

Don't get hooked by Phishing email

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

From: web19344 On Behalf Of UNIVERSITY OF HOUSTON
Sent: Wednesday, May 05, 2010 3:56 PM
To: bobbyray@uh.edu
Subject: Update Your Email Account



UNIVERSITY OF HOUSTON
Learning. Leading.

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.

BAD GRAPHICS
(fuzzy, not current logo)

BAD FROM: ADDRESS
(not complete,
inconsistent with message)

BAD CAPITALIZATION

**ASKING YOU
TO GIVE OUT
INFORMATION**

BAD GRAMMAR

NO SIGNATURE

NO CONTACT INFORMATION

What can I do to protect myself?

- Be careful about all emails you receive. **Think before you click.**
- If you get an email or pop-up message that asks for personal account or financial information, **do not reply.** Legitimate companies and organizations won't ask for your personal information.
- Do not open any attachments and do not click on any links embedded in the suspicious email. Instead manually enter the website address into your browser to access the website.
- Use an Internet search engine to research the subject line of a suspicious email to determine if that subject line is a known phishing scam.

Official Emails from the University of Houston:

- Will be signed by the person it is coming from
- Will have contact information so you can follow up
- Will NEVER ask you to send personal information in an email
- Will NEVER ask you for your USER NAME and PASSWORD

For more information visit:

<http://www.uh.edu/infotech/phishing>