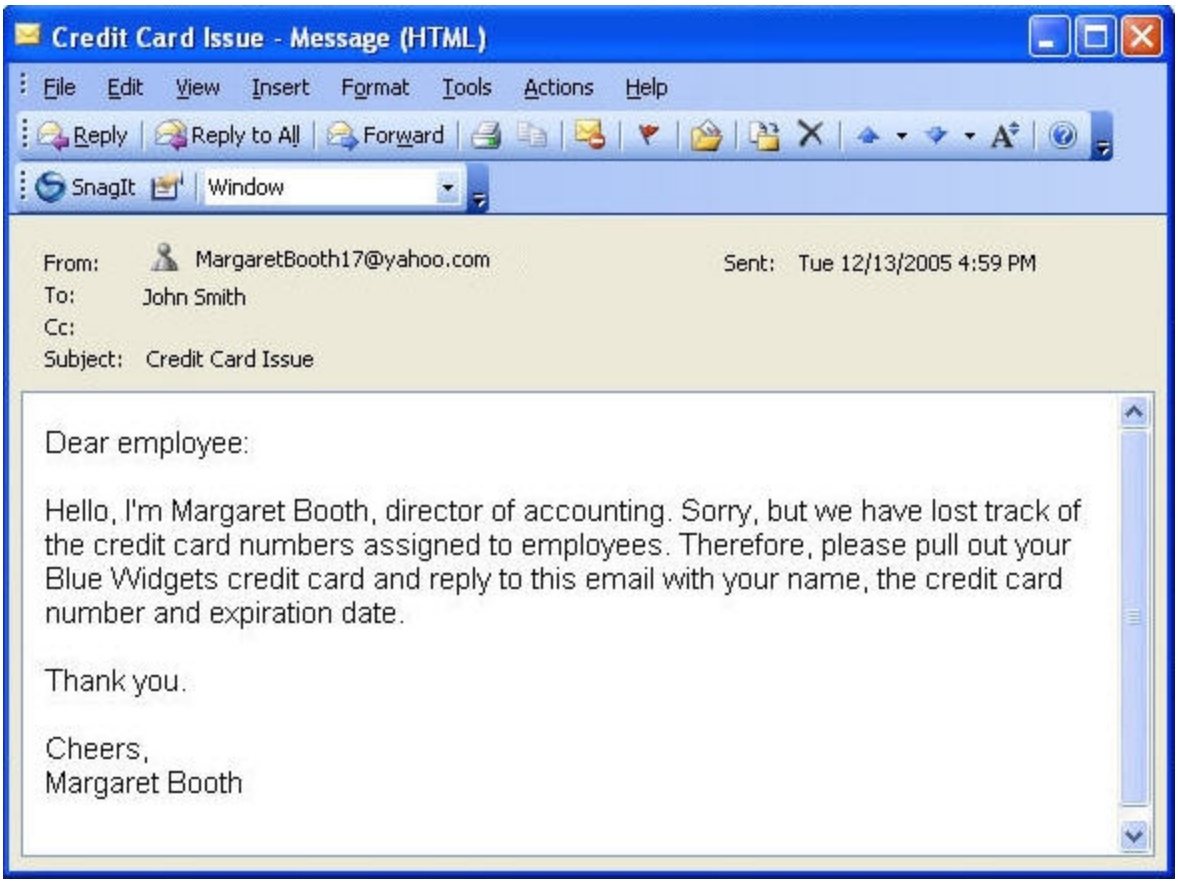
Spear-Phishing

While a single typical phishing spam is sent by the millions, a new variation called "Spear-phishing" is highly targeted and is typically sent only to the email addresses of one company, or even to just a few people. Often the purpose of spear-phishing is to collect computer account passwords so that the company's network can be hacked to collect business and personal information.

A spear-phishing scam email might look like this:



While this email might look suspicious, if you know that Jim Taylor is indeed your IT director, many people will automatically trust it and follow the instructions. The spammer probably got Jim Taylor's name by calling the company's operator and simply asking for it. Then, after purchasing "400 million email addresses - only $99", the spammer extracted just those email addresses which belong to that company, and sent those few emails. With the collected user names and passwords, the spammer might log-in remotely or sell them to dangerous hackers. Let us consider another spear-phishing scam:



Again, if Margaret Booth originally handed you the credit card, you will very likely trust this email and not be concerned that you are replying to a Yahoo account. Obviously this spammer can immediately use this credit card number.

Due to the highly targeted and low volume nature of spear-phishing, it is doubtful that any anti-spam system will be effective at blocking them.

Safe User Guidelines

The best defense is user education. www.SpamStopsHere.com recommends the following guidelines when confronted with a suspected phishing attack:

1. If an email asks to you log-in to your bank, Paypal, eBay or other personal account, assume it is a phishing scam.

   DO NOT UNDER ANY CIRCUMSTANCE CLICK ON THE LINK IN THE EMAIL

2. If you are concerned that the email might be legitimate, you can easily check it, but do not click on the link in the email.

   Instead, open your browser, and manually type in the URL for your bank, e.g. "www.chase.com". You should know it already. DO NOT use the URL in the email as a reference, as it may be the forgery.

3. Similarly, never enter banking information, your social security number or other sensitive information into any website that resulted from clicking a link in an email, no matter how official the website looks, not even if it is a secure website, not even if it is from a (supposedly) trusted source.

   For example, one phishing scam claims to be an official email from the US Government Social Security Administration. Another phishing scam tries to sell you "Phishing scam protection".

4. Do not enter your computer's user name or password into any email that requests it, not even if it claims to be from your IT manager or other co-worker, especially not if the email contains an attachment. These are often attempts by a spammer to infect your computer with a virus.

Finally, do not fall for a phishing scam just because you trust the "sender" of the email, as it is easy for a spammer to forge the sender's name.

In summary, treat any email that asks for your account, password, social security number, credit card number, or other sensitive information as a phishing scam.

The Future

Based on historic trends in spam, phishing and spear-phishing attacks seen by SpamStopsHere, another type of phishing scam will soon emerge. Instead of forging a bank site, it will forge a common on-line shopping site such as Amazon.com or BestBuy.com (some amateurish attempts already exist). The spam will offer a very low price on a popular product from a reputable vendor. However, the link in the email will go to a forgery in which the spammer appears to take the order, but actually only steals the credit card information with corresponding address.

When this type of phishing scam does emerge, it could greatly impact on-line sales as no one will be able to trust email offers, even from his/her favorite stores.

A literal reading of the "Safe User Guidelines" above states that one should never place an on-line order based on an email offer. While perhaps a bit unrealistic and unnecessary today, it is the only safe way to avoid all phishing scams.

Fortunately, the banking industry is taking steps to make on-line banking and on-line commerce safer from phishing scams and other criminal activities:

- On-line banking will soon require authentication beyond just an account name and password. Possibilities include restricted IP addresses or fingerprint recognition. While the later might sound like a James Bond movie, fingerprint scanners will be common on keyboards by 2007. A Microsoft fingerprint scanning keyboard is available now for under $100.

- Single-use credit card numbers. Ever more banks now offer an on-line service by which you can generate single-use credit card numbers for on-line purchases.

As more authentication methods become common on the Internet, on-line banking and on-line commerce will become safer and more universal. Phishing scams will then decrease as they become less effective. In the mean time, users must take extra precautions and should follow the "Safe User Guidelines" above, and be very wary of clicking on links within emails.

It is clear that the number of phishing scams will increase in the near future as an unfortunately high number of users are deceived by them.