College/Division Business Administrators Meeting

April 10, 2014

Mary Dickerson, MBA, CISSP, CISM, PMP
Executive Director, UIT Security
Chief Information Security Officer
mdickerson@uh.edu

UNIVERSITY of HOUSTON | UIT

Windows XP – End of Support

- No more updates from MS after 4/8/2014
- Targeted attacks from hackers
- Non-compliance – HIPAA, PCI, etc.

- If you still have XP systems:
  - Fully update (OS, Anti-virus, all software)
  - Remove un-necessary 3rd party software
  - Remove from the network
  - Notify UIT Security of any UH XP systems

Elevated Access Privilege Memo

- Email Message to All Employees with Elevated Access Roles in PS
  - Elevated Access = Increased Responsibility
  - Safeguard account information at all times
    - No use of same/similar passwords with other non-UH systems
  - Requirement for maintaining computer systems
    - Kept fully patched/updated at all times
      - » Operating System/Applications/Anti-virus
      - » Configured for regular virus scanning
      - » Regular use of Identity Finder
    - Applies to UH and Non-UH Devices

Elevated Access Privilege Definition

- Users with administrative page access to view and change FERPA & Privacy related info and organizational financial asset info

- Data Elements:
  - Date of Birth
  - Social Security Number
  - Direct Deposit
  - W4 Federal Tax
  - Email Address
  - Home Mailing Address
  - Home Phone Number
  - Student Grades
  - Student Transcripts & Records
  - Student Financials
  - UH System Finance & Budget Program

Elevated Access Privilege Cont.

Roles to Identify Elevated Access

- UHS_ADMIN_USER – PeopleSoft HR and Campus Solutions users who have the PS HR/CS icon within the AccessUH portal
- UHS_FINANCE_USER – PeopleSoft Financials application users who have PS Financials icon within the AccessUH portal
- UHM_CS_INSTRUCTOR, UHC_CS_INSTRUCTOR, UHV_CS_INSTRUCTOR

***NOTE: Individuals may be assigned multiple elevated access roles. For example a user may be an employee with elevated access in HR, in Finance, and also may be an Instructor for one of the campuses.**

Out-of-scope Employees who have PeopleSoft access

- Employees who only have access to PeopleSoft PASS site icon within AccessUH portal
- Example: Facilities personnel

Anti-Phishing Campaign

- Phishing threat continuing to escalate
- UH Multi-Prong Approach
  - Technology implementations
  - User awareness – how to identify real emails
  - Incident response changes

UNIVERSITY of HOUSTON | IT SECURITY

Safe. Simple. Secure.

Official UH Email Requirements

www.uh.edu/phishing

Formatting Requirements

Header

- Must use marketing approved College / Division / Department logo, if available, located on the UH Marketing & Communication website at the top of the email message.
  - If a logo is not available, the official University of Houston logo, available on the same website, must be used.
  - If the message will be in text only format, the following text must be at the top of the message in place of a logo:

University of Houston
College/Division/Department name

Formatting Requirements

Email Signature

- Must conform to the UH Graphic Elements for Email Signature

  Jane Doe, Department Manager
  Department Name
  University of Houston
  A Carnegie-designated Tier One public research university
  713-743-0000
  janedoe@central.uh.edu

- Phone number must be a UH extension
- Email address must be a UH address
- Use of departmental phone and email is acceptable

Formatting Requirements

Footer

- Must direct the recipient how to verify the validity of the message.

  This is an official message sent by University Information Technology. To verify the validity of this message, you may visit the UIT website at uh.edu/uit or contact John Smith at 713.743.1411 or via email at support @uh.edu.

Content Requirements

- Use correct grammar, punctuation and capitalization.
- Do not ask the recipient to provide personal information by email.
- Do not ask the recipient to provide their username and password.
- Do not use all capitalized letters in the subject line.
- Do not request recipients act in an urgent manner. Give them plenty of time to take action.

Content Requirements

- Do not include hyperlinks to web pages that require an individual to login. Instead direct them to the login location. For example:

  Please login to your myUH or PASS account through AccessUH to update your information.

- Do not include attachments. Instead, post the attachment on your official UH website and direct the individual there without including a hyperlink. For example:

  To view the flyer for this event, visit the website www.uh.edu/events in your web browser.

Phishing Response Process

- User reports phishing email to UIT Security
  - User Acknowledgement
  - Verification by IT Security email is phishing
  - Contact ISP to take down phishing site
  - Determine if msg can be blocked
  - Report msg to is-spam@sophos.com
  - Post msg information on IT Phishing site
  - Take other action as appropriate

Incident Reporting & Investigation (MAPP 10.05.02)

All users have an obligation to report:

- Actual incidents
- Suspected incidents
- Identified Vulnerabilities

Web: **uh.edu/infotech/security**

Email: **security@uh.edu**

Phone: **832-842-4695**

Anonymously: **www.mysafecampus.com**

To report a copyright violation: **dmca@uh.edu**

Questions?