INFORMATION SECURITY AWARENESS TRAINING

FULL COURSE TEXT (LAST REVISED: 2/12/2013)

COURSE INTRODUCTION

INFORMATION SECURITY AWARENESS | SLIDE 1

INSTRUCTION TEXT:
This course contains videos with audio. For the best experience, turn on your speakers or have your head phones ready.

ELEMENT TEXT:
Start Course

HOW TO NAVIGATE | SLIDE 2

INSTRUCTION TEXT:
Would you like to view the navigation instructions for this course?
Click one of the options below.

ELEMENT TEXT:
Yes
No

TEXT:
You can view the navigation instructions at any time by clicking the HOW TO NAVIGATE tab in the top right corner of the course player.

HOW TO NAVIGATE

INSTRUCTION TEXT: Click the forward arrow button in the top right corner to learn about navigating through this course and accessing unique features.

ABOUT THIS COURSE | SLIDE 3

By the end of this course you should be able to identify information security and safe computing practices, and the related policies, rules, and regulations.
There are practice activities and short videos throughout the training which will be used to illustrate certain topics.

This training may take approximately 45-60 minutes to complete.

In order to receive credit for this training, you will need to complete each of the five sections, and acknowledge completion of the training on the last slide.

**QUIZZES | SLIDE 4**

There are 5 quiz questions for each section which will test your knowledge of the concepts/information presented in the section. Answer all five questions correctly in order to complete a particular section. There are two ways of approaching the quizzes.

Option 1: Go through the section and correctly answer the five quiz questions presented at the end. You will have multiple chances to answer these questions correctly.

Option 2: Attempt the five quiz questions before viewing the section. If you get them all correct, you skip to the next section. However, if any are answered incorrectly, you will be taken to the beginning of the section and asked the questions again at the end.

**COURSE OUTLINE | SLIDE 5**

This course is divided into five sections with a course acknowledgement at the end.

- Account Usage
- Authentication
- Confidentiality
- Threats & Protections
- Other Safe Practices

**QUIZ OR VIEW SECTION? | SLIDE 6**

**INSTRUCTION TEXT:**

Topics covered in this section:

- Accountability
- Inappropriate Use
- Incidental Personal Use

Click the option below that best fits your needs.

**ELEMENT TEXT:**

Feeling good! I'm ready to take the quiz.

I would like to review the section first!
SECTION 1: ACCOUNT USAGE | SLIDE 7

Texas A&M University System agencies and institutions grant staff members access to computing resources and facilities through the use of computing accounts, such as e-mail and SSO.

State law requires that all authorized users of the institution of higher education’s information resources formally acknowledge that they will comply with security policies and procedures of the institution/agency before they are granted access to information systems.

(Texas Administrative Code §202.77)

You must take proper precautions to safeguard your account, and information associated with it.

ACCOUNTABILITY | SLIDE 8

Computing accounts are created for each individual so that the actions of those using particular computing resources can be accounted for.

Since computing accounts uniquely identify each user, you are responsible for any activity generated by your account.

SECURITY POLICIES | SLIDE 9

Require that you safeguard your accounts:

- Lock your workstation whenever you step away.
- Log out of sites where you enter your username and password.

VIDEO: LOCKING YOUR WORKSTATION | SLIDE 10

INSTRUCTION TEXT:

Video: Locking Your Workstation

Click one of the options below.

ELEMENT TEXT:

Play video

Skip video

NARRATION:

In this rather short tutorial, I'm going to show you how to lock your workstation.

It just involves pressing 2 keys. The Windows key, located between the Control and Alt key, and the L key.

Just simply hold down the Windows key, and press L, and your workstation will immediately be locked.
WHAT ARE MY RESPONSIBILITIES? | SLIDE 11

Comply with federal, state, and local laws, A&M System policies & regulations, university/agency rules, license agreements (e.g., copyright), & contracts.

- Use computing resources only for their intended purposes or incidental personal use.
- Act responsibly and ethically, and respect the rights of other users in online forums.
- Protect confidential information to which you have access.

CAUTION! | SLIDE 12

Failure to fulfill these responsibilities can lead to:

- The restriction or denial of access to computing resources or computing privileges
- Other disciplinary action by the University or agency
- Law enforcement involvement

INAPPROPRIATE USE | SLIDE 13

Computing accounts and other computing resources are to be used according to the institution’s activities for which they are assigned. However, it is possible to misuse your account and/or other computing resources.

EXAMPLES OF INAPPROPRIATE USE | SLIDE 14

- Allowing someone to use your account or someone else’s account (i.e., sharing accounts)
- Using a computer that has not been logged out of by the previous user (even if you’re not doing anything bad under the account)
- Using your account or computing resources for illegal activities (e.g., viewing or possessing child pornography)

EXAMPLES OF INAPPROPRIATE USE CONT’D | SLIDE 15

- Using your account or computing resources for unauthorized commercial purposes or personal gain
  - To operate or support a business not affiliated with your institution
  - For electronic advertising or spamming efforts

EXAMPLES OF INAPPROPRIATE USE CONT’D | SLIDE 16

- Gaining unauthorized access:
  - Breaking into systems/accounts by cracking passwords
  - Exploiting a vulnerability in order to gain elevated privileges
  - Altering, copying, or deleting data not belonging to you
- Intentionally accessing, creating, or storing obscene materials
EXAMPLES OF INAPPROPRIATE USE CONT’D | SLIDE 17

- Intentionally destroying or damaging equipment, software, or data belonging to the A&M System or other users
- Committing or assisting in acts of theft
- Attempting to circumvent security measures on any network or computer without the permission of the owner

EXAMPLES OF INAPPROPRIATE USE CONT’D | SLIDE 18

- Using computing resources to harass, threaten, or libel someone
  - E-mailing obscene, indecent or lewd material or other material which explicitly or implicitly refers to sexual conduct
  - Transmitting unsolicited information that contains profane language or relates to bigotry, sexism, or other forms of prohibited discrimination

EXAMPLES OF INAPPROPRIATE USE CONT’D | SLIDE 19

Note: Report suspected illegal or inappropriate use to your departmental IT staff and/or supervisor, or a designated reporting function.

INCIDENTAL PERSONAL USE | SLIDE 20

CALLOUT TEXT:
Can I send this personal e-mail?

RESPONSE TEXT:
Incidental Personal Use is an exception to the general prohibition against the use of computing resources for anything other than official state business. It states that employees may occasionally use computing resources for personal reasons, as long as it does NOT:

- Result in additional cost to the state or your University or agency
- Result in financial gain for the user
- Concern business purposes where the business is owned by the employee or the work is done for another business (e.g., consulting work)

INCIDENTAL PERSONAL USE CONT’D | SLIDE 21

- Occur excessively or for long durations
- Interfere with assigned job responsibilities
- Violate existing rules, policies, or laws
ACCOUNT USAGE QUIZ | SLIDE 22

INFORMATION ABOUT QUIZ:
This quiz consists of five questions which are randomly selected from a bank of nine questions. In order to receive credit for this section, you must pass the quiz with a score of 100%.

ACCOUNT USAGE SECTION COMPLETE | SLIDE 23
You have completed the Account Usage section. Click the forward arrow button below to continue.

QUIZ OR VIEW SECTION? | SLIDE 24

INSTRUCTION TEXT:
Topics covered in this section:
- Password Authentication
- Creating Strong Passwords
- Safeguarding your Password

Click the option below that best fits your needs.

ELEMENT TEXT:
Feeling good! I’m ready to take the quiz.

I would like to review the section first!

SECTION 2: AUTHENTICATION | SLIDE 25

Authentication is a means to control access to information resources by verifying the identity of a user logging into an account, or onto a computer or network. Knowledge of the password is assumed to guarantee that the user is authentic. The problem is that passwords can often be guessed, stolen, accidentally revealed, or forgotten. The information in this section can help you mitigate the risks associated with password authentication.

PASSWORD AUTHENTICATION | SLIDE 26

Authentication ensures that the user who attempts to access computing resources and perform functions in a system is in fact the user who is authorized to do so.

Texas A&M University System members use usernames (e.g., NetID) in conjunction with passwords to verify the identity of its users.

PASSWORD AUTHENTICATION CONT’D | SLIDE 27

Since passwords are the first line of defense against unauthorized access to your computer and your accounts, it’s important that you create strong passwords & keep them secure from disclosure.
PASSWORD GUIDELINES | SLIDE 28

INSTRUCTION TEXT:
Click the forward arrow in the top right corner to read the guidelines for creating strong passwords.

ELEMENT TEXT:
Passwords should contain:

- At least 8 characters
- At least 2 special characters (e.g., *$#^-)
- At least 2 numeric characters placed after the first, but before the last, character of the password
- A mix of upper (A-Z) & lower (a-z) case letters

Passwords should NOT contain:

- Keyboard patterns (e.g., qwerty or asdfg)
- Words associated with your school (e.g., Aggie or goTexanns)
- Sequential numbers or letters (e.g., abc123)
- Words or acronyms that can be found in any kind of dictionary (e.g., specialist, foreign language, and technical jargon)
- Consecutive redundant characters (e.g., aaa222bbb)

CREATING STRONG PASSWORDS | SLIDE 29

CALLOUT TEXT:
How do I create a strong password?

RESPONSE TEXT:
When creating your password, make sure it’s NOT:

- Associated with your username, NetID, or UIN.
- Based on personal information. Examples: name/nickname, birth date, child’s name, pet’s name, phone number, etc.
- A word preceded or followed by a number or symbol (e.g., 4secure or secure4).
- A publicized password example (e.g., a password that’s been listed as an example on a website).

CREATING STRONG PASSWORDS CONT’D | SLIDE 30

CALLOUT TEXT:
How do I create a strong password?

RESPONSE TEXT:
• Think of a sentence or phrase that's easy for you to remember, and difficult for others to guess. For example: “We Always Eat Pancakes On Sunday.”
• Convert your sentence to a password that contains the first letter of each word in the sentence. Using the example above, you'd get “waepos.”

CREATING STRONG PASSWORDS CONT’D | SLIDE 31

CALLOUT TEXT:
How do I create a strong password?

RESPONSE TEXT:
• Add complexity by making some of the letters uppercase and adding in or substituting numbers and special characters for some of the letters. Example: “we 6 ^lways Eat 8 Pancakes *n sunday” would become “w6^E8Pk*s.”

Some System members may have additional password requirements. Contact your IT office for more information. Texas A&M University employees may visit, http://hdc.tamu.edu/Connecting/Login_Accounts/Passwords/Tips_For_Creating_Passwords.php.

CREATING STRONG PASSWORDS | SLIDE 32

Tip: Deliberately misspelling one or more words can make your password harder to crack.

VIDEO: CREATING A STRONG PASSWORD FROM AN ACROSTIC | SLIDE 33

INSTRUCTION TEXT:
Video: Creating a Strong Password from an Acrostic

Click one of the options below.

ELEMENT TEXT:
Play video
Skip video

NARRATION:
In this tutorial, I will show you how to create a strong password with an acrostic from a particular saying.

In this example I will start with the phrase: "Don’t Cry Over Spilled Milk" from which I will derive my password. The first thing I will do is take some of more definitive letters from the phrase to make my initial set of letters: capital D, C, O lowercase e and r capital S and M and lowercase l.
From there I will select 3 of these letters and make them into symbols that look very similar. The capital C will become lowercase, the capital O will become an asterisk, and the capital S will become a dollar sign. And lastly I will take two more additional letters and make them numbers. The lowercase e will become a 3 and the lowercase l will become a 1.
This password is very secure and very strong and is not too terribly difficult to remember. Try it yourself with a phrase or saying that you like.

SAFEGUARDING YOUR PASSWORD | SLIDE 34

General Guidelines:

- Don’t share your password with anyone.
- Don’t write it down. If you have to write it down, store it in a secure place, away from your workstation and don’t include the username it’s associated with.
- When you receive a default password, remember to change it immediately after your initial use of it, and continue to change it periodically.

SAFEGUARDING YOUR PASSWORD CONT’D | SLIDE 35

CALLOUT TEXT:

W3H+t2b$E

RESPONSE TEXT:

- The best place to store your password is in your head.
- Never send your password via e-mail.
- Make sure no one is standing nearby when you type in your password (i.e., shoulder surfing).

VIDEO: SHOULDER SURFING | SLIDE 36

INSTRUCTION TEXT:

Video: Shoulder Surfing
Click one of the options below.

ELEMENT TEXT:

Play video
Skip video

DESCRIPTION:

An office worker looks over the shoulder of a fellow employee and steals her password.

AUTHENTICATION QUIZ | SLIDE 37

INFORMATION ABOUT QUIZ:

This quiz consists of five questions which are randomly selected from a bank of eight questions. In order to receive credit for this section, you must pass the quiz with a score of 100%.
AUTHENTICATION SECTION COMPLETE | SLIDE 38

You have completed the Authentication section.

Click the forward arrow button below to continue.

QUIZ OR VIEW SECTION? | SLIDE 39

INSTRUCTION TEXT:

Topics covered in this section:

- General Guidelines for Protecting Data
- Export Controls
- FERPA – Family Educational Rights & Privacy Act
- TPIA – Texas Public Information Act

Click the option below that best fits your needs.

ELEMENT TEXT:

Feeling good! I'm ready to take the quiz.

I would like to review the section first!

SECTION 3: CONFIDENTIALITY | SLIDE 40

Various types of information, such as student records are defined as confidential.

As an employee of the Texas A&M University System, you may have access to confidential information, the privacy of which you are obligated to protect.

CONFIDENTIALITY | SLIDE 41

All university/agency employees are responsible for becoming familiar with Federal and State laws, policies, and rules regarding confidential information in order to ensure that confidential information is appropriately protected and not disclosed to unauthorized persons.

DEFINITION | SLIDE 42

Confidentiality is the guarantee that information is disclosed only to those who are authorized to know it.

The unauthorized or unintended release of confidential information can result in negative publicity for an institution and personal embarrassment.
CONSEQUENCES | SLIDE 43
In instances of higher education, federal funds can be withheld from the entire university if breaches of confidential information are identified as a problem by the Family Policy Compliance Office.
Therefore, it is imperative that you know what information to protect and how to protect it.

BE PROACTIVE | SLIDE 44
If you know, or even suspect, that confidential information has been accessed by or unintentionally released to an unauthorized party, you should report the release to the appropriate person or department immediately.

PROTECTING CONFIDENTIAL DATA | SLIDE 45
The following guidelines apply to student educational records, confidential financial information, protected health information, and other private/personal information.

GUIDELINES FOR PROTECTING CONFIDENTIAL DATA | SLIDE 46

INTRODUCTION TEXT:
Click the forward arrow in the top right corner to learn guidelines for protecting confidential data.

ELEMENT TEXT:

ERR ON THE SIDE OF CAUTION
• When in doubt, don't give it out! If you are unsure as to whether or not to disclose certain information, err on the side of caution and don't release it.

PHONE AND E-MAIL
• Understand that e-mail is not secure; it can be forged, and does not afford privacy. Take precautions not to send anything by e-mail that you wouldn't want disclosed to unintended parties.
• Hold phone conversations and dictation in areas where confidential information cannot be overheard.

PLAN AHEAD
• Make arrangements to immediately retrieve or secure any document containing protected information that's printed, scanned, copied, faxed, etc.
• Position computer screens so they're not visible to anyone but the authorized user(s).
**DOCUMENTS**

- Store documents or physical media containing confidential information in locked file cabinets or drawers and hide the keys in a secure area (i.e., not in plain view or in an unlocked desk drawer).
- Encrypt confidential data stored on computers, portable computing devices (e.g., laptops and PDAs), or portable media (e.g., CDs, DVDs, or external hard drives).

**SHRED PAPER AND/OR CDS**

- Shred paper documents and/or CDs containing confidential information before disposal, and secure such items until shredding.

**EXPORT CONTROLS | SLIDE 47**

In today’s world, the collaboration of ideas and information is easier than ever before. However, there are some types of information, technologies, and goods and services that may be restricted by United States export control laws.

**WHAT ARE EXPORT CONTROL LAWS? | SLIDE 48**

Export control laws and regulations restrict or prohibit the transaction of business with certain countries, persons, and entities that have been sanctioned by federal agencies as a threat to important U.S. interests. Export control laws regulate the conditions under which certain information, technologies, and goods and services can be shared with foreign persons or entities in the United States or abroad.

**WHAT ARE EXPORT CONTROL LAWS? | SLIDE 49**

Most exports do not require specific approval from the federal government. Certain exports, however, require a license. Others are prohibited.

All A&M System employees must conduct their affairs in accordance with United States export control laws and regulations.

**HOW MIGHT THIS APPLY TO ME? | SLIDE 50**

Traveling outside the United States may trigger export control issues if you take your computer or other similar equipment with you.

Why?
Your computer may contain export-controlled encryption source code, or information relating to an export controlled research project you may have worked on. Additionally, the computer itself may be controlled depending on the country.
WHAT CAN I DO TO MAKE SURE I AM NOT IN VIOLATION? | SLIDE 51

To avoid an unintentional violation of the law, you should familiarize yourself with export control requirements. Additionally, consult your institution’s export control office for guidance when hiring foreign persons, speaking at multinational conferences, shipping items out of the country, and/or conducting business with international entities and foreign persons.

WHAT CAN I DO TO MAKE SURE I AM NOT IN VIOLATION? | SLIDE 52

If you are not sure who your Export Controls representative is, Texas A&M’s Export Controls Program can assist in directing you to the appropriate contact (ExportControls@tamu.edu, 979-862-6419).

Additional information can be found on the TAMU export control website.

FERPA | SLIDE 53

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student educational records, and prohibits the University from disclosing information from those records without the written consent of the student.

The security and confidentiality of student educational records is a matter of concern to all those who possess or process these records.

ABOUT FERPA | SLIDE 54

INTRODUCTION TEXT:

Click the tabs on the left to learn more about FERPA.

ELEMENT TEXT:

INTRODUCTION

Those who work with or have access to student educational records must:

- Understand what an educational record is;
- What information within the record may be disclosed; and
- To whom it may be disclosed.

Click the blue tabs on the left to learn more about FERPA.

EDUCATIONAL RECORDS

An educational record is any record directly related to a student that is maintained by an institution or by an agent acting directly for the institution.

It may be maintained in any medium: print, film, handwriting, electronic text (including ANY information displayed on a computer screen), etc. Examples: transcripts, grade reports, class rosters schedules, and ANY document containing information related to a student.
WHAT IS SPI?

Sensitive Personal Information (SPI): An individual’s first name or first initial and last name in combination with any one or more of the following items (if the name and items are not encrypted):

- Name, Social Security number, date of birth, or government issued identification number;
- Driver’s license number; or
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

All SPI should be encrypted, and unneeded SPI should be eliminated.

Note: Historical Social Security numbers should be replaced with UINs where feasible.

WHO MAY HAVE ACCESS?

University officials such as:

- Faculty & staff with a legitimate educational interest in a student’s record
- Agencies or organizations from which the student has received financial aid
- Officials from other educational institutions in which the student is seeking to enroll
- Students serving on official University committees or assisting eligible faculty and staff (teaching assistants, student workers, etc.)

Legitimate educational interest is any authorized interest or activity undertaken in the name of the University for which access to an educational record is necessary or appropriate to the proper performance of the undertaking.

DIRECTORY INFORMATION

Directory information is public information. Universities of the Texas A&M System are permitted to release this information without the student’s consent.

However, if the student has placed a hold on any directory information, it cannot be released without the prior, written consent of the student.

Check with your local registrar’s office for more information.

SAFEGUARDING PRIVACY

- Don’t leave student information lying out on your desk or left up on your computer screen when you are away from your desk.
- Grades should not be posted publicly, unless the form or method of posting can guarantee (absolute) anonymity.

Questions concerning FERPA may be referred to your Associate Registrar.
NON-DIRECTORY INFORMATION

To whom and under what conditions can non-directory information be disclosed without the written consent of the student?

- University officials who have legitimate educational interests
- Officials of another school in which the student seeks or intends to enroll
- U.S. Comptroller General, Secretary of the U.S. Dept. of Education, U.S. Attorney General, state and local educational authorities
- Third-party contractors, specifically, the National Student Clearinghouse
- Financial Aid representatives
- Law enforcement agents who have a lawfully issued subpoena
- Parent of a student under the age of 21 – for the disclosure of the student’s violation of any federal, state, or local law

PARENTS’ RIGHTS

Non-directory information may be released to parents or court-appointed guardians if:

- The student is claimed as a dependent on the parent/guardian’s Federal Income Tax Return.
- A Certification of Dependency form signed by the parent/guardian is on file with the Office of the Registrar prior to release. Contact your local registrar for more information.

SPOUSES

Spouses have no right of access to a student’s records, because:

- The Certification of Dependency form does not cover students’ spouses.
- Non-directory information (including class schedule) may be released to a student’s spouse only with a signed authorization from the student.

For more information, go to Ed.gov or TAMU's FERPA page.

TPIA | SLIDE 55

The Texas Public Information Act (TPIA), formerly known as the Open Records Act, specifies that all recorded information owned or accessed by a governmental body is presumed to be public information with certain exceptions.

EXCEPTIONS TO THE DISCLOSURE REQUIREMENTS | SLIDE 56

- Student educational records
- Restricted employee information (e.g., home address and phone number)
- Audit working papers
- Select personal information withheld from disclosure by the owner
EXCEPTIONS TO THE DISCLOSURE REQUIREMENTS CONT’D | SLIDE 57

- Information related to technological and scientific products, devices, or processes (including computer programs) that were developed at a state institution of higher education and have a potential for being sold, traded, or licensed for a fee
- Other information expressly prohibited by law

RIGHTS OF EMPLOYEES | SLIDE 58

CALLOUT TEXT:  
Do I want my address to public?

RESPONSE TEXT:

Each present and former official and employee shall decide whether to allow access to his/her home address and phone number, and whether the person has family members.

Newly hired employees will be provided a form which, when signed and returned, will restrict such access.

A change may be made in the status of the access by written notification to the personnel officer of the organization.

PUBLIC INFORMATION | SLIDE 59

Individuals seeking public information shall submit a written request to the appropriate public information officer (http://www.tamus.edu/offices/legal/openrecords-officers/).

Public information officers are required to promptly examine, approve, and release requested information.

For more information, visit www.txdps.state.tx.us/pia.htm

CONFIDENTIALITY QUIZ | SLIDE 60

INFORMATION ABOUT QUIZ:

This quiz consists of five questions which are randomly selected from a bank of eight questions. In order to receive credit for this section, you must pass the quiz with a score of 100%.

CONFIDENTIALITY SECTION COMPLETE | SLIDE 61

You have completed the Confidentiality section.

Click the forward arrow button below to continue.
INSTRUCTION TEXT:
Topics covered in this section:

- Malware
- Spyware
- Patches
- Personal Firewalls
- Social Engineering
- Phishing

Click the option below that best fits your needs.

ELEMENT TEXT:

Feeling good! I’m ready to take the quiz.

I would like to review the section first!

SECTION 4: THREATS & PROTECTIONS | SLIDE 63

There are many types of harmful and malicious threats that one might encounter when using a computer. Some threats are simply designed to cause damage to a computer, while others are designed to capture private and confidential information.

In this section, we’ll discuss some of the more common threats and what you can do to protect yourself and your computer from them.

ABOUT MALWARE AND SPYWARE | SLIDE 64

INTRODUCTION TEXT:

Malware is a generic term for software or code that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user’s information systems. Examples: viruses, worms, Trojan horses, Attack scripts and spyware.

To learn more about malware and spyware, click the forward arrow button in the top right corner.

ELEMENT TEXT:

WHAT CAN MALWARE DO?

Malware can:

- Delete or change files
- Erase your hard drive
• Release confidential information stored on your computer by e-mailing it to random e-mail addresses or the address of the virus writer
• Change your security settings

**HOW DO I KNOW MY COMPUTER IS INFECTED?**

Signs your computer may be infected:

• Programs open and close on their own, or no longer work
• Files are missing or unknown files appear
• Your computer suddenly runs significantly slower than normal
• Random error or warning messages begin to appear

**HOW CAN I PREVENT MALWARE?**

How to prevent malware from infecting your computer:

• Install antivirus software and keep it up-to-date. Check with your IT personnel to find out if you already have antivirus software installed on your computer, or if you have any questions.

**MORE TIPS**

• Scan files from portable media (e.g., CDs/DVDs, zip disks, or thumb drives) before opening them. You can do this manually, or you can set your software to automatically scan files being transferred to or copied from external media.
• Be cautious of unusually large e-mail attachments or those with executable extensions (e.g., .com, .exe, .bat, .vbs, .dll). Recognizing the name in the "FROM:" line does not ensure that the attached file is virus-free.

**ABOUT SPYWARE**

Spyware is a type of software installed on your system to capture and reveal information to third parties.

Spyware can:

• Capture keystrokes to collect passwords and information (e.g., credit card numbers) typed in web-based forms
• Read and track e-mail
• Record browsing habits (e.g., sites visited and links clicked) and tailor advertisements to these patterns
WHAT ARE THE SIGNS MY COMPUTER HAS SPYWARE?

Signs your computer may have spyware:

- Pop-up advertisements appear when your Internet browser is closed
- Your home page or search settings have changed without your knowledge
- You are redirected to websites other than the one you typed into the address bar
- New, unexpected toolbars appear in your web browser

HOW CAN I PROTECT MY COMPUTER FROM SPYWARE?

How to protect your computer from spyware:

- Use anti-spyware software.
- Don't click on pop-up advertisements or the links within them. Close them by clicking on the "x" in the upper right hand corner of the window.
- When installing something on your computer, carefully read the “End User License Agreement” (EULA), and make sure it doesn’t state that the vendor is allowed to install third-party software on your computer. This third-party software could include spyware.

MORE TIPS

How to protect your computer from spyware:

- Be wary of free downloadable software (e.g., subscriptions to online services, tool bars, screen savers, game demos, video clips, and programs), because spyware may be included.
- Don’t follow e-mail links claiming to offer anti-spyware software. These may actually be used to install spyware on your computer.

PATCHES | SLIDE 65

Patches are updates for your operating system (e.g., Mac, Linux or Windows) that fix problems that are found after the operating system has been released.

PATCHES CONT’D | SLIDE 66

In order to ensure your operating system is up-to-date, you should routinely download and install the latest security patches from your product vendor website, or configure your computer to perform these updates automatically.

If you have any questions about patches or patch management, please contact your local IT administrator.

PERSONAL FIREWALLS | SLIDE 67

A personal firewall is a piece of software that creates a protective barrier between your computer and potentially harmful content on the Internet. It can monitor communications to and from your computer, and allow you, the user, to permit or deny incoming and outgoing internet traffic (e.g., connection requests).
PERSONAL FIREWALLS CONT’D | SLIDE 68

Firewalls can block/notify the user of intrusion attempts, but they cannot protect against malware, so make sure you have some type of antivirus software installed on your computer and that you keep it up-to-date.

Also be sure to install and configure your firewall correctly; otherwise it will not work properly.

If you have any questions about firewalls or their use, please contact your local IT administrator.

SOCIAL ENGINEERING | SLIDE 69

Social Engineering is a practice of deceiving an individual in order to obtain information, and is often linked to malicious activities, such as identity theft.

It can be technical or non-technical, and can occur in person, over the phone, and online (e.g., phishing).

ABOUT SOCIAL ENGINEERING | SLIDE 70

INTRODUCTION TEXT:

Social engineering attacks are often successful because they exploit the human tendency to trust and the desire to be helpful. Click the blue tabs on the left to learn how you can recognize social engineering, and what you can do to defend yourself.

ELEMENT TEXT:

SOCIAL ENGINEERING TACTICS

Social Engineering Attacks often involve psychological triggers such as:

- Reciprocation - An attacker may set up a situation where the target encounters a problem, and must ask the attacker for help. Once the problem is solved, the target then feels obliged to return the favor, and perhaps gives out the information requested by the attacker.
- Instilling a sense of urgency in the target - Attacker may claim that "this is really urgent" or "if this isn't done before (a certain time) we are going to be in trouble with the auditors." Attackers rely on the fact that people under pressure make hasty decisions and often do things they normally wouldn't do.

HOW TO DEFEND AGAINST ATTACKS

There are many ways to defend against Social Engineering attacks (on the phone and in person):

- Be aware of the methods behind social engineering attacks, and retain a degree of skepticism.
- Think before you act or release information.
• Don’t avoid challenging (in a customer-friendly way) or verifying the credentials or requests of anyone you are uncertain about, regardless of the position or title he/she claims to have, how he/she is dressed, or how urgent his/her request may be.
• Don’t hesitate to notify your IT department or consult others regarding those you may have doubts about.
• Remember that no matter who you are, you can be vulnerable to a social engineering attack.

### EXAMPLES OF VERIFICATION PROCESSES

Always verify the identity of a person before giving him/her sensitive information such as:

• Ask the caller for his/her name and company or supervisor’s name. Seek the company’s or supervisor’s phone number from another source, and then call that number to verify the identity or validity of the caller.
• Put the caller on hold and seek advice from your supervisor - this also allows valuable thinking time.

### PHISHING | SLIDE 71

**CALLOUT TEXT:**

Subject: Online Alert? What could this be about?

### PHISHING | SLIDE 72

**RESPONSE TEXT:**

Phishing, an electronic form of social engineering, is an attack that relies on a combination of fraudulent messages and **spoofed websites** to deceive people into divulging personal or financial information.

### PHISHING CONT’D | SLIDE 73

**CALLOUT TEXT:**

What?! My bank says I won’t be able to access my account?!

### PHISHING CONT’D | SLIDE 74

**RESPONSE TEXT:**

Typically, phishers send an e-mail message made to appear as though it came from a legitimate bank or other business. They do this by spoofing brand names and logos.
PHISHING CONT’D | SLIDE 75

CALLOUT TEXT:
I’m supposed to click this link to verify my account? Wait! This has to be a scam!

PHISHING CONT’D | SLIDE 76

RESPONSE TEXT:
The message usually asks for some form of sensitive information or contains a link leading to a fraudulent website where the visitor is prompted to type in sensitive information.

SIGNS OF A PHISHING E-MAIL | SLIDE 77

INTRODUCTION TEXT:
Phishing is often a successful type of social engineering because it’s difficult to recognize phishing e-mails and determine the difference between legitimate websites and ones created by phishers to mimic legitimate websites.

Click the forward arrow button in the top right corner to learn how to identify a phishing e-mail.

ELEMENT TEXT:

GENERIC GREETING
Some phishing e-mails sent out in bulk are generically addressed to the e-mail recipients. However, this does not mean e-mails which address you specifically (e.g., by name) are legitimate, because sophisticated phishing e-mails can also be explicitly addressed to recipients.

VERIFYING ACCOUNT REQUEST
A request to update or verify your account information. Legitimate companies normally don’t ask for personal information by e-mail, especially if it’s information they should already have.

URGENCY
An urgent sounding phrase. Example: “If you do not respond in the next 48 hours, your account will be deleted.”

LINKS AND ATTACHMENTS
The e-mail encourages you to click on a link in the message, which leads to a login screen or form where you’re required to input sensitive information. Additionally, some phishing e-mails also have attachments that contain viruses or malware to weaken your computer’s security.
Click the forward arrow button in the top right corner to learn tips on how to avoid phishing scams.

**BE CAUTIOUS**

- Resist the impulse to act immediately without thinking. If you’re concerned about your account, go to the claimed sender’s official website by typing the web address (URL) directly into your browser and verify the request.
- Don’t respond to a suspect or “phishy” e-mail or use the contact information (e.g., e-mail address or phone number) presented in the message.

**BE WARY OF LINKS AND ATTACHMENTS**

- Don’t click links within the e-mail. The link could lead to a malicious website where keystroke loggers are waiting to capture the information you type in.
- Check the legitimacy of the link(s). Right-click the link and select Properties. Compare the link in the pop-up window to the one listed in the e-mail or on the web page. If they don’t match, you may not want to click the link.
- Be cautious about opening attachments and downloading files from e-mails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer’s security.

**VIDEO: VERIFYING A WEBSITE’S AUTHENTICITY**

**NARRATION:**

This tutorial is about to show you how you can validate a website as authentic.

And for those of you who do not know why this is important, a fake website can appear to be legitimate in every sense from graphics to web address, but underneath all that it’s simply a website to gain confidential information from you.

Now here in this example, we have the Information Technology Issues Management Secure page. It looks completely normal; same text, graphics, and web address, but we aren’t entirely sure if this is the correct site.

So what we should do is go down to the lower right corner of our browser and double click this inconspicuous lock icon. After you do so, you will see a window open up for you. If you click on the General tab at the top, you will be shown what we are looking for.

And you can see here that the address in the certificate is the exact same as the address in the URL. This means that we are at the legitimate site.
AVOID POP-UP WINDOWS

- Don't enter personal or financial information into pop-up windows. A common phishing technique is to launch a pop-up window when someone clicks a link in a phishing e-mail.
- Sometimes a pop-up will be displayed over a website you trust. Don't be fooled, close popup windows by clicking the “X” in the upper right corner.

EXAMPLES OF PHISHING SCAMS

Chase Bank

The People's Bank
http://www.thepeoples.com/index.cfm?objectid=C3BFCCCA-D60E-C259-6B0C2FECB815FBCD

Ebay and Paypal
http://editor.actrix.co.nz/byarticle/0408phishing2.html

To learn more about phishing go to www.antiphishing.org.

THREATS & PROTECTIONS QUIZ | SLIDE 79

INFORMATION ABOUT QUIZ:

This quiz consists of five questions which are randomly selected from a bank of nine questions. In order to receive credit for this section, you must pass the quiz with a score of 100%.

THREATS & PROTECTIONS SECTION COMPLETE | SLIDE 80

INSTRUCTION TEXT:

You have completed the Threats & Protections section.

Click the forward arrow button below to continue.

QUIZ OR VIEW SECTION? | SLIDE 81

INSTRUCTION TEXT:

The topics covered in this section:

- Physical Security
- Portable Device Security
- Encryption
- Data Backup
- Security Incidents

Click the option below that best suits your needs.
SECTION 5: OTHER SAFE PRACTICES | SLIDE 82

Security is a process, not a product. Therefore, the objective behind implementing good computing practices is that good computing habits will develop.

In addition to the safe computing practices previously discussed, there are few additional safe practices that one should utilize in order to help safeguard computing resources and sensitive information. These will be discussed in this section.

PHYSICAL SECURITY | SLIDE 83

Physical security describes the measures designed to protect computing resources, facilities, and information against physical threats, whether deliberate (e.g., theft or vandalism) or accidental (e.g., natural disasters or loss).

CONTROL ACCESS TO YOUR OFFICE/WORKSPACE | SLIDE 84

PUBLIC OR PRIVATE
Is it open to the public or only authorized personnel?

ENTRY/EXIT
Where are the entrances and exits?

COMPUTER
Is your computer located in an area that's easily accessible to outsiders?

OFFICE SETUP
Is your office occupied by others?

WORKSTATION ACCESS
Who has access to your workstation?

KNOW YOUR COLLEAGUES

Become familiar with the personnel in your work area, so that you can readily recognize the presence of a stranger or intruder.

PHYSICAL SECURITY AND UNKNOWN VISITORS | SLIDE 85

INTRODUCTION TEXT:

As mentioned in the previously, becoming familiar with your colleagues will help you in identifying strangers or intruders.

Click the forward arrow button in the top right corner to learn ways you can address these unknown visitors.

ELEMENT TEXT:

OFFER ASSISTANCE

Address any unknown visitor in your area and find out if you can assist him/her.

DOOR SECURITY

If you pass through a door that has to be opened with a key, swipe card, access code, or is otherwise locked to outsiders, make sure it closes completely.

COAT-TAILING & PIGGYBACKING

Prevent physical access breaches, such as Coat-Tailing & Piggybacking, where badge-reading systems are employed to log access into and out of a secure facility.

ADDRESS POLITELY

Explain in a polite and direct way that you’re not allowed to let anyone but yourself in through the door.

AVOID THE SITUATION

Avoid the situation altogether. If you’re walking toward a secured door at the same time as someone else, slow down and allow him/her to enter first.

SECURE YOUR OFFICE/WORKSPACE | SLIDE 86

- Lock your office door(s) when you leave for any significant time period (e.g., during lunch or for a meeting).
• Always “lock” or log off of your computer before leaving it unattended (even for a few minutes).
• Keep personal items, such as keys, purses, wallets, PDAs, thumb drives, & digital equipment in an appropriately secure place, and not readily accessible to others.

**PORTABLE DEVICE SECURITY | SLIDE 87**

Portable Computing Devices (e.g., laptops, PDAs, & smart phones) and Portable Storage Devices (e.g., flash/thumb drives, CDs, & DVDs) pose a special challenge to information security because of their small size, portability, and powerful capabilities (e.g., wireless access and storage capacity). The following safeguards can mitigate the risks associated with portable devices.

**SECURING PORTABLE DEVICES | SLIDE 88**

• Protect portable computing devices from unauthorized access by utilizing password protection.
• Portable devices should be physically secure (i.e., stored in a secure environment).
• Portable devices should not be left unattended in public areas, and when possible, should be hidden from view when left in a vehicle.
• If you must store sensitive or confidential information on a portable device, it should be encrypted with at least a 256-bit encryption program or other approved encryption techniques.

**SECURING PORTABLE DEVICES CONT’D | SLIDE 89**

• Do not enable a wireless connection on any portable computing device, unless it’s been secured with at least basic encryption (e.g., WPA) or other more secure encryption protocols.
• When possible, keep portable computing devices updated, and install anti-virus software and a personal firewall.
• Flash drives are easy to misplace. Be sure to keep track of these, as well as other portable devices, especially if there’s confidential or sensitive information stored on them.

For more information, visit [http://security.tamu.edu](http://security.tamu.edu).

**ENCRYPTION | SLIDE 90**

Encryption is the process of transforming plain text into an unintelligible form (i.e., ciphertext) that can only be read or deciphered by the person or computer with the appropriate key to decrypt it.

Decryption is the process of converting encrypted data back into its original, plain text form.

Encryption can help protect the privacy and integrity of data, so if you need to store or transmit confidential information, you should take steps to encrypt it.

**ENCRYPTION CONT’D | SLIDE 91**

Any unencrypted data traversing the Internet can be read by others, so be sure to encrypt sensitive or confidential data before transmitting it over the Internet.
Encryption programs that use at least a 256-bit encryption are recommended for encrypting sensitive data. Consult your IT personnel if you have questions.

VIDEO: ENCRYPTING | SLIDE 92

INSTRUCTION TEXT:

Video: Encrypting

Click one of the options below.

ELEMENT TEXT:

Play video
Skip video

NARRATION:

Encrypting sensitive files is a very important practice in today's world, but unfortunately, not many people know how to do it or how it works.

It begins with one person who wishes to send a sensitive document to a trusted individual, in this case tax documents. The sender first encrypts his or her file with an encryption program, then e-mails this file to the intended recipient.

The recipient then downloads the file from their e-mail and is ready to decrypt the file. The recipient then phones the sender and requests the highly secretive password that is required to decrypt the file. After the file is decrypted the file can be viewed freely by the recipient.

The following are recommended encryption programs that can be used in this manner.

The first is from cadabra software and it is called P-Encryption. This program allows multiple forms of encryption and supports up to 448bit encryption. The next program is from pmc ciphers and is called turbocrypt. This program relies on a polymorphic 512bit encryption that is sufficient for anyone this side of the government and military.

For those of you who use Windows, Windows XP has pre-installed encryption software that can be used for personal use. By this I mean that you can encrypt folders under your username and restrict access to anyone else that might log onto your computer.

If another user logs onto their account on your computer and attempts to open your encrypted folder, that user will be unable to do so.

In this example you see that I have a folder on my desktop labeled student grades. Inside of this folder are a few excel sheets that have all of my student's grades from this semester. This is a great example of something I should encrypt.

So to encrypt this folder all we do is simply right click on the folder on the desktop and select properties. An information box will then appear. Go down to this advanced button in the bottom right and click it. Now in this new window go down to the check box labeled "encrypt contents to secure data" and check it.
After you click ok on each window, a dialog box will appear asking whether you would like to encrypt only the folder or the folder and all of its contents. To be safe I would select the bottom option and encrypt all subfolders and files.

Click ok again and you will see Windows encrypt the files for you.

**DATA BACKUP | SLIDE 93**

**CALLOUT TEXT:**

How am I going to explain to my boss I lost the research proposal?

**RESPONSE TEXT:**

Data backup is an extremely important practice that can mitigate the stress and frustration associated with data loss. It enables the recovery of data and applications lost or corrupted due to user error, hardware faults, power failures, malware, theft, etc. Data backup can be used by anyone and for anything that he/she can’t or doesn’t want to re-create.

**AN EFFECTIVE BACK UP ROUTINE | SLIDE 94**

**CALLOUT TEXT:**

I am so glad I made a backup!

**RESPONSE TEXT:**

- Back up important information to at least two different forms of media (e.g., paper, CDs/DVDs, thumb drive/USB stick), and
- Store them in separate, secure locations.
- Routinely test backup procedures to ensure that individual files and directories are not corrupted and can be restored.

Note: Backups containing confidential data should be encrypted and stored in a lockable drawer or file cabinet.

**SECURITY INCIDENTS | SLIDE 95**

A security incident is an event, either accidental or deliberate, which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of computing information resources.

If you think that a security incident may have occurred, report it immediately to your departmental IT staff.

It is important that YOU know who to contact and how to respond to security incidents in a timely manner.
OTHER SAFE PRACTICES QUIZ | SLIDE 96

INFORMATION ABOUT QUIZ:

The Other Safe Practices consists of five questions which are randomly selected from a bank of ten questions. In order to receive credit for this section, you must pass the quiz with a score of 100%.

COURSE SUMMARY | SLIDE 97

You should now be able to identify safe computing practices, and related policies, rules, and regulations.

Remember the following:

- **Account Usage**
  - Guard your account information
- **Authentication**
  - Create strong passwords and keep them safe
- **Confidentiality**
  - When in doubt, don’t give it out!
  - Encrypt when necessary.
- **Threats & Protections**
  - Be wary of e-mail scams, and keep software and anti-virus applications up-to-date.
- **Other Safe Practices**
  - Be aware of your environment.
- **Click the forward arrow button below to proceed to the course acknowledgement.**

COURSE ACKNOWLEDGEMENT STATEMENT | SLIDE 98

To receive a completion for this training, select the acknowledgment statement below, and then click the SUBMIT button.

I acknowledge I have completed the Information Security Awareness training and will comply with all federal, state, and local laws; A&M System policies and regulations; university/agency rules; license agreements and contracts. I understand failure to do so may result in restriction or loss of access to computing resources or privileges, other disciplinary action, and/or law enforcement involvement.