

# SECURE OUR SYSTEMS

UNIVERSITY of **HOUSTON** SYSTEM  
INFORMATION SECURITY



# SOS Training

The purpose of Information Security Awareness Training is to educate employees on how to protect confidential and sensitive information maintained by the University of Houston System and its universities.

UNIVERSITY of  
**HOUSTON**

**UHD**  
University of Houston  
DOWNTOWN

**UHV**  
UNIVERSITY OF  
HOUSTON - VICTORIA

 University of  
Houston Clear Lake

The Texas Government Code, Texas Administrative Code Information Security Standards (TAC 202) and the Gramm-Leach Bliley Act (GLB Act), as well as other regulations and state and federal laws, require training for all System employees.

# Topics Covered

- 1** Information Security
- 2** Data Classification & Protection
- 3** Information Security Incidents
- 4** Best Practices to Safeguard Information & Information Systems
- 5** Email Security
- 6** Identity Theft
- 7** Copyrighted Material
- 8** Gramm-Leach-Bliley Act (GLB Act)
- 9** Health Insurance Portability and Accountability Act (HIPAA) and Texas Medical Record Privacy Laws

# Data Classification and IT

Data is our virtual fingerprint. Just like a fingerprint, we leave traces of it whenever we interact with anything in cyberspace, be it online shopping, banking, or any other digital interaction. Information Security is the protection of this data from unauthorized access, use, disclosure, disruption, or destruction. **The main goal of Information security is to protect the big three:**



- **CONFIDENTIALITY:** is the information accessible only to authorized parties?
- **INTEGRITY:** is the information original and unmodified by unauthorized users?
- **AVAILABILITY:** can the information be accessed at the user's discretion?

Threats arise whenever any of these are not protected.

# Vulnerable To Attacks

The University of Houston System and its universities are vulnerable to attacks from hackers, phishers, and spammers. They all share a common goal - to gain unauthorized access to a system. While their approaches are different, they are all collectively known as threat actors. Like their name implies, they seek to take advantage of threats in a system.

# Threats Generate Risks

A threat is a hole or vulnerability that has the potential to grant unauthorized access to information. These threats generate risk, a potential loss of information that can adversely impact university functions. Whenever a threat is acted upon, we classify it as an attack.

The purpose of an attack is to undermine the University of Houston System's mission, daily operation, perception, and image of its universities by destroying or modifying information.

# Data Classification & Protection

## Not all data is created equally.

In SAM 07.A.08, Data Classification and Protection, the University of Houston System classifies data in three ways, with each subsequent level requiring less security.

### LEVEL 1

#### *Confidential:*

- Social security number
- Healthcare information (HIPAA)
- Educational records (FERPA)
- Customer information (GLB)

#### *Sensitive:*

- Individual's name in combination with social security number, government-issued identification number (i.e., driver's license number), or account number with required security code or password
- Individually identifiable information related to an individual's health care

#### *Mission-Critical:*

- Information defined by the university or information owner to be essential to the continued performance of the mission of the university.

### LEVEL 2

#### *Protected Information:*

- Information that may be subject to disclosure or release under the Texas Public Information Act as requested.

### LEVEL 3

#### *Public Information:*

- Information readily available in the public domain, such as information posted on the component university's public web site, and any other information not classified as Level 1 or 2.

Level 1

Level 2

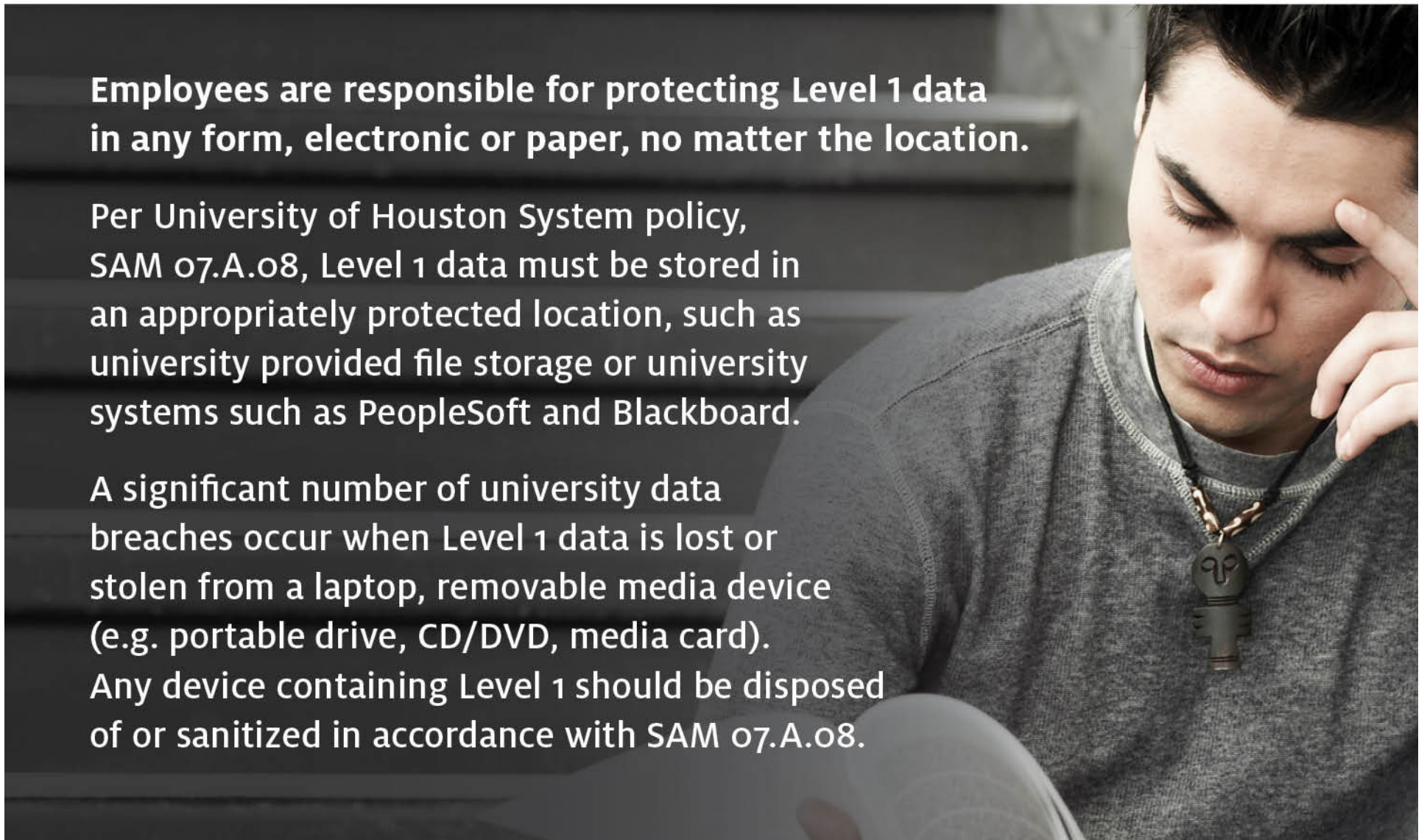
Level 3

# Security Starts with You

**Employees are responsible for protecting Level 1 data in any form, electronic or paper, no matter the location.**

**Per University of Houston System policy, SAM 07.A.08, Level 1 data must be stored in an appropriately protected location, such as university provided file storage or university systems such as PeopleSoft and Blackboard.**

**A significant number of university data breaches occur when Level 1 data is lost or stolen from a laptop, removable media device (e.g. portable drive, CD/DVD, media card). Any device containing Level 1 should be disposed of or sanitized in accordance with SAM 07.A.08.**





# Information Security Incidents

Information security incidents involve an actual or imminent breach of information security as it relates to information maintained by the University of Houston System and its universities.

Specifically, an information security incident may include:

- Unauthorized access of university data
- Unauthorized use of user's account
- Unauthorized copying or distribution of copyrighted or licensed software
- Misuse of computer resources



# Report an Information Security Incident

When an employee believes an information security incident has occurred, the UHS Information Security team should immediately be notified:



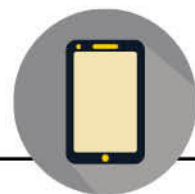
**EMAIL**

UH - [security@uh.edu](mailto:security@uh.edu)

UH-Clear Lake - [security@uhcl.edu](mailto:security@uhcl.edu)

UH-Downtown - [security@uhd.edu](mailto:security@uhd.edu)

UH-Victoria - [security@uhv.edu](mailto:security@uhv.edu)



**CALL**

UH - (832) 842-4695

UH-Clear Lake - (281) 283-2954

UH-Downtown - (713) 221-8638

UH-Victoria - (361) 485-4505

**To report an incident anonymously,  
visit the UHS Fraud & Non-Compliance Hotline.**

# Stolen Equipment?

To report theft of your personal device on campus or theft of a university owned device, file a police report with the appropriate campus police department IMMEDIATELY!

**UH Police – 713-743-3333**

**UH-Clear Lake Police – 281-283-2222**

**UH-Downtown Police – 713-221-8065**

**UH at Katy Police – 832-842-3911**

**UH at Sugar Land Police – 281-275-3302**

**UH-Victoria Police – 361-570-HELP (4357)**



# Security Best Practices

**As complex as the data we need to protect is, the methods of protecting it revolve more so around careful habit building as opposed to equally complex rule sets. Remember, you are the best firewall. Good rules of thumb usually involve the following:**

- Keep computers up to date with security updates/patches (software, applications, operating systems)
- Keep anti-virus software updated to the most recent version
- Log-off or lock devices when not in use

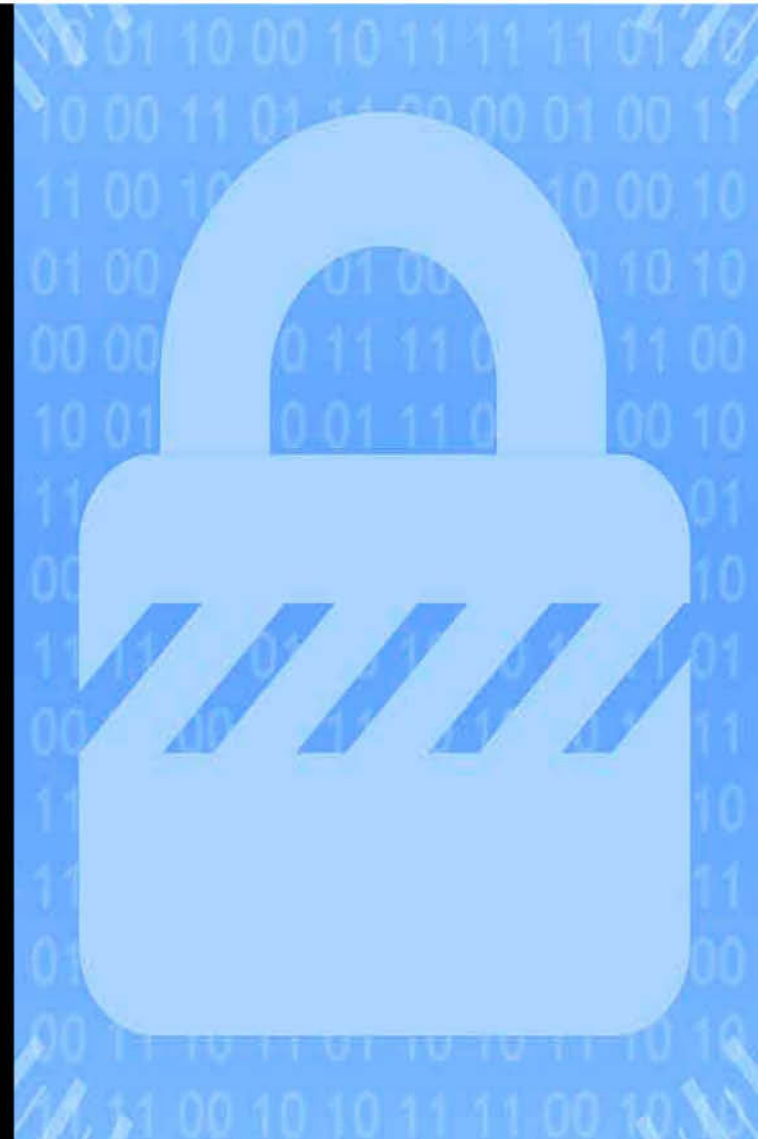
# Safeguard Information

- Backup files on a regular basis
- Eliminate storage of Level 1 data (i.e. Social Security numbers, etc.) where possible
- Comply with federal, state, UHS and university requirements for information security
- Use a strong password and follow good password management practices
- Credit card information should never be stored on individual computers



# Password Management

- Passwords should be at least 8 characters long and should contain a combination of lowercase and uppercase letters, numbers, and special characters
- Consider using a phrase that you can easily remember
- NEVER share your password
- Change your password at least every 180 days
- Use a unique password for different types of accounts (work, personal email, personal banking, etc.)



# Email Security

- Email is not private and can be intercepted, altered, or used to carry out crimes, including collecting your personal information
- Avoid becoming a victim – protect yourself against malware, viruses and information theft
- An email virus is a program or piece of code that is sent to computer users as an email attachment. The virus is activated when the attachment is opened



# Take Action

Delete, **DO NOT OPEN**, email messages with attachments you are not expecting. The attachment may contain malware or a virus.

**DO NOT REPLY** to spam or click the “Remove From Mailing” link in a spam message. Doing so will let spammers know they have reached an active email account and the amount of spam you receive will only increase.

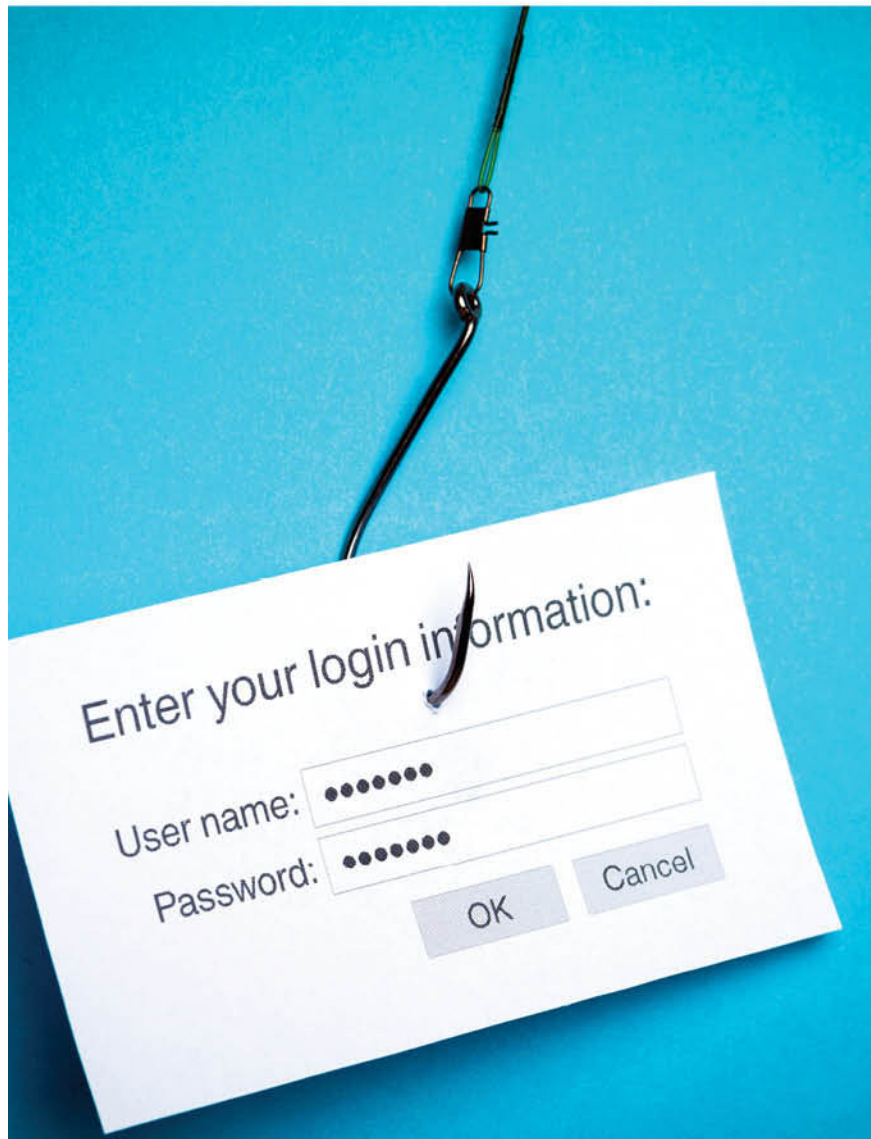




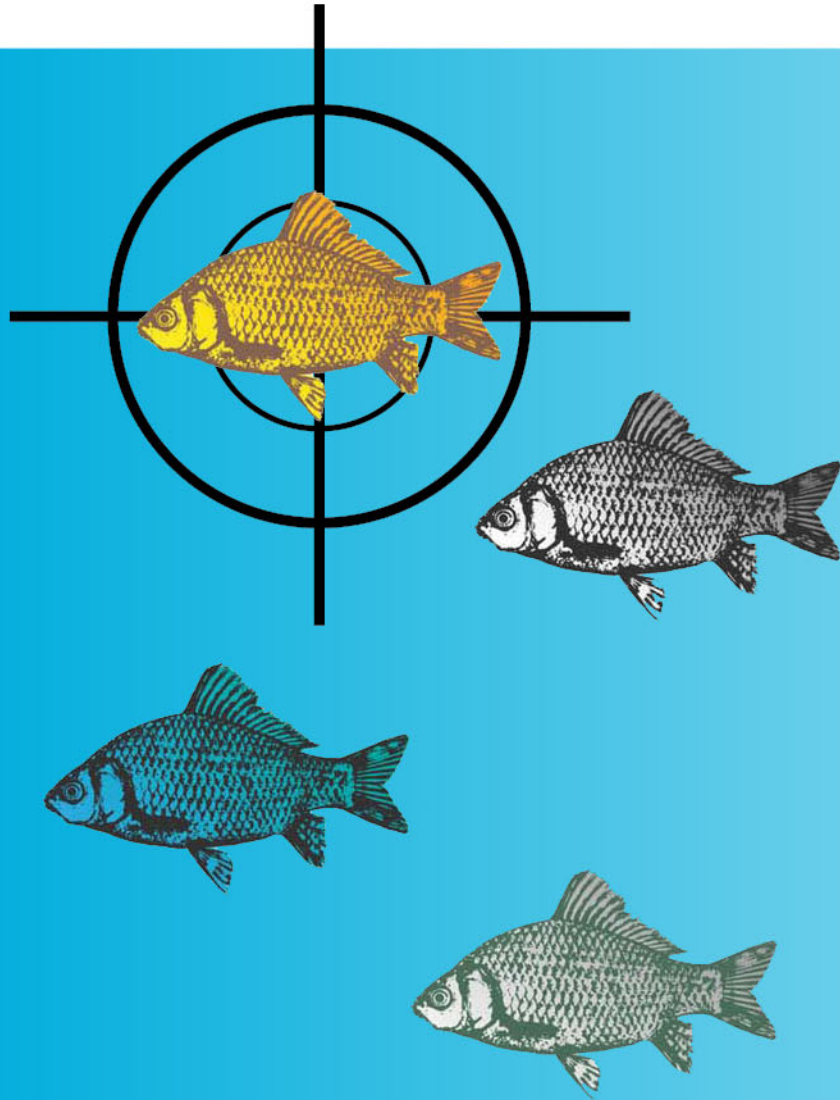
# Phishing Emails

## Don't Get Hooked

Phishing emails are some of the most common attacks carried out by malicious actors. The purpose of these attacks is to gain access to a user's login information. These attacks focus on "hooking" victims by disguising themselves as originating from a credible source.



# Spear Phishing Attempts

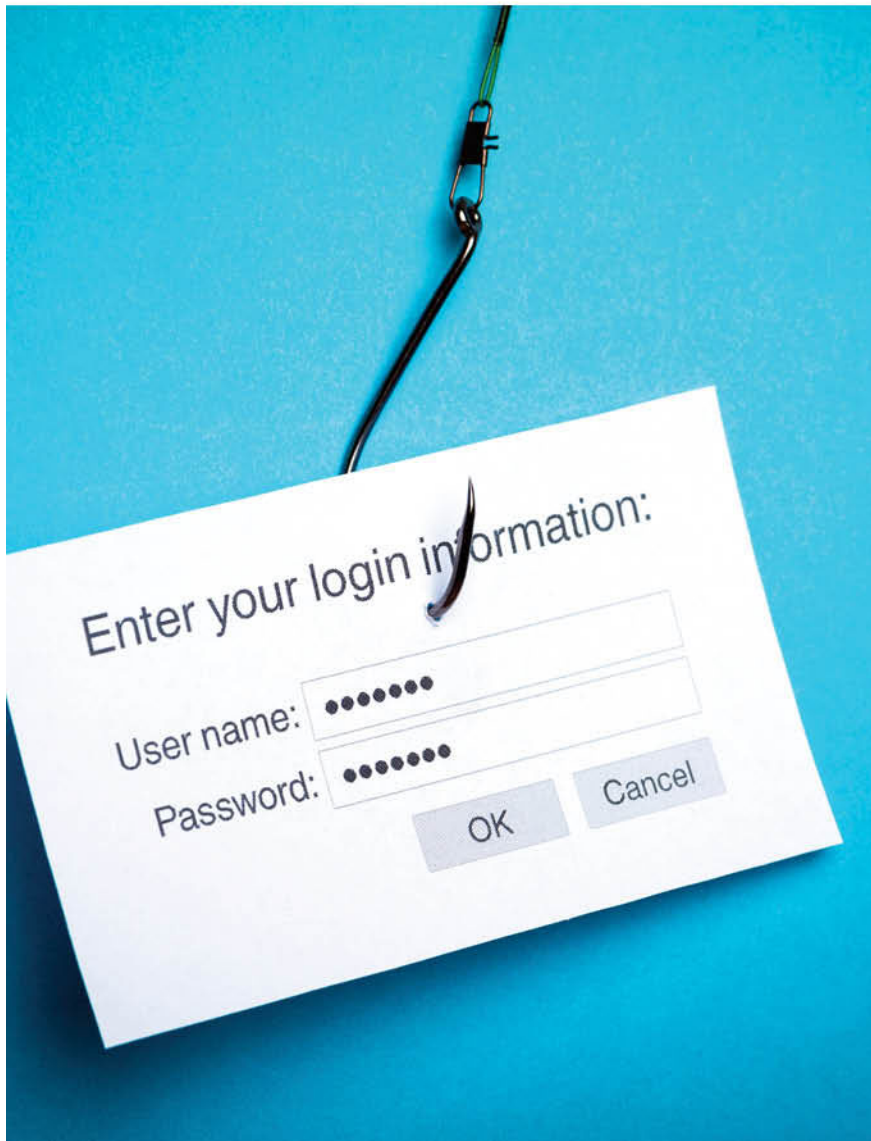


One specific type of phishing is called Spear Phishing. These phishing emails are sent to a specific person and include personalized information about the recipient, such as name or job title. This is to establish familiarity in the hopes that the recipient will feel more comfortable following the request in the message to provide information or click a link.

# Phishing Attempts

## Signs of a phishing attempt:

- Mimic trusted websites
- Appear as official messages from a reputable company but are sent from non-official email addresses
- Try to create urgency by providing a tight time window (usually 24 hours)



# Protection



## How to Outsmart a Phisher

- Do not reply to emails asking for personal information
- Do not click on links in the email
- Make sure that the email contains official contact information
- Remember that companies will never ask for usernames or passwords
- Verify the website's certificate

# Identify Theft

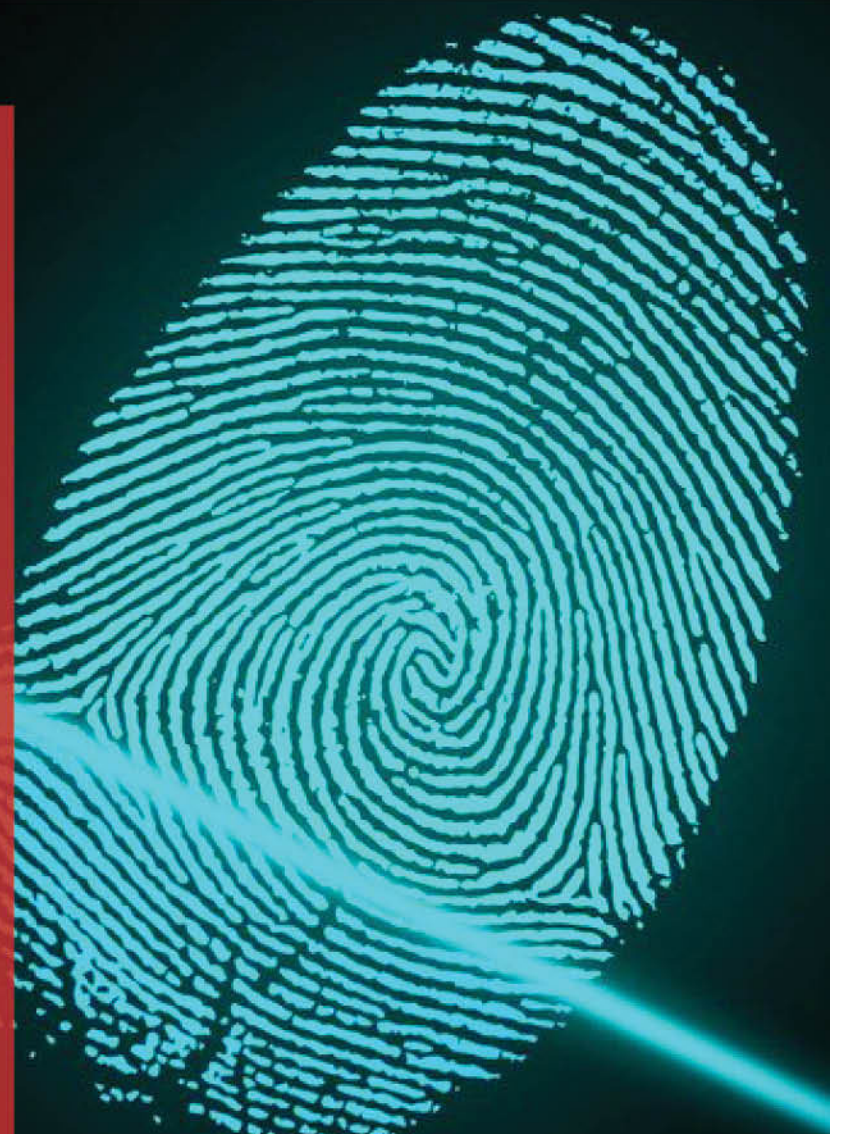
Identity theft is when someone steals identifying information (like social security number, DOB, and bank account number) to commit crimes.

Phishing is one of the most common methods that thieves use to obtain personal information.



# Tell-Tale Signs of Identity Theft

- Unexpected bills arriving at your house
- Credit denied for no reason
- Credit cards are mysteriously opened in your name
- You receive calls or letters about purchases that were not made by you.



# Identity Theft Tips

While there is no such thing as a 100% secure method, the following steps can help decrease identity theft significantly:

- Shred financial documents
- Avoid obvious passwords like birthdays or pet names
- Always use your browser to visit the website in an email, never click the link within an email
- Close accounts that have been modified illegally or created illegally
- Monitor your credit report regularly

# GLB Act

The Gramm-Leach-Bliley Act (also known as the GLB Act) is a federal law which mandates that financial institutions, including institutions or higher education, protect the security, confidentiality and integrity of customer information 16 CFR 314.1 (a)

**GLB**

Gramm-Leach-Bliley ACT



# What Does the GLB Act Require?

Mandates the University of Houston System, its component universities and employees safeguard financial information that is collected or maintained in connection with its financial institution activities.

The University of Houston System and its component universities must protect financial information in paper, electronic and other forms.

**GLB**

Gramm-Leach-Bliley ACT

# Customer information

“Any record containing nonpublic personal information... about a customer of a financial institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of (the University of Houston System, its component universities or its affiliates).” 16 CFR 314.2 (b)

“All financial information in the possession of the University of Houston System and its component universities must be safeguarded regardless of whether such information pertains to individuals with whom (the University of Houston System and its component universities have) a customer relationship, or pertains to the customers of other financial institutions that have provided such information to (another financial institution).” 16 CFR 314.1 (b)

# GLB Act Individuals Protects

The GLB Act requires UHS to protect the information of:

- Applicants
- Students
- Parents/Guardians
- Employers
- Donors

**GLB**

Gramm-Leach-Bliley ACT

# GLB Act Safeguards Information

## What type of information must be safeguarded?

- Credit card account numbers
- Bank account numbers
- Income histories
- Credit histories
- Social Security numbers

**GLB**

Gramm-Leach-Bliley ACT

# Potential Risks

## What are the potential risks of not safeguarding information?

- Unauthorized access of financial information by third parties
- Unauthorized transfer of data to third parties
- Interception of data during transmission
- Physical loss of data due to disaster or theft
- Compromise of computer system security



**GLB**

Gramm-Leach-Bliley ACT

# GLB Act Safeguards Customers

## The Federal Trade Commission (FTC) suggestions for safeguarding information:

- Always check applicant references
- Use password protected screensavers
- Change passwords frequently
- Keep anti viruses and computers regularly updated.
- Back up information regularly
- Encrypt and password protect emails that contain sensitive information
- Use two factor authentication
- Store sensitive information in secure areas
- Make sure areas are protected against natural disasters
- Shred sensitive information and secure it until it is discard
- Delete all customer information from computers and secure them until they are discarded
- Destroy all hardware that is meant to be discarded

**GLB**

Gramm-Leach-Bliley ACT

# GLB Act Contacts



## Who do I contact if I do not know what to do?

- It is important to recognize fraudulent attempts to obtain customer information
- If you suspect an attempt to fraudulently obtain a customer's financial information, immediately report the attempt to your supervisor who should then report the attempt to the Information Security Officer (ISO)

**GLB**

Gramm-Leach-Bliley ACT

# Digital Millennium Copyright Act

- Obtain written permission from copyright owners
- Check the terms and conditions of use or copyright information before downloading material from a website
- Obtain music, video games and other software from legal download sites
- Obtain a copyright for material that you have authored
- Do not assume that works that are in public domain are not copyrighted
- Avoid downloading free screen savers, free-ware or shareware applications or other copyrighted material


Review UHS policy – SAM 07.A.04, Digital Millennium Copyright Act





# HIPAA Privacy Laws

## Health Insurance Portability and Accountability Act (HIPAA) & Texas Medical Record Privacy Laws

- Ensures the confidentiality and integrity of protected health information that an employee or component receives, creates, collects, transmits and/or maintains
  - Protects such health information from reasonably anticipated threats, uses and disclosures
  - Individuals whose job requires specific HIPAA education will receive training in their department from the Office of the General Counsel
- 

UNIVERSITY of **HOUSTON** SYSTEM  
INFORMATION SECURITY

Even with the cutting-edge technology around us, it is important to remember that security starts with you. You are the most vulnerable and most valuable asset to an attacker. The protection of the University of Houston System's information rests in your hands.

