

**Presentation to College/Division
Business Administrators
October 13, 2011**

***Mary Dickerson
Executive Director, UIT Security
Chief Information Security Officer***



National Cyber Security
Awareness Month

October 2011

Our Shared Responsibility
staysafeonline.org

National Cyber Security Awareness Month

The Internet is a shared resource and securing it is
Our Shared Responsibility

- UH is an official endorser of NCSAM
- Sponsored annually since 2004 by:
 - National Cyber Security Alliance
 - Department of Homeland Security
 - Multi-State Information Sharing and Analysis Center
- Presidential Proclamation on Oct. 3, 2011



NCSAM at UH

- Theme of “Be A Curious Cougar”
 - Code words used to enter weekly drawings
- New IT Security Blog
- Security Tips posted on UH Facebook & Twitter Pages
- Workshops given by IT Security Staff
 - Cougar Trading Card Events!
- Presentations to campus departments & organizations

Workshops

- 10/13: Safe Computing & Device Protection– For Free!
- 10/18: How Safe Are You REALLY? Protecting Yourself Against Identity Theft
- 10/20: Exploring the Wild Wild Web and Living to Tell About It – Internet & Email Safety Tips
- 10/25: Can I “Friend” You? Safety Tips for Facebook and Other Social Media Sites
- 10/27: UH Data Classification and Protection, By the Books! New UH IT MAPPs Explained

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

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

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



BAD GRAPHICS
(fuzzy, not current logo)

BAD GRAMMAR

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.

ASKING YOU TO GIVE OUT INFORMATION

We Kindly ask you to confirm your Online Identity
Click here to confirm your [UPDATE](#)

BAD CAPITALIZATION

We offer you a new convenient and Safe Webmail Services.
Thank you.

NO SIGNATURE

NO CONTACT INFORMATION

- Don't reply to email requests for personal information.
- Hover over links in e-mails to see what the actual destination is.
- UH will never ask to verify your user name or password
- If in doubt, check it out! Send suspicious email to security@uh.edu for review.

Don't Get Hooked By PHISHERS!



Fast. Simple. **Secure.**

UIT now offers a secure option for wireless browsing on campus.

Visit <http://uh.edu/uhsecure> to learn more and configure your wireless device today.

Cougarnet account access required.

UNIVERSITY of
HOUSTON
UNIVERSITY INFORMATION TECHNOLOGY

- **Always use a SECURE wireless network whenever possible**
- **Unsecured = Open = Public**
- **When on an unsecured open network, avoid web sites asking you to enter personal or financial information.**

MAPP 10.05.03

Data Classification and Protection

3 Levels of Data

Level 1 = Confidential / Sensitive / Mission-Critical

- Confidential
 - Social Security numbers
 - Educational records (FERPA)
 - Health care information (HIPAA)
 - Customer information (GLB)
- Sensitive - First & last name in combination with:
 - SSN
 - Government-issued ID (e.g., driver's license) or
 - Account/Credit card/Debit card number & access code
- Mission-Critical – essential to the continued performance of the University or department

MAPP 10.05.03

Data Classification and Protection

3 Levels of Data

Level 2 = Public data not in the public domain

- Public information temporarily protected from widespread release
 - Professor's lecture presentation before the class takes place

Level 3 = Public data in the public domain

- Public information readily available
 - Information posted on the University public web site

MAPP 10.05.03

Protection Requirements

Level 1 – Required Protection

- Stored on critical information resource* (see definition in MAPP)
- Access controls (e.g., user ID and password)
- Must be encrypted if sent on a wireless network or thru email
- Stored on portable device only with valid business reason
 - Information must be encrypted
- Stored on non-university device only with valid business reason
 - Department Chair or Chief Information Security Officer must approve

Level 2 – Suggested Protection

- Stored on critical information resource
- Access controls (e.g., user ID and password)

Level 3 – No Protection Required

MAPP 10.05.03

Responsibilities

- Information Owner (ex. Registrar) – classify data
- Information Custodian (ex. System Admin) – ensure appropriate safeguards in place
- User – Know where data is stored
 - Use Identity Finder to locate confidential/sensitive data
 - Ensure Level 1 data is stored and protected appropriately
 - √ Dept. File Share
 - √ PeopleSoft
 - X Third party provider (“cloud”)
 - X Laptop
- Coordinate with C/D ISO to have Identity Finder run in your area – 100% UH computers by Dec 31

COMING SOON: ISO Workshop – October 19th

COMING SOON: UNIFIED LOGINS !

IT Security staff are available to:

- Give presentations to your department staff
- Assist with IT security best practices
- Hear your suggestions for UH IT security enhancements

www.uh.edu/uit/security

security@uh.edu

832.842.4695

“Be A Curious Cougar”

Code Word

IdentityFinder

Email the code word to
awareness@uh.edu to enter this
week's prize drawing!