“Phishing” for Information

Imagine receiving an email from SHU, your bank or credit card Company with the subject line “Urgent Notice”. The message states that several attempts to log into your account have been made, and the account is now being closed. In order to rectify the problem you are prompted to submit personal information verifying that you are the rightful owner of the account. If you ignore the request, the message warns that your account will be temporarily suspended.

Upon receiving an email like this your immediate reaction may be to respond in order to protect your assets – after all, the email has the appearance that it’s from a legitimate company you frequently do business with. However, you may have to think twice about responding to such an email. In this new age of identity theft and hacking, a technique known as “phishing” (pronounced “fishing”) is on the rise, and it has many innocent victims taking the bait.

In our continued efforts to protect the University community, it is extremely important that all are aware of the techniques employed in the “phishing” scam and not be a victim. As a result we have compiled this document that gives an overview of what is involved in phishing and measures to be taken by the end-users to prevent phishing.

What is Phishing?

Phishing is a social engineering attack and a very sophisticated cyber-crime that exploits users’ trust in the familiar to gain access to private information. It is the art of stealing the identity of an individual and obtaining confidential information by the attacker through social engineering techniques or fraudulent email messages that appear to come from legitimate businesses. It is essentially a kind of identity-theft, in which unsuspecting users are tricked into revealing sensitive personal information (credit card numbers, social security numbers, passwords etc.), thus making themselves susceptible to malicious intent.

The most popular phishing attack strategy is to trick the users by sending fraudulent messages into giving out information. Recently many SHU users received suspicious E-mail messages requiring them to verify account information via a forged URL and enter the login credentials to verify accounts".

A recent sample of the E-mail that was recently sent to SHU users is as follows

To: info@shu.edu
From: "messaging center" <webmaster@shu.edu>
Date: 08/06/2008 05:19AM
Subject: shu.edu E-mail upgrade.

Dear shu.edu Account Owner,

This message is from shu.edu messaging center to all shu.edu email account owners. The Office of Information Technology is in the process of migrating all shu.edu email accounts to upgraded central e-mail services. We are deleting all unused shu.edu email accounts to create more spaces for new accounts.

To prevent your account from being closed, you will have to provide the information below to update it so that we will be sure that your account is still...
CONFIRM YOUR EMAIL IDENTITY BELOW:

E-mail Username: ........... .....  
E-mail Password: .................  
Date of Birth: .................  
Location: ..................  

Warning!!! Account owner that refuses to update his or her email account within 30 days of receiving this warning will lose his or her email account permanently.

Thank you for using shu.edu  
Warning Code: VX2G99AAJ  
Case ID is 1578207.

Kind Regards,  
shu.edu Webmaster.  
Please accept our apologies for the inconvenience.
HOW PHISHING WORKS?

1. Attacker sends an email that appears to be from a source the user might trust like SHU, Bank or Credit Card Company.
2. User clicks on an apparently innocuous link in the email and is taken to a site that looks like the right one – but which is actually the attacker’s
3. User discloses passwords and other sensitive information, e.g., account numbers
4. The Phishing Server sends the confidential Information to the Phisher.
5. The Phisher uses the information to impersonate the user by making use of the compromised information to perform fraudulent transactions.

How to tell if an e-mail message is fraudulent?

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

- **"Verify your account."**
  SHU or other Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.

- **If you receive an e-mail from SHU asking you to update your Account information, do not respond: this is a phishing scam. "If you don't respond within 48 hours, your account will be closed."**

  These messages convey a sense of urgency so that you'll respond immediately without thinking. Phishing e-mail message might even claim that your response is required because your account might have been compromised.

- **"Dear Valued Customer."**
  Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

- **"Click the link below to gain access to your account."**
  HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site.
  The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site.

Avoiding Social Engineering and Phishing Attacks

How do you avoid being a victim?

- Do not click on any link received through mails, always type or use the bookmarks
- Do not send sensitive information like passwords or Financial Information such as banking pins through emails to anyone.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
• Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
• Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
• Don't send sensitive information over the Internet before checking a web site's security.
• Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
• If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.
• Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
• Contact the bank/organization incase of any suspicious transaction.

• Always use complex alpha-numeric passwords containing at least 8 characters. Refer to the posts related to passwords in this site.
• Change passwords frequently and avoid using the same password for multiple Websites.
• Set Internet browser security settings to “high”.
• Avoid visiting links containing “@” sign in the URL.
• Always make sure that financial or commerce Websites contain “HTTPS” before the URL and the “Padlock” at the status bar.
• Log out properly from all open accounts, such as email and online banking etc.
• Close the browser after completing any transaction.

What do you do if you think you are a victim?

• If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization.
• If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

Report Phishing!

To effectively counter a phishing attack, the early detection of such activity is important. If you are uncertain if an email that you have received at SHU is a phishing scam please contact the Technology Help Desk at 973-275-2222 (on campus ext. 2222) or via email at helpdesk@shu.edu. When contacting the Help Desk via email please forward the suspected email along with your request for assistance so that we may ascertain for you if in fact the message is legitimate or a "phishing" scam.
If you see something fishy...

REPORT IT!

Thanks for your Time and Attention!