Cybersecurity Awareness Training

Learning Outcomes

By completing the Cybersecurity Training Awareness, staff will:

1. Be able to identify acceptable information security habits and procedures to protect information resources
2. Be able to detect or identify basic information security threats
3. Be able to address and report basic information security threats in accordance with best practices
4. Serves as the District's compliance with House Bill 3834

Principles of Information Security

Information Security

What "Information Security" means to you.

Definition – "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Examples listed in the Galveston ISD Technology Responsible Use Policy:

- Unauthorized entry into a computer or files
- Impersonating another person online
- Sharing your password with others
- Locking or log-out on your computer when leaving it unattended

Principles of Information Security

Information Security

What types of information are you responsible for safeguarding?

Regulatory Requirements

- FERPA (Family Educational Rights and Privacy Act)
- COPPA (Children's Online Privacy Protection Act)
- EDGAR (Education Department General Administrative Regulations)
- CIPA (Children's Internet Protection Act)
- HIPAA (Health Insurance Portability and Accountability Act)

Confidential

- PII – Personally Identifiable Info. Information identifying personally owned property, such as vehicle registration information or title number and related information
  - Information about an individual that is linked or linkable to one of the below (i.e., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information

Principles of Information Security

Data Classifications

To fully understand what we are safeguarding, we need to define:

- What is data.
- Types of data.
- Where the data can be stored.
- How access needs to be safeguarded by unauthorized access and unauthorized use.
- What happens when the data is no longer needed and needs to be disposed or sanitized.

What is data?

According to the **NIST (National Institute of Standards in Technology)** data is any piece of information from which any understandable information is derived. An example might be a class roster in a spreadsheet. Another example might be a photo.

Principles of Information Security

Data Classifications

Let's break down our data types into the following common classification:

- **Restricted** - Do not share with anyone.
- **Confidential** - Only share with the people who need it to get their job done. This content should never be sent without using an encrypted email system. **DO NOT** store in Google Drive or OneDrive, the content needs to be password protected and/or encrypted in a secure location.
- **Agency-Internal** - Can be accessed and shared internally but not by anyone outside of the network or domain.
- **Public** - Should be stored on Google Drive or OneDrive and shared whenever needed.

Principles of Information Security

Data Classifications

Now that we know what type of data, we have let's look at what form and location the data might be found.

- **Form -** how the information can be stored.
  - File - Word Doc, Google Doc, email, photo
  - Communication - phone text message, app communication (example: class dojo)
  - Physical paper document
- **Location** - where the information can be stored.
  - Local media - local hard drive
  - USB - thumb drive / external Hard Drive
  - Attachment - email attachment, web attachment
  - File Cabinet, desk drawer, top of desk
  - Cloud

Best Practices

Safeguarding Information & Information Systems

How to safeguard against unauthorized access?

GISD Responsible Use Policy

- Staff only have access to data required for their perspective job function
- Confidential student and staff information should always be stored in a password protected location on our network
  - Never share network credentials
  - Change your password every 180 days
  - Create a complex password
  - Lock or log-out from your device when away
  - Use Multi-Factor Authentication (see MIS for help in setting up)

GISD Data Security

- Never send sensitive data by email
- Verify websites are legitimate
- Never share your passwords with anyone, even MIS staff
- Staff only have access to data required for their perspective job function

Best Practices

Safeguarding Information & Information Systems

Best practices for securely storing information.

Understanding where and how data is stored is very important to securing information. Different data types have different needs as to the level of securing the data. **Keep in mind that some data should be eyes only to specific users where other data is ok to be seen by everyone.**

Here are some ways to securely store information.

- Data stored on paper/archived on media needs to be in a locked room and if possible, in a locked file cabinet only accessible by authorized staff.
- Encrypt any detachable storage (i.e. usb drives, thumb drives, etc).
- Password Protect files that have restricted or confidential data or the organization feels needs limited access to the file.
- Have restricted use of file shares locally or on the cloud that are controlled by group access. Making sure these groups are updated regularly.
- Secure file transfer. Use of SFTP or HTTPS encrypts the data during transfer.

Best Practices

Safeguarding Information & Information Systems

Securely disposing & sanitizing information & information systems.

What do we do with the data after it is no longer needed. There is still information in the files that need to stay secure and private. **We can not simply throw away the file folder or media containing any type of sensitive data.** Here are some best practices on disposing or sanitizing the information.

- **Clear** - A method of sanitization that applies programmatic, software based techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge** - A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- **Destroy** - A method of sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data

Best Practices

Detecting, Assessing, Reporting & Addressing Information Security Threats

What is the meaning of "threat" with regards to information security?

A "threat", in the context of computer security, refers to anything that has potential to cause serious harm to a computer system.
A "threat" is something that may or may not happen but has the potential to cause serious damage.
"Threats" can lead to attacks on computer systems, networks and more.

To keep yourself protected it is important that you understand the most common threats related to Cyber Security and Information Security.

A threat is defined as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service" (Johnson, Badge, Wiltermire, Snyder, & Skorupka,2016).

Knowing what a threat is good but knowing how these "threat actors"(group or person posing a threat) are motivated helps us safeguard our information.

Best Practices

Detecting, Assessing, Reporting & Addressing Information Security Threats

What are the common "threat actors" and their motivations?

- **State-Sponsored** - usually are backed by a government entity. These threat actors can work for years and for the long haul to gain access to systems. Usually these target other government entities but have been seen aiming for new targets like schools, universities, and private organizations.
  - Motive - Cyberwarfare for military, economic or political gains.
  - Best Protection: vulnerability management and keeping systems patched.
- **Hacktivists** - these are groups that hack for social or political agenda.
  - Motive - Political, environmental, religious, social, etc
  - Best Protection: knowing if you might be a target because of their motives. Good Cyber Awareness
- **Lone Wolf** (single threat actor) - Gain access to your network and financial gain. These are ones that might write ransomware, malware, etc. They also "sell" their technology on the darkweb (cybercrime as a service) so others profit as well.
  - Motive - Network access, monetary gain
  - Best Protection: Good Cyber Awareness. Always think you might be one of their targets.

Best Practices

Detecting, Assessing, Reporting & Addressing Information Security Threats

What is the meaning of "risk" with regards to information security?

A "security risk" is any event that could result in the compromise of organizational assets i.e. the **unauthorized use**, **loss**, **damage**, **disclosure** or **modification** of organizational assets for the profit, person interest or political interests of individuals, groups or other entities.

What is the meaning of "attack" with regards to information security?

An "attack" is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.

It happens to both individuals and organizations.

Awareness of How to Identify, Respond to, and Report on Information Security Threats and Suspicious Activity

How to identify indicators for common attacks?

Why do we need to know what a threat is and who might be causing the threat? It is "risk". Risk in this case is the potential loss of information or the loss of ability to access information which would cause adverse impact on operations of the entity such as reputation, image, function, or mission.

Ultimately it boils down to "cost". We need to be as cyber aware as possible, so we keep our risk low. Loss of PII data can cost the district and the student or staff with financial or reputation damage for years to come.

An "attack" is what we call when a "threat actor" is trying to gain unauthorized access or compromise to systems and or information.

If you experience any of the following it is important to always notify the MIS Department.

- Phishing and Spear Phishing
- Malicious code
- Weak and default passwords
- Unpatched or outdated software vulnerabilities
- Removable media.

Awareness of How to Identify, Respond to, and Report on Information Security Threats and Suspicious Activity

How to respond to and report on common attacks or suspicious activity.

The most important step you can take is not to overreact to a security event. If you have identified a concern it is always important to notify your administrator and the districts MIS Department about the concern.

Never under any circumstances reach out to or communicate with the threat actor.

This could ultimately put you, the organization or your students at risk. If you become aware of a leak or sharing violation make sure to resolve it as soon as possible, but always notify a district authority.

There may be other ramifications that you are unaware of, so it is important that technology is aware of the situation in order to further investigate.

Using Public Wi-Fi

Dangers of Free Internet

"I'll take a sweet venti cold brew with extra sweet cream and add a side of honeypot identity theft! "

Hackers love coffee shops, and no you are never safe.

When you connect to any free internet service at coffee shops, restaurants, airports or other, you are at very high risk of giving loads of information to third parties or possibly even have your computer hijacked.

When you connect your computer to WiFi, it is designed to connect the closest access point with the most powerful signal.

If however someone has already connected to the free internet service and set up their radio WiFi you will likely pass through the hacker's device unknowingly before getting to the internet.

Using this device a hacker can let you have complete internet access but write a script that will redirect you when you go to email. Instead of hitting you actual email website you are redirected to the hacker's computer sitting next to you at the coffee shop.

The site you get looks just like a Office 365 Portal login, so you think nothing of it and type your username and password. That's all that is needed, and in seconds your account is completely compromised.

So, does this mean you will have your identity stolen anytime you connect to free public WiFi?

No, but it is important to understand that the danger exists, and you should be very careful where you go and what you do on these types of connections.

Also be aware of your surroundings. While these devices can be small, it's always a good idea to look around and see if there is anything out of place concerning the other patrons of the store.

Email Communication

Phishing & Spear Phishing

Scammers using Phishing a method of deceiving people into disclosing PII (Personal Identifying Information). This not only puts you and Galveston ISD at risk, but also the student's information that you are in care of.

A Spear phishing attack is a type of targeted phishing that focuses on a specific individual or group of individuals.

A good example of this would be accounts payable for the school district.
Or impersonating a high level official to request the purchase and transfer of funds via gift cards.

Email Communication

Phishing & Spear Phishing

Indicators: The following are suspicious indicators related to phishing and spear phishing:

- Uses e-mail
- May include bad grammar, misspellings, and/or generic greetings
- May include maliciously-crafted attachments with varying file extension or links to a malicious website
- May appear to be from a position of authority or legitimate company:
    - Your employer
    - Bank or credit card company
    - Online payment provider
    - Government organization
- Asks you to update or validate information or click on a link
- Threatens dire consequence or promises reward
- Appears to direct you to a web site that looks real

Email Communication

Phishing & Spear Phishing

Spear phishing specifically:

- Has a high level of targeting sophistication and appears to come from an associate, client, or acquaintance
- May be contextually relevant to your job
- May appear to originate from someone in your email address book
- May contain graphics that make the email look legitimate
- Effects include, but are not limited to:
- Deceiving you into disclosing information
- Allowing adversary to gain access to your and/or your organization's information

Email Communication

Phishing & Spear Phishing

Countermeasures

- The following countermeasures can be taken to guard against phishing and spear phishing:
- Watch out for phishing and spear phishing
- Delete suspicious emails
- Contact your system security point of contact with any questions
- Report any potential incidents
- Look for digital signatures
- Configure Intrusion Detection Systems (IDS) to block malicious domains / IP addresses

Do not:

- Open suspicious emails
- Click on suspicious links or attachments in emails
- Call telephone numbers provided in suspicious emails
- Disclose any information

If you suspect you may have been a target of phishing, report it to the district at spam@gisd.org

Spoofing

"Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security."

What is Spoofing?

This is a common problem with email and comes in many forms. I have seen employees receive emails from high-level employees in an organization requesting a bill to be paid immediately. Other times it's a company like UPS, Best Buy, a Credit Card, or any other number of possibilities.

The difficult part is emails like this often look very legitimate, but often seem a bit odd. There are ways to verify the authenticity of the email, but most organizations will not send you an email to reset password credentials, conduct a high-level transaction, or obtain sensitive information.

If you are unsure, it is always best to contact the person or organization directly to confirm that the email is legitimate.

Mobile Device Security

Applications and Extensions

With the birth of the iPhone and now Chromebook and Android operating systems, we have been flooded with options for Apps and Extensions to install on our devices and browsers. It's important to know that while many apps are fun or improve our productivity and internet experience, others have malicious intent.

For example, several apps for the game 2048 designed for Android and Chrome web stores.

The game played and seemed perfectly normal. However, in the background, it was, in fact, using the device to mine bitcoin.

The “Cloud”

Using and protecting us in the cloud

As more organizations begin adopting cloud platforms like, Google or Office 365 we find that information privacy is even more of a concern.

While providing immersive and collaborative environments, there are inherent issues with access permissions and sharing.

First and foremost, it is important to understand that the servers that you are storing your data on do not belong to you, and outside of privacy agreements that very few people read, you must have a level of trust for the organization you choose to do business with.

You are also at the mercy of the company's security practices and shortcomings. However, as mentioned earlier hackers are much more likely to be successful against individuals rather than large companies like Google or Microsoft, but this does not mean they don't try either.

The “Cloud”

Using and protecting us in the cloud

The next and probably largest risk to the cloud revolves around the security practices of you, the user. **If you don't have strong passwords, 2 step authentication, or if you are not careful how and who you are sharing information with, you may inadvertently provide access to people that are unintended.**

I have seen people in Google or Office 365 share an entire folder with a coworker or even someone outside of their organization and not realize that every file and folder underneath was also shared. I have also seen people intend to share with one person securely, but accidentally make files or folders public to the world.

This also brings up the issue of storing sensitive un-”encrypted” files inside of a third-party storage system like Google.

What happens if your account is compromised? Even if Google or Microsoft are 100% secure without any potential of being hacked, you are the weak link! If your account is compromised a “threat actor” gets full access to all those sensitive files that you thought were safe.

Digital Footprint

Did you know you have a digital footprint?

Have you ever noticed that when you search YouTube, Google, Amazon or look for anything online, you begin seeing advertisements the align with those same interests and searches?

Maybe you decide to stop at Best Buy and check out some of the newest tech or video games.

Don't be surprised if the next time you pop on your favorite website, there are ads for Best Buy electronics!

Even the location data on your phone that is tied in some way to your digital footprint connects the two and tries to pair your interest with available product.

Digital Footprint

Did you know it follows you everywhere you go?

It's no secret that the government monitors what you do online, but it goes much more in-depth than "big brother" is watching.

Everything you do online and offline is saved, searchable and recorded in some way.

When you first connect to the internet your Internet Service Provider (ISP) saves and monitors your traffic habits, the government keeps a record of your activity, and most websites are tied in with large companies like Google, Amazon, and online ad agencies so you can receive personalized ads that address your interests.

Passwords

Importance of Complex Passwords

It cannot be over-emphasized how important a strong password is.

The following are some basic guidelines for creating a strong password:

- **Don't use Dictionary or personally identifiable words.**
- Use special characters
- Replace letters with characters ie, techpass2018 = T3ch*p@$s2018!
- Abbreviate ie, "Joes birthday is on 9/3/76
  - J0bD@S3!
- Use phrases rather than words
  - It's a long way two the ^ if U wanna Rock Roll
  - S@lly S3lls Sea She!!s by the Seashore
  - An Open <3 = an Open MIND!
- Try not to repeat passwords

Passwords

Importance of Complex Passwords

Saving Passwords

- Every browser available has an option to save passwords. You can see this in action when you log into a site and your browser prompts you to save the password.
- If you are going to use this feature, you should only use it with the lowest level of password you have with accounts you are least concerned about. While this can be a major convenience, it is a huge security risk. While these services have a basic level of security, you can extract the actual password from any one of these systems without a tremendous amount of effort.
- As mentioned earlier in the section about extensions, there are some great programs like LastPass that allow you to save and encrypt your passwords in one place.
- Some of these services cost money but paying for that is much more secure than storing them in a browser that can be compromised more easily.

Hacking with USB Drives

Have you ever found a USB drive?

I attended a security awareness conference where the speaker gave examples of how he conducts penetration testing for businesses.

A penetration test is essentially where a business pays a hacker a large sum of money to ethically hack their organization. They find the problems, write a report and instruct the technical staff or administration on how to fix vulnerabilities.

He said one of his go-to tools was using flash drives to gain remote access to the clients' computers.

Hacking with USB Drives

Have you ever found a USB drive?

He had a very interesting methodology that was both intriguing and downright scary. Once the penetration test had begun, he would take a day and walk through the parking lot of the business and strategically drop nice flash drives in plain sight.

Anyone who has purchased a good flash drive knows they run about $15 - $50. Wouldn't it be great to walk through a parking lot and find a $50 flash drive?

You may want to think twice next time you have the opportunity; this tester preloaded malicious content on the drives before sprinkling them across the parking lot so that once a user plugged them one into a computer, it would immediately run a script giving him unattended access to that machine.

Hacking with USB Drives

The scary thing here outside of the obvious is that the user never actually knows their machine is compromised. If a good hacker is doing their job well, your computer will be compromised, and your data taken off or actively monitored, and you will never know.

Once the hacker has access to the computer, he/she begins mining that machine to extract any credentials or identifying information.

This allows the hacker to not only further exploit the person but also their friends and coworkers.

So, next time you find a free flash drive laying on the ground, it might be in your best interest to just keep on walking!

What did you learn?

Which of the following can cybercriminals use to gain access to confidential information:

A. Printer
B. Network-attached copiers
C. Scanners
D. Fax Machines
E. All of the Above

Which of the following can cybercriminals use to gain access to confidential information:

A. Printer
B. Network-attached copiers
C. Scanners
D. Fax Machines
E. All of the Above

Certain features associated with these Multi-functional devices (MFDs) can pose a serious infrastructure and information security risk. As with all other Information Resource, MFDs must be managed in a secure manner to assure protection against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information.

Galveston ISD devices, personal laptops, mobile devices, and desktops that connect to the Galveston ISD network are subject to Galveston MIS monitoring, security and management standards.

A. True
B. False

Galveston ISD devices, personal laptops, mobile devices, and desktops that connect to the Galveston ISD network are subject to Galveston MIS monitoring, security and management standards.

A. True
B. False

All hardware connected to the Galveston ISD network is subject Galveston ISD MIS management, security, and monitoring standards.

Mobile devices are generally not secure and inherently at risk for data loss. As such, Galveston ISD _____ information should not be stored on a mobile computing devices.

A. Confidential or sensitive
B. Syllabus
C. Marketing
D. Course Catalog
E. All of the Above

Mobile devices are generally not secure and inherently at risk for data loss. As such, Galveston ISD _____ information should not be stored on a mobile computing devices.

A. Confidential or sensitive
B. Syllabus
C. Marketing
D. Course Catalog
E. All of the Above

Many mobile devices offer services beyond making phone calls, texting, and receiving email.

With such a wide variety of mobile devices and options for connectivity, we strongly recommend that you exercise caution and be diligent about practicing safe computing.

Emails in my inbox and files I have created and stored on Galveston ISD owned/provided resources are my personal property.

A. True
B. False

Emails in my inbox and files I have created and stored on Galveston ISD owned/provided resources are my personal property.

A. True
B. False

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of Galveston ISD are not private. The Galveston ISD Technology Division has stringent policies, procedures, and monitoring for all staff. We adhere to a rigorous check-and-balance system and are subject to periodic internal and external audits. Integrity and high ethical codes of conduct are cornerstones of our security program.

It is the responsibility of Galveston ISD to safeguard and secure student's personal information, and as an employee of Galveston ISD, I share in this responsibility.

A. True
B. False

It is the responsibility of Galveston ISD to safeguard and secure student's personal information, and as an employee of Galveston ISD, I share in this responsibility.

A. True
B. False

A wide variety of third parties have entrusted their information to Galveston ISD for business purposes, and all staff of Galveston ISD must safeguard the privacy and security of this information. The most important of these third parties is the individual student, student data is accordingly confidential, and access will be strictly limited based on business need for access.

A virus is software/application that securely manages my data.

A. True
B. False

A virus is software/application that securely manages my data.

A. True
B. False

A **virus** is one of the most common types of malware. They are capable of replicating and spreading to other computers by attaching to messages or programs when a recipient opens the message or launches the program.

We are all responsible!

Remember, you have a critical role to help keep our district safe.

- Ensure employees & student complete professional development and trainings.
- Follow district approval processes and procedures.
- Report suspicious emails to spam@gisd.org
- Contact MIS @409-766-5175

National Cyber Security Alliance. Stop. Think. Connect. Retrieved from https://www.stopthinkconnect.org.