Information technologies are a part of your daily work. Understanding information security and protecting Texas HHS Information and Information resources is critical.

Employee Responsibilities

As an employee, you are a user of Texas HHS information and information technology. You may be authorized to read, enter, or update information.

- It is your responsibility to use Texas HHS Information Resources only for the purposes for which you have been approved.
- You must also comply with Texas HHS security measures, including those in the HHS Acceptable Use Agreement (AUA) which is signed within the HHS System Portal by employees.
- The HHS System Portal administered by HHS Identity and Access Management is used to electronically track AUAs, including yearly re-validation for all state employees, contractors, and private providers.
- You are accountable for all actions performed under your user identification (user ID).
- Protect your area by keeping unauthorized individuals away from your equipment and data (including printed documents with confidential data).
- Report information security threats or violations by following your agency's security reporting procedure.

Supervisor Responsibilities

When an employee, contractor, or vendor leaves a Texas HHS agency, supervisors **are required** to immediately terminate access to all HHS Information Resources, in accordance with agency procedures.

Failure to properly separate an employee from HHS, could result in the organization receiving costly fines or penalties for allowing unauthorized access to confidential data or systems.

Data Classification - Understanding Types of Data

Texas HHS has three types of data. Learning the different types will help you understand the various rules for protecting information (any communication or record whether oral, written, electronically stored or transmitted, or in any other form).

Data is classified as:

- Confidential
- Agency Sensitive
- Public

The Texas HHS Data Classification Standard provides additional guidance on the required protections for information. Below are the definition, examples, and potential consequences that could occur for public disclosure of each type.

Public Data Classification

Public	
Definition	• Information that is freely and without reservation made available to the public • Information intended or required for public release as described in the Texas Public Information Act
Examples	• Agency publications • Press releases • Public web postings
Consequences of Public Disclosure	• No adverse consequences

Agency Sensitive Data Classification

Agency Sensitive	
Definition	• Information that is not subject to specific legal, regulatory or other external requirements, but is considered Texas HHS sensitive and should not be readily available to the public • Information must be protected even though disclosure is not specifically restricted by legal or regulatory requirements
Examples	• Legal information such as non-disclosure agreements and contracts • Financial information such as balance sheets, purchase orders and budget information • Internal organizational charts and contact lists • Internal communications • Internal operational procedures • Information pertaining to HHS legal proceedings Intellectual property, such as copyrights, patents, and trade secrets
Consequences of Public Disclosure	• Loss of reputation • Loss of trust

Confidential Classification

Confidential	
Definition	• Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement • Information that is exempt from the Texas Public Information Act • Certain types of confidential data come with additional requirements beyond normal confidential levels. These types of data can come with additional civil and criminal penalties if mishandled

Examples	"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to Contractor or that Contractor may create, receive, maintain, use, disclose or have access to on behalf of HHS that consists of or includes any or all of the following: • Client Information • Protected Health Information (PHI) in any form • Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521 • Federal Tax Information (FTI) • Personally Identifiable Information (PII) • Criminal Justice Information • Social Security Administration (SSA) Data including Medicaid Information • Education Records • All privileged work product • All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552. • Other regulatory data type
Consequences of Public Disclosure	• Criminal Penalties, Civil Penalties, Severe reputational harm, Lack of public trust • Federal investigation or loss of right to collect or match information through data sharing agreements • Criminal charges that may result in imprisonment for misuse of HHS Information Resources or confidential Information • Immediate suspension of access privileges and revocation of access to HHS Information Resources, confidential information or agency sensitive information • Disciplinary action, up to and including dismissal

Protecting Confidential Data - Regulated Data

The Internal Revenue Service Federal Tax Information (IRS FTI), Social Security Administration (SSA), Federal Bureau of Investigation (FBI), and Centers for Medicare/Medicaid Services (CMS) are Federal Agencies that share data with HHS.

Some Federal programs such as the SSA have unique data protection requirements or safeguards (e.g. restricted use, proper usage and protections, and disposal of information, etc.) These requirements instruct the employees, contractors, and agents of the safeguards necessary to meet compliance.

It is the information owner and custodian responsibility to ensure the system and its users meet the necessary compliance requirements prior to accessing a system with Federal agency data (e.g. IRS, SSA, CJIS). This includes ensuring that contractors adhere to the safeguard requirements of the Federal agencies when mandated by a contract and interconnection security agreement.

For a complete list of applicable standards for each Federal agency see IS-CONTROLS 2.1.2.

Protecting Confidential Data – E-mail: Internal Requests

Internal requests are emails sent to anyone at HHS, DSHS or DFPS are sent using secure methods. Information in the body of the email should be kept to the minimum necessary to conduct the business at hand.

If you have any questions about how to respond to a request, contact the Texas HHS Privacy Office: privacy@hhsc.state.tx.us. DSHS staff should direct their privacy questions to the DSHS Privacy Office:HIPAA.Privacy@dshs.texas.gov.

Protecting Confidential Data – E-mail: External Requests

External Requests are email requests for confidential or agency sensitive information from outside any of the Texas HHS agencies that:

- Only provide the requested information to the individual the information relates to, or the person's legally-authorized representative.
- Do not include confidential or sensitive information in an email response. This may require deleting confidential information sent in the original email.

If the answer to the inquiry requires you to include confidential information, email the requestor **using a Texas HHS approved encryption method**.

Approved Encryption Methods for Sending Secure Emails

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not prevent interception but denies the unauthorized persons and software the ability to interpret the message content.

You can use a designated trigger word or symbol in the subject line or body of the email. This will automatically change the sensitivity of the message from "Normal" to "Confidential." Use "$$", "[encrypt]" or "***secure***" and this will cause Outlook to automatically encrypt the email.

The other method is changing the message sensitivity. You must:

1. Open a new message.
2. Click on the File tab.
3. Click on the Properties box.
4. Click the Sensitivity drop-down menu and choose Confidential.

Approved Encryption Methods for Sending Secure Emails, Cont.

If you send a secure email to an external recipient, they will get a message with an encrypted attachment. To see the content, they must sign in with a Microsoft account or use a one-time passcode. They can find instructions for reading an encrypted email and signing up for a Microsoft account on the HHS Email Encryption webpage.

Do not place "confidential" or "agency sensitive" in the subject line of any email. The subject line is not protected by encryption. This includes social security numbers, or other personally identifiable information. For a list of confidential information see the previous pages on Data Classification

Password-protected documents are not considered a secure method to send confidential information. The password may be broken using tools available on the internet.

For help on sending and receiving encrypted messages, see the How to Send Secure Emails PDF.

Skype for Business and Instant Messaging

Instant messaging (IM) software allows you to communicate in real time with other Texas HHS employees. It is important to remember the following information about IM:

- Use of other IM systems is prohibited except for specific instances approved by an IRM for Texas HHS agency business purposes only.
- Messages are subject to security monitoring and employees should have no expectation of privacy.
- IM communication is not approved (to include screen sharing) for certain types of confidential information (e.g. Federal Tax Information, Social Security Administration Data, Criminal Justice data, etc.).
- Usage of the IM for confidential data or any changes or exceptions must utilize the Enterprise Change Management process. This change will be initiated by the respective agency's Office 365 administrative lead according to the process as defined in the Enterprise Skype for Business Change Management Process, see the HHS Instant Messaging Policy (Microsoft Skype for Business) –HHS-IT-02
- Personal use must not interfere with the normal performance of work duties and must not result in direct costs to any Texas HHS agency.

Skype for Business and Instant Messaging, Cont.

All IM communication should contain only transitory - not substantive - information. Transitory Information records are:

- For state record retention purposes
- Records of temporary usefulness
- Not essential to the fulfillment of statutory obligations,
- Not regularly filed within an agency's recordkeeping system
- Required only for a limited time to complete an action

As a result of their transitory content, IMs will not be retained by IT beyond 48 hours from the day on which they are created.

The Profile photo for Office 365, which is displayed in Skype for Business, must be an actual business appropriate photograph of the user and suitable for purposes of physical identification.

Texting

Text messaging is not an approved method for communicating confidential information.

All text messages sent or received through a cellular device to conduct state business are the property of Texas HHS and therefore subject to records retention requirements. This includes text message sent through personal devices as well as state-owned devices.

The HHS Text Message Policy, that provides information for documenting text messages in order to meet the state records retention requirements, can be located here: https://hhsconnection.hhs.texas.gov/rights-responsibilities/records-management#text-message.

Contact your supervisor for guidance if you think your job responsibilities may require you to use text messages.

Faxing

Faxing confidential and agency sensitive data is an approved, secured transmission method.

Use a cover sheet with the following statement:

Confidential: This transmission is confidential and intended solely for the use of the individual or entity to which it is addressed. If you received this transmission in error, please return to sender.

When sending faxes:

- Verify recipient's fax number prior to sending information.
- Make sure someone authorized to receive the information is there to receive the fax.

- Don't leave information on fax machines after faxing.

Faxing, Cont.

When receiving faxes:

- Quickly retrieve faxes transmitted to you.
- Secure faxes that have not been retrieved.
- If you are expecting a fax and have not received it, follow-up to ensure the sender has the correct fax number.

	If protected information is sent to an incorrect fax recipient, report it immediately to the HHS IT Help Desk, agency Information Security Officer (ISO) and agency Privacy Officer.

Information Resources and Expectation of Privacy

Texas HHS has the legal right to monitor use of Texas HHS Information Resources. Texas HHS monitors use to ensure these resources are protected and to verify compliance with applicable law, Texas HHS policy, and security standards and controls.

By using Texas HHS Information Resources, you consent to the monitoring of your use of these resources and information in any form and on any device. You have no expectation of privacy when using any of these resources.

Without advanced notice, Texas HHS agencies reserve the right to:

- Monitor voicemail and text messages
- Monitor messages sent over the email system
- Monitor internet usage
- Monitor the electronic files of HHS employees
- Examine any state-owned equipment or property

Acceptable Use - Internet

The Texas HHS internet connection is intended to support official agency business. You may use the internet for limited personal purposes in the same way you may use the telephone for limited personal purposes.

You must NOT use the internet for activities that interfere with the performance of official Texas HHS duties and normal work activities, including:

- Listening to or watching audio or video broadcasts that are not work-related
- Initiating, distributing, or forwarding chain letters
- Subscribing to unauthorized mailing lists, mail services, list servers, chat rooms, or electronic discussion groups
- Solicitation
- Personal business activities
- Viewing offensive or harassing statements, including comments based on race, color, national origin, age, sex, religion, disability, genetic information or veteran status
- Viewing, sending, downloading, or storing sexually oriented messages or images

The HHS Social Medial Policy (Circular - 042) details what is allowed when using social media.

Acceptable Use - Office Equipment

You must limit personal use of state office equipment. Personal use must not increase the state's costs for supplies, such as paper or toner. Printing personal documents is prohibited.

Do not use Texas HHS Information Resources to play computer games unless there is an HHS-approved, business-related purpose. For example, using a computer game for therapy or rehabilitation with a consumer would be considered an agency-approved, business-related purpose.

Acceptable Use - Email

Your Texas HHS email address may be used for limited personal purposes in the same way the telephone may be used.

Do not respond to requests for your work email address, except for business-related purposes. Giving your agency email address provides a potential opportunity for businesses and individuals to send spam or junk email to you. Spam or junk email may contain harmful code and viruses.

More information on the Acceptable Use Policy (AUP) and Acceptable Use Agreement (AUA) can be found here: https://hhsconnection.hhs.texas.gov/it/information-securitycybersecurity/information-security-policy-other-requirements.

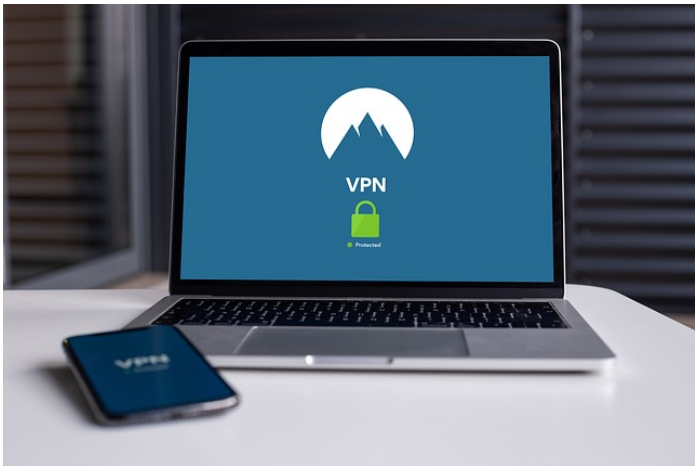
Remote Access Security

Be vigilant about protecting Texas HHS information and information resources when on travel or working at remote locations. It is your responsibility to protect HHS technology and resources that are assigned to you when you are outside of the office.

Here are more important tips for protecting information systems while working outside the office.

- Turn off your laptop while traveling so that encryption is enabled. If you are unsure if your helpdesk is encrypted contact the HHS Helpdesk for confirmation prior to traveling.
- Always maintain possession of your laptop and other mobile devices.
- Ensure that the wireless security features are properly configured by using only the approved secure Virtual Private Network (VPN).
- Be cautious when establishing a VPN connection through a non-secure environment (e.g., hotel, coffee shop, etc.). Do not work on sensitive material when using an unsecure connection.

- Report a loss or theft of your laptop or other government furnished device immediately to the HHS IT Consolidated Help Desk. For more information see HHSC Reporting a Lost/Stolen Device Process.



Teleworking

It is important to protect information and data while teleworking. In order to protect information, remember the following:

- Always maintain possession of your laptop to prevent loss or theft.
- Only use authorized equipment in authorized locations.
- Use a screen protector so sensitive information cannot be seen by others.
- Report lost or stolen equipment immediately.

Teleworking, Cont.

There are special responsibilities for protecting PII during telework: You must follow standard security procedures when removing official records from the office, and have permission from your manager to transport, transmit, remotely access or download sensitive or classified information during telework. Texas HHS encryption is critical. It's extremely important to store sensitive information on authorized mobile devices or remote systems with appropriate safeguards. Remotely access sensitive information by using authorized methods (e.g., VPN).

You must receive approval and satisfy Texas HHS requirements for telework. For more information see: https://hhsconnection.hhs.texas.gov/hr/pay-benefits-telework.

Physical Security

Physical security is an important information systems safeguard. Limiting physical access to information system resources and infrastructure to authorized personnel diminishes the likelihood that information will be stolen or misused.

Locked doors, security badges, and security guards also protect you and your co-workers. These security measures:

- Restrict access to authorized persons only.
- Reduce exposure to malicious threat.
- Allow access privileges to be revoked quickly, if necessary.
- Prevent Piggybacking.

Physical Security - Computing Device

Computing devices include desktops, laptops, tablets, smart phones, USB devices, and other technology used to access agency data. Take precautions to ensure that mobile computing does not compromise the security of Texas HHS Information Resources or data.

Confidential and sensitive information, in paper or electronic form, must be protected from unauthorized use or disclosure. To prevent unauthorized use, you should:

- Secure paper documents with confidential or sensitive data in a locked cabinet
- Lock your workstation when you leave your desk
- Always take the device with you – avoid leaving portable devices unsecured

Physical Security - Security Badges

Security badges identify you, identify your access privileges, and prevent unauthorized access. Badge-reading devices must not be disabled or bypassed. Electronic card readers log the identity, time, date, and access privileges of each entry attempt.

Never share your security badge. All employees, visitors and vendors must wear visible photo ID badges issued by security guards in HHS buildings. If you forget or misplace your badge, go to your building's security desk to get a temporary one.

Physical Security - Security Badges, Cont.

Unauthorized entry into the workplace is always considered a security risk. If you notice a fellow employee not wearing a badge, you can politely remind them about the policy if you're comfortable doing so. Otherwise, report it to building security or your supervisor.

If the problem continues, contact your local office coordinator if you work in a regional office. If you work in a state office, call Facility Management at 512-424-6970 or email facilitymanagement@hhsc.state.tx.us.

Physical Security - Tailgating

Tailgating happens when an unauthorized individual follows an authorized individual to enter a secured area, resulting in a breach of physical security.

In order to combat tailgating, use the following information:

- Employees must use their own badge to enter security doors.
- Never allow anyone to follow you into a secure area without his or her badge.
- Be aware of procedures for entering a secure area.
- Securing your workstation when you leave the office and during emergencies.
- Escort visitors to and from your office and around the facility.
- Do not allow anyone else to use your employee badge for building or secure area access.
- Report any suspicious activity to the security office.

Access to System Security - User Credentials

You are required to enter a user ID and password to use Texas HHS Information Resources. Your credentials are a security measure and must be used only by you.

Under no circumstance can you allow your credentials to be used by any other individual, nor can you use credentials belonging to someone else. Do not share your password with anyone.

Access to System Security - Passwords

Passwords are used to prevent unauthorized access to confidential information, provide user authentication and establish user accountability.

Create passwords that are not easily discoverable by others. Use a combination of upper and lower case, numbers and special characters. Change your password no less than every 90 days.

Passwords are used to grant access to:

- Systems that reside at any Texas HHS facility
- The Texas HHS network
- Stored Texas HHS information

Access to System Security – Passwords, Cont.

All passwords should be treated as confidential.

- Do not share your Texas HHS password with anyone, including administrative or IT staff.
- Do not write passwords down and store them anywhere in your office.
- Do not use the same password for HHS accounts and non-HHS account.
- Do not use the "Remember Password", auto logon, embedded scripts, or hard-coded password features outside of approved Texas HHS systems.

Access to System Security – Passwords, Cont.

If you suspect that your password has been discovered or used by another person, immediately change your password and report the incident to the HHS IT Consolidated Help Desk.

Self-service password reset tool, Password Manager, allows you to change or reset your Windows password. Open How to Manage Your Windows Password for helpful information on how to get started with password manager, change your password, and more.

Records Management

Records management is a system for keeping records for the appropriate length of time. Government Code 441.185 requires state agencies to maintain and dispose of records according to each agency's established retention schedule. Your retention schedule is a document that lists general types of records, called "record series," and how long they are legally required to be kept.

The format of a record does not affect how long it is retained, it is the information contained in a record that determines the length of time it is kept. Records may be electronic files such as Word, Excel, and PowerPoint documents; email; website content; social media posts; text or instant messages; databases; or scanned images. Records may also be in other formats such as paper, microfilm or microfiche.

Records are classified by their content and not by format, so there is no record series for "email" for example, but instead, what is discussed in the email determines what record series it is classified under.

Records Retention

Records that have met retention requirements must be disposed of appropriately, and agencies are required to document the disposition. The HHS Records Management Office can provide information on how to document the disposition of your records using the System of Automated Records (SOAR).

For information about your agency's retention schedule, visit the Records Management Webpage or contact the HHS Record Management Office at records@hhsc.state.tx.us.

Media Protection - Media Disposal

Simply deleting electronic files does not necessarily prevent access to the sensitive information stored on electronic media. Sensitive or confidential information stored on electronic hardware and media (e.g., hard drives, CDs, smart phones, printers and faxes with storage capabilities, etc.) must be destroyed in a secure manner. Contact HHS IT Consolidated Help Desk for questions regarding the proper deletion of confidential information.

Items that may also require secure disposal include: paper documents, audio or video recordings, magnetic tapes, removable disks, cassettes, flash drives and hard drives.

Most HHSC and DSHS offices have locked bins for collection of confidential records to be shredded. Before placing official state records into the bins, the destruction must be documented (this does not apply to convenience copies or non-records).

Visit Document Services for more information.

Media Protection - Media Marking

Stored data must have, at a minimum, the following data clearly identifiable by labels:

- System Name
- Creation Date

- Sensitivity Classification (based on applicable record retention regulations)
- HHS Contact Information

Media Protection - Media Storage

Media used in the provision of backup storage must be protected in accordance with the highest level of sensitivity of the information being stored. Remember the following when protecting stored information:

- Digital media includes diskettes, magnetic tapes, external/removable hard disk drives, flash/thumb drives, diskettes, compact disks, and digital video disks.
- Non-digital media includes, for example, paper and microfilm.
- For confidential data, encrypt digital media via a FIPS 140-2 compliant encryption module.
- If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information.

Media Protection - Media Transport

Digital media must be protected and controlled during transport outside of controlled areas by using encryption and for nondigital media tamper-evident packaging. Use the following guidelines for transporting media:

1. If media is hand carried, use a securable container (e.g., locked briefcase) via authorized personnel.
2. If media is shipped, it must be trackable with receipt by commercial carrier.

Activities associated with transport of Texas HHS Information System media must be restricted to authorized personnel only.

Bring Your Own Device (BYOD)

Under the BYOD program, Texas HHS lets you use a personal cellphone to access agency resources such as email, contacts, and calendar. You must read the applicable policy documents which outlines the responsibilities you and HHS have for managing and securing agency data on the device. The BYOD program requires certain control over your personal device in exchange for access to HHS resources. The following is important to know if you will be using the BYOD program:

- You must meet BYOD eligibility requirements.
- Texas HHS has no responsibility for BYOD devices or their costs.
- Notify the HHS IT Consolidated Help Desk immediately if your BYOD device is lost or stolen.

For additional information and requirements on the BYOD program please visit: https://hhsconnection.hhs.texas.gov/it/equipment-software/personal-wireless-device-or-bring-your-own-device.

Software and Subscription Services

Only properly licensed software may be used on Texas HHS Information Resources. Employees cannot install or use any software on HHS Information Resources that has not been approved for use in accordance with HHS policies and procedures. Downloading unapproved software risks introducing malicious code into the network.

See the HHS IT Software and Subscription Service Policy for information on requirements for software and subscription services including requirements related to requesting, purchasing, licensing, installing, removing, auditing, and tracking.

What are Threats, Vulnerabilities, and Risks?

Threats and vulnerabilities put information assets at risk.

Threats are the potential to cause unauthorized disclosure, change, or destruction to an asset. The impact of threats is potential breach in confidentiality, integrity failure, and unavailability of information.

There are three types of threats:

- Natural
- Environmental
- Manmade

Vulnerabilities are any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.

Risk is the likelihood that a threat will exploit a vulnerability.

Threat Actors

A threat actor is an individual or a group posing a threat and can be an individual, autonomous attacker to a well-resourced group operating in a coordinated manner.

These individuals perform activities called attacks on organizations in an attempt to gain unauthorized access to system services, resources, or information or attempt to compromise system integrity, availability, or confidentiality.

Different types of threat actors and their motivations include:

- **Government Sponsored** groups are often looking for competitive information, resources or users that can be exploited for espionage purposes
- **Organized Crime** are typically either looking for the personally identifiable information (PII) of your customers or employees, such as social security numbers, health records, credit cards, and banking information, or to hijack and ransom critical digital resources

Threat Actors, Cont.

Different types of threat actors and their motivations include:

- **Government Sponsored** groups are often looking for competitive information, resources or users that can be exploited for espionage purposes.
- **Organized Crime** are typically either looking for the personally identifiable information (PII) of your customers or employees, such as social security numbers, health records, credit cards, and banking information, or to hijack and ransom critical digital resources.
- **Hactivists** have a political agenda and their ultimate goal is to either create high-profile attacks that help them distribute propaganda, or to cause damage to organizations they are opposed to.
- **Insider Threat** attackers operate inside an organization and are typically disgruntled employees or ex-employees either looking for revenge or some type of financial gain.
- **Opportunistic** actors are usually amateur criminals who are driven by the desire for notoriety.
- **Internal User Error** actors are employees making mistakes with configurations and can be the largest threats to an organization.

Malware

A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge that performs malicious actions. It can self-replicate, inserting itself onto other programs or files, infecting them in the process.

Malware is a malicious computer software program designed to infiltrate and damage computers without the user's consent.

Malware, Cont.

Malware is the general term covering all the different types of threats to your computer safety such as:

- **Viruses** – a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
- **Spyware** – unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.
- **Worms** – a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.
- **Trojans** – a malware that is often disguised as legitimate software.
- **Rootkits** – collection of malicious software designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.
- **Ransomware** – a malware designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by visiting an infected website.

Tips to Combat Malware

Use the following tips to combat malware:

- If possible read email in plain text and do not use the preview pane.
- Scan attachments with antivirus software before downloading.
- Always think twice before clicking on links or opening attachments (even if they look like they are from someone you know).
- Delete suspicious emails without opening them.
- Make sure you are on a secure connection. Look for the padlock icon to the left of the URL. If it's there, then that means the information passed between a website's server and your browser remains private. In addition, the URL should read "https" and not just "http."
- Use strong passwords. Never use the same password on multiple accounts.
- If it's suspicious, report it to the HHS IT Consolidated Help Desk. This is an important habit in general; if something doesn't seem right, ask!

Virus Protection Software

Computer virus protection software is installed on your computer. It is the first line of defense against an attack and **must not** be disabled or bypassed. Never cancel anti-virus software scans. This leaves your computer vulnerable, which can allow for a virus to move onto the network.

Immediately contact HHS IT Consolidated Help Desk for further instruction for any of the following situations:

- A virus is on your computer, that is not automatically cleaned by the virus protection software.

- An email with an attachment is received and you suspect it contains a virus or other malicious code. Do not open or forward the attachment. This will cause the virus to spread and has the potential for causing very serious damage to your computer and the entire computer network
- Your antivirus software or other core software on your computer is not patched, or up-to-date.

Social Engineering

Social engineering is typically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and information for fraudulent or criminal purposes. Social engineering attacks are more common and more successful than computer hacking attacks against the network.

Some individuals may appear trustworthy but may be sophisticated cyber criminals. They use social engineering techniques to obtain your personal information, access sensitive government information, and even steal your identity.

Social Engineering Attacks

Social engineering attacks are based on natural human tendencies such as:

- Trust
- Desire to help
- Desire to avoid conflict
- Fear
- Curiosity
- Ignorance
- Carelessness

Common targets are:

- Passwords
- Financial information
- Access to secure areas of the building
- Employee's personal information
- Sensitive or confidential agency information

Phishing

Phishing is when an attacker uses fraudulent emails or texts, or copycat websites to get you to share sensitive information– such as account numbers, Social Security numbers, or your login IDs and passwords. Attackers use your information to steal your money, identity, or both.

Phishing attacks are **specific, targeted strikes** against you and your organization most commonly presented in emails with file attachments or mislabeled hyperlinks. With the popularity of social media today, hackers are able to easily research information about their victims, and then choose how they want to launch an attack.

Below is a list of the types of phishing. Each will be defined on the following page:

- Email
- Texting (SMS)
- Phone Scams
- Keyloggers and Screenloggers
- Session Hijacking
- Pharming
- Content Injection
- Spoofing
- Network Fraud
- Pretexting

Types of Phishing

Types of Phishing	Description
Email	Email phishing attempts are the most common tactic used by hackers to access your personally identifiable information.
Texting (SMS)	Text message phishing (also called smishing), is a method used by attackers to gain access to your personally identifiable information by sending you a false or misleading text message.
Phone Scams	Voice phishing is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information for the purpose of financial reward.
Keyloggers and Screenloggers	These are two specific types of long-term phishing and malware attacks used to capture user data and collect it over a specific period of time. Attackers often can then either use the collected data for personal gain or sell the information to a third party.

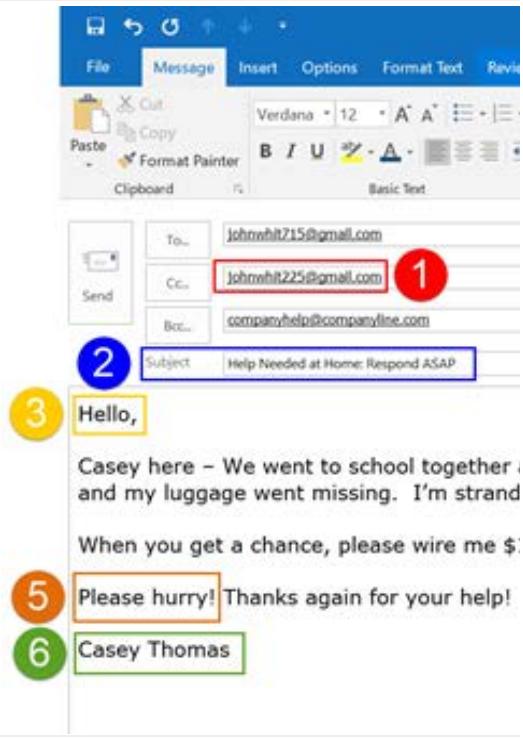
Types of Phishing	Description
Session Hijacking	Session hijacking is a long-term phishing attack, designed to be completely inactive and undetectable until a user accesses a certain website. Once a victim accesses a certain website and enters authentic user information (such as a username and password), the attacker can then access that captured information and operate on a website without any interference from the original user.

Types of Phishing, Cont.

Types of Phishing	Description
Pharming	Pharming focuses on attackers redirecting victims to fake web sites, even after they have typed in the correct website address. This attack can occur on any website but is often most likely found on websites dealing with more personally identifiable data, such as a banking website.
Content Injection	Content injection deals with websites that have vulnerabilities open to attackers that can be exploited for potential gain. When an attacker notices an opportunity, they will often create a fake copy of a piece of the website (often a form) and supply that to the user instead.
Spoofing	Spoofing is a type of phishing when the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
Network Fraud	Act of gaining unlawful use of a computer system.
Pretexting	Fictional situation created for the purpose of obtaining personal and sensitive information from an unsuspecting individual.

Identifying a Phishing Email

1. Email address you don't recognize or email addresses that look official
2. Suspicious subject lines or unsolicited emails
3. No recipient name in the email
4. Questionable hyperlinks
5. Sense of urgency

6	Questionable sender	

Don't Become a Victim of Phishing: Tips to Remember

✓	**Slow down**. Spammers want you to act first and think later. If the message conveys a sense of urg skeptical; never let their urgency influence your careful review.
✓	**Research the facts.** Be suspicious of any unsolicited messages and do your own research.
✓	**Don't let a link be in control of where you land.** Stay in control by finding the website yourself u where you intend to land. Hovering over links in email will show the actual URL at the bottom, bu
✓	**Beware of ANY download.** If you don't know the sender personally and expect a file from them,

✓	**Foreign offers are fake.** If you receive an email from a foreign lottery or sweepstakes, money fro transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.
✓	**Email hijacking is rampant.** Hackers, spammers, and social engineers taking over control of peo communication accounts) has become rampant. Once they control an email account, they prey on t when the sender appears to be someone you know, if you aren't expecting an email with a link or a opening links or downloading.

Phone Scams

Every year, thousands of people lose money to telephone scams — from a few dollars to their life savings. Scammers will say anything to cheat people out of money. Some seem very friendly — calling you by your first name, making small talk, and asking about your family. They may claim to work for a company you trust, or they may send mail or place ads to convince you to call them.

Pretexting often involves a scam where the liar pretends to need information in order to confirm the identity of the person he is talking to. After establishing trust with the targeted individual, the scammer might ask a series of questions designed to gather key individual identifiers such as confirmation of the individual's social security number, mother's maiden name, place or date of birth or account number

If you get a call from someone you don't know who is trying to sell you something or if they pressure you about giving up personal information — hang up!

Signs of a Scammer

The following signs can be helpful in identifying a scammer:

- They want your personal information
- They're collecting a debt you don't remember incurring
- They threaten you
- They won't answer your questions
- They're selling you something
- They say you've been a victim of fraud
- They say you owe money on your taxes
- They say you've won something or are "selected" to receive money

Tech Support Scams – Phone Calls

Tech support scammers use many different tactics to trick people. Spotting these tactics will help you avoid falling for the scam.

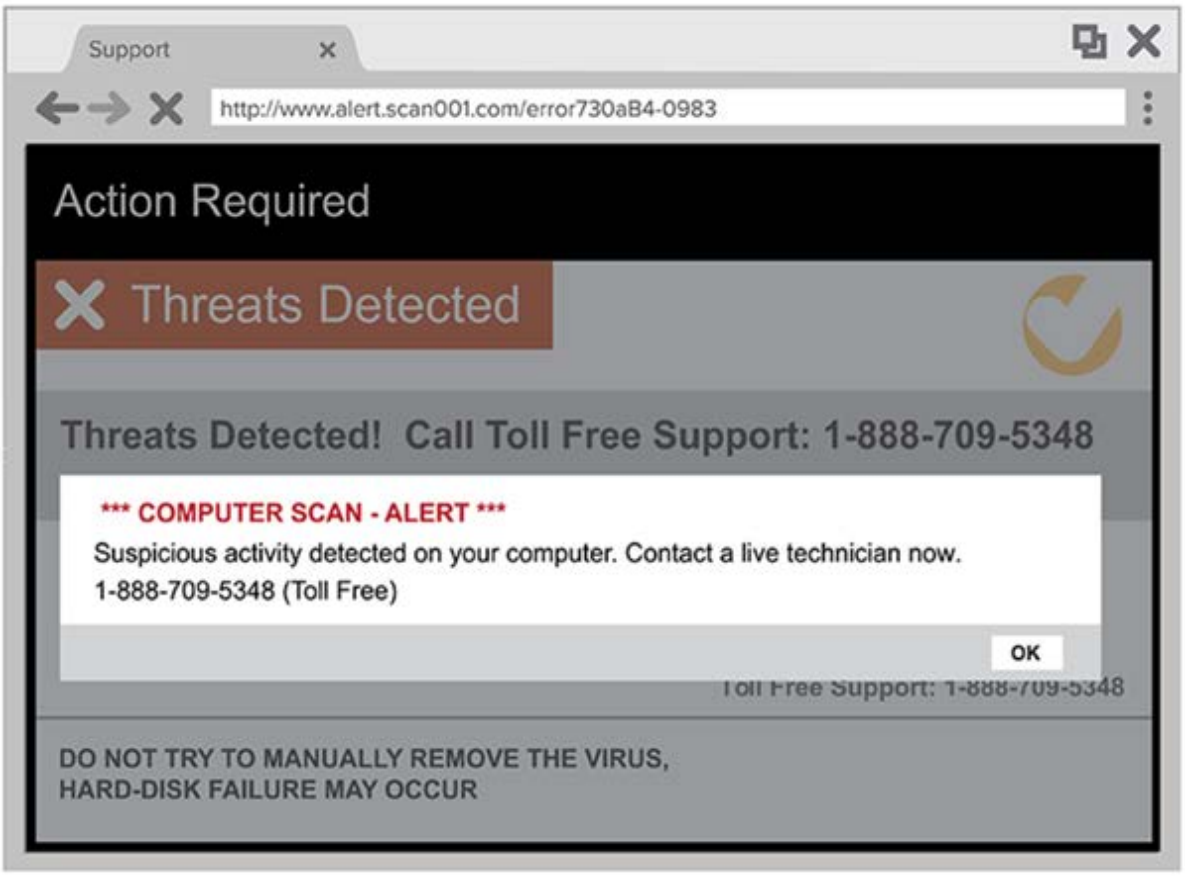
Phone calls are a common type of tech support scams. Tech support scammers may call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn't exist. Listen to an FTC undercover call with a tech support scammer.

If you get a phone call you didn't expect from someone who says there's a problem with your computer, HANG UP, and report the incident to the HHS Consolidated Helpdesk.

Tech Support Scams – Pop-Up Warnings

Another scam that tech support scammers use is Pop-Up Warnings.

Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.



Insider Threat Overview

A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically and can mitigate the threat of an outsider stealing company property. However, the criminal who is harder to detect and who could cause the most damage is the insider—the employee with legitimate access.

An insider may steal solely for personal gain, or that insider may be a "spy"—someone who is stealing company information or products in order to benefit another organization or country.

An insider threat is anyone with authorized access to the information or things an organization values most, and who uses that access - either wittingly or unwittingly - to inflict harm to the organization. When an insider becomes a threat, it can have far-reaching consequences on organizations. Especially those that have confidential data such client information governed by regulatory requirements.

He pled guilty on March 13, 2014 for unlawfully retaining classified national defense information at his home and for willfully communicating classified national defense information to a person not authorized to receive it. Bishop was sentenced to 87 months in prison and 3 years of supervised release.

Indicators of Insider Threat

The previous case studies might point towards a possible insider threat. Examining past cases reveals that insider threats commonly engage in certain behaviors. For example, not all insiders act alone.

While some insiders volunteer, others are targeted and recruited by adversary groups. For this reason, you should be aware of common signs someone is being recruited. And once an insider turns on his or her organization, that person will start collecting information. So, you need to be able to detect clues that that might be happening. Once they have information, insiders must then transmit it. If you know the signs of information transmittal, you will be better prepared to detect it. And insiders often exhibit other common suspicious behaviors you need to know about.

Not all of these indicators will be evident in every insider threat and not everyone who exhibits these behaviors is doing something wrong. However, most of the insider threats discovered displayed at least some of these indicators. It is important for you to be aware of these behaviors, so you can combat the insider threat and protect your organization.

Reportable Indicators

Reportable indicators include, but are not limited to:

- Recruitment

- Information Transmittal
- General Suspicious Behavior

Recruitment

The first indicator is **Recruitment**. Indicators of recruitment include:

- Signs of sudden or unexplained wealth
- Unreported foreign travel
- Unreported request for critical assets outside official channels
    - Critical assets are assets essential to an organization's mission or to national security that, if exploited, could result in serious harm and include the following:
        - Classified information
        - Proprietary information
        - Intellectual property
        - Trade secrets
        - Personnel security
        - Other information that could compromise or harm your organization's resources, including information, facilities, or personnel
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Unreported offer of financial assistance, gifts or favors by foreign national or stranger: Beware of those bearing gifts

Information Transmittal

If you notice someone failing to follow procedures for safeguarding, handling, and transmitting classified information, it may be a sign of an **Information Transmittal** insider threat:

- Unreported request for critical assets outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Unreported offer of financial assistance, gifts or favors by foreign national or stranger: Beware of those bearing gifts

General Suspicious Behavior

General Suspicious Behavior can be an indicator of an insider threat. Please note that none of these indicators alone mean that an individual poses an insider threat. In fact, many indicators are often easily explained or represent a personal issue that poses no threat to the organization. **The following are examples of general suspicious behavior:**

- Attempts to expand access
- Questionable behavior
- Changes in financial circumstances
- Attempts to compromise individuals
- Exhibits actions or behaviors associated with disgruntled employees
- Inordinate, long-term job dissatisfaction
- Bullying or sexual harassment of fellow employees
- Workplace violence
- Violations of organizational policies, procedures, directives, rules or practices

Insider Threat

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries will help you ascertain if there is a spy in your midst. However, if you believe an employee is acting inappropriately, or is stealing organizational information, do not alert the person to the fact that he/she is under suspicion, but seek assistance by reporting it to your supervisor or the Office of Inspector General if you do not feel comfortable reporting to your supervisor.

Unfortunately, insider threats often go unreported until it is too late. In the majority of past cases, relevant information was available, yet went unreported. How different might things have been had someone said something?

When you fail to report, you risk both your physical security and the information security of your organization.

Reporting Security Incidents

If you suspect a potential security incident immediately report the incident to the HHS IT Consolidated Help Desk.

Examples of a security incident include but are not limited to are:

- Malware or ransomware infection
- Compromised credentials
- Phishing emails
- Telephone scams
- Unauthorized use of computer accounts and systems
- Loss of agency assets or BYOD
- Data loss
- Security breach

Reporting Privacy Incidents

Suspected privacy incidents of unauthorized disclosure should be reported as quickly as possible. Some regulatory types require escalated reporting.

- A suspected SSA or IRS breach should be reported within one hour.
- Suspected breaches of other types of data, should be reported within 24 hours.

Privacy incidents are reported using Form 0402 Potentially Privacy/ Security Incident (PPSI). Privacy/Security Incident Form Instructions are located on the Privacy Connection website. If you have any questions, you can contact the Privacy Office at 1-877-378-9869 or email at privacy@hhsc.state.tx.us.

Incident regarding IRS Federal Tax Information should also be reported to the IRS Coordinator at irs_fti_safeguards@hhsc.state.tx.us.

The Texas HHS Privacy Division reviews each incident and begins the process of investigation. If necessary, the privacy officer will provide additional reporting steps.

DSHS staff should direct their privacy questions to the DSHS Privacy Office: HIPAA.Privacy@dshs.texas.gov.

HHS Privacy and Information Security Relationship

HHS Privacy and Information Security works together. You can have security with no privacy, but you can't have privacy without security. Security safeguards physical, administrative, and technological areas. Privacy safeguards confidential data, ePHI, SPI, PII, ad other regulatory requirements.

You can review privacy training on System Training Solutions (STS) or contact the Privacy Division at privacyrisk@hhsc.state.tx.us.

Reporting to the Office of Inspector General (OIG)

If the following types of incidents are suspected or are occurring, they must be reported to the OIG:

- **Improper use of resources related to email, the internet, or other Texas HHS Information Resources**
- **Insider Threat**
  - An insider threat is anyone with authorized access to the information or things an organization values most, and who uses that access - either wittingly or unwittingly - to inflict harm to the organization.
- **Sexually Oriented Content**

- There are rare circumstances where sexually-oriented content is work-related. Examples may be because of investigation or medical responsibilities.
- If you observe someone viewing or downloading sexually explicit information on an Texas HHS information resource and it is not related to job duties, report it to your supervisor or the HHS Inspector General (IG)—Internal Affairs Section at 800-436-6184.
- If you are a supervisor and suspect this is happening, do not initiate a search. Report the incident to HHS Inspector General—Internal Affairs Section. IG staff will provide directions to you and designated information technology personnel. For more information visit https://oig.hhsc.texas.gov/.

Summary

Texas HHS Information and Information Resources (IR) are valuable assets that must be protected from unauthorized disclosure, modification, use, or destruction.

Every member of the organization must:

- Ensure information and resources maintain their integrity and confidentiality and that their availability is not compromised by protecting information from unauthorized use and disclosure.
- Report security and privacy incidents by following appropriate agency reporting procedures.
- Comply with Texas HHS security measures, including those identified in the HHS Acceptable Use Agreement (AUA).
- Understand the laws, regulations, policies, procedures and best practices to safeguard the particular types of information with which they handle.
- Comply with all required training which may include additional role-based training.

By using Texas HHS Information Resources, you consent to the monitoring of your use of these resources and information in any form and on any device. You have no expectation of privacy when using any of these resources.

Failure to follow agency policies, procedures, and state and federal laws may result in:

- The loss of access to computer systems
- Disciplinary action which may include termination
- Prosecution, fines, and/or penalties in civil or criminal court

Guidelines, Rules and References for Protecting Information

Guidelines, Rules and References for Protecting Information Including but not limited to:

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202, Information Security Standard and the Information Resources Management Act (Texas Government Code, Chapter 2054)
- HB 2004 — which relates to a breach of computer security involving sensitive personal information, as well as the protection of sensitive personal information and certain protected health information.
- Texas Penal Code (Chapter 33)

- Government Code 441.185
- Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521
- Health Insurance Portability and Accountability Act (HIPAA) 45 CFR §164 Part C, 164.308.5 (i-ii)
- IRS Publication 1075, Other Safeguards—IRC 6103(p)(4)(D)
- SSA -The Privacy Act of 1974, as amended, The Social Security Act, Section 1106; Computer Matching and Privacy Act of 1988, as amended and related policies and regulations.
- CJIS - Federal Information Security Management Act and CJIS Security Policy.
- HHS Acceptable Use Policy (AUP)
- HHS Acceptable Use Agreement (AUA)
- IS-Controls
- HHS Information Security Data Classification Standards
- HHS Text Messaging Policy
- HHS Human Resources (HR) Work Rules in the HHS HR Manual
- HHS HR Manual Work Rules state employees must keep all HHS information confidential unless the information is releasable under law - the Public Information Act, Texas Government Code, Chapter 552.
- Consumer-related information may be released only in accordance with state and federal regulations, and HHS policies and procedures.

Contact Information

Information Security/Cybersecurity

Email Address: infosecurity@hhsc.state.tx.us

HHS Privacy Office

Email Address: Privacy@hhsc.state.tx.us

DSHS Privacy Office

Email Address: HIPAA.Privacy@dshs.texas.gov

Records Management Office

Email Address: records@hhsc.state.tx.us

IRS FTI Coordinator

Email Address: irs_fti_safeguards@hhsc.state.tx.us

Congratulations!

You have successfully completed the **HHS Information Security/Cybersecurity Training for Contractors** training presentation.

To get credit for this course, you must:

- close this window (Click the Exit (X) button in the upper right corner) and
- return to the HHS Learning Portal to take the Quiz with score higher than 85 and print your Certificate