OPERATIONS DEPARTMENT – CYBERSECURITY TRAINING – JUNE 2021

When You Report, We Get Stronger – COVID-19 PAB

An important message from your security team regarding cybercrime and COVID-19

You heard the old phrase "*see something, say something*". Great advice, right? But how do you do it? That's where the phish alert button or PAB comes in (look for the "hook" icon in the toolbar of your email client)

Right now, cybercriminals are taking advantage of all the fear, disruption, and confusion surrounding COVID-19 and one of the biggest ways they are doing that is by sending phishing emails. You may already know to avoid these texts and messages when you spot them. But now more than ever it's super-important that you report these threats through the PAB. (Use the PAB to report suspected phishing attempts).

If you have any questions about the legitimacy of an email, report it. Even if it's just a gut feeling, use the PAB. Doing so give us a chance to investigate, defend the organization, and keep the bad guys out.

When you report, we get stronger. Remember: ***KEEP CALM AND DON'T CLICK***

Welcome to KnowBe4 - Cybersecurity Awareness Training of Texas

Can you recall receiving an email or text that just seems suspicious? Pay attention to those feelings because cybercrime is big business and a growing global concern.

Texas House Bill 3834 (86R) was created to require the state and local government employees as well as contract employees take mandatory cybersecurity training to help better protect Texas for these growing threats.

This course focuses on information security habits and procedures that protect information resources and teach best practices for detecting, assessing, reporting and addressing information security threats.

By the end of this course you will:

- Understand the principles of information security
- Have an awareness of information security threats
- Know best practices for safeguarding information
- Be able to properly identify, respond to, and report information security threats and suspicious activity

The content in this course includes portions of the following KnowBe4 training modules which have been selected to meet these state requirements: (1) Defining and Handling Sensitive Information; (2) 2020 Your Role: Internet Security and You.

Sensitive information is considered valuable because it's personal or proprietary information that shouldn't be publicly available because in the wrong hands it can cause serious harm to an individual or an organization.

Let's go ahead and explore five types of sensitive information.

1. ***Personal Information***, or PI, is defined as "information that can be used or distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information." Some PI by itself isn't necessary risky to have out there. For example, your name, the town you live in, and the type of car you drive, are all publicly available.

Other types of PI are sensitive and shouldn't be publicly available. Examples of these items include:

- Driver's License or other government issued ID number
- National identification number (for example, SSN in the U.S.)
- Passport Number

- Medical History
- Credit (or debit) card number and expiration date
- Bank and financial information
- Wage or Salary information

Additionally, some information is not identifiable by itself but can become identifiable when added to another piece of PI. For example: Racial or ethnic origin, Political affiliation/opinions, Religious or philosophical beliefs, Trade union membership, Genetic or biometric data, Wearable fitness tracker health data, Data related to sexual habits or sexual orientation.

Some other terms you may hear used interchangeably for this type of data are: Personal identifiable information (PII), Personal identity information (PII) and, Personal data (PD).

2. ***Protected Health Information***, or (PHI), is the recorded information about an individual's health, health care history, provider records, or payment for health care. Some examples include:

- Medical Records
- Health plan beneficiary number
- Private information about the patient, including date of birth
- National Identification Number (NIN)
- Social security Number (SSN)
- Biometric identifiers, including DNA as well as finger and voiceprints
- Full-face photographic images and other identifiable images

3. ***Merchants and entities that store, process, or transmit payment card information*** (PCI) must protect certain information according to regulations defined by an industry-wide security council.

Protected payment card data includes: Cardholder name, Card number, Expiration date, Card verification number, Personal identification number (PIN), Data from the magnetic strip on the back of the card, Data from the chip on the front of the card.

PCI standards apply globally and failure to comply with them can result in penalties and increased transaction costs for your organization

4. ***Controlled Unclassified Information***, or CUI, is a type of sensitive information specially related to the U.S. government. CUI is defined by Department of Defense (DoD) regulations and applies to any state, local, tribal, private sector, and foreign partner that uses DoD information.

The first step in understanding what makes something CUI is recognizing the difference between classified and controlled unclassified information.

Classified information is any information the U.S. government determines can harm national security if it gets into the wrong hands. For example, nuclear launch codes would be classified information.

Controlled Unclassified Information (CUI) is a step below classified information.

This information isn't a risk to national security, but its release could be harmful to individuals or organizations, so it must be protected. Examples include: Personal information, Financial information, IT security information, Law enforcement and court records, Patents and technical documents.

Generally speaking, proprietary information is information an organization wants to keep private and away from the general public. Examples include, but are not limited to:

- Non-public organizational information, including production methods and processes as well as trade secrets
- Passwords, user IDs, and internal network information
- Strategic plans or board decisions
- Confidential financial data
- Information that could hurt the organization, a coworker, or a customer if it were to be disclosed

This type of information is typically controlled through the use of Confidentiality agreements or Non-disclosure agreements (NDAs). Legal actions are possible for breaches of those contracts.

In a world where information is abundant, we must be careful with how we handle personal and sensitive information. Even a little information can go a long way. For example:

A hacker has someone's first name, last name, and social security number. Using online search engines and social media, they find a street address, date of birth, and other identifiable information. The hacker then combines all the information to begin opening credit cards under the individual's name and has them shipped to a different location.

Perhaps the hacker has acquired a first name, an email address, and knows what company the individual works at. They use that information to perform an attack and steal the victim's login credentials!

Now they have access to the organizations network and all of its proprietary information.

Remember, cyber criminals only need a little bit to cause a lot of damage.

5. ***Sensitive information.*** Working with sensitive information means protecting that information beyond what the law requires. The simple act of asking for access to someone's sensitive information carries with it the understanding – and the obligation – that you will do everything you can to keep private information private.

Without this trust, your customers, clients, consultants, and coworkers would not be willing to share their information. In turn, the operation and reputation of the organization will suffer.

In fact, when we talk about coworker information, that includes your own information. So, make it practice treating everyone's information with the same degree of care that you'd expect them to use with your information.

Some jobs require employees to handle or share sensitive information, others don't. But sometimes, you may have access to private information -such as an applicant's personal details (like current wage information or National Identification Number/Social Security Number) revealed on a job application.

A good rule of thumb is that if you don't need to handle sensitive information, don't -and alert your manager if you are given access to it unnecessarily.

Now that we have looked at some best practices for handling sensitive information, let's go over what to do if you have to share sensitive information with others.

Before you share any sensitive information -either with organizational personnel or with outside parties- be sure to ***stop, look, and think*** first.

This can help ensure that the sensitive information is kept private. Here is how:

First, ***stop*****.** Take a moment to consider what you're about to do.

Next, ***look*** at the information you're about to share. Does it contain some type of personal or sensitive information? Remember, improperly sharing this information can be illegal, cause security concerns, as well as harm your organization's reputation.

Finally, consider: what am I supposed to **think** about before I share sensitive information? When you are thinking about sharing sensitive information, ask yourself: Am I authorized to share this information? Is the other party authorized to receive it? Am I certain that they are who they say they are? Do we have appropriate confidentiality/non-disclosure

agreements (NDAs), contracts, and/or other legal protections in place? Have I taken all possible steps to keep this information safe?

And most importantly, make sure you are asking yourself, “Should I share this?” rather than, “Can I share this?” When in doubt, contact your supervisor or security team and ask.

Let’s take a few moments and explore why it is important that you are familiar with sensitive information and the best practices for protecting that information.

As an employee, YOU are a target. Hackers want to trick you into helping them harm your organization. What’s more, falling for an attack by these cybercriminals can damage you personally. All it takes is for you to make one mistake-like clicking on a link that then exposes the name, driver’s license number, date of birth, and bank account number of every employee hired by your organization in the past decade. Your organization would need to spend significant financial resources to remedy this single error -and your coworkers would spend months, maybe even years, battling personal identity theft. The security of your organization does have something to do with you. As you continue your training, pay attention to the common threats that you and your organization face daily. Learn the role you play in protecting your organization and yourself by discovering the things you should and should not do when the hacker targets you. Let’s begin by exploring some common strategies the bad guys like to use.

STRATEGY 1 - SOCIAL ENGINEERING is the art of manipulating, influencing, or deceiving you into taking some action that isn’t in your own best interest or in the best interest of your organization. The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network.

STRATEGY 2 - MALWARE stands for “malicious software,” an umbrella term for all the software out there that is being used by cybercriminals to spy on you and steal your information. Once your computer becomes infected, some malicious apps can log all your keystrokes, including your username and password. Some apps take over your computer and can even allow the hacker to turn on your webcam and spy on you or listen to your conversations.

One type of malware that’s in the news a lot is called *ransomware.* This type of malware can spread to all of the devices and files across a network and denies access until a ransom is paid. Ransomware scrambles the data in computer files and makes them unreadable. The hacker does this to force the organization to pay a ransom. Once paid, the organization will be sent a “key” that unlocks the computer files and returns them to the original state.

STRATEGY 3 - DISINFORMATION is false information created and distributed with the specific intention of manipulating you. Although this strategy is not a new one, it has become more common due to the reach of social media and the ease with which information can be spread via these networks. You and your organization can suffer financial or reputation damage as a result of a successful disinformation campaign.

An example of this was when a series of tweets and ads from Starbucks went viral. A “Dreamers Day” promotion was offering free beverages and discount for undocumented immigrants. This campaign was not a real promotion and was created by a group of anonymous individuals who wanted to harm the organization’s reputation.

One of the best ways to fight the spread of disinformation is to verify information’s truthfulness. Stop and fact-check before acting upon or sharing information.

STRATEGY 4 - PRETEXTING creates a fictional scenario where the bad actor pretends, they are someone else to gain your trust and get information from you. It can happen in person, on a phone call, through text or email.

For example, you get a call from someone saying they are from IT and work with Sam -who is someone you know. They say they need your username and password to verify a system update. Pretexting scenarios can be very convincing, and

these types of attacks are on the rise. It's important to never give information over the phone, in person, or online unless you have confirmed the identity of the person who is asking.

The methods used by cybercriminals to hack your device and break into your organization's network are referred to as the *threat landscape.* Today's threat landscape is extensive and getting bigger every day.

Whatever device you are using in the office or working remotely, hackers might be trying to use one of the following types of attacks on you. Knowing what they are helps ensure you don't let criminals in. As you learn more, you will be given brief knowledge checks along the way.

ATTACK 1 - PHISHING is the most common digital attack. Phishing is the process in which bad guys try to trick you into giving out sensitive information or taking a potentially dangerous action, like clicking on a link or downloading an infected attachment. They do this, using emails disguised as contacts or organizations you trust, so that you react without thinking first.

For example, you receive an email that looks like it's coming from your IT department, telling you that there's a problem with your email account and you need to reset your password. You are asked to click the link in the email. The link takes you to a password reset page with a password field, which is what the hacker is after. Once he has your password, he can gain entry into your account. He'll use this to access your computer and tunnel into your organization's network.

ATTACK 2 - SPEAR PHISHING is a small, focused attack via email on a particular person or organization. The goal is to penetrate your organization's defenses. In this attack the criminals invest time researching a specific target using social media and other open sources of information. Armed with this information, they send you a personalized message designed to trick you into taking an action that will put your organization at risk. Spear phishing attacks can be convincing, but just like in any phishing attack, you must take an action for it to be effective.

One very common form of spear phishing targets top management typically people who interact with your organization's CEO. A hacker impersonates your CEO and emails you with instructions to do something that could harm the organization. This tactic is called CEO fraud and is growing in popularity. It can even happen via phone with a fake voice message!

ATTACK 3 - SMISHING stands for "Short Message Service (SMS) phishing" or phishing that occurs through text messaging. For example, they send a text message asking you to call a number or click on a link. The message could look like it's from your bank and may even contain most, or all, of your account number, data usually obtained illegally by hackers. Even if the message you are reading contains your password or your account number, it can still be fraudulent.

Some cyber-attacks don't start with an email and can succeed without requesting you to knowingly take a specific action.

ATTACK 1 - WEBSITES. Any website is potentially dangerous, but some are more dangerous than others: gambling and sexually explicit sites and those that offer free downloads, to name a few. But reputable, high-traffic sites can also become infected with malicious advertising, and you don't even need to click on the ad for your computer to be compromised. This malware can infect your workstation just by landing on a web page. This is called a drive-by download. Consult your IT department or your organization's security policy on how to avoid this kind of attack. Never connect to public Wi-Fi unless you are using a VPN or Virtual Private Network. This technology creates a safe internet connection that shields your online activity from the bad guys. Be aware of your surroundings, and always use VPN when connecting to public Wi-Fi.

ATTACK 2 - SOCIAL MEDIA SHARING. One of the biggest threats from social media is the abundance of shared information that can be used by social engineers to trick you or your coworker. Travel plans are an obvious example of information that you should never share online. Announcing that you won't be home is never a good idea. But there are less obvious pieces of information that can put you and your organization at risk. Any type of sensitive information is like gold to hackers. Think about it from the perspective of a social engineer. Will the information you are about to post be useful in conning you or your co-worker? Make sure you understand your organization's policy regarding sharing information on social media.

ATTACK 3 - FAKE PROFILES. Another effective trick that criminals use is to create a profile with a bunch of real or fake connections that all look very convincing. For instance, the profile could appear to be a headhunter who wants to talk to you about a career move, a potential romantic interest, or someone in your industry who wants you to speak at an upcoming conference. But fake profiles are growing trend throughout social media and are designed to trick you. So, take a close look at any requests that you receive. Some common aspects of a fake profile include model-quality or celebrity look-alike profile photos, an incomplete or generic profile, poor spelling and/or grammar, or a suspicious work history. Fake profiles will often lead you on for a while and then send you a link to click on in the message that seems to make sense tin the context of the conversation. But this link leads to a site that is able to infect your device with malware. Now the hacker can begin to tunnel into your organization's network.

Cyber-attacks can also be set into motion in-person or with a simple phone call.

ATTACK 1 - TAILGATING. A classic example is tailgating. This is where the hacker scouts an area like the outside section at your company and then joins your group, participating in your group's conversation. When your group returns to work, he follows you in just like any other employee and then finds a workstation he can hack and infiltrates your company's network.

ATTACK 2 - One highly effective **PHYSICAL ATTACK** entirely relies on human curiosity. Hackers typically use flash drives to deliver malware that will infect your device. Attackers leave a flash drive that says "Payroll" where it can be easily found, like in your office parking lot, the lobby of your building, or a restroom. Or they could send you an envelope via postal mail with a flash drive inside that looks like it comes from a customer or a vendor. Once someone gets curious enough to plug that flash drive into their computer, that computer is then "owned" by the bad guys and the organization's network can be compromised.

ATTACK 3 - VISHING. Another name for phone-based social engineering is voice phishing or "vishing." Like phishing, vishing is when the hacker calls you and tries to con you into a surrendering confidential information. For example, a hacker calls you with a pre-recorded message that is supposed to be from a customer support rep from your bank. He says that there's a problem with your account and asks you to call a fake customer support number to clear things up. The support rep is part of the con. She will ask for personally identifiable information (PII) like your credit card info, PIN or other sensitive details. Once she has this information, she can access your account and steal your identity and money.

There's no getting around it -you are the last line of defense for your organization. Understanding your role in safeguarding your organization's sensitive information is a critical first step towards making informed decisions and helping your organization manage to ongoing problem of cybersecurity threats. Remember, it only takes one mistake to expose all the valuable sensitive information that you are responsible for. This is why it is extremely important to always **stop, look** and **think** before taking any sort of action, including clicking on a link, opening anything you receive, or sharing sensitive information. And remember, if something seems suspicious, take the time to verify it's a legitimate request with your supervisor, the security team, or someone responsible for information security at your organization before you act.

Thank you for completing the training!