Information Security Awareness - Print Version

Last updated: 02/2022

1. Introduction

This course has audio and closed captioning. This course can take 60-90 minutes to complete. You can pick up where you left off when you return.

1.1 Customize Your Experience

You have several options to customize your experience.

- If you prefer to navigate with a keyboard, download the list of keyboard shortcuts.
- Download an accessible text version of this course and other resources to have available for reference.
- You can mute the audio or adjust the volume levels at any time.
- Turn the closed captioning on and off by selecting the speech bubble icon.
- Select the gear icon to enable or disable the accessible text or keyboard shortcuts.

1.2 About This Course

How serious is the risk if your identity is stolen?

How does it impact other people?

How does it affect your organization?

There are people trying to steal any confidential data you have access to, and they bet they can outsmart you. But don't get tricked!

Information security is about protecting your data, accounts, and devices from unauthorized access, disclosure, modification, destruction, or disruption.

You play an important role in preventing illegal access to confidential information.

This course will identify the tools you'll need to protect you and your organization from data theft.

1.3 Course Objectives

By the end of this course, you'll be able to:

- Classify the types of data you are required by law to keep confidential
- Protect your confidential data from theft or loss
- Explain your responsibilities for using and protecting your user accounts and your organization's computing resources
- Identify methods criminals use to access your confidential data or computer systems
- Apply strategies to prevent unauthorized access to your computing devices and confidential data

1.4 Course Outline

This course is divided into five sections:

- The Data You Need to Protect,
- Protect Your Data,
- Protect Your Accounts,
- Protect Yourself, and
- Protect Your Devices.

You will have an opportunity to test out of each section. Or, you can view each section, and pass the test at the end in order to advance.

Once you pass all five sections, you'll read and verify you agree with the terms in the A&M System Data Use Agreement to receive a completion for the course.

2. Section 1-The Data You Need to Protect

There are several federal and state laws that determine what types of information are considered confidential and therefore must be protected. This section focuses on the laws most employees of higher education and government agencies should be familiar with: the Family Educational Rights and Privacy Act, Sensitive Personal Information, the Texas Public Information Act, and export control laws.

2.1 Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act, also known as FERPA, is a federal law that protects the privacy of student education records and prohibits the release of those records without the student's written consent.

If you have access to student education records, you need to know three things:

- What is considered an education record
- The difference between directory and non-directory information
- To whom and when you can give out information

2.2 Education Records

An education record, with some exceptions, is 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. For example, it could be in print form, film, handwriting, or electronic text. This includes ANY information displayed on a computer screen.

Examples include transcripts, grade reports, class rosters, schedules, or ANY documents containing information related to a student.

2.3 Directory vs. Non-directory Information

Student information contained in education records is categorized as either directory or non-directory information.

Directory information includes information that would not be considered harmful or an invasion of privacy if disclosed.

Directory information may be made public unless specifically withheld by the student.

Check with your local Registrar to see what is considered directory information at your institution.

Any information that is not specifically categorized as directory information is considered non-directory information. Directory information specifically withheld by the student is treated as non-directory information.

Non-directory information may not be released without the prior written consent of the student. However, there are some exceptions allowed by FERPA, and they are defined by the institution.

2.4 Non-directory Exceptions

Examples of exceptions include, but are not limited to:

- School officials, third-party contractors, or organizations with legitimate educational interest in a student's record. An example of an organization would be the National Student Clearinghouse.
- Parents of students who are claimed as dependents* on federal income tax forms.
- Compliance with judicial orders or lawfully issued subpoenas
- Financial aid processing

*Spouses have no rights to access student records even if they are claimed as a dependent on federal income tax forms.

Seek guidance from your local Registrar's office for your institution's FERPA policies.

2.5 Sensitive Personal Information

Sensitive Personal Information, also known as "SPI", is defined by the State of Texas as an individual's first name or first initial and last name in combination with any one or more of the following items:

- 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.

Social Security numbers should be replaced with another means of identification, such as the Universal Identification Number, or UIN. Check your institution's rules and administrative procedures for specific instructions on use and retention of Social Security numbers.

2.6 Texas Public Information Act

Another law all state employees need to be aware of is the Texas Public Information Act (TPIA). It specifies that all recorded information owned or accessed by a governmental body is presumed to be public information.

Items not considered public information include:

- Student education records
- Restricted employee information (for example, a home address or phone number)
- Audit working papers
- Select personal information withheld from disclosure by the owner
- Medical records
- 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
- Personally Identifiable Information, which is information that can be used to identify an individual such as name, social security number, financial account number, or date of birth

2.7 Export Controls

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.

2.8 Export Control Laws

What are export control laws?

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.

They also 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.

Most exports do not require specific approval from the federal government. However, certain exports require a license, and others are prohibited.

2.9 How Export Controls Might Apply to You

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

Your computer may contain export-controlled encryption source code, or information related to an export-controlled research project you may have worked on. Additionally, the computer itself may be controlled depending on the country.

2.10 Export Controls-Your Responsibilities

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

To avoid an unintentional violation of the law, 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 or foreign persons.

2.11 Contacting Your Export Control Representative

If you are not sure who your Export Controls representative is, contact the A&M System Research Security Office at rso@tamus.edu or 979-458-6094.

Additional information can be found on the Research Security Office Export Controls page.

2.12 Section 1 Summary

Follow FERPA guidelines when working with student education records.

As a state employee, be aware of the types of information that are public and protected, and comply with all laws, policies, regulations, and System member rules.

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

Be familiar with export control requirements and contact your local export controls office when you need assistance.

3. Section 2-Protect Your Data

This section provides guidelines for protecting your confidential data and proper backup procedures.

3.1 Consequences and Responsibilities

The unauthorized or unintended release of confidential information can lead to a loss in federal funding, negative publicity for your institution, and personal embarrassment.

As an employee of the Texas A&M University System, you or your accounts may have access to confidential information, and you must protect the privacy of that information.

If you know or suspect that confidential information has been accessed by, or released to an unauthorized party, report it to the appropriate person or department immediately.

3.2 Guidelines for Protecting Confidential Data

Accidents happen, but there are actions you can take to protect confidential information. The following guidelines apply to all types of confidential information.

- Do not provide information to anyone unless you know they are authorized to have it. When in doubt, don't give it out!
- Do not post grades publicly unless you can guarantee absolute anonymity.
- Hold phone conversations and meetings in areas where confidential information cannot be overheard.
- Be careful what you send by email. Your organizational email is not considered private, and it can also be forged.
- Pick up confidential documents immediately from office printers, scanners, copiers, and fax machines.
- Position your computer screen so it's not visible to anyone but you.
- Keep papers with confidential information secured in a locking file cabinet.
- Store keys in a secure area.
- Lock your computer anytime you are going to be away from your desk.
- Properly shred paper documents and/or CDs containing confidential information before disposal.
- Keep storage media (i.e., hard drives, flash drives or CDs) with confidential information encrypted and secured in a locking file cabinet.

3.3 Encryption

Proper encryption prevents your data from being viewed if it is ever lost or stolen.

Encryption is the process of transforming plain text so that it is unreadable to anyone but you, or your intended recipient.

The recipient can access your data only if you give them the password or key.

Encrypt all types of confidential information anytime you need to store or share it with others.

Consult your IT staff with specific questions or assistance with encryption.

If you'd like to learn more about encryption, review the following videos.

["About Encryption" video-transcript below]

["How to Encrypt a Microsoft Word Document in Office 365"-transcript below]

3.3.1 Video Transcript: About Encryption

Many hotels, coffee shops, airports and other places offer free Wi-Fi hotspots. They're convenient. Unfortunately, they often aren't secure.

That could make it easy for someone else to access your online accounts or steal your personal information. So, what can you do to reduce your risk?

Encryption is the key to keeping your information secure online. When information is encrypted, it's scrambled into a code so others can't get it.

How can you be sure your information is encrypted?

Two ways: one, use a secure network to access the internet. Don't assume that a public Wi-Fi network uses encryption. In fact, most don't. You can only be sure that a network uses effective encryption if it asks you to provide a WPA or WPA2 password. If you aren't sure, it's best to assume the network is not secure.

The second way to protect your information is to send it through a secure website. A secure site will encrypt your information—even if the network doesn't. If the web address starts with "https," then your information is encrypted before it's sent. The "s" stands for "secure." Look for the "https" on every page you visit, not just when you log in.

If you use an unsecured Wi-Fi network to login to an unencrypted website, strangers using that network can hijack your account and steal your private documents, contacts, family photos, even your username and password. If that happens, an imposter could use your email, or social networking account to pretend to be you and scam people you care about. Or, a hacker could use your password from one website to try to login to a different account and access your personal or financial information.

Here are some steps you can take to protect yourself when you use a public Wi-Fi hotspot:

- Only log in or enter personal information on secure sites that use encryption. Again, look for a web address that begins with “https”
- Don’t use the same username and password for different sites. It could give someone who gains access to one of your accounts access to many of your accounts.
- Never email financial information including credit card, Social Security, and checking account numbers, even if the network and website are secure.
- Don’t stay permanently signed into accounts.
- When you’ve finished using a site, log out.

The bottom line? Secure Wi-Fi hotspots require a password. Secure websites start with https.

And remember: it’s easy to find trusted information about computer security. Just visit OnGuardOnline.gov, the federal government’s site to help you be safe, secure and responsible online.

3.3.2 Video Transcript: How to Encrypt a Microsoft Word Document

This video demonstrates how to encrypt and add a password to files in Office 365. The process is the same across the Office 365 Suite. This example uses Microsoft Word.

1. In Word, open your document. Select File.
2. From the Info tab, select Protect Document.
3. Select Encrypt with Password.
4. The Encrypt Document dialog window appears. Type in a strong password and then select OK.
5. Re-enter your password in the Confirm Password window and select OK.
6. Your document is now encrypted and password protected.

3.4 Data Backup

Data and applications can get lost or corrupted due to problems such as user error, hardware faults, power failures, malware, or theft.

It is essential that you or your IT staff back up all your important information and plan for how to recover from a system failure. Contact your unit's IT staff to find out whether they are backing up your data, or if you are expected to do it.

3.5 Guidelines for Backing up Data

Back up important information to at least two different forms of media and store them in separate, secure locations.

Create backups before major changes such as upgrading your operating system, editing files, or upgrading applications or programs.

Routinely test backup procedures to ensure that individual files and directories are not corrupted and can be restored.

Backups that contain confidential data must be encrypted and kept physically secure.

3.6 Section 2 Summary

You or your accounts may have access to confidential information and you're responsible for protecting that information.

Follow the proper guidelines for protecting confidential information and backing up data.

Contact the appropriate person or department if you know or suspect confidential information has been accessed by or released to an unauthorized third party.

4. Section 3-Protect Your Accounts

This section covers your responsibilities to protecting your computing accounts and creating strong passwords to prevent unauthorized access.

4.1 Individual Computing Accounts

Assigning individual computing accounts helps ensure that only authorized individuals have the appropriate access to various computing resources.

Your computing account uniquely identifies you.

You are responsible for any activity generated by your computing account such as accessing files, changing passwords, or deleting information.

Someone else gaining access to your account poses a security concern for you and your institution.

To comply with state law, you must safeguard your computing accounts such as your SSO login or institution-specific accounts.

4.2 Your Responsibilities

So, what are your responsibilities?

- Comply with federal, state, and local laws, Texas A&M System policies & regulations, university or agency rules, license agreements, and contracts.
- Use computing resources only for their intended purposes or incidental personal use.
- Act responsibly and ethically, and respect the rights of others in online forums, and
- Protect confidential information to which you have access.

If you fail to fulfill these responsibilities you may experience:

- The restriction or denial of access to your computing resources or computing privileges;
- Other disciplinary action by the university or agency; and/or
- Law enforcement involvement.

4.3 Examples of Unauthorized Use

You are not allowed to use your A&M system accounts or computing resources for:

- Illegal activities
- Gaining unauthorized access to systems, networks, accounts, or data
- Intentionally destroying or damaging equipment, software, or data belonging to the A&M System or other users
- Intentionally accessing, creating, storing, or sharing obscene materials
- Harassing, threatening, or libeling someone
- Transmitting unsolicited information that contains profane, offensive, bigoted, sexist content, or relates to forms of prohibited discrimination

4.4 Personal Use

Occasional personal use of your organization's resources is acceptable until it:

- Results in additional cost to the state or your university or agency
- Results in your financial gain
- Becomes for your own personal business reasons, or the work is done for another business (e.g., consulting)
- Occurs excessively or for long durations
- Interferes with your assigned job responsibilities
- Violates rules, policies, or laws

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

4.5 Protecting Your Account from Unauthorized Access

Authentication is the process or action of verifying your identity, and it helps protect against unauthorized access to your account, computer, or device. Authentication may take the form of:

- Something you know - a password, pass phrase, or personal identification number
- Something you have - a smart card, ID card, or other security token and/or
- Something you are - fingerprint, retinal pattern, or other biometric identifier

All these things must be protected. The following section focuses on password security, as that is likely to be the most relevant for you.

4.6 Multi-Factor Authentication

Multi-Factor Authentication is a security approach that requires you to provide multiple types of proof of your identity in order to log in to your account. The types of proof used within the A&M System are "something you know" and "something you have".

The first factor is your password, which satisfies the "something you know" test. A second factor requires you to use something you have. For example, it could be your office phone or mobile device. After you log in, a notification is sent to your phone or device for you to approve the login request.

You can also choose to purchase a USB device to use.

If you have been issued any type of card or token, including your employee ID card, keep it in a secure location and report its loss or theft to the appropriate authorities as soon as possible.

4.6.1 Where can Multi-Factor Authentication be used?

Multi-factor authentication is used to log into the Texas A&M University System's Single Sign-On application, also known as SSO, and Texas A&M University's Central Authentication Service or CAS.

4.6.2 Who should use Multi-Factor Authentication?

- Anyone with access to confidential data. This might include some faculty or administrators who work with financial or personal information and some researchers and their teams.
- Administrators of certain HR and Payroll applications.
- All users of SSO and CAS.

4.6.3 Why should I sign up for Multi-Factor Authentication

A&M System employees have been victims of phishing and other social engineering attacks designed to steal usernames and passwords for SSO, CAS, and other authentication systems.

Multi-factor authentication is currently the best method to block phishing attacks and other methods compromising your secure accounts.

If you aren't enrolled in multi-factor authentication for SSO or CAS, instructions can be found in the Resources menu in the top right of the course player.

If you have access to data you feel should be protected by multi-factor authentication, contact your departmental IT staff.

4.7 Creating a Strong Password

Attackers target weak passwords to gain access to computing resources.

Strong passwords contain:

- At least 8-10 characters
- Uppercase and lowercase characters
- Letters, numbers and special characters

A passphrase or series of words makes your password stronger and easier to remember, such as “I love puppy breath!!”

4.8 Password Tips

- Never share your password with others.
- Use a different password for each account. That way, if someone does get one of your passwords, they won’t have access to all of your accounts.
- Use an encrypted password vault to keep your passwords safe.
- Don't use your personal information like your name, home address, license plate, phone number, or social security number.
- Don't include names of your spouse, children, pets, or friends.
- Don't use a single dictionary word, even when combined with letters and numbers.
- Don't use repeated letters or numbers or simple patterns, because these passwords are easily hacked.
- Don't use words connected to a sports team or school you are associated with.
- Don't let websites, web browsers, or applications “remember” your password.

4.9 Section 3 Summary

You’re responsible for any activity generated by your computing accounts.

You can protect your accounts by using multi-factor authentication and creating strong passwords.

5. Section 4-Protect Yourself

This section covers how to recognize social engineering, deceptive phishing and spear phishing attempts, insider threats, and how to manage the information you share on your social networking sites.

5.1 Social Engineering

State agencies and Institutions of higher education are under constant attack from bad actors (e.g., cyber criminals) who use social engineering to gain access to sensitive information, or to trick business staff into transferring funds into fraudulent accounts.

Social Engineering is a practice of manipulating or deceiving an individual to steal information. It is often linked to malicious activities, such as identity theft, data theft, or financial fraud.

It can be technical or non-technical, and can occur in person, over the phone, or online.

Social engineering attacks are often successful because they exploit the human tendency to trust and the desire to be helpful.

5.2 Social Engineering Tactics

Consider what happened to Devon:

Devon: I knew not to give passwords or personal information to anyone through email or over the phone to people who claimed to work for a company with which we do business. I was also pretty good at inspecting all links in emails.

One day, I get a call from “Joe” who worked for a local charity that I regularly support.

Joe said the charity was holding a raffle for tickets to a sporting event, which happened to be for my favorite team. I would be entered in a raffle in exchange for a donation.

I didn't want to give Joe my credit card information, so Joe offered to email me a PDF that had more information about the fundraiser. Then, he asked me for my email address and version of Adobe Reader I was running.

Opening the PDF in Joe's email gave him access to my computer. He gained access to my accounts, my contacts – basically anything he wanted.

What made it worse, was that this was my work computer.

It didn't take long before I and other coworkers stopped receiving our paychecks. The investigation later revealed that Joe had located the charity and sports team information from my social media account.

I couldn't believe it! Now I know to be more skeptical. If I hadn't acted so quickly, I would have realized that the charity would have already had my email address on file. Also, I should've gone to the charity website myself to verify the fundraiser information.

Now I realize that anyone can be vulnerable to a social engineering attack.

5.3 Financial Transactions Example

Fraudsters also target employees who initiate or approve financial transactions.

Angie: While I was processing a $35,000 payment for equipment for our new science building, I received an urgent email that appeared to be from the dean. The email said that the equipment vendor was changing banks and the receiving account number had changed. The funds needed to be transferred by 3pm that afternoon. I was afraid to say no, so I executed the transfer. Later I learned the email was fraudulent, and the new account number actually belonged to an impostor. It was too late to get our money back.

5.4 Other Ways Social Engineers Attack:

Social engineers are also known to attack by:

Calling and pretending to be an employee that has forgotten a password in order to get the password reset to one the attacker knows.

And by following or "tailgating" someone through a secure entrance by looking like they belong.

5.5 How to Defend Against Social Engineering Attacks

You, not your IT staff, are the best defense against social engineering!

So how do you defend against social engineering attacks?

- Verify the credentials or requests of anyone you are uncertain about.
- Ask the person for their name and company or supervisor's name. Seek the company's or supervisor's contact information from another source, and then contact them to verify the identity or validity of the solicitor.
- Put the caller on hold and seek advice from your supervisor - this will give you valuable thinking time.
- Don't hesitate to notify your IT department or consult others regarding those you may have doubts about.

A&M System finance/business staff are required to follow specific processes when transferring funds. For more information, see TrainTraq course no. 2114125: *Fiscal Transactions - Preventing Impostor Fraud*.

5.6 Phishing

A few years ago, nine Texas A&M University employee SSO accounts were compromised by hackers. They changed the bank account numbers where paychecks are deposited for several of these employees. It is believed the login information used in this attack was obtained through an email phishing scam.

Phishing is an electronic form of social engineering. It relies on a combination of fraudulent messages and spoofed websites to deceive people into giving out personal or financial information.

There are at least two types of phishing attacks that everyone should be aware of: Deceptive phishing and Spear phishing.

5.7 Deceptive Phishing

Typically, deceptive phishers send an email, text, or instant message made to appear as though it came from a legitimate bank or other business. They do this by spoofing brand names and logos.

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.

These messages are generally impersonal and vague on purpose and are sent to massive lists of email addresses and telephone numbers they've

purchased off the dark web hoping to get a small percentage of the recipients to fall for the scam.

5.8 Spear Phishing

Spear phishing is a more sophisticated “targeted” attack. It is a variant of phishing which uses email, social media sites, instant messaging applications, and other platforms to trick users into giving out personal information or unknowingly giving the attacker access through their computer (i.e., downloading an attachment or clicking a link to a website which installed malicious software) in order to perform actions that cause network compromise, data loss, or financial loss.

Spear phishing is more successful because the attacker has already done reconnaissance and usually has some or all of the following information about the victim: their name; email address; place of employment; job title; and specific information about their job role.

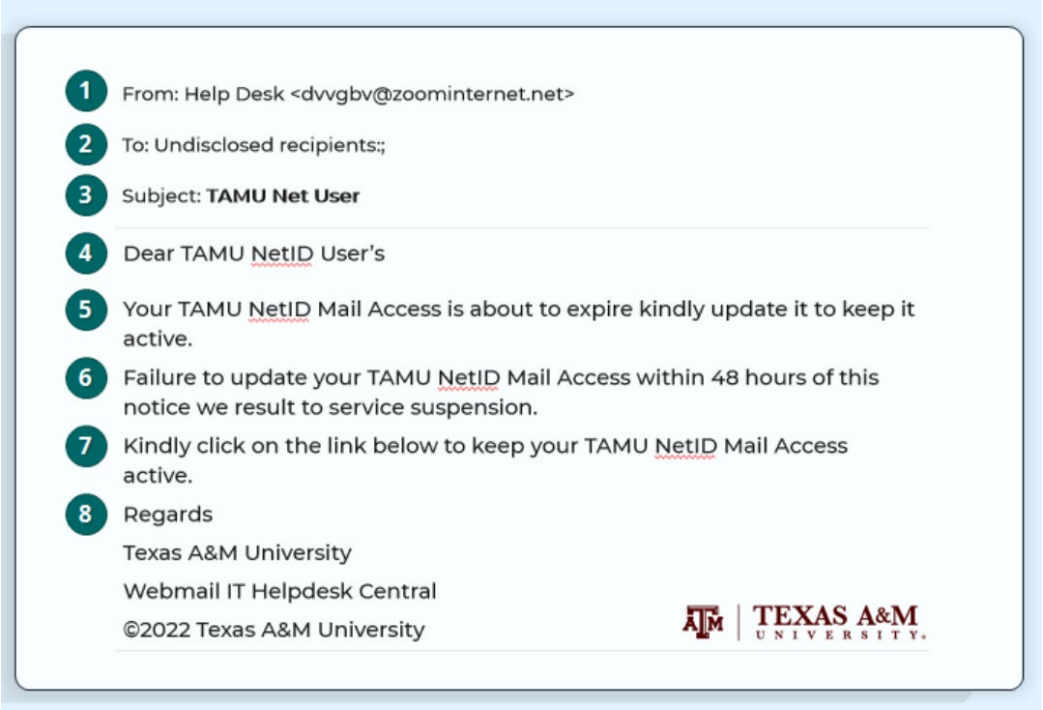
5.9 Reporting Phishing Attempts

Both deceptive and spear phishing can be successful because at a quick glance, it’s difficult to determine the difference between legitimate websites and ones created by phishers.

Report suspected phishing attempts by forwarding the message to your local IT staff. For instance, at Texas A&M University – College Station, you can forward phishing emails to helpdesk@tamu.edu. Check with your local IT staff for general reporting rules as they may differ across organizations.

5.10 Phishing Email Example

The following example was taken from an actual phishing attempt.



The "From" field indicates the email is from the "Help Desk," but the email address is, "dwgbv@zoominternet.net". This email address is probably not from your IT department.

The "To" field is, "Undisclosed recipients:;". It is a good idea to check to whom the email is addressed. Some phishing emails are sent out in bulk.

The "Subject" field is, "TAMU Net User". The subject may be an obvious clue. For example, it is common for phishing emails to have misspellings or grammatical errors. If you were a TAMU NetID User, you would probably wonder why the subject for this particular email was only labeled, "TAMU Net User."

The greeting of the message is, "Dear TAMU NetID User's". Some phishing emails are sent out in bulk, and they are generically addressed to the email recipients. However, it is more common for them to address you specifically and make a request to update or verify your account information. This should be a red flag, since legitimate companies normally don't ask for personal information by email, especially if it's information they should already have.

The opening sentence of the message is, “Your TAMU NetID Mail Access is about to expire kindly update it to keep it active.” This sentence contains grammatical errors and is a common sign of a phishy email.

The sentence, “Failure to update your TAMU NetID Mail Access within 48 hours of this notice we result to service suspension” relays a sense of urgency, which is often a sign of a phishy email. Remember, these hackers are trying to steal your information.

The message provides the following instructions, “Kindly click on the link below to keep your TAMU NetID Mail Access active. http://www.tamu.edu”. Messages sent through email, instant messaging, or even using social media like Facebook and Twitter, encourage 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. If the message is sent through applications like Facebook, even clicking the link can share your personal information with third parties because of loose privacy settings. Additionally, some phishing emails also have attachments that contain viruses or malware to infect your computer.

The email signature and Texas A&M University logo is provided in the email. Although the email signature and logo may not be suspicious, it’s important to remember phishy emails spoof brand names and logos.

5.11 Four Ways to Protect Yourself from Phishing Emails

The following are strategies to avoid getting hooked on a phishing email.

- Don't respond to a suspicious message or use the contact information presented in the message.
- Don't click links within suspicious emails, instant messages, or social media applications. The link could lead to a malicious website where keystroke loggers are waiting to capture the information you type in.
- Never enter personal or financial information into unsecured sites or pop-up windows. A common phishing technique is to launch a pop-up window when someone clicks a link in a phishing email which captures any data you enter.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. If you are not expecting a file, there is a good chance it contains malware.

5.12 Insider Threats

An insider threat arises when a person with authorized access to A&M System resources uses that access for unauthorized and/or illegal reasons. These include but are not limited to the following: fraud; sabotage; and the theft or destruction of intellectual or physical property, research data, and/or personal identifiable information of students, former students, staff, and faculty. (National Counterintelligence and Security Center, 2016)

5.13 Insider Threat Example 1

For example, a retired research scientist was convicted of stealing trade secrets from their former employer and selling them to foreign companies. The former employee conspired with several current and former employees, traveled extensively to market the stolen information, paid current and former employees for material and information, and bribed a then-employee with $50,000 in cash to provide a process manual and other information. They were sentenced to 60 months in prison, two years supervised release, a $25,000 fine, and were ordered to forfeit $600,000. (Federal Bureau of Investigation, 2016)

5.14 Insider Threat Example 2

A disgruntled employee was fired from their job due to poor performance. They kept numerous computer files with their employer's trade secrets. They entered into a consulting agreement with a rival foreign-based company and gave them the stolen trade secrets. They were sentenced to 18 months in prison and ordered to pay their former employer over $187,000. (Federal Bureau of Investigation, 2016)

5.15 Potential Behavioral Indicators

There are several behaviors that may indicate a possible insider threat. For example, someone who:

- takes proprietary or other material home without need or authorization
- inappropriately seeks or obtains information on subjects not related to their work duties
- has interest in matters outside the scope of their duties
- unnecessarily copies material, especially if it is proprietary or classified
- remotely accesses the computer network at odd times
- violates the organization's policies, procedures, directives, rules, and/or practices
- works odd hours without authorization
- has unexplained income, and/or
- overwhelmed by life crises or career disappointments

Note: Many people experience or exhibit some or all of these behaviors to varying degrees; however, it does not automatically mean they are an inside threat.

If you have reason to believe someone is an insider threat, contact your Information Security Officer. (Federal Bureau of Investigation, 2016)

5.16 Social Networking

Social networks can be great tools to collaborate and share experiences with others, but they can also be used by attackers to gather information about you.

A huge risk of social networking is the oversharing of personal or private information.

Do not post private or confidential information related to your organization on a social network. Even if accidental, it can lead to serious repercussions.

5.17 Third Party Apps

Review the privacy policies of any social network sites you use and of each third-party app that wants access to your profile to determine what data they collect from you and how they use it. Some third-party apps may have loose privacy settings and may exploit your personal information.

Be wary of clicking on links sent through the app itself; your account can be compromised in a matter of seconds. Be suspicious of messaging requests and pop-ups.

5.18 Section 4 Summary

There are several methods bad actors use to access information or to trick business staff into transferring funds into fraudulent accounts.

Verify the credentials or requests of anyone you're uncertain about.

Beware of phishing emails.

If you have reason to believe someone is an insider threat, contact your Information Security Officer.

Review the privacy policies of your social networking sites, and don't post private or confidential information.

6. Section 5-Protect Your Devices

Hackers have the time and tools needed to take advantage of you and compromise your accounts, computers, and mobile devices.

This section covers malware, traveling tips, how companies get information about you, how firewalls can protect your computer from unauthorized access, the proper disposal of state-owned property, and your responsibilities in reporting security incidents.

6.1 Malware

Malware includes everything from adware, Trojan viruses, worms, spyware and other malicious programs that are often received from downloaded files, email attachments, or surfing the web.

Some common indicators that your computer might be compromised with malware include:

- Frequent pop-ups or other problems preventing you from browsing the internet
- New browser toolbars and web browser crashes
- Your web browser frequently redirects uninitiated
- Your PC recently became much slower or is too slow to use
- You have new suspicious files
- Some of your files are encrypted, and you didn't encrypt them yourself
- You are warned of a malware infection or asked to pay for malware removal
- Your PC frequently crashes

6.2 Preventing Malware

The following can help prevent against malware:

- Install and update antivirus software regularly
- Download software only from websites you know and trust
- Don't buy security software in response to unexpected calls or messages
- Use a pop-up blocker
- Don't click on links or open attachments in emails unless you know what they are

6.3 If You Suspect Malware

- If it’s a work computer, seek help from your IT staff
- If it’s a personal computer, seek help from a reputable professional, company, or retail store that provides tech support. Additionally:
    - Stop doing things that require passwords or personal info, such as online shopping or banking
    - Use a different computer to change your passwords
    - Update your security software and run a system scan
    - Allow your antivirus software to automatically delete files flagged as malware

Watch the following video on Malware for additional information.

6.4 Video Transcript: Malware

Would it surprise you to learn that millions of computers in the US are infected with malware? That's a lot of computers. So what's malware, and why should you care?

Malware, short for malicious software, includes viruses and spyware that get installed on your computer or mobile device without you knowing it. Criminals use malware to steal personal information and commit fraud. For example, they may use malware to steal the login information for your online accounts or to hijack your computer and use it to send spam. An infected computer can lead to serious problems, like identity theft.

The good news, there's a lot you can do to protect yourself and your computer. One of the most important steps you can take, install security software from a reliable company and set it to update automatically. The bad guys constantly develop new ways to attack your computer, so your software must be up to date to work.

Set your operating system and your web browser to update automatically too. If you're not sure how, use the help function and search for automatic updates. Don't buy security software in response to unexpected calls or messages, especially if they say they scanned your computer and found malware. Scammers send messages like these to trick you into buying worthless software, or worse, downloading malware.

What else can you do? Use a pop up blocker, and don't click on links and popups. Don't click on links or open attachments in emails unless you know what they are, even if the emails seem to be from friends or family.

Download software only from websites you know and trust. Free stuff may sound appealing, but free downloads can hide malware. Make sure your web browser's security setting is high enough to detect unauthorized downloads. For example, use at least the medium security setting.

Even if you take precautions, malware can find its way onto your computer. So be on the lookout for these signs. Your computer runs slowly, drains its battery quickly, displays unexpected errors or crashes, it won't shutdown or restart, it serves a lot of popups, takes you to web pages you didn't visit, changes your home page, or creates new icons or toolbars without your permission.

If you suspect malware, stop doing things that require passwords or personal info, such as online shopping or banking. Use a different computer, maybe one at work or at your local library, to change your passwords. Update your security software and run a system scan. Delete files it flags as malware.

If you can't fix the problem on your own, get help from a professional. Your computer manufacturer or internet service provider may offer free tech support. If not, contact a company or retail store that provides tech support.

Keep in mind, the most important thing you can do to prevent malware is to keep your computer software up to date. And remember, it's easy to find trusted information about computer security. Just visit onguardonline.gov, the federal government site to help you stay safe, secure, and responsible online.

6.5 Traveling Considerations

When traveling, there is no expectation of privacy. Always assume eavesdropping may take place on all electronic communications.

When traveling internationally, officials may search and copy the contents of your laptop and expect you to divulge credentials and encryption keys as necessary. Refusal to comply can result in seizure of the device or denial of entry into the host country.

Once in the country, risks to confidential, controlled, and sensitive data continue. Some countries legally prohibit encryption, and others view all encryption suspiciously. Physical loss and digital espionage also put confidential information (or tools to access it) on your devices at risk.

Don't travel with confidential, sensitive, proprietary, research or controlled information even if it's encrypted. U.S. export control regulations forbid the transport of certain data outside of the country. If you have questions about the types of information in your possession when traveling internationally, consult your System member export controls office.

There are several actions you should take to protect your devices, accounts, and information before, during, and after travel. Download the **International Travel Handout** in the Resources tab for more information.

[The **International Travel Handout** is a separate document]

6.6 Targeted Advertising

Now let's talk about targeted advertising.

Through data mining, companies advertise their products and services to people who are statistically more likely to purchase them. When you browse the web, companies use information based on your search patterns and sites you visit to load advertisements on pages you view - hoping that you'll click on them.

Some Internet browsers and web applications do allow you to opt out of some advertising in their settings, but others aren't as open about their ad targeting.

In theory, the information gathered through data mining has been anonymized, but companies are able to build very detailed advertising profiles for individuals. The practice is controversial, and many consider it an invasion of privacy.

One way your computing device can be tracked is through cookies, which are very small files stored on your computer by sites you visit. You can control whether or not websites are allowed to push cookies to your computer through the privacy settings of your web browser.

In fact, some companies that provide free email service even data mine your email content. Emails are scanned, so the company can match up paid

advertising with associated keywords found in your messages. You should be wary of any advertising online, as malware can be hidden in these ads or pop-ups.

6.7 Personal Firewalls

A firewall blocks hackers, viruses, and other potentially malicious traffic on the internet. Most computers have a built-in firewall that is designed to protect it from attack. To keep your computer protected, you should make sure your firewall is always turned on. You can check the firewall status of most computers by accessing the Control Panel (or “System Preferences” for iOS users) and checking the security settings.

Visit the vendor website for specific information about your product. If you have any questions about firewalls or their use, please contact your local IT administrator.

6.8 Secure Disposal

When computing devices become obsolete or no longer usable, they must be disposed of in a secure manner to protect the confidentiality of any data on the device. The State of Texas requires secure disposal of computing and storage devices to protect confidential data.

This applies to desktop and laptop computers, and any device that can store data, such as removable hard drives, USB flash drives, tablets, and other portable devices. It even applies to removable media such as CDs, DVDs, and backup tapes.

When you are ready to dispose of any computing equipment, contact your IT staff and follow the proper procedure.

6.9 Reporting Security Incidents

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

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

If you have an urgent or ongoing IT security incident that requires immediate assistance, and your IT staff are unavailable, contact your campus IT Service

Desk or IT Security staff - whichever is appropriate at your institution or agency.

It is important that you know who to contact and how to respond to security incidents in a timely manner. So, contact your unit in advance and have that information handy.

6.10 Additional Resources

Additional courses are available in TRAINTRAQ to all Texas A&M System employees that cover other aspects of information security such as FERPA, HIPAA, international travel safety, export control laws, FAMIS, and COMPASS. These courses provide specific information not mentioned in this training. Check the Resources link in the top right for Internet resources mentioned in this course, a traveling tips handout, and a print version of this course.

6.11 Section 5 Summary

Know the warning signs of malware, follow the prevention strategies and seek immediate help if you believe your computing device is compromised or infected.

Take action to protect your devices, accounts, and information when traveling. Download the **International Travel Handout** for more information.

Use your computer's firewall to block hackers, viruses, and other potentially malicious traffic on the Internet.

Contact your IT staff when it's time for the secure disposal of your computing or storage devices.

Report security incidents immediately to your IT staff.

7. Mastery Test and Data User Agreement

If you're completing the alternative version of this course, you must complete the 25-question test, and then read the Texas A&M System Member Data Use Agreement and course acknowledgement. Once completed, submit your answers to training@tamus.edu, and verify you've read the Texas A&M System Member Data Use Agreement and agree to comply.

7.1 Test Questions

1. Which of the following are examples of education records protected by FERPA? Select all that apply.

    a. Transcripts

    b. Grade reports

    c. Disciplinary records

    d. Student employment records

2. Select the following parties who can obtain non-directory information without written permission from the student under FERPA. Select all that apply.

    a. University officials who have legitimate educational interests.

    b. Third-party contractors or organizations (e.g., the National Student Clearinghouse) that have a legitimate educational interest in the student's record.

    c. A law enforcement agent who has a lawfully issued subpoena.

    d. The spouse of the student.

3. The Texas Public Information Act (TPIA) specifies any recorded information owned or accessed by government institutions are presumed to be public. Which of the following are NOT considered public? Select all that apply.

    a. Employee emails

    b. Employee home address and phone number

    c. Audit working papers

4. How can you ensure that Sensitive Personal Information (SPI), such as Social Security Numbers, remains confidential? Please choose all that apply.

    a. Review and follow my institution's procedures on use and retention of Social Security Numbers.

    b. All SPI should be encrypted.

    c. Unneeded SPI should be eliminated.

    d. Social Security Numbers should be replaced with another means of identification, such as the Universal Identification Number, or UIN.

5. Which of the following circumstances can your export control office provide guidance? Select all that apply.

    a. Hiring foreign persons

    b. Speaking at multinational conferences

    c. Shipping items out of the country

    d. Conducting business with international entities and foreign persons

6. Which of the following sets of items should be encrypted when stored or shared with those that have an approved business need?

    a. directory information and budget reports

    b. student records and medical records

    c. student participation in officially recognized activities and student participation in sports

7. A teaching assistant goes to a coffee shop so he can focus on grading his students' essays. He leaves his laptop and papers on the table as he gets up to refill his coffee. When he returns, his laptop is gone, which had the list of his students' names, ID numbers, email addresses, and their grades. Even though this was an accident, what are the potential consequences the teaching assistant and his university could face? Select all that apply.

    a. reduction in federal funding

    b. negative publicity for the university

    c. personal embarrassment

8. What process should you use before sending or storing confidential information so that it is only readable to you and your intended recipient?

    a. Stenography

    b. Encryption

    c. Translation

9. Select all the following actions that will protect your data and ensure it is available when you need it.

    a. Save a copy of the file to at least two forms of storage media.

    b. Update your backups anytime your data changes.

    c. Check with my IT staff to make sure my data is being backed up.

10. True or False? You should routinely test backup procedures to ensure that individual files and directories can be restored properly.

    a. True

    b. False

11. Assigning individual computing accounts to people helps ensure that:

    a. Only authorized individuals have appropriate access to computing resources

    b. Everyone can be logged in simultaneously.

    c. Individuals can share their login information to only those of their choosing.

    d. IT staff are able to get an accurate headcount of users for audits and self-assessments.

12. Which of the following are your responsibilities as a user of A&M System computing resources? Select all that apply.

    a. Complying with laws, policies, regulations, rules, licensing agreements, and contracts

    b. Only using computing resources for their intended purposes or incidental personal use

    c. Acting responsibly and ethically, and respecting the rights of others in online forums

    d. Protecting confidential information to which you have access

13. Which of the following consequences may happen if you fail to fulfill your responsibilities with computing resources? Select all that apply.

    a. The restriction or denial of access to computing resources or privileges

    b. Disciplinary action

    c. Law enforcement involvement

14. Which of the following are unauthorized uses of computing resources? Please choose all that apply.

    a. Using your account or computer for illegal activities.

    b. Reporting individuals for misconduct.

    c. Intentionally damaging or destroying property that belongs to the A&M System or other users.

    d. Transmitting unsolicited offensive, profane, obscene, bigoted, sexist, or other discriminatory

15. Which of the following criteria must be met to use A&M System computing resources for personal reasons? Select all that apply.

    a. I don't do it excessively or for long durations.

    b. It does not interfere with my assigned job duties.

    c. I don't use it for personal financial gain.

    d. I don't use A&M System-owned computing resources to support a non-A&M System business.

16. Which of the following tactics are used in social engineering? Select all that apply.

    a. impersonation

    b. manipulation

    c. brute force password cracking

17. Spear phishing emails may contain:

    a. Your name

    b. Your job title

    c. Specific information about your job role

    d. All of the above

18. True or False? You are not allowed to share confidential information about your organization on social media.

    a. True

    b. False

19. What are some ways to verify the validity of an email you're unsure about? Select all that apply.

    a. Reply back to the sender and ask for more information

    b. Check the sender email address to see if it is from an official account

    c. Hover your mouse to reveal misleading hyperlinks

    d. Open the attachments

20. Social networks can be used by attackers to gather information about you. Which of the following messages minimizes the amount of personal information you share about yourself?

    a. Sharing details about your upcoming vacation

    b. Sharing about your vacation experience after you return

    c. Sharing the name of your bank and your recent experience

21. Which of the following are indicators that your computer might be compromised with malware? Select all that apply.

    a. Your PC frequently crashes

    b. You have suspicious new files

    c. Your PC works faster than normal

    d. You notice encrypted files you didn't encrypt yourself

22. Which of the following actions should you take if you suspect malware on your personal device?

    a. Ignore it

    b. Stop doing things that require passwords or personal info

    c. Delete files your antivirus flags as malware

    d. Update your security software and run a system scan

23. True or False? Don't travel with confidential, sensitive, proprietary, research or controlled information even if it's encrypted.

    a. True

    b. False

24. If you think a security incident may have occurred, you should:

    a. try to investigate it yourself.

    b. report it to your IT staff the appropriate person in your organization (e.g., IT staff, IT Security, IT Service Desk).

    c. not worry about it because IT staff probably detected it already.

    d. immediately turn off the computer and unplug it

25. The State of Texas requires secure disposal (destruction or sanitization) of which of the following items? Please check all that apply.

    a. Removable hard drives

    b. Tablet computers

    c. USB flash drives

    d. Backup tapes

End of Mastery Test. Please review the Data Use Agreement below.

7.2 Texas A&M System Member Data Use Agreement

- Revised: June 29, 2018

Please read the following agreement carefully and completely before agreeing.

This Agreement applies to any user of Texas A&M System member institution (hereafter referred to as "institution") Information Resources. The purpose of this Agreement is to inform you of your principal obligations concerning the use of institution Information Resources, and to document your Agreement to abide by these obligations.

"Information Resources" has the meaning defined in Texas Government Code § 2054.003(7): ". . .the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors." Additionally, data impacted by the aforementioned is included as Information Resources.

Under Texas Administrative Code §202.72(3), the user of an information resource has the responsibility to:

(A) use the resource only for the purpose specified by the institution or information-owner;

(B) comply with information security controls and institution policies to prevent unauthorized or accidental disclosure, modification, or destruction; and

(C) formally acknowledge that they will comply with the security policies and procedures in a method determined by the institution head or his or her designated representative.

7.2.1 Confidential and Controlled Information

As an employee of the member institution, you may have access to confidential or controlled information through use of institution Information Resources or through your associated activities with institution information systems. Confidential and controlled information includes identifying information, federal tax information, personal health information, criminal justice information, or any information that is classified as confidential or controlled by federal or state law, by institution policy, or is defined as "Personal Identifying Information" under Texas Business and Commerce Code §521.002(a)(1) or "Sensitive Personal Information" as defined by Texas Business and Commerce Code §521.002(a)(2).

As a user of institution systems, you are required to conform to applicable laws, Policies, Regulations and institution Rules, Standard Administrative Procedures and Controls governing confidential and controlled information.

Your principal obligations in this area are outlined below. You are required to read and to abide by these obligations.

I UNDERSTAND THAT:

- In the course of my job, I may have access to confidential and controlled information related to:
    - Customers, employees, users, contractors, and volunteers (e.g., records, conversations, applications, financial information). This may include any information by which the identity of a person can be determined, either directly OR indirectly.
    - institution functions (e.g., information protected by the attorney-client and attorney work product privilege, financial information, employment records, contracts, federal tax information, internal reports, memos and communications.).
    - Third parties (e.g., vendor information, customer information, contracts).

I AGREE THAT:

- I will, at all times, safeguard and retain the confidentiality, integrity and availability of confidential and controlled information.
- I will only access confidential and controlled information for business needs.
- I will not in any way divulge, copy, release, sell, loan, review, alter, or destroy any confidential or controlled information except as authorized.
- I will not misuse or carelessly handle confidential and controlled information.
- I will ensure that confidential and controlled information when appropriate, including when emailing such information outside the institution and when storing such information on portable electronic devices and portable storage devices is encrypted.
- I will safeguard and will not disclose my password or other authorization I have that allows me to access confidential and controlled information, except as permitted by law.

- I will report activities by any other individual or entity that I suspect may compromise the confidentiality, integrity or availability of confidential and controlled information.
- My privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.
- I have no right or ownership interest in any confidential or controlled information referred to in this Agreement. The institution may revoke my access to confidential and controlled information at any time and without notice.

7.2.2 Authorized Use

I AGREE THAT:

- I will use Information Resources only for official state-approved business.
- I will not use Information Resources for personal reasons unless there are specific limited use exceptions permitted by the institution division to which I am assigned.
- I have no right to expect privacy in my use of institution Information Resources or in the content of my communications sent or stored in institution Information Resources. All user activity is subject to monitoring, logging, and review.

7.2.3 Personal Security Identification Codes (User IDs and Passwords)

I AGREE THAT:

- I will receive and will be required to use a personal security identification code (e.g., User ID and Password) to gain access to and to use Information Resources.
- My user ID and password are security measures that must be used only by me and I will not disclose my password to anyone.
- I will be held personally responsible for any transactions initiated, actions taken, or for any harm, loss, or adverse consequences arising from the use of my user ID and password, including any unauthorized use by a third party if such party gains access to my user ID and password due to my misconduct or failure to abide by institution policy.

7.2.4 Software

I AGREE THAT:

- I will only install or use software on institution computers that has been properly licensed and approved for my use in accordance with institution policies and procedures.
- If installing or authorizing the installation of software on institution computers, I will be responsible for ensuring that such software is only used in a manner that complies with the terms of the applicable software license agreement and all applicable institution policies and procedures.

7.2.5 Access to Data

I AGREE THAT:

- Proper authorization is required for access to all data owned by institution, except data that has been authorized by the institution for public access.
- I will not attempt to access or alter any data that I am not authorized to access in the performance of my job duties or incidental use.
- I will use appropriate measures to prevent others from obtaining access to institution data, such as securing my workstation either by logging off or using a password-protected screen saver.
    - Before leaving a workstation with access to files containing confidential or controlled information, I will log-off or activate a password-protected screen saver.
    - If I receive a request for the release of institution information or data, I will follow institution's policies and procedures for the release of information.

7.2.6 Security of Equipment

- I AGREE THAT:
- I will not remove Information Resources from institution property without proper prior authorization and approval of staff with appropriate authority.
- I will immediately report all security incidents, including the loss or theft of any Information Resources or data, to institution management and to the institution Information Security Officer.

7.2.7 I agree that:

- I am required to be aware of, read, and comply with the information presented in my institution's Rules, Standard Administrative Procedures (SAPs), and Controls, regarding information security.
- I must also comply with the Rules, SAPs, and Controls concerning Information Resources set out by my institution as well as any changes to those policies.
- I must comply with the information security practices and guidelines of the institution division that employs me, including any changes to those practices and guidelines if such practices and guidelines exist.
- My failure to comply with this Agreement may result in loss of access privileges to institution Information Resources or other disciplinary action up to and including termination for employees; termination or alteration of employment relations in the case of temporaries, contractors, or consultants; or dismissal for interns and volunteers. Additionally, individuals could also be subject to additional civil liability, and/or criminal charges.

7.2.8 System Member Rules, SAPs, and Controls

Please review the rules, SAPS and Controls for your institution or agency.

Texas A&M AgriLife Extension

Texas A&M AgriLife Research

Texas A&M Forest Service

Texas A&M University

- Texas A&M Information Security Controls Catalog
- Texas A&M University Rules and SAPs

Texas A&M University at Galveston

- Texas A&M Information Security Controls Catalog
- Texas A&M University Rules and SAPs

Texas A&M Health Science Center

- Texas A&M Information Security Controls Catalog
- Texas A&M University Rules and SAPs

Texas A&M Transportation Institute

- Texas A&M Transportation Institute Security Controls Catalog
- Texas A&M Transportation Institute Rules

7.2.9 Course Acknowledgement

I acknowledge I have completed the Information Security Awareness training, and I 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.

7.2.10 Final Instructions

When submitting your completed mastery test to training@tamus.edu, please indicate you have reviewed the User Agreement, and that you agree to follow the terms.