

## 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:

Example 1: A phishing email from Facebook. The text includes: "Hello! As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account." A yellow callout bubble labeled "Spelling" points to the word "Copyrights". Another yellow callout bubble labeled "Links in email" points to the URL "http://www.facebook.com/application\_form". A third yellow callout bubble labeled "Threats" points to the sentence "Note: If you dont fill the application your account will be permanently blocked." A fourth yellow callout bubble labeled "Popular company" points to "Facebook Copyrights Department".

**Sent:** Thursday, March 20, 2014

**Subject:** Bank of America Merrill Lynch: Completion of request for ACH CashPro

**You have received a secure message from Bank of America Merrill Lynch**

**Read your secure message by opening the attachment, securedoc.html.** You will be prompted to open (view) the file or save (download) it to your computer.

For best results, save the file first, then open it in a Web browser.

If you have concerns about the validity of this message, contact the sender directly.

**First time users** - will need to register after opening the attachment.

**Help** -

<https://securemail.bankofamerica.com/websafe/ml/help?topic=RegEnvelope>

## This is NOT an official UH email and here's why...

The diagram shows a phishing email with several red flags highlighted by yellow callout boxes:

- BAD FROM: ADDRESS** (not complete, inconsistent with message) points to the sender information: "From: web19344 On Behalf Of UNIVERSITY OF HOUSTON".
- BAD GRAPHICS** (fuzzy, not current logo) points to a blurry UH logo.
- BAD GRAMMAR** points to the salutation "Dear Member,".
- ASKING YOU TO GIVE OUT INFORMATION** points to the text "We kindly ask you to confirm your Online Identity" and a link "Click here to confirm your [UPDATE](#)".
- BAD CAPITALIZATION** points to the phrase "Please to prevent us from Suspending your online access.".
- NO SIGNATURE** points to the bottom of the email where a signature is missing.
- NO CONTACT INFORMATION** points to the bottom of the email where contact details are missing.

The email text includes: "Sent: Wednesday, May 05, 2010 3:56 PM", "To: bobbyray@uh.edu", "Subject: Update Your Email Account", "Dear Member,", "We noticed you changed your email access, we detected this out of newly installed software & hardware to improve our services and support your subscription.", "Please to prevent us from Suspending your online access.", "We kindly ask you to confirm your Online Identity", "Click here to confirm your [UPDATE](#)", "We offer you a new convenient and Safe Webmail Services.", "Thank you."

### -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](mailto: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://us.norton.com/security_response/phishing.jsp)
- <http://www.antiphishing.org/resources/overview/avoid-phishing-scams>