Identifying and Reporting Phishing Activity

Phishing is the act of masquerading as a known or well-established entity and contacting people as such in order to obtain personal or financial information. In other words, the actor is trying to 'fish' for sensitive information hoping someone will take 'the bait'. People who conduct this activity are known as **phishers**.

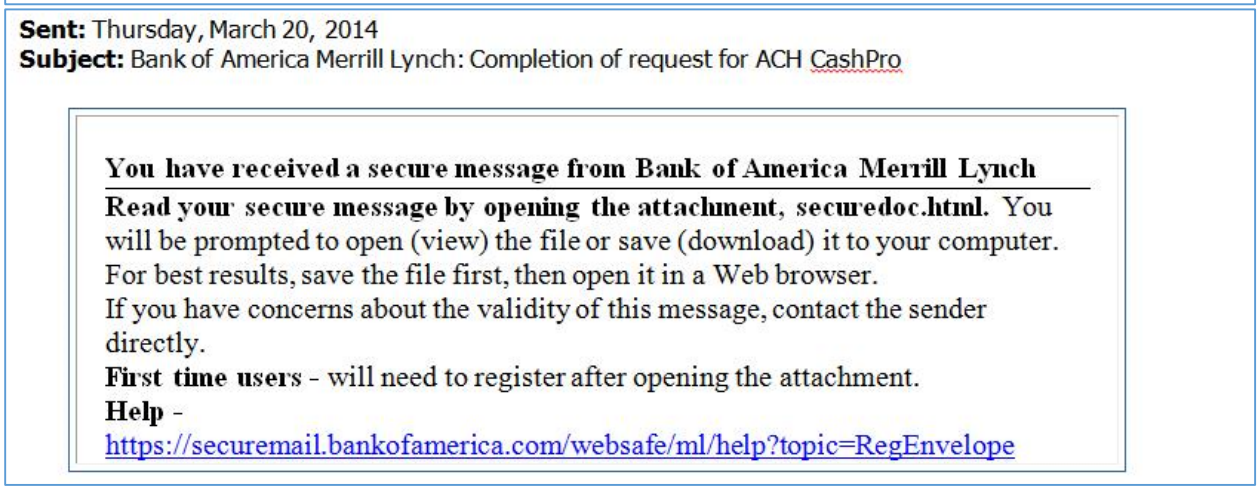
-Phishing Emails

Phishing emails are electronic letters sent through the web to users hoping to obtain sensitive information. Often you'll run into two types of phishing emails:

1) Emails that ask you to reply to the message with **confidential information**, such as your user ID and password. **Never** respond to any email with confidential information. UH and other legitimate businesses will **never** ask for this information via email.

2) Emails that ask you to click on a link to a web page, which then asks you to provide **confidential information**. Many times these web pages **look like** legitimate sites, such as Bank of America or PayPal, **but they are not**. When you provide your user ID and password, this information is captured by the phisher, who can then use it to log into the legitimate site.

Examples:



-Red Flags

Things that might indicate a phishing email that you should watch for:

- Bad Spelling
- Bad Grammar
- Bad Capitalization
- Bad Graphics
- Bad Email Layout
- Use of CAPS
- No contact information
- No Signature
- Vagueness
- Incorrect information
- Popular company name
- Asking to click links
- Asking to download files
- Odd sender address
- Odd recipient address
- Multiple recipient addresses
- Use of threats
- Asking for personal information

-Reporting Phishing

If you suspect an email to be 'fishy' do the following:

- **Do not** listen or do anything the email instructs you to do.
- **Do not** click on any links in the email.
- **Do not** download anything attached to the email
- **Do not** reply back to the sender of the email.
- DO forward the suspicious email to security@uh.edu with its full header information
- DO delete the email.

Even if you are not sure if the email is legitimate, notify security/IT and they will be able to assist you.

-Helpful Links

- http://www.uh.edu/infotech/security/secure-data/Spam-Phishing/index.php
- http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx
- http://www.onguardonline.gov/phishing
- http://us.norton.com/security_response/phishing.jsp
- http://www.antiphishing.org/resources/overview/avoid-phishing-scams