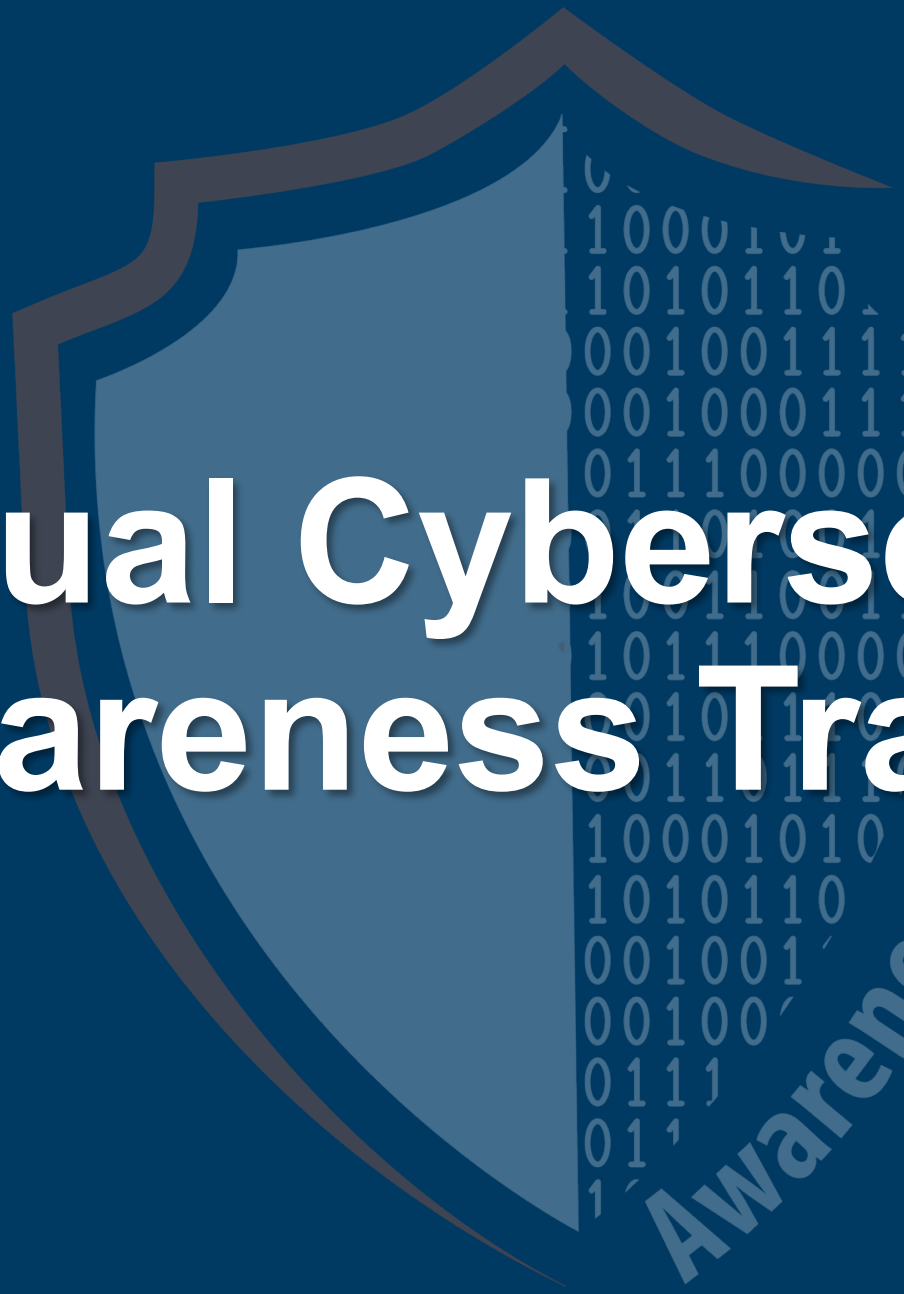
Annual Cybersecurity Awareness Training



Sam Houston State University

Texas Government Code Section 2054.5191

AWARENESS IS MY ARMOR

About This Training

This training will provide you with additional resources to help you stay up to date with SHSU specific cyber-attacks and tips on how to defend against them.

Information Security Habits and Procedures to Protect Information Resources

Section 1

Principles of Information Security

Why is awareness training important?

- enhance security
- ensure compliance with laws
- promote positive behaviors
- aid in better decision-making
- prepare individuals for emergencies
- build organizational reputation

AWARENESS IS MY ARMOR

What is Information Security?

Provides:

- Confidentiality
- Integrity
- Availability

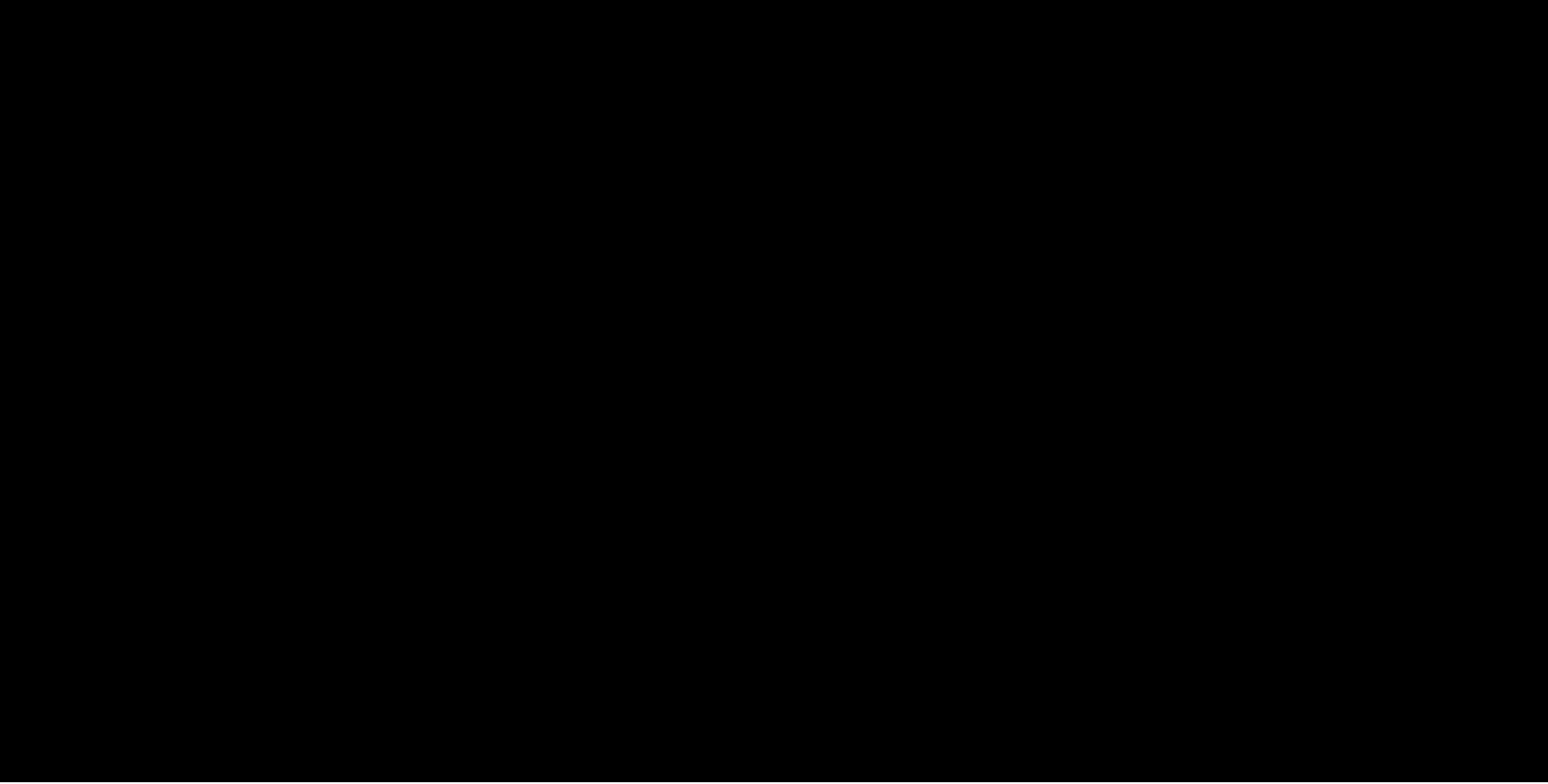
Protects Information Systems & Data from:

- Disclosure
- Modification
- Destruction
- Unauthorized Use

Everyone is responsible

Know Your IT Policies

- SHSU and TSUS IT Policies
  - https://www.shsu.edu/intranet/policies/information_technology_policies/



Forms and Locations of Information

Forms of Information:

- Digital
- Physical
- Interpersonal

Locations where Information is found:

- Email
- Network shares
- Desktops & Laptops
- File cabinets & Desks
- Scanners & Printers

Classifications of Information

Public:

- Information open to the public

Protected:

- Information that must be reviewed for redactions prior to release

Confidential:

- Information that is not open to the public

IT-06: Data Classification Policy

Knowledge Check #1

Who is responsible for Information Security?

A. Information Security Office
B. IT
C. My Supervisor
D. Everyone

What is protected information?

A. Information freely distributable to the public
B. Information available through the Texas Public Information Act or Open Records Requests.
C. Information that is protected from unauthorized disclosure or public release based on state or federal law.

Why is awareness training important?

A. Promotes negative behavior
B. Enhances security
C. It is a waste of my time

Best Practices to Safeguard Information and Information Systems

Section 2

How to Safeguard Against Unauthorized Access and Use

- Don't Reuse Passwords
- Encrypt confidential information
- Audit who has access and authorization to view your information
- Keep track of who accesses your information and when
- Protect personal devices with lock screens & encryption

AWARENESS IS MY ARMOR

How to Safeguard Against Unauthorized Access and Use

- Keep all appropriate doors, cabinets and safes closed and locked
- Don’t store information in inappropriate locations
- Verify vendors or delivery identification
- Lock or sign off when not in use
- Keep unauthorized individuals from seeing and hearing your devices

Safeguarding Information with Multi-Factor Authentication

- DUO – SHSU's multi-factor authentication system
- Remote working and learning caused an increase in cyberthreats
- Over the last year, our security systems have blocked over **55 MILLION** phishing scams
- Multi-Factor Authentication adds an extra layer of security on ALL accounts, including personal ones
- Provides on and off campus information security

Sanitizing and Securely Disposing of Information

- Follow Records Retention Schedule
- Sanitization is a process used to render information unusable or unreadable
  - Encrypt devices
  - Shred paper and media
  - When disposing equipment
    - Securely delete data
    - IT will destroy hard drives and flash drives

Working Remotely

- Never use unsecured public networks
- Secure your remote or home wireless router by
  1) changing the default name of your router and the default wireless SSID.
  2) changing the default password on your router
  3) use WPA2 or WPA3 security
  4) use a firewall – most routers have one built-in, be sure to enable it.
- Use SHSU Devices
- Create a dedicated physical workspace to ensure others cannot see your screen while you work.

Working on Personal Devices

When using a personal computer to work

- Use MyWorkspace or MyAccess
- Verify your computer is encrypted with firewall enabled
- Keep your operating system up to date
- Routinely run anti-malware software
- Run as a limited user, never as a local administrator

Knowledge Check #2

How do you protect your account?

A. Setup Multi-factor authentication
B. Use a different password for each account
C. Lock or sign off devices when not in use
D. All of the above

When protecting your personal computer, you should not

A. Run as a local administrator
B. Keep your Operating System up-to-date
C. Run anti-malware software
D. Use a firewall

AWARENESS IS MY ARMOR

Detecting, Assessing, Reporting and Addressing Information Security Threats

Section 3

Threat, Threat Actor, Risk and Attack

What is a Threat?

A threat is any circumstance or event with the potential to adversely impact organizational operations through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.

Common Threat Actors and Their Motivations

- Poses as a threat to the University
- Four types:
  - Cyber criminals
  - Hacktivists
  - State sponsored attackers
  - Insider threats

What is a Risk?

The probability of exposure or loss resulting from a cyberattack or data breach on your organization.

Risk=Impact X Likelihood

What is an Attack?

An attack is an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Section 3 Quiz

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality

A. Risk
B. Threat
C. Attack
D. Threat Actor

Identifying, Responding To, and Reporting Threats and Suspicious Activity

Section 4

Indicators for Common Attacks

- Antivirus alert
- Pop ups
- Email rules appear
- Password no longer works.
- Sent messages from your email or social media that you didn't send
- Files become inaccessible

If you suspect an attack, report it! Better safe than sorry.

How to Respond to and Report Common Attacks or Suspicious Activity

Social Engineering

- Definition: use of deception to manipulate individuals into divulging information that may be used for fraudulent purposes.
- How to identify: the bad actor will attempt manipulate you into breaking security protocols.
- How to respond: follow all security protocols without exception.
- How to report: submit your report at www.SHSU.edu/report-it.

AWARENESS IS MY ARMOR

Phishing

- Definition: tricking individuals into disclosing sensitive personal information through deceptive computer-based means
- How to identify: check www.shsu.edu/phishbowl; suspicious "From" address; questionable links; uncommon word usage; asking you to do something out of the ordinary and/or with urgency; unexpected attachments
- How to respond: never reply or click on any links in the messages
- How to report: forward the message to abuse@shsu.edu and then delete the message

AWARENESS IS MY ARMOR

Spear Phishing

- Definition: tricking **targeted** individuals into disclosing sensitive information through deceptive computer-based means
- How to identify: check www.shsu.edu/phishbowl; ”From” name seems correct, but “From” address is suspicious; questionable links; uncommon word usage; asking you to do something out of the ordinary and/or with urgency; unexpected attachments
- How to respond: never reply or click on any links; if you know the alleged sender, call using the number in your contacts, not the number in the email
- How to report: forward the message to abuse@shsu.edu and then delete the message

AWARENESS IS MY ARMOR

Quishing

- Definition: Use of quick response (QR) codes to redirect victims to malicious websites or prompt them to download harmful content.
- How to identify: The URL associated with the QR code is **NOT** what you intend to access (Try it out with the QR code to the right).
- How to respond: Don't click to go to that URL or if you did, immediately close your browser.
- How to report: Submit your report at www.SHSU.edu/report-it.

https://www.shsu.edu

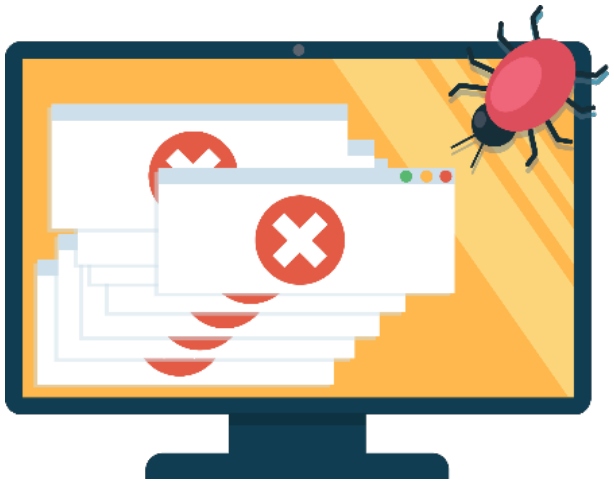
AWARENESS IS MY ARMOR

Scamming

- Definition: using messages to trick you into give them money or unwittingly assist them
- How to identify: too good to be true; boss won't ask for gift cards; unexpected; source address of message is suspicious
- How to respond: never reply or click on any links in the messages
- How to report: forward the message to abuse@shsu.edu and then delete the message

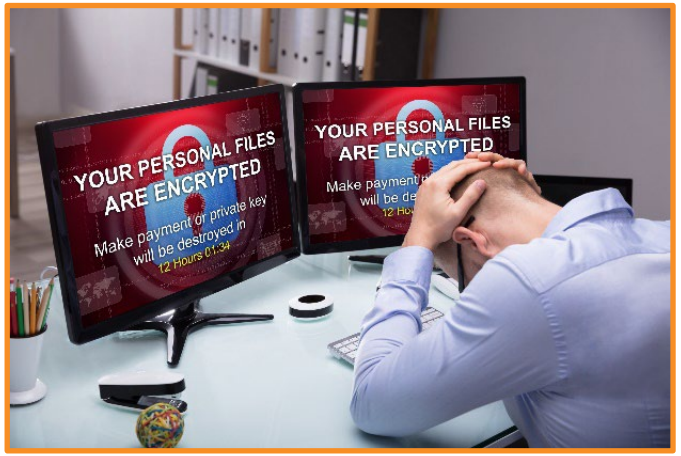
Malware

- Definition: software or firmware intended to perform an unauthorized process that will adversely impact an information system
- How to identify: unexpected popups; new toolbar items; redirected to unexpected webpages; computer may run slower; firewall is disabled; computer may crash regularly; social media or email activity that you did not post/send; anti-malware notification
- How to respond: stop using the device immediately, verify that your security software is up to date and running, run a security scan. If needed, consult an IT professional for personal equipment
- How to report: for SHSU equipment, contact the IT Service Desk immediately



Ransomware

- Definition: malware that requires the victim to pay a ransom to access encrypted files
- How to identify: files on your computer become corrupt or inaccessible; a splash screen may pop up that contains instructions on how to pay the threat actor to regain access to your computer; files may appear on your computer named similar to "decrypt your files" or "open me".
- How to respond: immediately turn off the computer, do not pay, consult an IT professional on personal equipment to restore your system from a backup
- How to report: for SHSU equipment, contact the IT Service Desk Immediately



AWARENESS IS MY ARMOR

Lost or Stolen Devices

- Definition: threat actors may steal your IT devices
- How to identify: device is missing
- How to respond: track your device (Find my Device, etc.) if stolen; remotely wipe your device (Apple, Android, OWA for Active Sync, Deactivate device on Microsoft365)
- How to report: if SHSU confidential information was on the device, report the incident using the https://www.shsu.edu/report-it website. Always file a police report for stolen devices.

AWARENESS IS MY ARMOR

Report IT Security Incidents

- SHSU maintains a website for assisting you with reporting IT security incidents
- https://shsu.edu/report-it
  - Data Breaches
  - Hacking Attempts
  - Physical Attacks on IT facilities or systems
  - Misuse of State Information Resources
  - Lost or Stolen devices
  - Phishing

AWARENESS IS MY ARMOR

Knowledge Check #4

What is the most common attack?

A. Phishing
B. Scamming
C. Malware
D. Ransomware

Where do you report phishing attacks?

A. Your Supervisor
B. abuse@shsu.edu
C. Your co-worker
D. You don’t report, you just delete the message.

Final Thoughts

Section 5

Artificial Intelligence

- Safeguard sensitive and confidential data.
- Use AI responsibly.
- Adhere to established academic integrity policies.
- Adhere to university, system, and state policies when seeking to purchase AI tools.

Technology Prohibited by Regulation

- Due to changes in state and TSUS policies, some devices and software are no longer permitted for State of Texas Institutions.
  - TSUS Technologies Prohibited by Regulation (June 2023): https://www.tsus.edu/about-tsus/policies.html
  - Senate Bill 1893: https://capitol.texas.gov/tlodocs/88R/billtext/pdf/SB01893I.pdf
  - Texas Department of Information Resources: https://dir.texas.gov/information-security/prohibited-technologies

- SHSU Website: https://www.shsu.edu/ProhibitedTech

- Exceptions to the policy must be approved by the university's President. An Exemption Request Form is required to begin this process.

Remember the Bearkat Creed

I AM A **BEARKAT**.
I will **SECURE** my information.
I will **PROTECT** my passwords.
I will **IGNORE** unknown links.
I will **REPORT** sketchy emails.
AWARENESS IS MY **ARMOR**.

I AM A
BEARKAT

Pro Tips

- Update devices regularly (turn on auto-update)
- Enable multi-factor authentication on ALL accounts, not just at SHSU
- Run security software
- Backup your devices
- Remember AWARENESS is your ARMOR so follow the Bearkat Creed against cyberthreats.
- If it sounds too good to be true or has a sense of urgency, it is most likely a phish or scam
- Check the Phish Bowl (https://www.shsu.edu/phishbowl)
- Don't overshare on social media or in conversations
- When in doubt, call the IT Service Desk at (936) 294-1950
- Follow IT Service Desk on social media

AWARENESS IS MY ARMOR

Thank You!

For more cybersecurity articles and tips take a look at our website or follow us:

Contact the Service Desk at 936-294-1950 for any of your technology needs.

AWARENESS IS MY ARMOR

Please click **Exit Course** to close your browser window.