Sam Houston State University

Security Awareness Training

Outline

- Introduction
- SHSU Responsibilities
- Your Responsibilities
- Acceptable Use Basics

Welcome to SHSUs Security Awareness Training. This video was prepared to educate individuals on the basic responsibilities needed to continue utilizing State of Texas information technology resources, and to ensure each person has the knowledge to protect those resources and themselves.

This program applies equally to all individuals granted access privileges to any SHSU information technology resource.

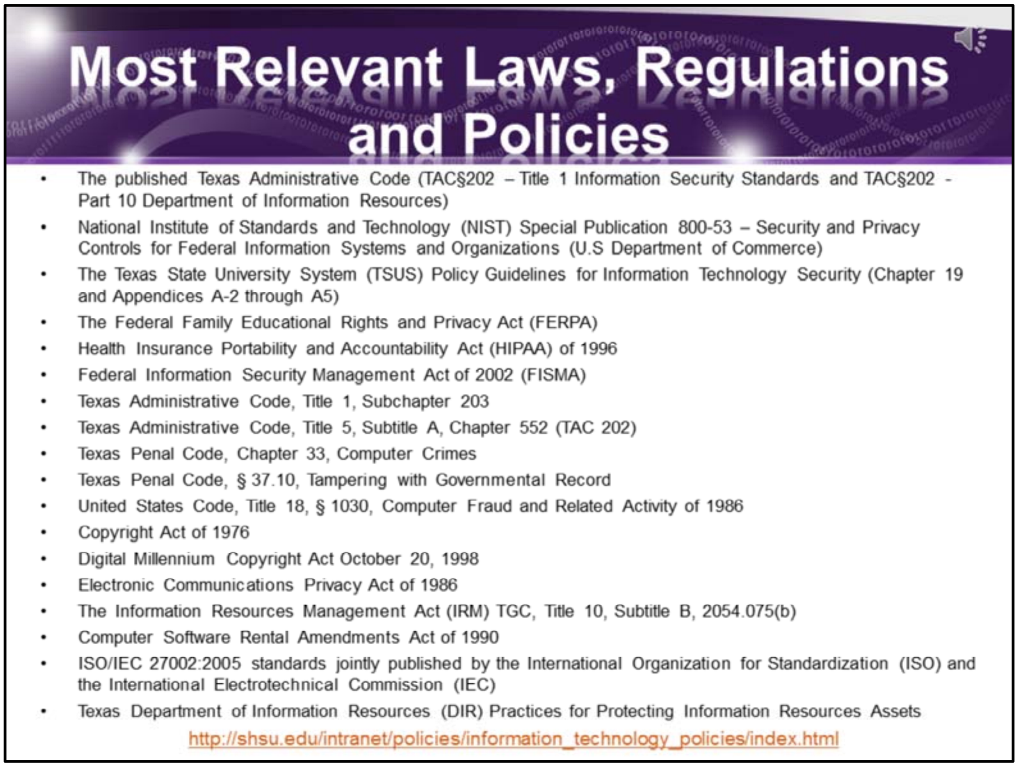
The items we will cover today are:

An Introduction to the laws and policies that govern our security program and where to find them.

The responsibilities of SHSU relating to information security training and education.

Your responsibilities as a user of SHSU information technology resources.

And finally, a review of the acceptable use basics you need to know to be a responsible employee of SHSU.



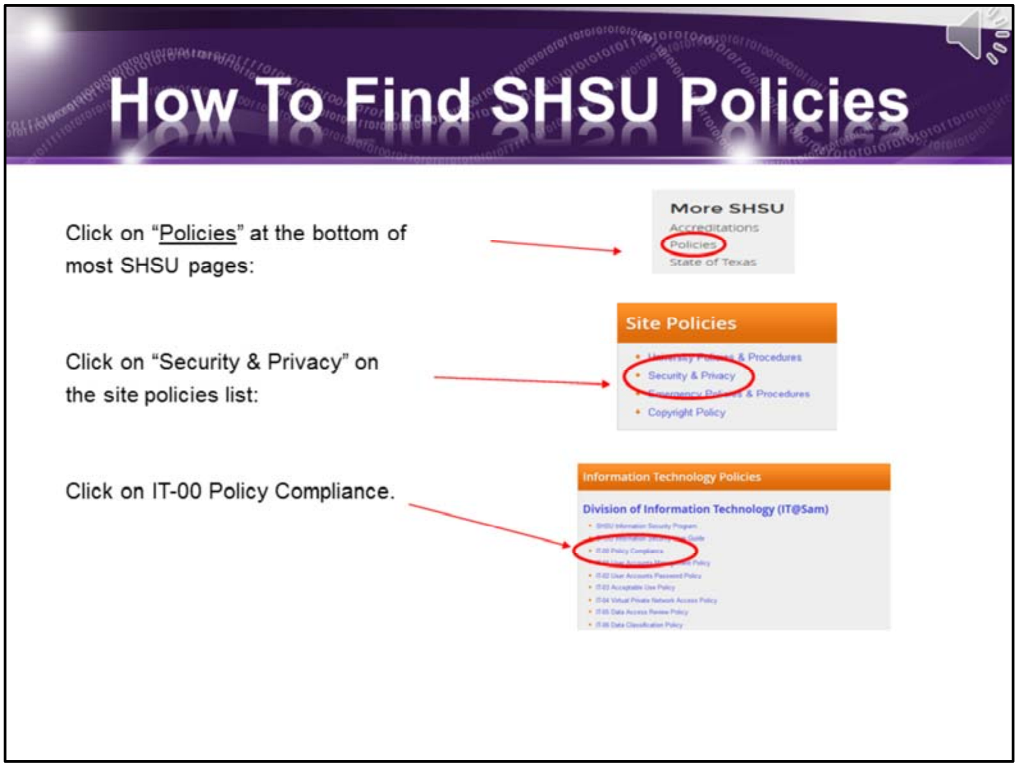
Most Relevant Laws, Regulations and Policies

- The published Texas Administrative Code (TAC§202 – Title 1 Information Security Standards and TAC§202 - Part 10 Department of Information Resources)
- National Institute of Standards and Technology (NIST) Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations (U.S Department of Commerce)
- The Texas State University System (TSUS) Policy Guidelines for Information Technology Security (Chapter 19 and Appendices A-2 through A5)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act of 2002 (FISMA)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Administrative Code, Title 5, Subtitle A, Chapter 552 (TAC 202)
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, § 37.10, Tampering with Governmental Record
- United States Code, Title 18, § 1030, Computer Fraud and Related Activity of 1986
- Copyright Act of 1976
- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B, 2054.075(b)
- Computer Software Rental Amendments Act of 1990
- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Texas Department of Information Resources (DIR) Practices for Protecting Information Resources Assets

http://shsu.edu/intranet/policies/information_technology_policies/index.html

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed here.

Don’t let this lengthy list frighten you, they are listed in IT-00, our Compliance Policy for you to refer to any time you need. I’ll show you how to find the Information Security Policies.



How To Find SHSU Policies

Click on "Policies" at the bottom of most SHSU pages:

More SHSU
Accreditations
Policies
State of Texas

Click on "Security & Privacy" on the site policies list:

Site Policies
- University Policies & Procedures
- Security & Privacy
- Emergency Policies & Procedures
- Copyright Policy

Click on IT-00 Policy Compliance.

Information Technology Policies

Division of Information Technology (IT@Sam)
- SHSU Information Security Program
- SHSU Information Security User Guide
- IT-00 Policy Compliance
- IT-01 User Accounts Management Policy
- IT-02 User Accounts Password Policy
- IT-03 Acceptable Use Policy
- IT-04 Virtual Private Network Access Policy
- IT-05 Data Access Review Policy
- IT-06 Data Classification Policy

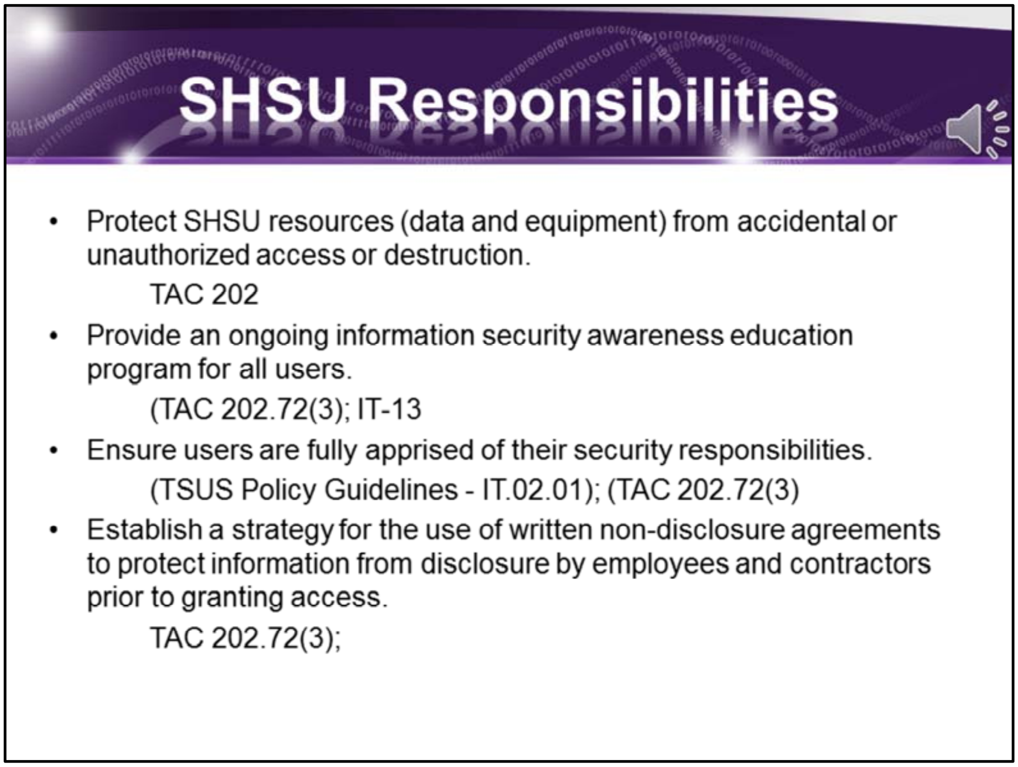
SHSU security policies are derived from the previous list laws, regulations and policies, particularly The Texas Administrative Code (known as TAC 202).
Under the guidance of the Department of Information Resources, these laws were transformed into thirty IT policies and categorized by subject matter
so it s easier to find a particular policy. Our job is to keep the policies up to date and aligned with state and federal laws and guidelines.

At the bottom of most of the SHSU web pages you will find a frame with important links to internal and external sites.

To access all IT policies, click on "Policies" at the bottom of the page.

click on "Security & Privacy" on the site policies list.

Click on the policy that you are interested in (e.g. IT-00) If you have any problems, please contact the service desk.



SHSU Responsibilities

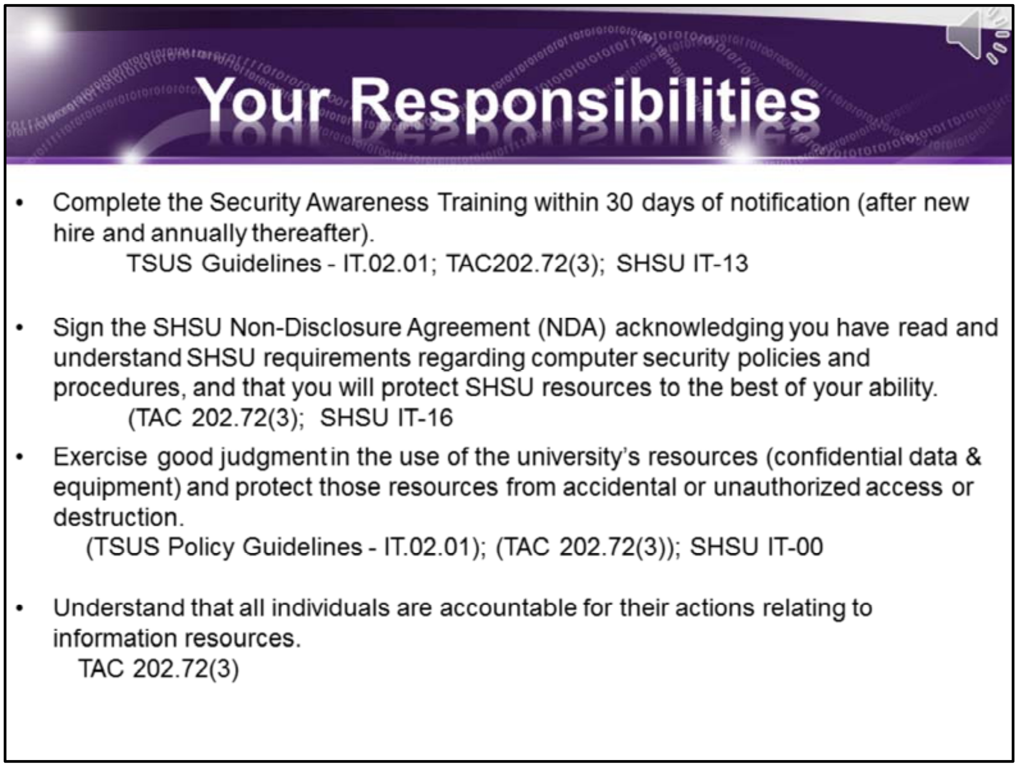
- Protect SHSU resources (data and equipment) from accidental or unauthorized access or destruction.
  TAC 202
- Provide an ongoing information security awareness education program for all users.
  (TAC 202.72(3); IT-13
- Ensure users are fully apprised of their security responsibilities.
  (TSUS Policy Guidelines - IT.02.01); (TAC 202.72(3)
- Establish a strategy for the use of written non-disclosure agreements to protect information from disclosure by employees and contractors prior to granting access.
  TAC 202.72(3);

It’s not only important for you to understand YOUR responsibilities, but it helps to understand ours. We are here to help you.

The following responsibilities are directly from the Texas Administrative Code, TSUS Policy Guidelines, and our own Security Policies identified under each paragraph.

We must protect SHSU resources from accidental or unauthorized access or destruction.
Provide an ongoing information security awareness education program for all users.
Ensure users are full apprised of their security responsibilities.
And establish a strategy for the use of written non-disclosure agreements.

Both the security awareness program and non-disclosure agreements will be administered through the Talent management system.

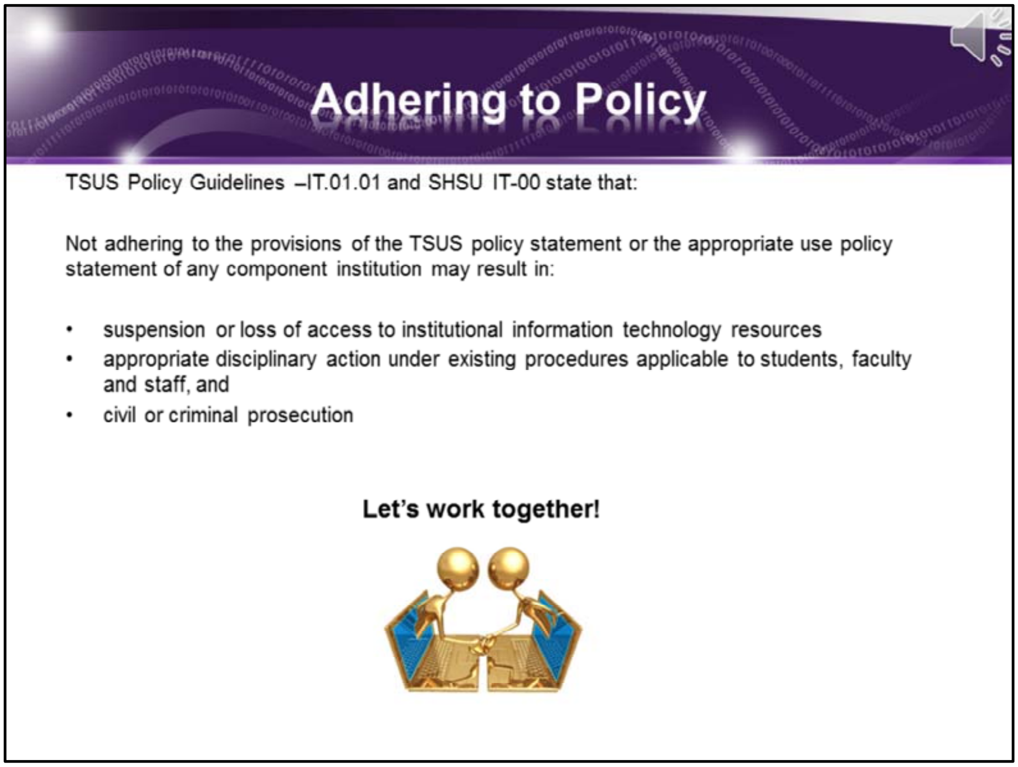


Your Responsibilities

- Complete the Security Awareness Training within 30 days of notification (after new hire and annually thereafter).
  TSUS Guidelines - IT.02.01; TAC202.72(3); SHSU IT-13
- Sign the SHSU Non-Disclosure Agreement (NDA) acknowledging you have read and understand SHSU requirements regarding computer security policies and procedures, and that you will protect SHSU resources to the best of your ability.
  (TAC 202.72(3); SHSU IT-16
- Exercise good judgment in the use of the university's resources (confidential data & equipment) and protect those resources from accidental or unauthorized access or destruction.
  (TSUS Policy Guidelines - IT.02.01); (TAC 202.72(3)); SHSU IT-00
- Understand that all individuals are accountable for their actions relating to information resources.
  TAC 202.72(3)

The following responsibilities, your responsibilities, as directed by the identified Texas Administrative Code, TSUS Policy Guidelines, and our own Security Policies under each paragraph.

You must
Complete the security awareness training, through talent management, within 30 days of notification and annually thereafter.
Sign the Non-disclosure agreement acknowledging you understand SHSU requirements and will protect SHSU resources to the best of your ability.
Exercise good judgment in the use of the university's resources. We will get a little more in depth further into this presentation.
Understand that you are accountable for your actions relating to information resources.



Adhering to Policy

TSUS Policy Guidelines –IT.01.01 and SHSU IT-00 state that:

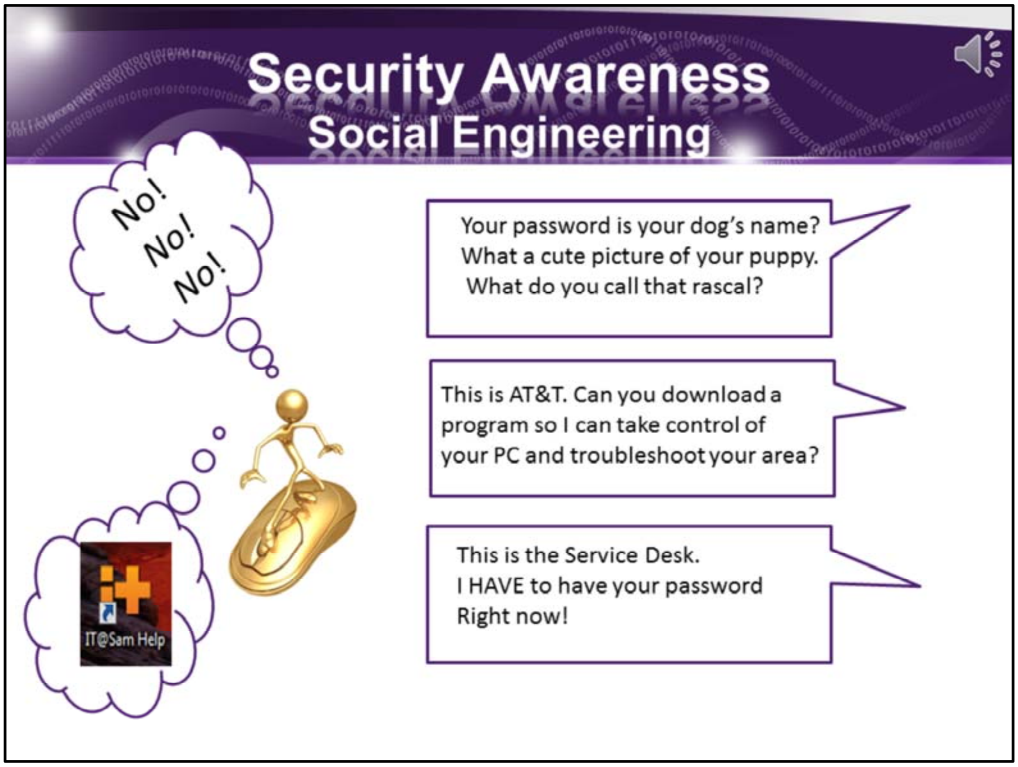
Not adhering to the provisions of the TSUS policy statement or the appropriate use policy statement of any component institution may result in:

- suspension or loss of access to institutional information technology resources
- appropriate disciplinary action under existing procedures applicable to students, faculty and staff, and
- civil or criminal prosecution

Let's work together!

Our guiding authority, Texas State University System's guidelines, requires that you understand the consequences of not adhering to the information security policies. Depending on the severity of your actions and whether a law has been broken, consequences could range from loss of access to the network, suspension, to civil or criminal prosecution.

Let's work together to fulfill our responsibilities and protect our information resources.



Security Awareness
Social Engineering

No!
No!
No!
IT@Sam Help

Your password is your dog's name?
What a cute picture of your puppy.
What do you call that rascal?

This is AT&T. Can you download a
program so I can take control of
your PC and troubleshoot your area?

This is the Service Desk.
I HAVE to have your password
Right now!

Here at SHSU, security is a top priority, which is why we want to inform you about the policies and standards that will protect both you and the university, as well as keep us in compliance with laws and regulations. You help play a big part in information security.

Not only does the law recognize that the #1 reason for data breaches is the Human; but so does the criminal. Criminals target individuals as well as companies. And the best way to get through a company's defenses is through the individual. This is usually accomplished through social engineering, which is psychological manipulation of people into performing actions or divulging confidential information. They trick you into thinking they are your bank, your help desk, a co-worker or your internet provider and convince you to disclose information you normally wouldn't.   If they are asking for information they shouldn't have, or create a sense of urgency or persistence, be wary, they are probably trying to manipulate you.

For example, someone calls you identifying themselves as an AT&T technician and ask you to go out to the internet and download a small program that will help them troubleshoot wireless problems in the area.   Be suspicious. If you are uncomfortable with their request, tell them that you are very busy and ask for a call back number and name to get with later. This will usually make them just hang up.   You can also direct them to the service desk.

Security Awareness

Other Social Engineering

Shoulder Surfer

Very interesting!

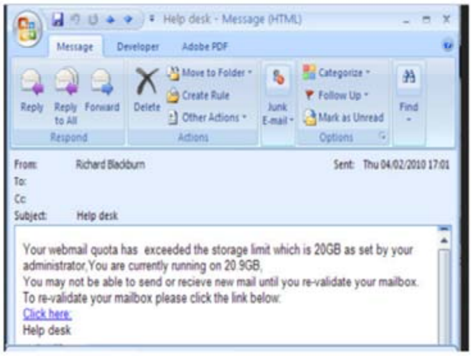
Lock your screen every time you step away

Darn! It's locked…. grumble…
Out to Lunch
+ L

All reasonable precautions to prevent data compromise should be taken when using pcs, laptops, tablets, smart phones, or other campus computing resources. Shield your screen from passive viewing (like "shoulder surfing" which is someone viewing your screen from over your shoulder, and password protect your screen whenever you step away). If you walk away from your computer leaving it logged in and exposed, remember anyone sitting down to use it will have access to anything YOU would have access to – Banner, your payroll information on MySam, etc. Lock your screen by either using the Ctl+Alt+Del keys and Choosing 'lock this computer' or easier still… hold down the Windows key on the keyboard and press the letter L. Your programs will continue to run behind the locked screen, but safe from roaming eyes.

Security Awareness
Phishing

Don’t get hooked….



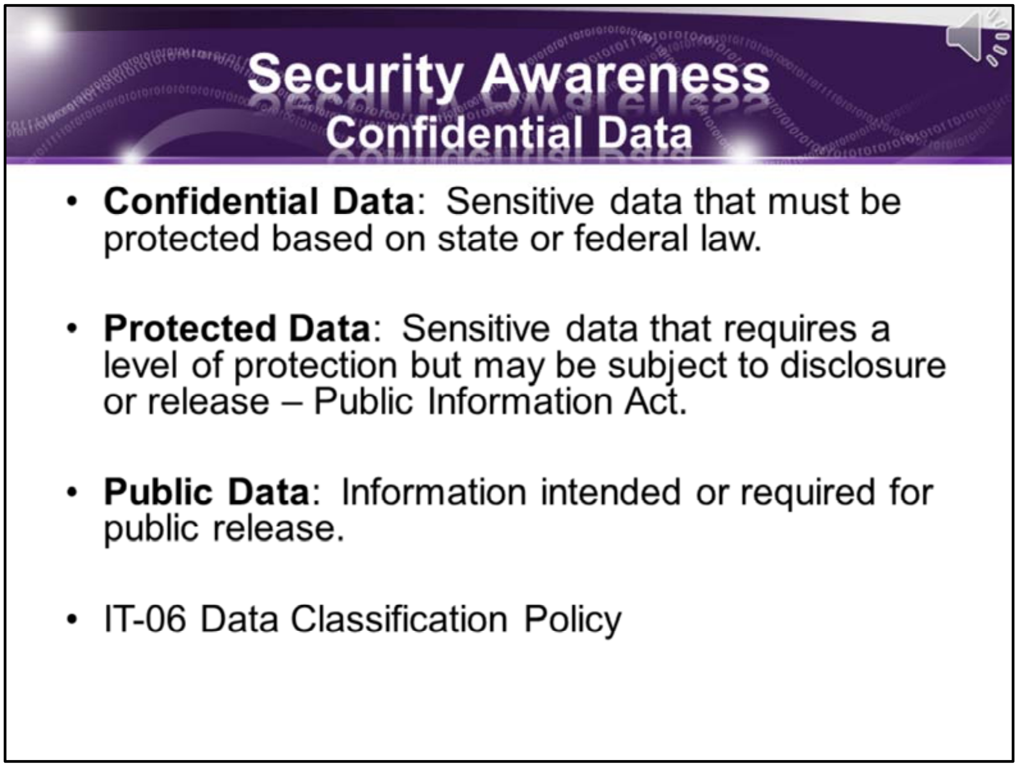
From: Richard Blackburn Sent: Thu 04/02/2010 17:01
To:
Cc:
Subject: Help desk

Your webmail quota has exceeded the storage limit which is 20GB as set by your administrator,You are currently running on 20.9GB,
You may not be able to send or recieve new mail until you re-validate your mailbox.
To re-validate your mailbox please click the link below:
Click here:
Help desk

One of the most common examples of social engineering is phishing. Phishing is the activity of deceiving an individual through email. Usually an email is received from someone you think you trust, with a link to click on that leads to a fake site that requests confidential information. They could be asking for account numbers, personal information, or your log on credentials (username and password) for your bank, home account, SHSU account, etc. Know that SHSU will never send you an email requesting your logon credentials. If you receive one that appears to be from IT@Sam requesting your credentials, do not comply, it is most definitely a phishing scam. If you think an email COULD be from your bank or another trusted source, do not use the link in the email. Go to your browsers list of favorites where you always access that site and log in through it. If there is correspondence from them that is legit, it will be on the REAL page as well.

Be suspicious of any email that threatens to shut down your email account or bank account, any email that looks like it comes from a reputable organization but has bad grammar or misspellings, or one that creates a sense of urgency by requesting Immediate Action. Before clicking on a link, hover your mouse over the link to display the real website and compare to the legitimate website. Don’t click on attachments unless you are expecting them – it could be carrying a virus that will infect your computer without you knowing. If you are suspicious, delete it.

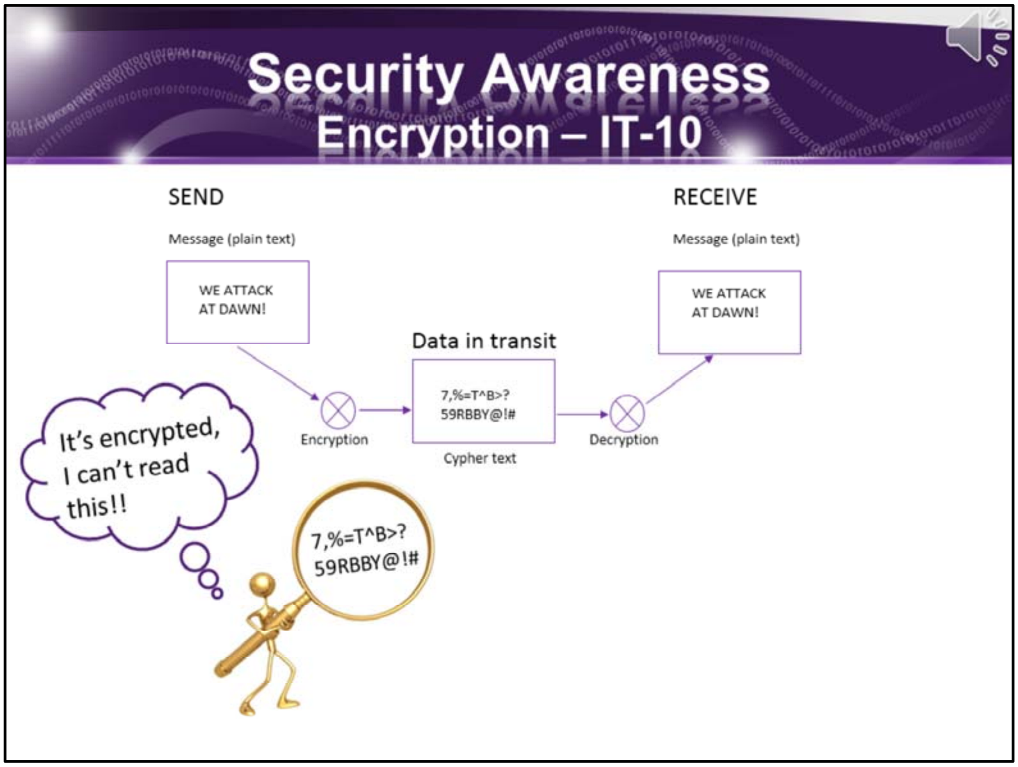
The information you give can end up compromising your account and allow them to gain access to confidential data, bank account information, medical history, or identity theft; or they can gain total control of your computer to hack others or distribute SPAM. If you think they have nothing to gain from accessing your account, remember, whatever you have access to – they will have access to because of Single Sign on. They could open IE and access your MySam portal which has your personal information and payroll information. They would also have access to anything in Banner that you can access, which includes students personal information and grades.



Security Awareness
Confidential Data

- **Confidential Data**: Sensitive data that must be protected based on state or federal law.
- **Protected Data**: Sensitive data that requires a level of protection but may be subject to disclosure or release – Public Information Act.
- **Public Data**: Information intended or required for public release.
- IT-06 Data Classification Policy

Always understand the confidential level of the information that you work with. If you don't know, ask your supervisor. A general description of the different types of information and examples are outlined in IT-06 Data Classification Policy.



Security Awareness
Encryption – IT-10

SEND

Message (plain text)

WE ATTACK AT DAWN!

Data in transit

7,%=T^B>?
59RBBY@!#

Encryption

Cypher text

Decryption

RECEIVE

Message (plain text)

WE ATTACK AT DAWN!

Take care when copying, saving or transporting confidential data. Never attach a document that contains confidential data to an email unless you have encrypted that file.

Unencrypted documents are called 'clear text'. This means if a hacker gains access to your unencrypted document it is read easily in clear text. Encryption 'scrambles' the content of your data with mathematical algorithms to ensure hackers cannot read it, this is called 'cypher text'. The data stays scrambled while it is in transit, so it remains safe.

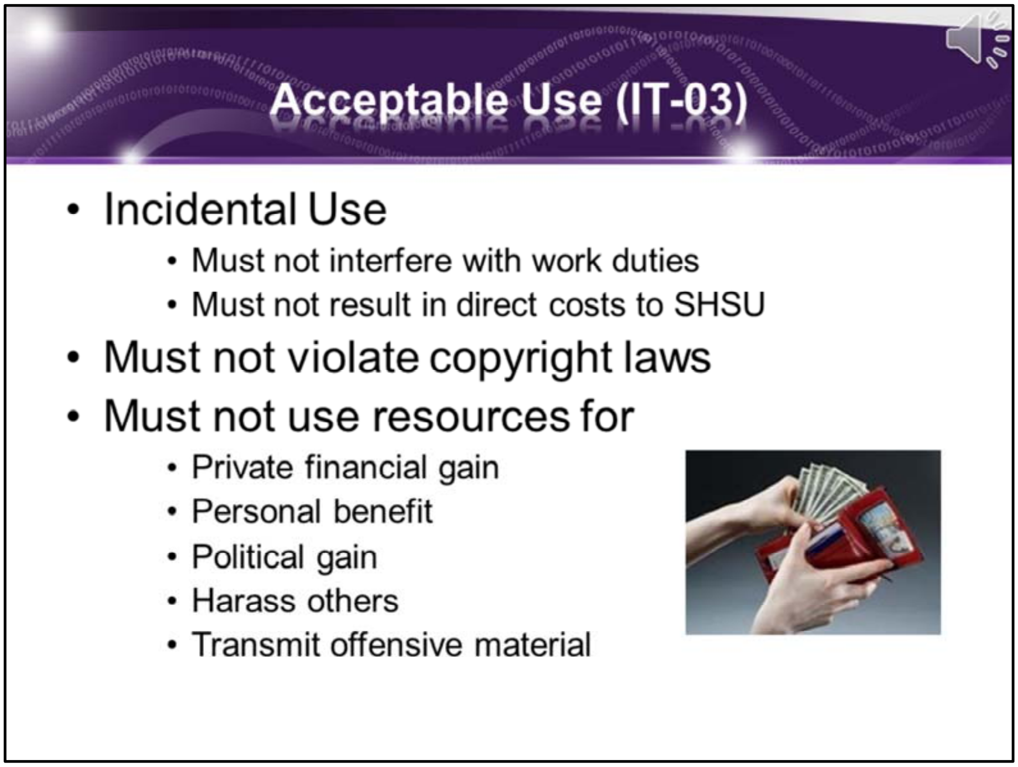
When it reaches it's destination, decrypting will put it back to it's original form.

If you store confidential data on a laptop or tablet, it must be protected with encryption. Please contact the service desk to obtain help with encrypting files and devices.

Never store confidential data on public 'cloud' drives like skydrive, google docs, etc. There is no way we can be assured of the security around that confidential data.

Security Awareness
Web Browsing

When using your web browser to browse the internet, there is always the risk of going to an infected website. . There is no simple way to tell if a website is malicious or has been compromised. Criminals will use unprotected, unpatched browsers to gain control of your computer. SHSU IT@Sam's team patches the university's servers and PCs every month when Microsoft releases them, which remediates any known vulnerabilities, to give you the best possible protection. We ask that you use good judgment when browsing the web. If something looks wrong, it probably is.



Acceptable Use (IT-03)

- Incidental Use
  - Must not interfere with work duties
  - Must not result in direct costs to SHSU
- Must not violate copyright laws
- Must not use resources for
  - Private financial gain
  - Personal benefit
  - Political gain
  - Harass others
  - Transmit offensive material

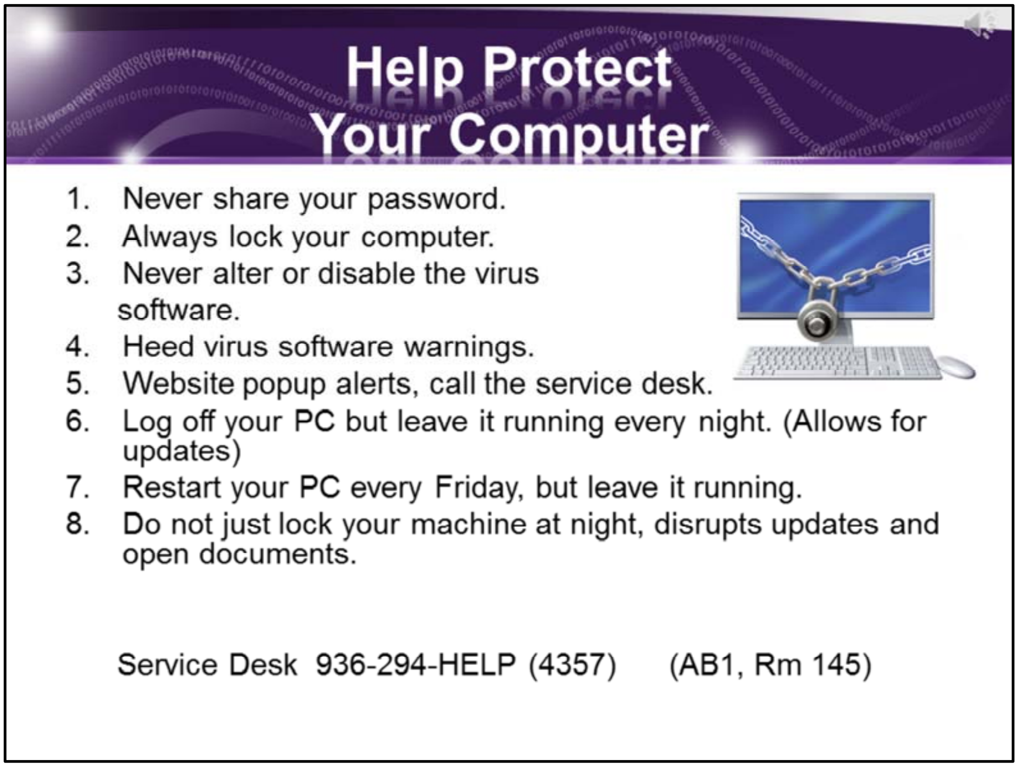
The state of Texas, TSUS system and SHSU allow for “incidental use” while on campus. Incidental use would be “personal use” like checking your personal email, facebook, twitter, etc.
While there is no definitive timeframe for how much time you spend on incidental use, you must check with your individual supervisor to find out if your department has a restriction as to the amount of personal use you are allowed. **Excessive use is determined by your supervisor or department head.**

The laws that govern incidental use:
Personal use must not interfere with the normal performance of an employees work duties.
-must not result in direct costs to SHSU – color printing, etc.

-users must not violate copyright laws – so no downloading protected works such as copyrighted movies or music.

-users must not use the SHSU resources for
private financial gain,
personal benefit (such as running a personal business or trading stocks from SHSU.
or political gain.
-users must not
threaten or harass others or
intentionally access, create, store or transmit material that may be offensive, indecent or obscene.

Again, use good judgment.



Help Protect Your Computer

1. Never share your password.
2. Always lock your computer.
3. Never alter or disable the virus software.
4. Heed virus software warnings.
5. Website popup alerts, call the service desk.
6. Log off your PC but leave it running every night. (Allows for updates)
7. Restart your PC every Friday, but leave it running.
8. Do not just lock your machine at night, disrupts updates and open documents.

Service Desk 936-294-HELP (4357) (AB1, Rm 145)

NOT RECORDED YET:

There are steps you can take to help us protect your computer.
1. NEVER share your password with anyone. Remember it is the keys to the kingdom!
2. Always lock your computer when you are away – Never leave it unattended. “Windows” key +L.
3. Never alter or disable the virus protection software. If there’s an abundance of pop-ups or messages– there’s a reason. Contact the service desk for help.
4. If your virus software warns that there is a problem that cannot be fixed, call the service desk immediately.
5. If you get a pop-up from a website alerting you of any problems, call the service desk immediately. It could be that you have already been infected with a virus or malware.
6. Log off, and leave your computer up and running, every evening so IT@Sam can push the necessary updates to protect your computer. And restart it on Friday evening or first thing Monday morning.
7. Restart our PC.
8. If you just lock your computer leaving yourself logged in overnight, updates might be disrupted. Or worse, there are updates that will restart your computer and open documents could be lost or corrupted.

Help Protect Your Mobile Devices

1. Password protect your phone and tablet.

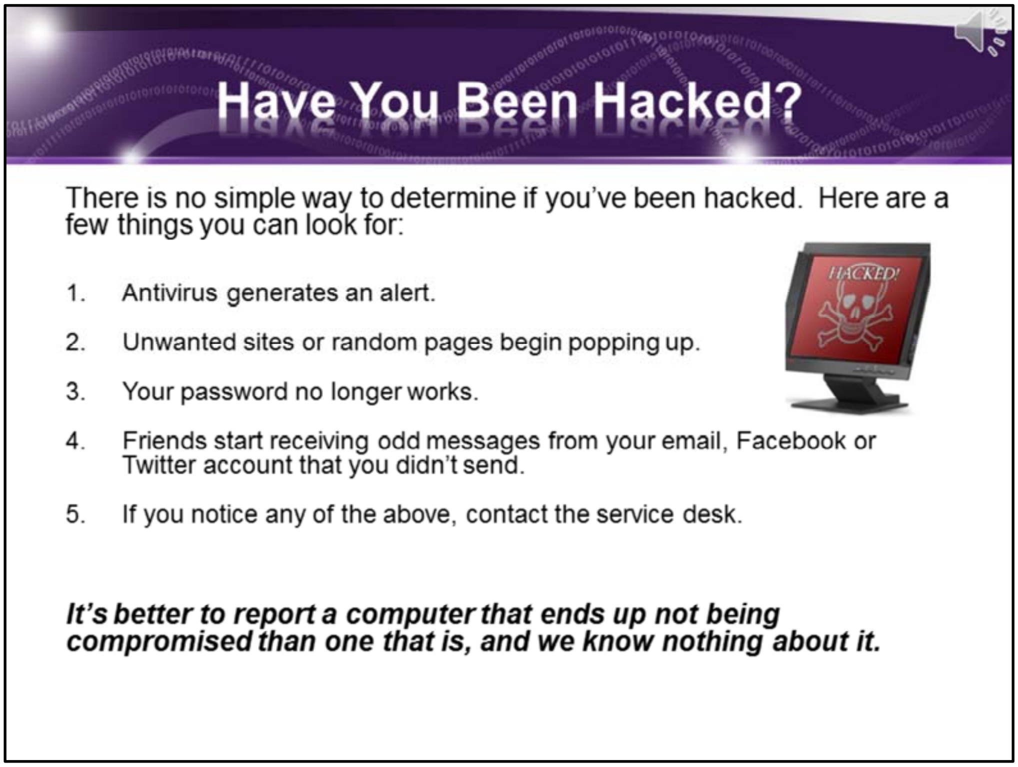
2. Install antivirus and/or malware checker on both & keep it updated. (freeware: AVG, Avast, Malwarebytes)

3. Turn off Bluetooth and WiFi when you are not using it.

4. When using public wireless points, never log into sites that require a password and allow you access to confidential data (bank, credit card).

Protect your Mobile devices both at work and at home. Think of your phone or tablet as a mini-PC – and treat it as such.

1. Password protect your phone or tablet.
2. Install an antivirus or malware checker on your phone and tablet and keep them updated – there are plenty of free apps out there that are great. There's no need to pay for them.
Eg AVG, Avast, Malwarebytes.
3. Turn off Bluetooth and wifi when you are not using it, this will help keep hackers from attacking you when you least expect it.
4. When working on public wireless points, never log in to sites that require a password to allow you access to confidential data like your bank or credit card company. A hacker could be 'sniffing' the open network and pick up your logon credentials – to later log into your account.



Have You Been Hacked?

There is no simple way to determine if you've been hacked. Here are a few things you can look for:

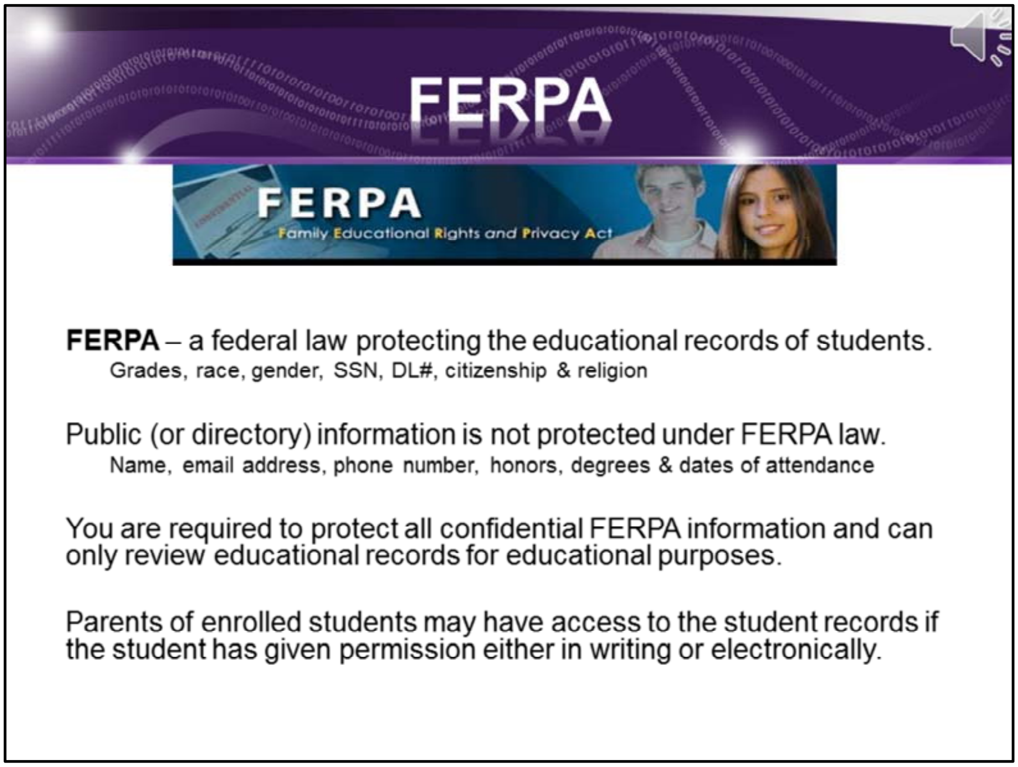
1. Antivirus generates an alert.
2. Unwanted sites or random pages begin popping up.
3. Your password no longer works.
4. Friends start receiving odd messages from your email, Facebook or Twitter account that you didn't send.
5. If you notice any of the above, contact the service desk.

It's better to report a computer that ends up not being compromised than one that is, and we know nothing about it.

Unfortunately, there is no simple way to determine if you've been hacked. Here are a few things you can look for:
Be suspicious

1. If your antivirus generates an alert, this mean there's something unusual going on and it needs to be investigated.
2. If your browser is taking you to unwanted sites or random pages begin popping up, there is a problem.
3. Your password no longer works. Hacker could've already gained your credentials, logged on and changed it. Go thru your 'password reset' process to regain control of your account.
4. Friends start receiving messages from your email, facebook or twitter account that you know you didn't send. Your account has been hacked. Reset your passwords.
5. If you notice any of the above or need help, contact the service desk.

It's better to report a pc that ends up not being compromised than one that is and we know nothing about it.


FERPA
Family Educational Rights and Privacy Act

FERPA

FERPA – a federal law protecting the educational records of students.
Grades, race, gender, SSN, DL#, citizenship & religion

Public (or directory) information is not protected under FERPA law.
Name, email address, phone number, honors, degrees & dates of attendance

You are required to protect all confidential FERPA information and can only review educational records for educational purposes.

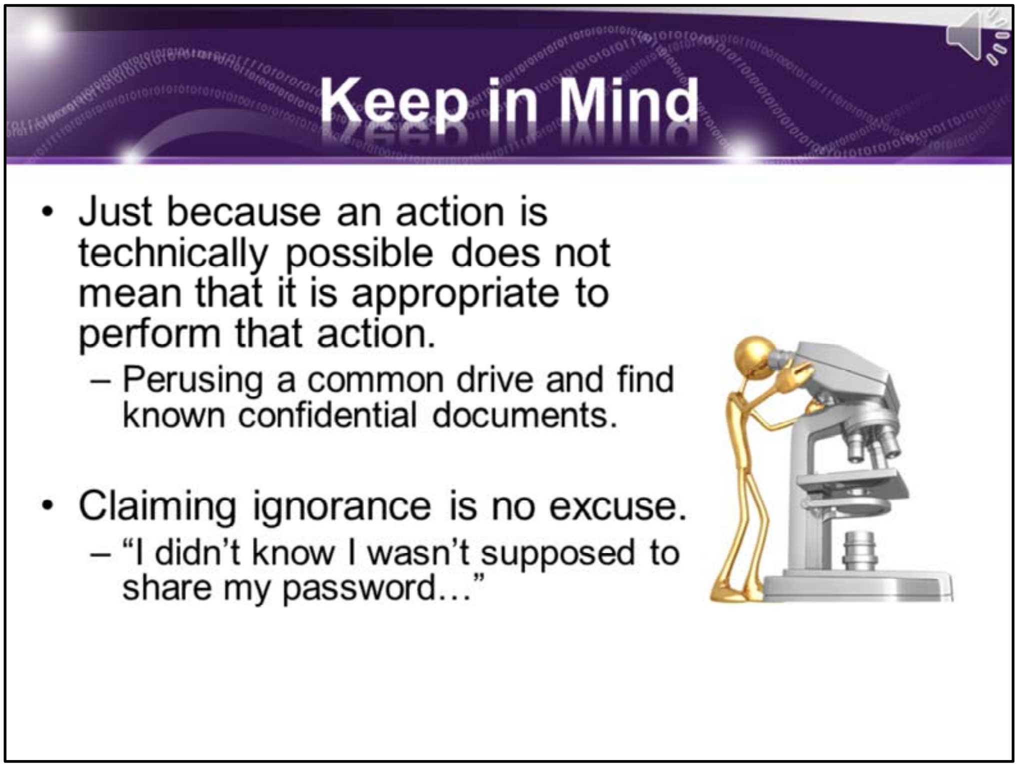
Parents of enrolled students may have access to the student records if the student has given permission either in writing or electronically.

Every university employee is tasked with adhering to FERPA laws
FERPA – a federal law protecting the educational records of students. (eg, Grades, race, gender, ssn, DL#, citizenship and religion)

Public (or directory) information is not protected under the FERPA law, such as: Name, email address, phone number, honors and degrees, and dates of attendance

You are required to protect all confidential FERPA information. This includes discussing the educational records of students with other staff and faculty. You can only review educational records for educational purposes.
An example of educational purposes might be that a student asks you to write a letter of recommendation for him or her. This is a legitimate reason to need to review their educational records.
But if a student applies for a job in your department, you may not review his or her educational records to make that decision – this is not a legitimate educational purpose.

Parents of enrolled students may have access to the student records if the student has given permission either in writing or electronically.



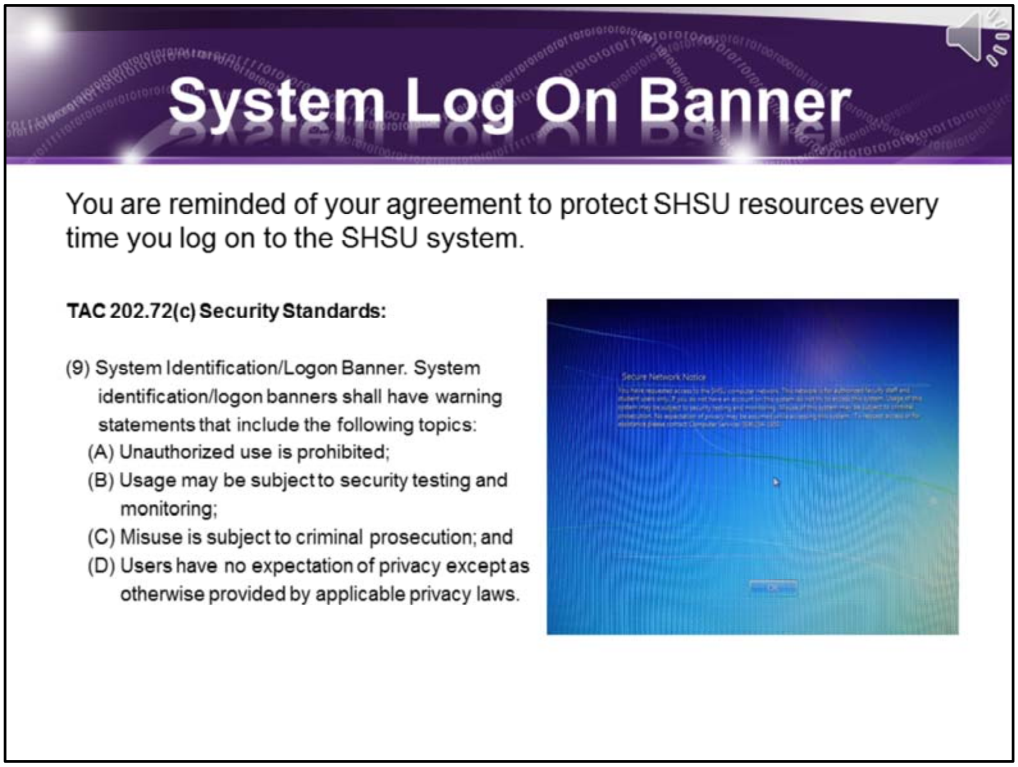
Keep in Mind

- Just because an action is technically possible does not mean that it is appropriate to perform that action.
  - Perusing a common drive and find known confidential documents.
- Claiming ignorance is no excuse.
  - “I didn’t know I wasn’t supposed to share my password…”

There are 2 things to keep in mind:
Just because an action is technically possible does not mean that it is appropriate to perform that action.

For instance, you are in the T: drive- your departmental drive. You come upon a folder named “Performance Evaluations” and open it. Inside you find your co-workers performance evals, filled out with grades and private comments. You know this is information you aren’t supposed to have access to. Use good judgment and ethics. Immediately get out of the folder and contact the service desk. Tell them you ran across a folder that you feel you probably shouldn’t have access to. They will fix the permissions on that folder.

Claiming ignorance is no excuse. Such as “I didn’t know i wasn’t supposed to share my password”. You are exposed to these basics at New Hire Training and annually through Talent Management. In addition, October is Cyber Security Awareness Month where we reinforce the basics of information security campus wide for the entire month.



System Log On Banner

You are reminded of your agreement to protect SHSU resources every time you log on to the SHSU system.

TAC 202.72(c) Security Standards:

(9) System Identification/Logon Banner. System identification/logon banners shall have warning statements that include the following topics:
(A) Unauthorized use is prohibited;
(B) Usage may be subject to security testing and monitoring;
(C) Misuse is subject to criminal prosecution; and
(D) Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

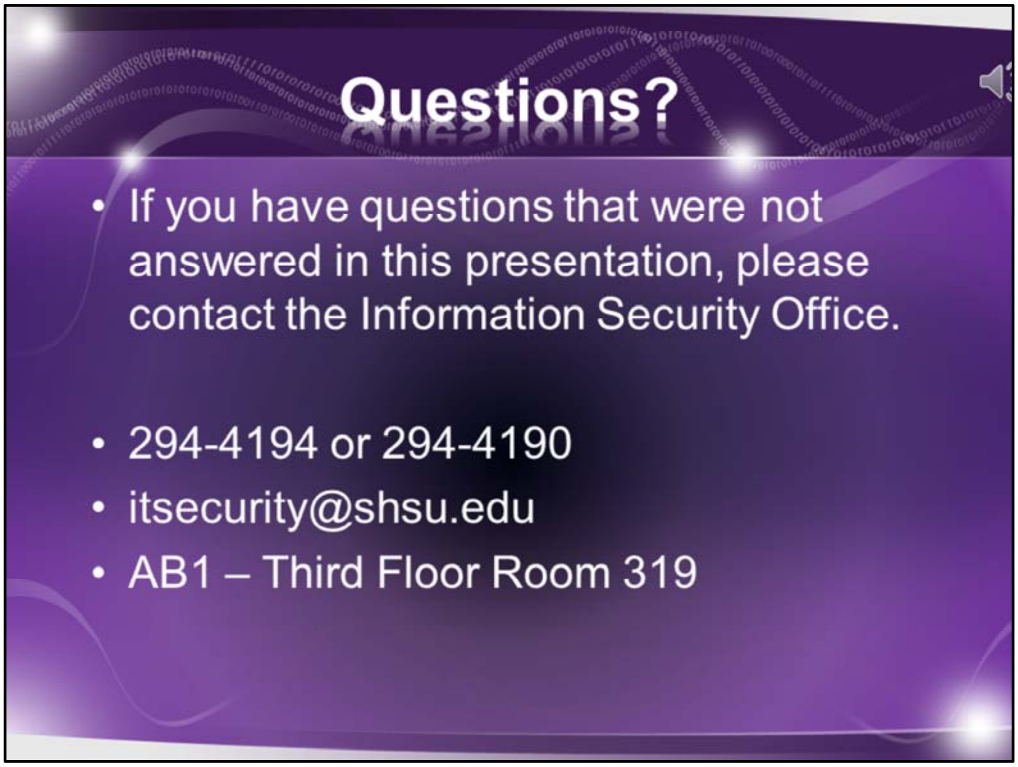
Secure Network Notice

[illegible]

Every time you log into the SHSU network, you are reminded through a System Log On Banner called “Secure network Notice“ of your responsibility to protect SHSU resources.

TAC 202 clearly points out that we are required to remind you every time you log on that:

Unauthorized use is prohibited
Usage may be subject to testing and monitoring
Misuse is subject to criminial prosecution
And users have no expectation of privacy.



Questions?

- If you have questions that were not answered in this presentation, please contact the Information Security Office.
- 294-4194 or 294-4190
- itsecurity@shsu.edu
- AB1 – Third Floor Room 319

This concludes your annual basic security awareness training.

If you have access to special data such as PCI, HIPAA or CJ data, you will have additional training to attend through Talent management.

If you have any questions, please contact the Information Security Office.

To exit this training please click on the “X” at the top right corner of this window.

“To exit this training, please click on the “X” at the top right corner of this window.”