CYBER SECURITY AWARENESS TRAINING

ESC100

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 entity's compliance with House Bill 3834

WHAT IS INFORMATION SECURITY?

PRINCIPALS OF INFORMATION SECURITY

Information Security

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

WHAT TYPES OF INFORMATION ARE YOU RESPONSIBLE FOR SAFEGUARDING?

PRINCIPALS OF INFORMATION SECURITY

Confidential Information

Personally Identifiable Information (PII) - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

- Examples of PII:
  - Full name
  - Personal ID numbers - Social Security, driver's license
  - Financial information - Bank account number, credit card number
  - Street address
  - Email address
  - Medical Records
  - Student records

WHAT TYPES OF INFORMATION ARE YOU RESPONSIBLE FOR SAFEGUARDING?

PRINCIPALS OF INFORMATION SECURITY

Sensitive Information

Information where the loss, misuse, unauthorized access, or modification could lead to breach of data systems or adversely affect the privacy of an individual.

- Examples of Sensitive Information
  - Chromebook, computer, and email account usernames and passwords
  - Information regarding the structure/configuration of security controls
  - Procedures needed to gain access to secured resources
  - Any other information an organization considers private and/or does not wish to make publicly available

WHERE IS THE INFORMATION YOU ARE RESPONSIBLE FOR SAFEGUARDING LOCATED?

PRINCIPALS OF INFORMATION SECURITY

Form - How is the information you need to protect stored?

Examples:

- **Files** – Word and Google docs, Excel and Google spreadsheets, photos
- **Communication** – Email, text, communication app
- **Physical paper document** – Report cards, medical records, student records

Location - Where is the information you need to protect stored?

Examples:

- **Local electronic copy** – Your computer, phone, thumb drive, external drive, etc.
- **Cloud** – Gmail, Drive, Dropbox
- **Applications** – Eduphoria, Skyward, Canvas, Seesaw
- **Local physical copy** – Filing cabinet, desk, backpack, car

BEST PRACTICES
Safeguard Information and Information Systems

How can you safeguard against unauthorized access to information, information systems, and secure facilities/locations?

- Data stored on paper should be in a locked room and file cabinet, only accessible by authorized staff.
- Do not store sensitive or PII data on USB drives, thumb drives, or any external drive.
- Google Drive is the only district-approved solution for cloud storage.

BEST PRACTICES
Safeguard Information and Information Systems

How can you safeguard against unauthorized access to information, information systems?

- Never share computer or Google usernames and passwords with anyone (other employees, substitute, part-time, consultants).
- Do not log into a device or Google account for someone using your username and password.
- Do not write your computer or google usernames and passwords down anywhere including under your keyboard
- Do not give staff more access than required by their job function.

BEST PRACTICES
Safeguard Information and Information Systems

How can you safeguard against unauthorized use and access to systems and information?

- Confidential student and staff information should always be stored in a password protected location
- Never share computer or Google usernames and passwrods with family members.
- Either lock or log-out from your device when away
- Never send sensitive or confidential (PII) data by email
- Verify websites are legitimate.

BEST PRACTICES
Safeguard Information and Information Systems

How can you securely dispose of devices that contain sensitive or PII data?

- Do not throw away media, computers, disk drives, USB drives, thumb drives, external drives, or any device that may contain sensitive or confidential (PII) data
- Submit a technology support incident, email your technology department, or contact the Helpdesk if you have any devices you wish to dispose of
- Your Technology Department or a certified contracted partner will remove the data from the devices with a method that conforms to appropriate standards
- Shred any papers that contain sensitive or confidential (PII) data.

AWARENESS

What is a Security Threat

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

- A security threat refers to anything that has the potential to cause serious harm to a computer system, information, or unauthorized access to information. Threats can lead to attacks on computer systems, networks, and websites.
- Examples of threats include phishing email, ransomware, trojans, and malware.

AWARENESS
Who are threat actors?

Who are common “threat actors” and what are their motives?

- Insiders are current or former employees with access to an organization's networks, systems, or information. Malicious insiders intentionally misuse their access to negatively affect the confidentiality, integrity, or availability of the information systems. They are motivated by revenge or financial gain.

- Unwitting insiders unintentionally cause damage to their organization's information systems through their actions, such as clicking on malicious links in an email.

AWARENESS

Who are threat actors?

Who are common “threat actors” and what are their motives?

- Cybercriminals are largely profit-driven and represent a long-term, global, and common threat. They target information to sell, hold for ransom, or otherwise exploit for monetary gain.

- Nation-State actors aggressively target and gain persistent access to public and private sector networks. Their goal is to compromise, steal, change, or destroy information for espionage, political, economic, or military reasons

AWARENESS

Who are threat actors?

Who are common “threat actors” and what are their motives?

- Hacktivists are politically, socially, or ideologically motivated and target victims for publicity or to effect change, which can result in high profile events.

- Terrorist Organizations are identified by the U.S. Department of State. Their cyber activity is typically disruptive or harassing in nature. Their motivations are political or ideological, possibly for financial gain, espionage, or as propaganda.

AWARENESS

What is a security risk?

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

- A security risk is any event that could result in the compromise of student or district information.
- Passwords stored where others have access (e.g., under keyboard).
- Confidential information (student data) stored on personal devices, or stored on personal online storage accounts (e.g., Dropbox, personal Google, OneDrive, Box) is a security risk.

AWARENESS
What is an attack?

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

- An attack is an attempt to gain unauthorized access with intentions to destroy, expose, alter, disable, or steal student, employee, or district information.

- Outcomes include identity theft (students and employees), modified grades, posting of student information, and destruction of student, employee, or business information.

IDENTIFY
Security Threats

What are the most common types of cyberattacks and how can you identify and protect against them?

The majority of cyberattacks start with some combination of phishing, spoofing, social engineering, and spear phishing. Threat actors use these methods to acquire sensitive information such as usernames, passwords, SSN, address, and credit card information.

Phishing

Scammers use email or text messages to trick you into giving them your business or personal information. They send emails that appear to be from your colleague or someone you would expect to receive an email. They may try to steal student, district, or your personal passwords, account numbers, or Social Security Numbers.

IDENTIFY
Security Threats

What are the most common types of cyberattacks and how can you identify and protect against them?

Spoofing

Email spoofing for example: John, the sender of email forges (spoofs) an email address and the message appears to be from Bill's email address. Look for misspellings, odd word phrases, and uncommon characteristics in how the email is written.

Social Engineering

The use of deception to manipulate individuals into divulging confidential, sensitive, or personal information that can be used for fraudulent purposes. Be suspicious of anyone asking for information. For example if you receive and email, text, or chat message requesting information simply call the bank, person, or business to answer the question.

IDENTIFY
Security Threats

What are the most common types of cyberattacks and how can you identify and protect against them?

Spear Phishing

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user’s computer. These emails or electronic communications often use clever tactics to get victims' attention.

.

IDENTIFY
Security Threats

What are the most common types of cyberattacks and how can you identify and protect against them?

TIPS: Identify a Cyberattack and Stay Safe

Two Most Important Takeaways!

- Don’t click on links in emails. Perform a Google search or type the address in the browser yourself.
- Trust your gut feeling. If you have the slightest amount of suspicion about an email, DELETE IT! If the email was important, Technology can recover it or the sender can resend it!

IDENTIFY
Security Threats

What are the most common types of cyberattacks and how can you identify and protect against them?

TIPS: Identify a Cyberattack and Stay Safe

- Beware of any urgent emails! - If the email is from your supervisor and contains an urgent request for you to disclose sensitive/PII data or purchase something for them. BE SUSPICIOUS and call your supervisor.
- Don’t reveal personal or financial information in an email - Do not respond to email solicitations for this information.
- Pay attention to your Gmail warnings – Just because an email appears to be from someone you know doesn’t mean that it is. If there’s a warning about an email that appears to be from someone you know, DELETE IT!

RESPOND AND REPORT
Security Threats

Respond and Report – What should I do if I'm suspicious of a cyberattack and who do I report it to?

- DELETE the email
- Call your Help Desk, email your Technology Department, or open technology support incident.

WHAT DID YOU LEARN?

WWW.ESC100.NET

Dave, your substitute, can't log in and asks you to log in so he can show the students their assignments for the day. How should you respond?

A. Login to his computer
B. Give him your username and password to save time
C. You're busy and don't have time to help Dave. You know Mike down the hall has her password under her keyboard. Tell Dave so he can use Mike's login.
D. Advise him to call the Technology Department
E. All of the Above

Dave, your substitute, can't log in and asks you to log in so he can show the students their assignments for the day. How should you respond?

A. Login to his computer
B. Give him your username and password to save time
C. You're busy and don't have time to help Dave. You know Mike down the hall has her password under her keyboard. Tell Dave so he can use Mike's login.
D. Advise him to call the Technology Department
E. All of the Above

Giving anyone your log in information or logging into another computer for someone else gives them access to sensitive and confidential information, student or staff information. It also violates the Acceptable use Policy.

You receive an email from a co-worker letting you know you were left off of an email your boss sent with an attachment. Your co-worker included the attachment, which has to be filled out and turned in by the end of the day. Which are acceptable responses?

A. Download the attachment, fill it out, and return to your boss
B. Email your boss and let her know you didn't receive the email she sent earlier today with the attachment
C. Call your co-worker and ask if he sent the email
D. Call your boss and explain you didn't receive the email and request he send it to you
E. None of the Above

You receive an email from a co-worker letting you know you were left off of an email your boss sent with an attachment. Your co-worker included the attachment, which has to be filled out and turned in by the end of the day. Which are acceptable responses?

A. Download the attachment, fill it out, and return to your boss
B. Email your boss and let her know you didn't receive the email she sent earlier today with the attachment
C. Call your co-worker and ask if he sent the email
D. Call your boss and explain you didn't receive the email and request he send it to you
E. None of the Above

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. A few ways to spot suspicious emails are misspellings, language that is not quite right, sense of urgency, generic greeting. When you receive emails containing links to pay bills, update information, or access your account make a practice to type the address in the web browser yourself. This practice eliminates the threat actor's ability to steal your login and account access.

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.

You receive an email from a co-worker asking why Jane, a student of yours, has a test accommodation. How do you respond?

A. Answer the email explaining Jane's physical disabilities
B. Forward the email and ask the Special Education person who evaluated Jane to provide the details
C. Advise your co-worker to go to the source and email Jane's parents
D. None of the above

You receive an email from a co-worker asking why Jane, a student of yours, has a test accommodation. How do you respond?

A. Answer the email explaining Jane's physical disabilities
B. Forward the email and ask the Special Education person who evaluated Jane to provide the details
C. Advise your co-worker to go to email Jane's parents
D. None of the above

Only teachers, counselors, or others who are involved directly in Jane's education are allowed access to her information. Never send sensitive or confidential information through email unless it is an appropriate FERPA and/or HIPAA compliant email service and is approved by the your Technology Department.

You receive an email that appears to be from your bank. The message informs you there was a suspicious activity with your account, and it's suspended. To reactivate, follow the link and log in, but you notice a word is misspelled. You recognize the email as a phishing attempt. Which two actions should you take?

A. Delete the email
B. Follow the link to find out where it takes you
C. Call your bank to notify them
D. Forward the email to your spouse
E. None of the above

You receive an email that appears to be from your bank. The message informs you there was a suspicious activity with your account, and it's suspended. To reactivate, follow the link and log in, but you notice a word is misspelled. You recognize the email as a phishing attempt. Which two actions should you take?

A. Delete the email
B. Follow the link to find out where it takes you
C. Call your bank to notify them
D. Forward the email to your spouse
E. None of the above

Look up the website or phone number for the company or person who's contacting you. Call the company or person directly. Use a number you know to be correct, not the number in the email. Tell them about the message you got.

District devices, personal laptops, mobile devices, and desktops that connect to the District network are subject to the District IT monitoring, security and management standards.

A. True
B. False

District devices, personal laptops, smartphones, and desktops that connect to the District network are subject to District IT monitoring, security and management standards.

A. True
B. False

All hardware connected to the District network is subject to the District IT management, security, and monitoring standards.

Smartphones are generally not secure and inherently at risk for data loss. As such, the District's_____ information should not be stored on a smartphone.

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

Smartphones are generally not secure and inherently at risk for data loss. As such, the District's_____ information should not be stored on a smartphone.

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

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

Smartphones introduce a wide variety of security vulnerabilities. Practice safe computing and don't access confidential or sensitive information using a smartphone.

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

A. True
B. False

Emails in my inbox and files I have created and stored on District 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 the District are not private. The District's Technology Department has stringent policies, procedures, and monitoring for all staff.

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

A. True
B. False

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

A. True
B. False

All staff of the District must safeguard the privacy and security of student information.

info@esc100.net