Spam and Phishing Emails

Phishing emails are messages sent by individuals trying to "fish" for personal or financial information. Phishers are getting better every day at making their messages look authentic. There are 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.

What to do if you get a phishing email

1. Send any phishing emails you receive, including its full header information to security@uh.edu.
   - If you suspect it may be a phishing email, UIT Security can review the message and advise if it is legitimate or not.
   - If you know it is a phishing email, UIT Security can take measures to have a phishing web site taken down.
2. Never respond to any email with confidential information. UH and other legitimate businesses will never ask for this information via email.
3. Use your mouse to hover over links in an email. This will show you the actual website you will be directed to if you click on the link. It is always best to type the address yourself into your web browser, rather than clicking the link.

How to identify a phishing email

Here are ways identify phishing emails,

- Phishing emails may request your username and password be sent back in a reply email.
- Phishing emails may show the sender on behalf of someone, such as the University of Houston and generally do not contain the sender's email.
- Phishing emails may contain fuzzy logo symbols which are not genuine.
- Phishing emails may not contain email signatures or any contact information.
- Phishing emails generally use bad grammar and unwanted capitalization.
- Phishing emails generally require you to take quick action, such as verifying your account to prevent it from being deactivated.

Be particularly vigilant during holidays or significant events since attackers heighten their activity during these times.

Current Phishing Scams

- Notice PayPal: Account Notifications
- Apple Giveaway Contest
  (notice the poor grammar and punctuation)
- Pay Your AT&T Bill Online

How to Protect Yourself

Here are some best practices that will help protect you and your computers:

- Beware of messages that claim your account has been suspended.
- Be suspicious of any email with urgent requests for personal financial information.
- Never click on a link in an email. Instead, always type the legitimate Web address of the site you want to reach directly into your Web browser.
- Be suspicious of email messages and other electronic communications from sources you do not know or recognize
- Use the latest versions of your operating system (OS) and applications.
- Have the latest security software updates (patches) installed. This includes patches for your OS and applications.
- Keep your anti-virus software up to date.
- Report any suspicious emails