DON'T LET PHISHERS HOOK YOUR UH ACCOUNT

> Never respond to any email with personal information

> Be suspicious of all email messages, especially those with attachments you are not expecting or from companies you do not already do business with

> Do not click on links in messages. Type website addresses directly into your browser.

> Report suspicious emails to security @uh.edu

Official emails sent from the University of Houston to large internal audiences follow these requirements:

From: John Smith [uhecomm@uh.edu]
Sent: April 30 at 9:15AM
To: You [youremail@uh.edu]
Subject: Beware of phishing emails

PHISHING noun \f-shr\'

The practice of using fraudulent emails and copies of legitimate websites to extract personal financial data from computer users for purposes of identity theft.

John Smith, Systems Analyst 1
Information Technology
University of Houston
A Carnegie-designated Tier One public research university
713-743-1411
support@uh.edu

This is an official message sent by the University of Houston. To verify the validity of this message, visit uh.edu/phishing or email security@uh.edu.

Need to send email to large internal UH audiences?
Contact ecomm@uh.edu for assistance!

Get more tips at uh.edu/phishing