Cybersecurity Awareness Training

Principles of Cybersecurity

What's Your Role?

What does "Cybersecurity" mean to you and the district?

Cybersecurity is in the news a lot these days. The problem is that both individuals and organizations large and small have become targets of cybercriminals. Organizations like ours are fighting back with information security.

It's all about protecting the confidentiality, integrity and availability of information.

The goal is to prevent unauthorized access, use, modification, and destruction of our vital information.

As an employee, you have an important role to play in the solution.

Principles of Cybersecurity

What to Know

Utilizing cybersecurity best practices to protect against these common scam scenarios.

- Business Email Compromise
  - Business Email Compromise is a phishing-based scam with the aim of extorting a large amount of money from organizations and/or individuals.
- Phishing Emails
  - Phishing is a type of scam used by cybercriminals to trick people into providing personal and financial information or downloading malware.
- Malware
  - The term "malware" covers a whole range of malicious programs designed to infiltrate and damage the computers and networks we use every day.
- Ransomware
  - This is what happens when a device is infected with ransomware; the user is unable to access the device or its files until a fee is paid.

Business Email Compromise

Scam Scenarios

Two Common Business Email Compromise scams.

- CEO Fraud - Fraudsters impersonate a senior executive, such as a district administrator, and using the email address, they send an urgent request. The employee, believing the request comes from an administrator, follows the instructions and transfers the funds to a fraudulent account.
- Fraudulent Invoices - Posing as a known supplier, fraudsters request payment for a fake invoice. The employee clears the invoice and makes the payment to a fraudulent account, using the modified account details provided.

How they do it?

- Phishing - Using phishing messages to trick employees into providing information such as, account passwords, financial operations and procedures, or tax or direct deposit account details.
- Hacking – Using malware and other tools to either "hack" email accounts or spoof an email address to make it look as if the email comes from the person they are impersonating. A small change in the spelling of an email address, (microsof.com instead of microsoft.com) can be an indication of a forged/spoofed email address.
- Impersonating - Using the information acquired and the compromised email account, the fraudster can impersonate key people involved in money transfers to trick victims into transferring funds into a fraudulent account.

Business Email Compromise

Best Practices

Avoid being tricked by a business email compromise fraud.

- If a request **makes you uncomfortable**, pause and ask yourself, does this employee or executive usually write to me, or am I really the person who should reply to this request?
- Be suspicious of any email **urgently requesting a large transfer of funds** in an unusual manner. Be even more vigilant if the sender pretends to be unreachable (e.g., I'm on holidays; I lost my phone) or requests secrecy.
- Before providing sensitive information by email or telephone, **verify the identity of the individual requesting** it and **confirm the legitimacy** of his or her request.

Phishing Emails

Scam Scenarios

Most Common Techniques

Phishing by email - An email that appears to come from within the district or a well-known institution, such as a bank or a tech company. The email urges the victim:

- To click on a link, which redirects the victim to a fraudulent phishing website
- To open an attachment, which infects the victim's device with malware

A phishing website is a fake site designed to look like a company's legitimate website. It is used to collect personal and financial information which can be used to commit identity theft or divert funds.

Spear Phishing - Cybercriminals target specific employees. These phishing attempts are sophisticated, customized and well prepared, and are thus very convincing and harder to detect. Techniques include:

- Using information about their targets to write convincing messages
- Using malware and other techniques to compromise email accounts
- Spoofing email addresses to deceive the recipient

In a variation known as whale phishing, cybercriminals impersonate high-level executives in emails to trick employees into transferring large sums of money to a fraudulent account.

Phishing Emails

Best Practices

Avoid being tricked – Review the anatomy of an email.

- From Field - Make sure you know and trust the sender
  - Since the email address could be forged, hover your mouse over the sender's name to see the full email address and look for mistakes, like microsof.com instead of microsoft.com.
- Subject Field - The subject line is often worded to convey a sense of urgency, to trigger immediate action on your part.
- Attachment - The message may contain an attachment, which could be used to install malware on your computer.
- Message Content - Phishing messages often:
  - Use a generic salutation (e.g., Dear Client) instead of your name
  - Contain grammatical errors and misspellings
  - Call for an immediate reaction
  - Include a hyperlink or a button that you are asked to click
  - Ask for personal or financial information
  - Ask you to update your account information or password
- Email Signature - The signature will often be generic, with no indication of how to contact the sender.

Malware

Scam Scenarios

Types of Malware

- Computer Virus - A program capable of attaching itself to a document or to a genuine program. It usually makes copies of itself, in order to infect and corrupt additional files.
- Trojan Horse - A malicious program disguised as a legitimate one. The malicious code is usually hidden (or embedded) in an email attachment or in a useful or interesting program, such as a computer game, in order to trick users into installing it.
- Spyware - A malicious program that is usually secretly installed on a computer. Once activated, it gathers and transmits users' information or actions, such as passwords, credit card numbers or web browsing habits, without their knowledge.
- Ransomware - A type of malware that uses encryption to prevent victims from using their computer or accessing their files until a fee is paid. Once it has infected the computer, a message informs the victim that a given amount must be paid in order to have the files decrypted or to remove the restriction

Malware

Best Practices

Avoid malware infections.

1. Never modify or disable antivirus software or any other protective mechanism installed on your computer.
2. Stick to legitimate sites for your application purchases and downloads.
3. Always be cautious with a suspicious or an unsolicited email message. Do not click on a link or a button within the message. Do not download or open the email's attachments.
4. Avoid browsing websites that provide pirated material.
5. When browsing the web, make a habit of carefully reading the content of a pop-up window before choosing an option or accepting an offer.
6. Contact your technical support team if you believe that your computer may be infected with malware.

Ransomware

Scam Scenarios

How Ransomware Works

<u>How does a network become infected?</u>

The most common way of delivering ransomware to a computer is through email-based phishing scams that trick you into:

- Opening a malicious email attachment
- Clicking on a link and visiting a malicious website
- Installing an infected application

<u>What happens?</u>

Ransomware can:

- Lock you out of your computer or device, preventing you from using it
- Encrypt your files with a secret key to prevent you from accessing them
- Ransomware can also spread and encrypt files stored on our organization's network.

<u>How do you know?</u>

Once a computer has been infected, a window will be displayed, telling you:

- That your files have been encrypted
- That you must pay a ransom if you want the key required to decrypt them

Attackers will even provide instructions on how to buy the bitcoins needed for the ransom payment.

Ransomware

Best Practices

Reduce Your Risk

- Do not click on links and buttons in unexpected or suspicious emails or text messages.
- Never install an app or program obtained from an unknown or untrusted provider.
- Never modify or disable antivirus software or any other protective mechanism installed on your computer.
- If you fall victim to a ransomware attack, do not contact the cybercriminal, and do not pay the ransom.
- Instead, notify your manager and the MIS Support Team immediately. They will determine the best course of action.

Ransomware is often delivered by phishing messages; therefore, you must be vigilant when you receive unexpected emails and texts, and never click on links or open attachments.

Principles of Cybersecurity

Conclusion

By adopting the practices described, you contribute to the protection of our network.

Whether deliberate or accidental, a security incident can have long-lasting, negative impacts on our organization and its reputation.

As an employee, you have an important role to play.

By being prudent, you help protect our sensitive information against the threats posed by cybercriminals. Additionally, you reduce the risk of human error that could also result in a security incident.

Remember to immediately report any potential cybersecurity incidents.

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.