# Cybersecurity Awareness Training Program

Texas Government Code 2054.5191
Approved Lesson Plan

# Cybersecurity lesson plan/facilitator's guide

## (meets guidelines of Texas Government Code section 2054.519)

## Provided by Texas Municipal League Intergovernmental Risk Pool

The purpose of this cybersecurity awareness training (PowerPoint slides and Lesson Plan) is to educate local government employees about the risks of using computers, networks, and electronic devices. Texas Government Code Section 2054.5191 requires that certain local government employees and public officials complete annual training and provides options for meeting training requirements. The Texas Municipal League Intergovernmental Risk Pool has created this program to assist its members.

The format is a training package for a local government to assign a course administrator to provide training to the entity's personnel.

**Training Resources:**

- Lesson Plan (Cybersecurity Awareness Training Lesson Plan)
- PowerPoint (Cybersecurity Awareness Training)
- Cybersecurity Awareness Participant Handout
- Phishing: Do Your Part to #BeCyberSmart
- Test/Assessment Questions
- Completion Certificate
- Sign-In Log
- TMLIRP Cybersecurity Training Video

**Steps to Administer the Course:**

- Use Lesson Plan for an understanding of corresponding PowerPoint utilized for training.
- Be familiar with the use of PowerPoint presentation equipment and projectors, speakers, and other equipment necessary for presenting the program
- Create a learning environment that is conducive to the students and have all students sign-in when attending
- Administer program using PowerPoint and lesson plan
- Utilize test/assessment questions to administer a test of comprehension
- Review test/assessment and assure all student assessments are corrected to 100%
- Complete certificate for student file
- Check Department of Information Resources requirements for submission of documentation
- Remember annual requirements for completion of awareness training

# Table of Contents


Facilitator Information Page 1

Table of Contents Page 2

About this Program Page 3

What is information security? Page 7

Types of Information Page 9

- Classification Page 9
- Forms Page 10
- Where is information stored? Page 11

Principles of Information Security—The 4 Pillars Page 12

- Machine Level Page 13
- Data Level Page 19
- Network Level Page 23
- Internet Level Page 25

Threats to Our Security Page 26

- What is a Threat? Page 27
- Who is Causing the Problem? Page 28

Cyber Risk Page 30

What Is an Attack? Page 32

How to Recognize Common Attacks Page 33

Types of Tactics Used Page 34

Reporting an Attack Page 40

Training Page 41

Conclusion Page 42

Assessment/Test Page 43

Answer Key Page 45

*Phishing Do Your Part to #BeCyberSmart* Handout Page 46

***About this Program***

These instructor-led modules are designed to accompany the Cybersecurity Awareness Program materials, including the PowerPoint.

***Learning Objectives***

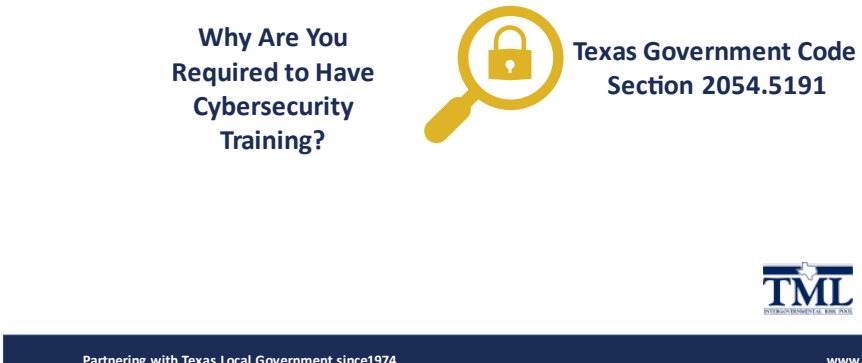
- **Know the basics of information security**
- **Be aware of the threats to information security**
- **Know motivations of threat actors**
- **Communicate best practices for your organization**

***For the facilitator:***

- Regular text is for talking
- ***Bold italics are notes to the facilitator***
- Left side section is for notes and keys for the facilitator

## *What is Information Security?*


Opening Slide



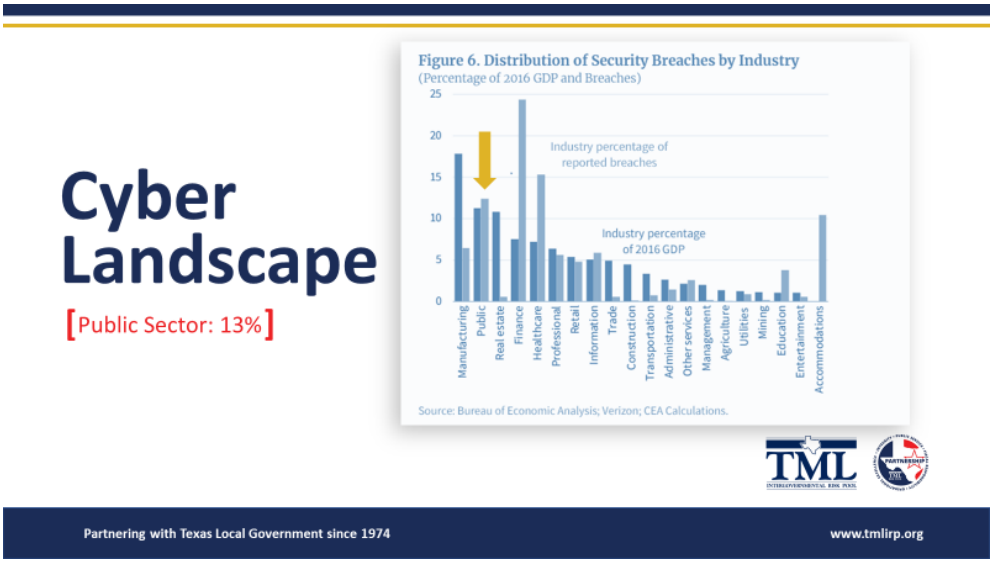

***Consider whether you will hand out the following at this time or later in the discussion:***

***Phishing Do Your Part to #BeCyberSmart Handout***

***Cybersecurity Awareness Training Handout***

***Your entity might have a directory on its website. In this case, anyone has access to your organization's email addresses and titles. Cyber threats are not necessarily a reason to remove this information because it is a service to your community and allows your entity to serve its citizens. This stresses the need for the education of email users.***


For example, when an entity is hacked by an outsider who wants information to sell, it is estimated that the response costs an average of $158 per record. Examples of costs include detection, post breach response, notifying the affected user, and lost business costs.




The above slide indicates the impact of security breaches by industry, with the Public Sector noted by the red arrow. The Public Sector experienced 13% of breaches in 2016.

***According to one study, cyber criminals got away with $1.5 trillion in 2018 throughout the world. Many of these criminal activities start in other countries and it is difficult to stop.***

***The City of Atlanta, Georgia was crippled by a cyber-attack in 2018 that affected many services and programs including courts, utilities, and parking.***

***We'll talk about ways to recognize scams and not be a victim.***

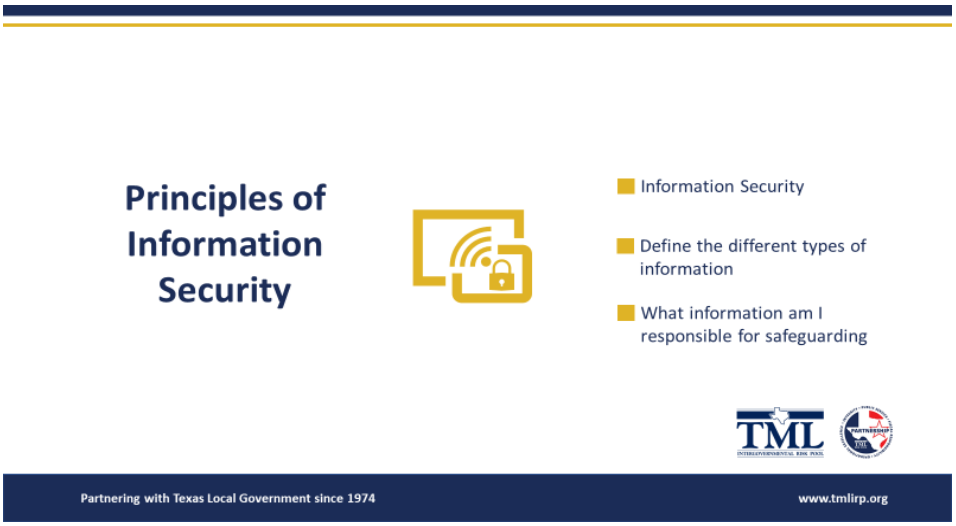


Texas has a lot of people, so it's understandable that a large number of cybercrime victims are Texans. Texas is number 2 in the country in terms of the amount of losses.

Practicing safe computing and data storage will help not only our entity, but you personally. Think if criminals have your personal information and how they can exploit you with false credit cards.

Public organizations collect and store a lot of data that is of value to cybercriminals. The criminals illegally use stolen data such as credit cards, personal information, and health data. They also capture and hold data needed for daily operations in return for money through ransomware.

# *What is Information Security?*




**"Information security"** is a broad term that covers protection of data and the systems that contain it, from the storage location through all connections to it. It includes the users who view, handle, and transmit it, and the devices they use to do so. The first step to developing a comprehensive information security plan and a culture of cyber-security is to recognize the need to have such a plan.

No user is safe from threats, no matter their position or authority. For an outsider who might want to intrude on or attack an organization, something simple like an org chart or address book can be valuable information. While it is obvious that certain information should be kept strictly confidential, something as mundane as the names and contact information of management or executives can be used against the organization in many ways.

Users should be cautious to the point of suspicion when dealing with any proprietary data. When entering a password or credit card number, sending an email or transferring a file, one should only do so on a known, managed system and connect through a known, managed connection. Continual vigilance is a hard lesson to learn, but computers never rest, so users should understand that they should not falter in their procedures.

A high-level view lets us break down information security into smaller sections that would be managed by different groups. The IT department is not the only department that can make a difference for preventing cybercrime. The most important group is an organization's users. This means all of us are responsible for cybersecurity.

The cliché of a chain being as strong as its weakest link is applicable, for all the firewalls, anti-virus software, and encryption in the world is useless when a user clicks on something he or she should not click.

# Data Classification

**Procedures to classify data include:**

**- Set the criteria for classifying the data.**

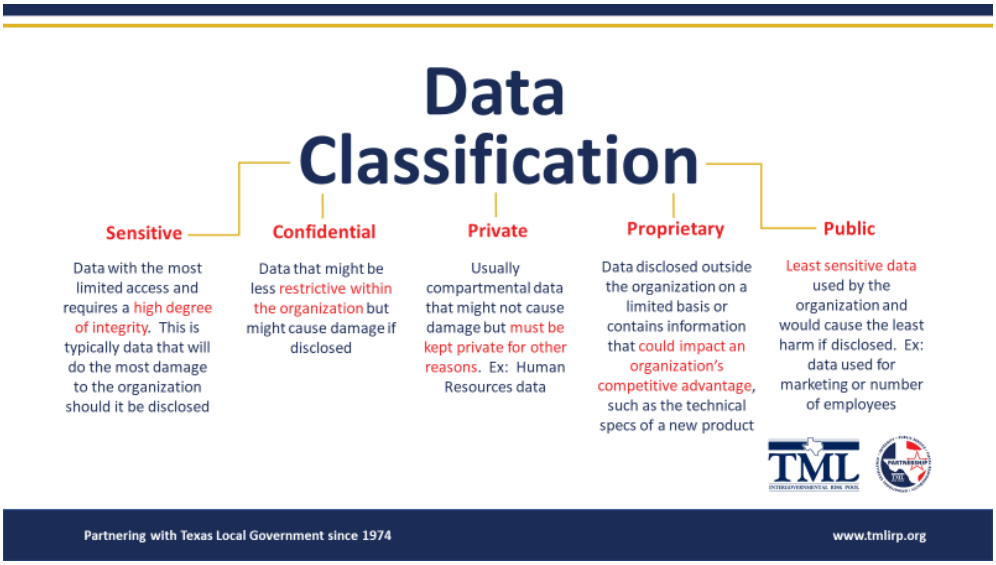
**- Determine the security controls that will be associated with the classification.**

**- Identify the data owner(s) who will set the classification of the data.**

**- Document any exceptions that might be required for the security of this data.**

**- Determine how the custody of the data can be transferred.**

**- Create criteria for declassifying information.**




The table above shows a way to classify data. This helps determine the security needed to protect it.

**Instructor Resource**

http://www.pearsonitcertification.com/articles/article.aspx?p=30287&seqNum=9

# *Forms of Information*

You need to be aware of the forms of information and the location of the information that you are responsible for safeguarding

Discrete files (MS Office documents, PDFs, image/video/sound, text) and folders containing said files.

***Examples:***

- *Microsoft Word documents*
- *Excel Spreadsheets*
- *PowerPoint Files*
- *PDF*
- *Images*
- *Videos*
- *Any text document*

**Database files** (for example files ending with .sql or .mdb or .accmdb).

Microsoft Access is a commonly used application that can be seen by users. In other applications, not many users will see the database file.

# *Where is Information Stored?*

**Where is information stored?** Knowing where information is stored provides focus on where to look. The challenge is that data is in many places.

**Local system**—the computer, phone, tablet, or other device itself

Network locations– our organization's servers and storage. We can share and access files on our network, but they are not necessarily shared with others.

**Other user computers**

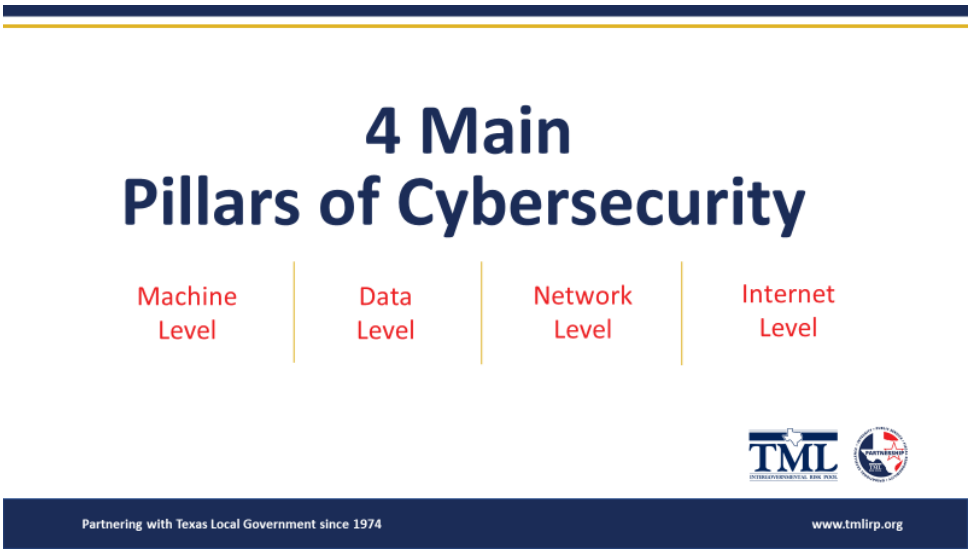
**Cloud storage**—storage with a third party provider (Microsoft OneDrive, Google Drive, Dropbox)

**Portable media** (USB/flash thumb drives or hard drives, CD, floppy disc, zip drive, tape)

**Other devices** (cell phone, tablet, extra computers including home or borrowed systems)

Data tends to be retained by systems on which it is viewed. Users should be aware of this and understand how to remove it.

# The 4 Pillars of Cyber-Security




A cybersecurity culture places the load on four main pillars:

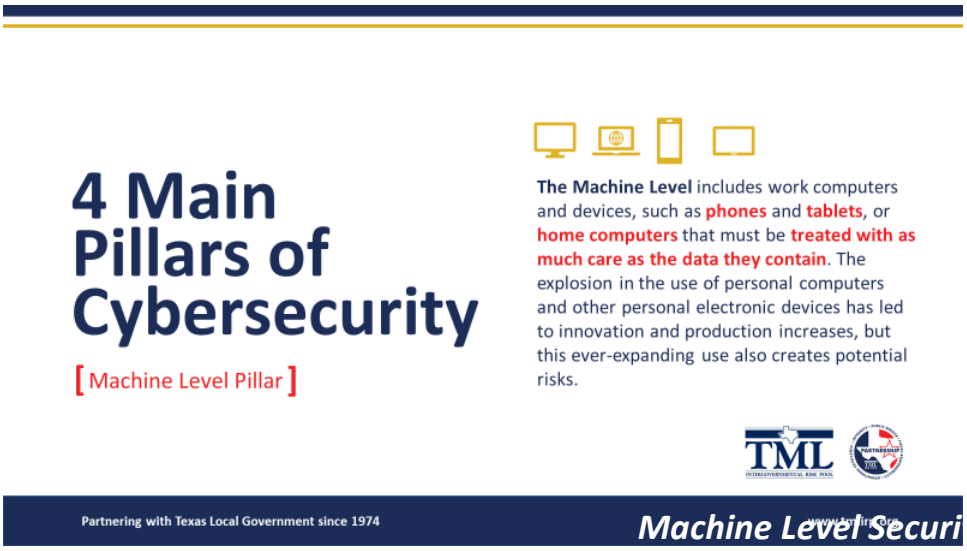
**Machine level** – A user's computer(s) and other devices such as phones and tablets or personal computers should be treated with as much care as the data it contains

**Data level** –Treat the organization's data as if it was bundles of cash

**Network level** – No computer is an island these days, and things are connected in ways most users do not imagine even in the smallest office

**Internet level** –When connecting with the outside world, only let in exactly what you need, and only let out exactly what you are willing to give away.

# *Safeguarding Machines*




The Machine Level includes work on computers and devices, such as phones and tablets, or home computers that must be treated with as much care as the data they contain. The explosion in the use of personal computers and other personal electronic devices has led to innovation and production increases, but this ever-expanding use also creates potential risks.

**Potential exposures to your organization:**

- Weak passwords that are never changed allow hackers access to machines (single word passwords unacceptable)
- Anti-virus software is not installed or not updated
- Employees are not aware of dangers lurking related to cybersecurity
- Email rules and training are lacking or non-existent (clicking on links or attachments)
- Lack of control of flash drives and other portable connections
- No controls for accessing public Wi-Fi connections
- Lack of administrator controls to prevent downloading of apps or programs onto machines
- Lack of cybersecurity training

# Facilities and Physical Security

Facilities have a role in safeguarding machines. You must guard against unauthorized access to facilities, data, and the systems on which it is stored.

Access to offices, data centers, warehouses, or any other workplace where computers are present should be strictly controlled. Once inside, further steps should be taken to guard information that is being accessed.

Badged entry, with “tailgating” prohibited.

Ensure outer doors are locked where possible, and those doors are not propped open (exits to smoking areas are notoriously porous due to frequent, repetitive use).

Where possible, inner areas may require additional steps for entry.

Non-employees should not be allowed to roam unattended.

Monitors should be fitted with privacy screens to prevent over-the-shoulder theft of login credentials or sensitive data.

Computers should be locked with passwords required to unlock whenever left unattended, including those for use in managing other devices like printers.

Cabling and peripheral ports on all computers should be regularly inspected for sniffer devices, keyloggers, or other devices that could be monitoring computer input or network traffic.

Networking devices (routers, switches, modems, networked computers such as servers) should be kept in locked areas.

When possible, security guards should be employed to monitor building entry by non-employees.

Locations such as rooms and control boxes that house electronic control systems, such as traffic lights, water and wastewater system controls, etc. should be securely locked to prevent tampering.

# Safeguarding Machines

***Note on machine level security—we often think about computers, tablets and smart phones as targets.***

***Consider other examples of machines at your entity— SCADA (supervisory control and data acquisition) systems for utilities, servers, traffic control boxes, streetlights, library computers, security systems, flood and tornado warning systems, and others.***

No computer should ever be left unsecure. It should be locked (electronically) while in use but locked up physically when not in use. Old computers can contain valuable data for a thief to exploit.

Obtain authoritative authentication to access the system.

For a phone, prove you are who you say you are with Multi-Factor Authentication (MFA). Be aware that you should enable your mobile phone with passcodes, and fingerprint or facial awareness. It would be a big problem to lose your phone and an even bigger one to have it easy for a thief to access your texts, mail, social media, passwords, and payment apps.

Enable apps on phones and other portable devices to identify the device's location remotely. Common apps also allow you to lock, wipe, or disable the device remotely. These tools must be enabled BEFORE the devices get lost. Know your passwords and how to use the "find my phone" function.

**Video resources for instructor:**

Practical physical security: https://www.youtube.com/watch?v=b70-hr8RLzM

Authentication: https://www.youtube.com/watch?v=t4kTgjQabV4

MFA: https://www.youtube.com/watch?v=ZXFYT-BG2So

Apple "Find my iPhone": https://www.youtube.com/watch?v=xt8W6K2IVVs

**Refer to your organization's procedures.**

# Passwords and Access

***Multi-Factor Authentication (MFA) is "Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric)"***

***Password management tools such as browser plugins, secure storage sites, or files stored locally with password records are common options but require study and decisions to be taken by each organization.***

Passwords are a favorite topic in information security. There are many theories about how best to handle them, or even how to do without them. Until something better comes along, they must be managed and handled with care.

Password length is more important than complication. "P@$$w0rd!" is much easier for brute-force attacks to guess than

"MyPasswordIsReallyLongAndThereforeSaferButStillNotReallySafe".

**Instructor Resource:**

https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

Avoid single words found in a dictionary or proper nouns.

Do not keep copy of passwords where others can see them, preferably not on paper anywhere, or in any clear-text electronic format.

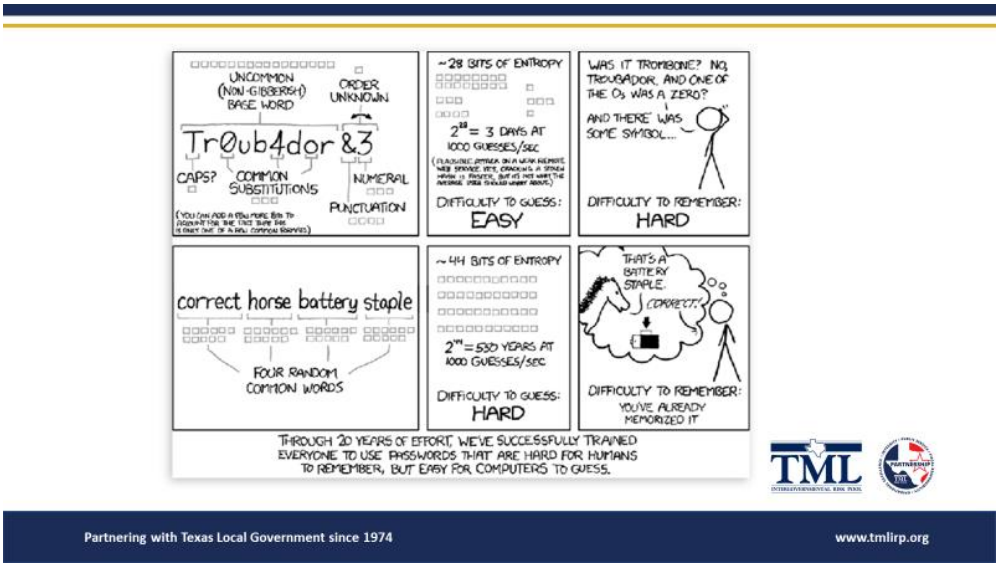
Do not share your passwords to anyone else.

Do not use the same passwords, or close variation, on multiple systems, including personal ones.

Enable Multi-Factor Authentication (MFA) on all systems possible. This system uses at least two ways to verify the person trying to access the system.

For example, some systems will send the user a text message with a code and the user must enter the code in addition to using their password on a computer.

***Note: Cartoon XKCD linked to [https://xkcd.com/936/](https://xkcd.com/936/) per the Creative Commons License.***




This slide shows the differences between two thoughts of selecting a password.

The top line says that a mixture of letters, punctuation, numbers, and symbols can be easy for computer programs to guess, while they are hard for the person to remember.

The second line of the comic strip points out that a longer password of random words is harder for a computer to guess but can be easy for the person to remember.

Systems sometimes have specific rules for passwords, so you might not have the choice, but consider this information if you do have a choice to have a long password, as it can be easier to remember.

## Protection Against Unauthorized Use

Maintaining physical security is one part of effective defense. Keeping data secure is another. Several key elements to keep in mind are a combination of passive and active tools for retaining control of systems and the data they contain.

- Password protection on every system, with Multi-Factor Authentication wherever possible.
- Employ secure connections at all times.
- Any system access credentials should be created by the IT department with proper roles, groups, and policies applied to the account before the credentials are given to a user.
- Credentials should not be shared, and passwords should be changed as quickly as possible if they ever are.


The Data Level applies to the quantities, characters or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical or mechanical recording media. The organization's data must be treated as it is "bundles of cash" due to the efforts necessary to recreate, if even possible. Data is like cash in that if you lose cash or it gets stolen, you will likely not get your individual dollar bills back. Once data is gone, it's gone.

**Potential exposures to your organization:**

- Employees are not aware of the data created by all organizations and the importance of that data or the cost and effort necessary to restore damaged or lost data (if possible to be restored)
- "Off-site" data backup is not provided, or backups are not performed regularly
- Employees do not believe their organization's data is relevant or "important enough" for a cyber attack
- Organization's data is not encrypted to protect from hackers

# *Protecting and Safeguarding Data*

Technical aspects of data security are handled primarily by IT staff. But users should be aware of proper handling techniques. Many modern techniques require little or no technical savvy but are still effective.

Data should be backed up regularly.

Ensure Anti-virus and anti-malware is installed on your machine and configured to receive updates automatically when released.

Ensure all your devices are patched at minimum once a month and receive critical updates automatically when released.

Make sure your computer always connects to secure WiFi locations (do NOT connect to free public WiFi).

Encrypt your data on USB drives and other portable media.

Ensure your computer, mobile devices, and tablets have auto-lock feature turned on and require a password to unlock.

# Proper Storage of Sensitive Information

One puzzle to be solved in a cyber-secure culture is developing the ability to store data safely without the protective layers becoming a hindrance for authorized users.

- Keep your workspace clean both in terms of securely destroying sensitive data on paper or hardware when not needed
- Keep their electronic spaces clean as well, deleting old or obsolete files and not leaving copies of sensitive material in different locations
- Follow guidance and rules for password length and complexity, and enforce periodic changes to passwords, ensuring one of the rules is dissimilarity to recent passwords.
- All network traffic should be conducted with secure connections between every point, including between servers, routers/switches, and the user's device.
- Users should never connect to a network or enter their credentials into a system they do not control, or connect to a public Wifi, especially one that does not require a password.
- Storage media (USB/flash drives, CD/DVDs, floppy discs, zip discs, tapes) should be kept in secure areas and handled as if it was cash.
- Contractors or vendors should be vetted, and any credentials issued for their access should grant the minimum access necessary, then revoked immediately upon completion of their work.

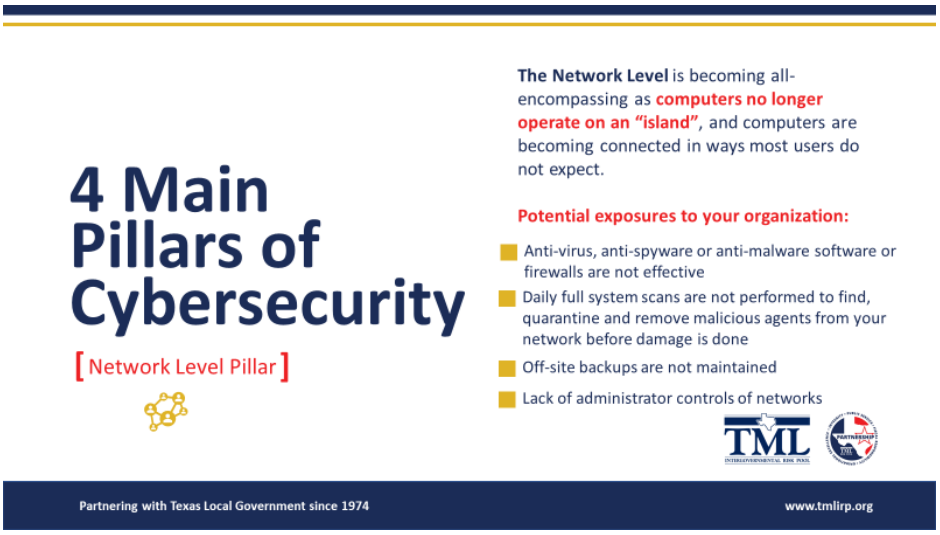
# Sanitation and Disposal of Storage Media

***Records retention laws affect how long data must be maintained. These requirements must be considered to protect rights under the Public Information Act.***

***Computers might need to be backed up before disposal.***

The media containing information (hard drives both portable and fixed, USB/flash drives, CD/DVDs, internal RAM/ROM memory cards, discs of all kinds) should be handled carefully when no longer needed. Simply deleting files through the user interface is rarely effective.

- In old desktops and laptops, hard drives should be erased by completely reformatting them where possible, or else erased with a physical erasure device or hard drive eraser software
- Before being sent on, hard drives should be removed and destroyed where possible from computers as well those in copiers, printers, and scanners, which can retain data they process for years
- Follow manufacturer instructions for reformatting the memory of devices such as phones, tablets, and other peripherals
- Phones and other cellular-enabled devices should have SIM cards removed and destroyed in addition to wiping memory
- Paper records in the workplace should be handled safely and disposed of in protected receptacles
- Reputable, professional services should be contracted for record destruction if not done in-house
- Writable portable media should be erased following manufacturer instructions
- Non-writable media should be physically destroyed




IT staff face many challenges in defending our network. These are some of the issues that can result in problems for organizations.

# Protecting Our Network

***Review any procedures with supervisors about notifying IT about staff changes.***

***What is the process when an employee leaves or employment is terminated? Are all the systems that a former employee used still accessible?***

***This discussion will depend upon what your organization's IT policies are. It is an opportunity to explain why your entity has these processes.***

Steps that needs to be taken to protect computer networks, whether connected to the internet or not. These are typically managed by IT staff, but users should know key elements:

Enable user authentication against an authoritative database under the organization's strict control. This system involves the IT professionals setting up and maintaining a list of authorized uses.

Manage roles and permissions set on user accounts and groups and apply those settings to folders and files within a file system.

User policies set on individual users.

Wireless security in public and private should be handled carefully. Connections should only be made to known networks, and never free, password-less ones.

Wherever possible, employ secure connections such as Secure Shell (SSH) or Virtual Private Network (VPN).

# Connecting to the Internet


When connected to the internet, attacks can come through many approaches. Many attacks succeed because a user opens the door for them. This slide lists potential issues.

**In later sections, we will discuss:**

- Protecting you and computers from online threats
- Phishing and social engineering
- Understanding how web browsers work and the warnings they can provide
- Recognizing secure versus unsecure connections
- How to protect you against malware and viruses and what you should do if your device gets infected.

**Best Practices for Detecting, Assessing, Reporting, & Addressing Threats**

Partnering with Texas Local Government since 1974 www.tmlirp.org

This is a transition to learning about cyber threats:

- What is a threat?
- Who are “threat actors”?
- How to detect a threat?
- What are the options to take when there is a threat?

# What is a Threat


Simply put, a threat to information security can be defined as a risk of intrusion or disclosure of confidential information to unauthorized people.

**An organization's data has three aspects to consider:**

- Confidentiality – the data should be accessible only by authorized users
- Integrity – the data should be accurate
- Availability – the data should be accessible when needed

**Common threats include:**

- Theft of confidential, proprietary, or sensitive information
- Modification of existing data, and the compromise of how that data is collected, processed, and stored
- Unauthorized access allowing an external user to gain control of a system to block access to data

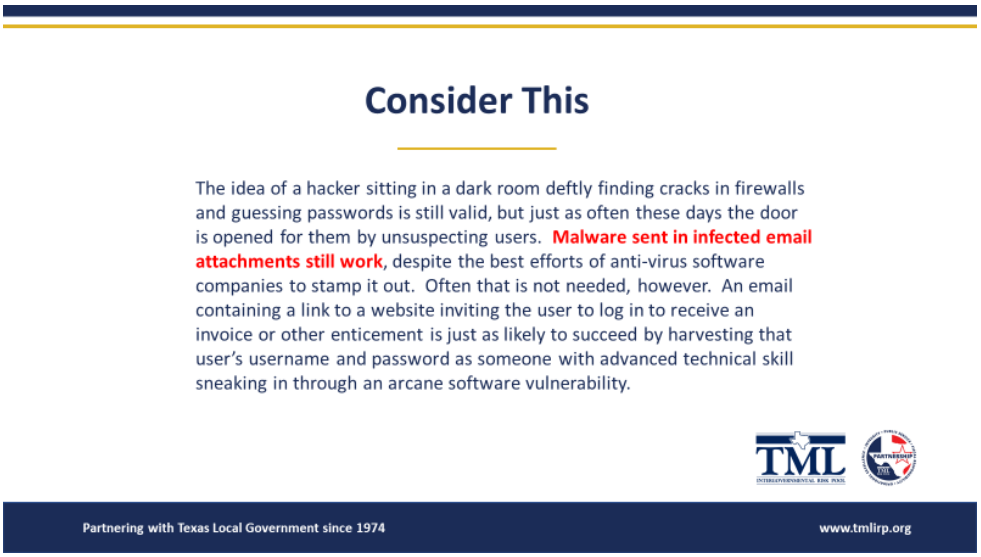
# Who or what is a "threat actor"?


A threat actor is anyone who tries to exploit vulnerabilities in an organization's systems or users. It does not matter how sophisticated the attack is or how far it goes. Their motivations and goals can range widely.

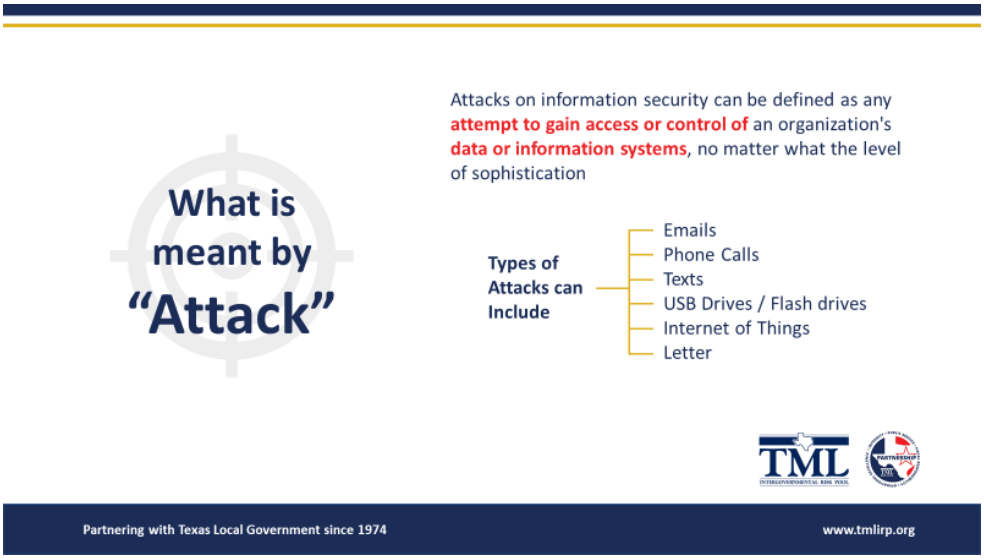
**They might include:**

- Profit, financial or otherwise
- Damaging the victim, financially or otherwise
- Damaging the reputation of the victim (defacing a website, using an email account as a source of spam or malware leading to other attacks, or causing mail from that organization to be blacklisted)
- Gathering data that might be used in future attacks (an attacker might start with an initial round of information gathering, leading to a more technically-sophisticated attack later)
- Gathering data that might be traded or sold to other actors
- Curiosity or malice (many attackers start out simply, and try to take actions simply because they can)

It is important to remember that there need not be a particular reason why an attack was made, though understanding the potential attacks allows better defense to be designed. Also, realize that value can be found in all sorts of data. Users might not understand why it is important to keep top financial staff confidential, but to threat actor those names can then be targeted with attacks to try to gain financial benefit. It's easier to try to get a wire sent if you know who the CFO is and then claim to be the CFO or direct an action in the CFO's name.



# What is "Risk"




Information security risks are defined by choices made by an organization in its technology and personnel. The goals of the organization to protect its systems and data against the goals of potential attackers require decisions to be made in view of the needs of its users, usually for accessibility.

For example, the modern office today is highly connected to the internet. Email, websites, file transfer systems, cloud storage, and Software-as-a-Service (SaaS) providers require clear connections to the outside world. Complicating things is that access must be accommodated on many different devices and from any location. These connections thus create potential porousness in defenses. An organization's data can be made much safer if connections to the internet were not allowed. However, that would greatly impact user productivity and likely that data's utility. Most organizations will accept the risk of connecting to the internet in favor of its ease of use.

***In 2017, Equifax was hacked, impacting 143 million U.S. consumers. Data included social security numbers, birth dates, addresses, and some driver's license numbers.***

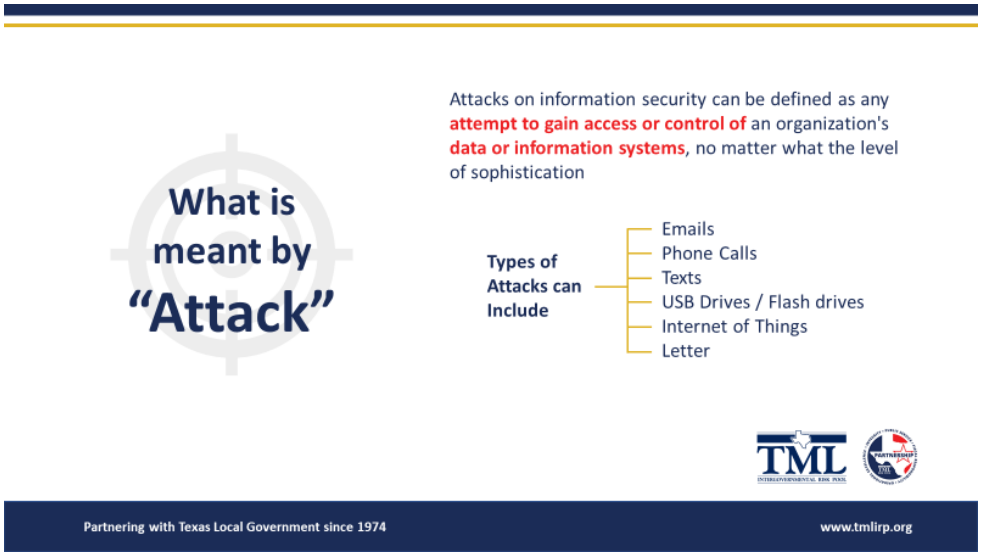
***How did this happen? The reports are that the company failed to implement a patch on a part of the company's website.***

***https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html***

***Does your entity have any computers that are rarely used? Make sure they get regular updates and that your personal computers are updated too.***

There are risks of inadequate user knowledge and having dependence on manufacturers of the hardware and software. The news frequently carries stories of devices with vulnerabilities that were previously unknown or, worse, known but left untended by a user or the IT department. When a vulnerability is found in Windows, for example, Microsoft will send out a patch as part of its regular round of updates. If the risk is deemed to be an emergency, they can push one out sooner. But it is incumbent on the user or, preferably, the IT department, to ensure it is applied in a timely manner.

# What is an "Attack"




Attacks on information security can be defined as any attempt to gain access or control of an organization's data or information systems, no matter what the level of sophistication. Attacks can be simple emails or even phone calls, emails with malware attached, or full-scale electronic attack on a system's points of access.

# How to Recognize Common Attacks

*TMLIRP has sample wire transfer policies and procedures for local government entities at the following website:*

*https://www.tmlirp.org/wp-content/uploads/sample-wire-transfer-procedures-1.pdf*

*Or search www.tmlirp.org for "Sample Wire Transfer Procedures"*

*Or refer to your finance department for specifics.*


Common attacks include impersonation, phishing and its variants, social engineering, and malware sent via email or other means.

One of the simplest attacks, and one that remains curiously effective, is simple impersonation of a user authorized to make financial payments. A common trick is to create an email on a free service such as Gmail or Hotmail, in the name of the CFO or other person authorized to send a wire. The sender claims to be on vacation and to excuse the personal email, but he or she cannot access work mail. It's suddenly a priority to send a payment and provides wiring instructions.

It is important to note that impersonation attacks are not limited to email. Bold attackers might call on the phone, for example, counting on the user to not recognize a voice or question directives.

Imitation is not limited to employees of the organization. Another common attack, again either with a throwaway email account or a real, compromised account, is to impersonate a vendor and send out messages with "new wiring instructions" so that the next time a bill to that vendor must be paid, the funds will be sent to the attacker's account.

**Instructor resource**: www.onguardnline.gov

# Types of Tactics Used in an Attack

***Have a Word document or email with links and demonstrate how to hover over the link and show the actual destination.***

***Sometimes the link is a word or a phrase, but you can determine the destination of the link by using your mouse pointer and not clicking.***

**Phishing** is the attempt to acquire information such as usernames, passwords, and credit card numbers by pretending to be another entity such as a social website, financial institution, or IT administrator.

The email or message might contain nothing other than a sentence or two and a link to an outside website. The link might be disguised, as the text displayed can be different from the destination encoded in the link. Placing a mouse-pointer on the link without clicking will display the destination of the link in a floating box directly above the link or in the lower left corner of the window. On mobile devices, there may be other ways to display the link without clicking. Users should try to understand how to read the link and decide if it is valid. Often the destination of the link might seem harmless or safe; no software is downloaded, or other intrusive action taken. But a message is shown that in order to access the document the user should log in with his or her username and password. Often the landing pages of services like Gmail or Office 365 are imitated, including logos and other visual cues. What lies beyond that page is often nothing, or some random document. That is irrelevant, but the important information was already stolen, the user's login credentials. In certain environments, such as organizations that have cloud services like Google or Office365 to provide authentication and authorization across many systems beyond email, a username and passwords can be keys to the kingdom.

**Spear Phishing** is a phishing email targeted at a specific individual or department within an organization that appears to be from a trusted source.

**Whaling** is a phishing attempt that targets high-ranking executives at major organizations.

**Social engineering** applies to any kind of contact intended to gain information or access through non-technical means. It might come through email but also through phone calls, instant message, social media, or any other avenue of communication. When a user gets a call from an unknown person and through possibly pleasant conversation reveals key information about the organization that can be used later.

**Ransomware** is defined as vicious malware that locks users out of their devices or blocks access to files until a sum of money or ransom is paid. Annual ransomware costs are estimated to be $11.5 billion by 2019.

**Vishing** is a type of phishing attack conducted by phone, utilizing voice. messages to potentially steal protected information.

# Types of Tactics Used in an Attack


**Malware**, a term covering software with many names like viruses, trojans, worms, backdoors, spyware, and so on, is very common and destructive. While there are many reputable companies doing excellent work to combat it, it is always true that some get through, especially new formulations that have not yet been recognized.

The risk of lack of user knowledge in how to handle attachments comes into play. No attachment should be delivered to an inbox without scanning for viruses, and a user should not open a document without scanning it again.

# Identifying a Phishing Email


***Use examples and/or refer to the Phishing Do Your Part to #BeCyberSmart Handout***

***Provide the handout if you haven't already.***

Examples:

Tip #2: Instead of chase.com the phishing email has chasebank.com

Tip #8: Email says someone "knows what you did" and your laptop camera can prove it.

***Beyond email, scammers have other techniques.***

- Phishing can be tried though other means including text messages, phone calls, fax, or even in person.
- Malware often spreads through contact lists, so it's more likely to come from someone you know.
- If you get a suspicious message, find a phone number to call the sender. Do not assume any number in the email or signature is genuine.
- It may be hard, but caution in any electronic communication should be the default.

# How to respond to and report attacks or suspicious activity

**Responding To and Reporting Common Attacks**

TML

Partnering with Texas Local Government since 1974 www.tmlirp.org

**Responding to an Attack**

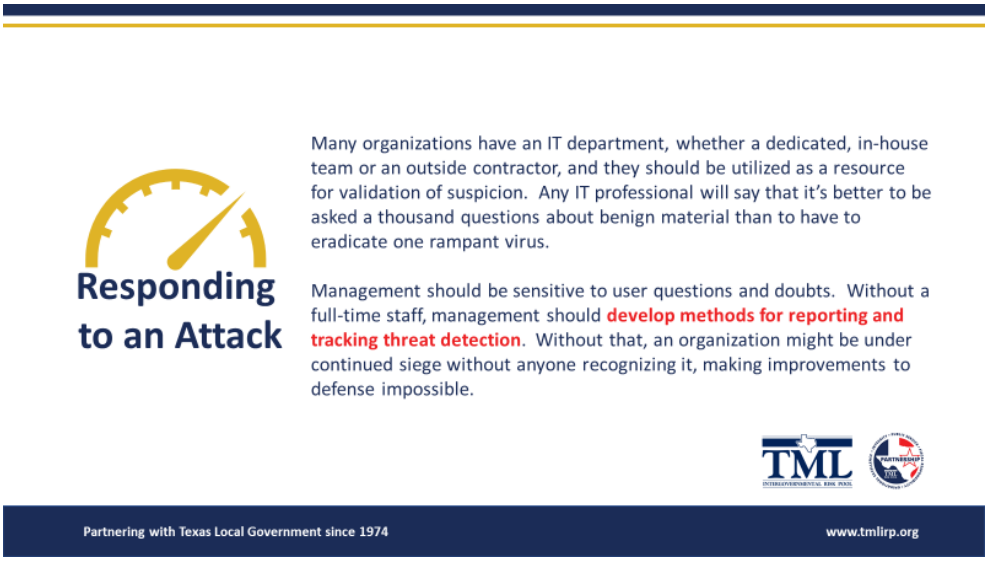
The common thread to all the attacks outlined previously is the reliance on the user not to question or verify the actions requested. The internet was built on trust, with all the threats present today not even imagined when much of the technology at its core was created. Thus, **responsibility falls on the users and organization** to employ a sustained, suspicious vigilance in any contact.

The most powerful key in any security system is the "delete" key. When a user receives **an email that is even a little suspicious, deleting it is usually the best course of action**. Where possible, verification by calling a known phone number is best. The email might contain a phone number to call in case of questions, but better for the user to find a number independently if not already known.

TML

Partnering with Texas Local Government since 1974 www.tmlirp.org

The common thread to all the attacks outlined previously is the reliance on the user not to question or verify the actions requested. The internet was built on trust, with all the threats present today not even imagined when much of the technology at its core was created. Thus, responsibility falls on the users and organization to employ a sustained, suspicious vigilance in any contact.





The most powerful key in any security system is the "delete" key. When a user receives an email that is even a little suspicious, deleting it is usually the best course of action. Where possible, verification by calling a known phone number is best. The email might contain a phone number to call in case of questions, but better for the user to find a number independently if not already known.

Many organizations have an IT department, whether a dedicated, in-house team or an outside contractor, and they should be utilized as a resource for validation of suspicion. Any IT professional will say that it's better to be asked a thousand questions about benign material than to have to eradicate one rampant virus.

Management should be sensitive to user questions and doubts. Without a full-time staff, management should develop methods for reporting and tracking threat detection. Without that, an organization might be under continued siege without anyone recognizing it, making improvements to defense impossible.

Training should be provided to users to identify risks and how to handle them, and that training should be repeated and refined, with periodic testing and review. Attackers might send out a million phishing messages a day with virtually no cost. Failure to recognize even one of these attacks can yield thousands of dollars to the attackers and a blow to the reputation of the organization, not to mention the employee.

*Your entity should have a person designated to receive and act upon reports.*


Management should be sensitive to user questions and doubts. Without a full-time staff, management should develop methods for reporting and tracking threat detection. Without that, an organization might be under continued siege without anyone recognizing it, making improvements to defense impossible.

Training should be provided to users to identify risks and how to handle them, and that training should be repeated and refined, with periodic testing and review. Attackers might send out a million phishing messages a day with virtually no cost. Failure to recognize even one of these attacks can yield thousands of dollars to the attackers and a blow to the reputation of the organization, not to mention the employee.

*Before administering the test, consider referring to the Cybersecurity Awareness handout as a summary.*


Cybersecurity Awareness Training Assessment of Knowledge (Test)

Employee Name (Printed): _____ Date: _____

Employer: _____ Department: _____

Original Test Score: _____ Corrected Test Score: _____

Please complete each question (10 questions) and pick the correct answer. (Circle one letter).

1. Which of the following are personal identifiable information?
   A. Your IP address (an example is the number assigned to your computer)
   B. Your birthplace
   C. Driver's license number
   D. All of the above

2. If you are suspicious of an email, what should you do?
   A. Do not click on the links provided in the email.
   B. Do not open any attachments in the email.
   C. Do not provide personal information or data.
   D. Forward the email to your IT department
   E. All of the above

3. If you receive a phone call or email from an unknown individual asking about your invoice payment process, you should:
   A. Provide full and complete answers to all questions
   B. Take all questions down and send answers via email
   C. Answer only questions for which you know the answer for sure
   D. Do not answer questions, but take the caller's contact info, and consult your IT department and purchasing department

4. Which is a good password practice?
   A. Avoid single words found in a dictionary or proper nouns.
   B. Do not keep copies of passwords where others can see them, preferably not on paper anywhere, or in any clear-text electronic format.
   C. Do not share your passwords to anyone else.
   D. Do not use the same passwords, or close variation, on multiple systems, including personal ones.
   E. All of the above are good practices

5. What is ransomware?
   A. Software that protects your computer from viruses
   B. Cryptocurrency, like bitcoin
   C. Malware that locks users out of their devices or blocks access to files until a sum of money is paid

6. What is the meaning of "threat" with regards information security?
   A. The use of strong language to get wanted reaction
   B. The potential targeting of a network or system in an attempt to damage, harm or disrupt its capability to operate.
   C. Continual texting and communicating through social media
   D. None of the above

7. Which is **not** a good security practice?
   A. Use Multi-Factor Authentication for your accounts
   B. Use one complex password for all your accounts
   C. Use face recognition and/or password for your smartphone
   D. Verify the email sender's domain of a suspicious email and if you need to call, find another source for the phone number outside of the email.

8. Which of the following are types of tactics used in a cybersecurity attack?
   A. Phishing
   B. Malware
   C. Ransomware
   D. All of the above

9. What type of tactic used in a cybersecurity attack would be best described as "an email targeted at a specific individual or department within an organization that appears to be from a trusted source"?
   A. Robocalling
   B. Ghosting
   C. Catfishing
   D. Spear Phishing

10. If you click on an unknown link or attachment in a suspicious email and then wonder "what you just clicked", what if any actions should you take?
   A. Watch the screen for at least five minutes to make sure nothing out of the ordinary occurs
   B. Restart your computer to make sure it has not been infected
   C. Contact your IT department or person in your organization who is responsible for computer operations
   D. Continue with your normal activities and let the organization's firewall or virus scan address the threat

## Cybersecurity Awareness Training Assessment

## Answer Key

1. D— All of these are considered personal data.

2. E – All of the above are suggested if you are suspicious of an email's content or origin.

3. D – Phone calls or emails requesting information about your organization's payment process should be treated with suspicion. Do not respond unless it is determined that the caller is legitimate.

4. E — All are steps that should be taken with your passwords.

5. C— Cybercriminals attempt to encrypt data or block access to your system for financial gain with ransomware.

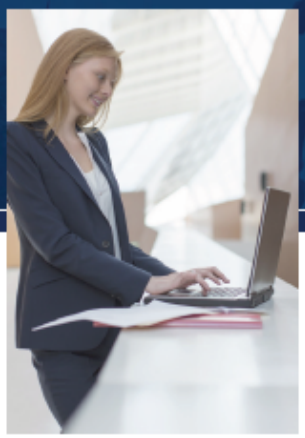
6. B - Threats can involve the intrusion or disclosure of confidential information to unauthorized people.

7. B – Repeating password across accounts is not recommended, even if it is a complex password.

8. D – All of the above are tactics used by cybercriminals, and there are others.

9. D– A criminal that uses spear phishing utilizes details to make the email seem legitimate.

10. C – If you make a mistake, timing is critical. Notify your IT professionals immediately.



# Phishing: Do Your Part to #BeCyberSmart

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts.

## HOW CRIMINALS LURE YOU IN

The following messages from the Federal Trade Commission's OnGuardOnline are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit **https://www.irs.gov/privacy-disclosure/report-phishing**

## SIMPLE TIPS

**Play "hard to get" with strangers.** Links in email and online posts are often the way cybercriminals compromise your computer. If you're unsure who an email is from — even if the details appear accurate — do not respond, and do not click on any links or attachments found in that email. Be cautious of generic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.

**Think before you act.** Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks "phishy," reach out to them via customer service to verify the communication.

**Protect your personal information.** If people contacting you have key details from your life — your job title, multiple email addresses, full name, and more that you may have published online somewhere — they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

**Be wary of hyperlinks.** Avoid clicking on hyperlinks in emails and hover over links to verify authenticity. Also ensure that URLs begin with "https." The "s" indicates encryption is enabled to protect users' information.

MFA

**Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token — a small physical device that can hook onto your key ring.

**Shake up your password protocol.** According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts.

**Install and update antivirus software.** Make sure all of your computers, Internet of Things devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and antispyware.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Source: CISA National Cybersecurity Awareness
https://www.cisa.gov/publication/national-cybersecurity-awareness-month-publications

(800) 537-6655 · **www.tmlirp.org**