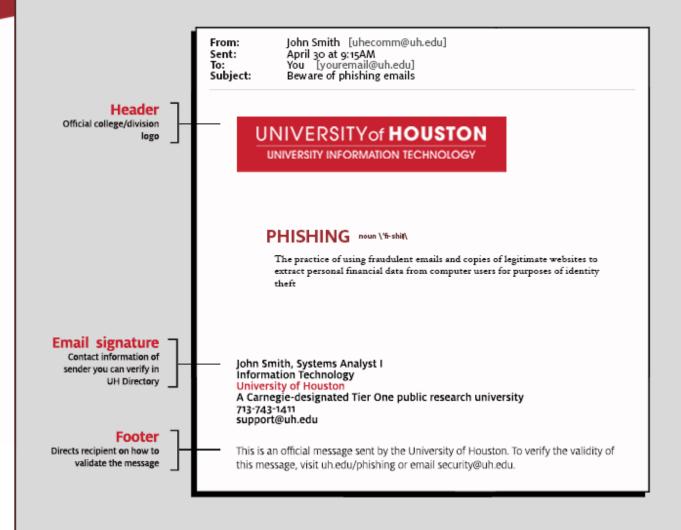# DON'T LET PHISHERS HOOK YOUR UH ACCOUNT

PROTECT YOURSELF

›› **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

Header
Official college/division logo

UNIVERSITY of HOUSTON
UNIVERSITY INFORMATION TECHNOLOGY

PHISHING   noun \ 'fi-shiŋ\

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

Email signature
Contact information of sender you can verify in UH Directory

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

Footer
Directs recipient on how to validate the message

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.

UNIVERSITY of **HOUSTON**
UNIVERSITY INFORMATION TECHNOLOGY
uh.edu/infotech

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

Get more tips at **uh.edu/phishing**