Security Awareness 2024

Introduction

Cybersecurity attacks persists in major headline news every week. Why are there so many cyber-attacks? Part of the answer is that information technology (IT) is a critical infrastructure that is targeted for attack because it supports how people work, shop, and live life. Every facet of our lives is driven by IT. The work we do to serve the public is reliant upon our ability to safely use the systems, devices, and data entrusted to us.

Course Goals

This is an awareness level cybersecurity course. Consider this course the equivalent of learning to navigate the seas for beginners. You are learning basic cybersecurity rules of navigation and security. Just because you have a boat (computer), sails (Wi-Fi) and an open sea (Internet), you are not automatically a safe and experienced seafarer. The goals of this course are to:

- Help you navigate the safe use of your devices, systems, and data entrusted to you.
- Inform you of proper reporting protocol.
- Give an overview of information types and the rules and regulations that govern them.
- Give practical advice on recognizing social engineering.

The "Threat Landscape"

Threat Landscape is a common phrase describing the dangers lurking in the information technology world. Just like sea travel has dangerous elements that you must be on the lookout for, the cybersecurity threat landscape has threats that exploit possible weaknesses that cause harm, damage, or destruction. Weaknesses can be found in systems, codes, processes, procedures, and even human behavior. There is a lot of information available on the true meaning of terms such as risk, asset, threat, vulnerability, and threat actor. However, the approach for this course is to keep it simple so try to not get up hung up on semantics and technical/legal jargon.

What is lurking in the depths?

A lot!

This security awareness course helps users to identify just a few of the important hazards, including suggestions on how to avoid those hazards while working for a large organization like state government and even apply them to your own personal cyberspace adventures.

Remember - government networks, systems, assets, and data are irresistible for Cyber Pirates.

Ransomware

Ransomware is a type of malware that denies access to data until a ransom is paid. If the ransom is not paid, the data is permanently deleted or made public. This is the equivalent of pirates overtaking your ship and forcing you to walk the plank unless you pay.

Which one of these outcomes depends upon what the "pirate" thinks would motivate the victim to pay the ransom more: loss of data or exposure of data?

What can you do at work? The best defense against ransomware is prevention. In terms of being a State of Illinois employee, contractor, or vendor, you need to understand that while using work resources, the most common way a computer is infected by ransomware is through social engineering. This training will discuss how to be on the lookout for phishing emails, suspicious websites, and other scams.

Ransomware in your personal life

What to consider in your personal life? Understand that your personal devices can become infected the same way your work devices can. Social engineering is generally the culprit but visiting malicious websites or downloading malicious content are also factors. Do you have anti malware or anti virus software on your computer at home? You likely do not have a maritime crew of security or tech team at your house so you are responsible for maintaining your own offline backups of photos, information, and systems.

You will want to create secure backups of your data on a regular basis. You can purchase dedicated USBs or an external hard drive for saving new or updated files. Additionally, you can utilize cloud storage services/solutions. Just be sure to physically disconnect the devices from your computer after backing up your files. Otherwise, your backup devices can be infected with ransomware as well.

Social Engineering (Loose Lips Sink Ships)

Simply put, social engineering is the art of tricking people into divulging personal information or other confidential data. Social Engineering is a broad term that covers malicious

emails, texts, or calls (also known as phishing, smishing and vishing).

This is where YOU become the weakest link in your organization's security perimeter, as the malicious user is trying to use you to open the hatch to access the "galley and cabin" of your organization. You are a target at home and at work.

- Social engineering attacks are more common and more successful than computer hacking attacks.
- Unlike hacking, social engineering relies more on trickery and psychological manipulation.

Social Engineering -What can you do?

At Work - Be on the lookout for suspicious looking emails. If in doubt, submit using the Phish Alert Button (PAB) or forward to security. The preferred method is PAB. The faster you report a suspicious email using PAB, the faster it can be stopped across the entire organization. For those familiar with the flair guns, using the PAB, is the equivalent to firing a flare gun straight up in the air to alert a response team. Reports using PAB immediately notify the security operation center and kicks off an investigation.

Personal life and devices - Since you most likely do not have an automated reporting tool at home or a security division, you need to simply delete suspicious emails.

Administrative Rights: If you are tasked with assigning administrative rights. In your personal life or at work, follow a practice of "access of least privilege". This means you assign accounts the least amount of access required to accomplish tasks. For work, that means ensuring that people aren't given elevated privileges if they don't need it for their job and if they do require it, give the absolute minimum required. At home, don't use an administrative account as a daily use account and ensure a password is properly set on the administrative account.

An employee with approved elevated technical rights/privileges, who is found to have abused or misused their elevated rights/privileges, may have their elevated rights/privileges suspended and/or terminated. Additionally, an employee may be subject to disciplinary action, up to including discharge.

Remember If in doubt...throw it out.

Sam is assisting their CIO with a sensitive document, there are several users that are collaborating on this project and Sam has been instructed to share access to the document following the principal of least access. What is the best way for Sam to allow collaboration without compromising integrity of the systems and information?

- A. Sam knows that everyone in the office is trustworthy and might have good input for the CIO. Sam gives the entire office Read/Write Access to the document.

- A is not the best answer. Sam would have no way of knowing if someone would misuse the data. It also does not follow the "access of least privilege" principle.

◦ B. Sam understands that collaboration is key to the success of their organization, but that too many hands in the pot can make messes. Sam grants Read only access with the ability to leave comments and recommend changes that can be reviewed and approved by Sam or the CIO.

- Correct: B! This allows the collaborators to provide input in a controlled method. The final approval is controlled while also limiting access to the fewest people with the least access required to collaborate!

◦ C. Sam is highly suspicious of peers in the office and trusts no one. Sam doesn't grant anyone besides themselves any access to the document and all requests and collaboration must be sent via email for Sam to consider.

- C is not the best answer. Sam is funneling everything through themselves and their CIO, which means suggestions and collaboration will be greatly reduced and result in delays in completing tasks in a timely manner.

---

10 Black Flags of Phishing Emails

Phishing is one of the most common attack methods used by cyber criminals. Fortunately, there frequently are signs to help determine if the email is a scam. This list is a good reference for both your work and personal life. (KnowBe4, 2023) Please scroll through the entire list. The scroll bar is on the right hand side of the screen.

Clue	Explanation
Asking for Personal Information	Most reputable organizations will never email you asking for your address, phone number, ID number, or other personal data. Same for username and password.
Inconsistencies in Links	Always hover over links with your mouse pointer to display the full URL. If it leads somewhere that doesn't logically belong within the context of the email, or generally looks nonsensical, don't click!
Unrealistic Threats	Phishing emails often feature threatening language, such as "Payment overdue!" or "Your account has been compromised!", to generate a response from their targets.
Generic Greetings	Unlike legitimate entities that will address you by your full name or username, phishing emails usually opt for generic greetings, such as Dear Customer or Dear Sir/Madam.
A Sense of Urgency	Like unrealistic threats, emails that urge you to click on a link or download an attachment or update your account immediately are likely scams.
You're Asked to Send Money	Like unrealistic threats, emails that urge you to click on a link or download an attachment or update your account immediately are likely scams.
Too Good to Be True	The old saying remains true to this day: if it's too good to be true, it's likely untrue. Keep that in mind any time you get an email claiming you won the lottery or are due a large family inheritance. (Tend to see this more in personal email accounts)
Poor Spelling & Grammar	Most generic phishing attempts contain spelling and grammar errors or feature awkward wording/phrasing.

Clue	Explanation
Suspicious Attachments	Attachments aren't always malicious but use extreme caution whenever you receive them unexpectedly. This is a serious concern for your work account. These attachments could be the source of malware.
From a Government Agency	In almost every case, government agencies don't use email to communicate anything of consequence. The IRS, for example, will never email or text you about your taxes or payments.

Phishing Black Flags

Read the sample email below. Try to spot potential flags or warning signs to the receiver (KnowBe4, 2023). The next slide will focus on different ways to look for flags in emails. Flag = something that should trigger suspicion.

From: [External]hr@outsideorganization.znet

To: Sam@yourorganization.net

Date: Tuesday, December 3:00 AM

Subject: Survay

Hi Sam, Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. These must have be completed by the end of the day. Click here to take the [Survay] or download the attachment. Thanks in advance for your cooperation!

Flag - Sender

These are things you should be asking yourself or thinking about when reviewing emails.

- I don't recognize the sender's email address as someone I ordinarily communicate with.

Flag - To and Date

These are things you should be asking yourself or thinking about when reviewing emails.

- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.

Flag - Subject and Attachments

These are things you should be asking yourself or thinking about when reviewing emails.

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)

Flag - Hyperlinks

These are things you should be asking yourself or thinking about when reviewing emails.

- I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website. (This is a huge flag.)

Flag - Content

These are things you should be asking yourself or thinking about when reviewing emails.

- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?

What to do when you see a black flag or a suspicious email?

Always report! Reporting is easier than ever. The preferred reporting procedure is to use the Phish Alert Button in your Illinois.gov Outlook account.

1. Submit to **Phish Alert button** (PAB)
2. If you can't find the Phish Alert button, simply forward to DoIT.Security@illinois.gov
3. If you have given up your username and password, then in addition to the above, please contact the Help Desk.

Help Desk contact information:

Springfield: 217-524-DoIT

Chicago: 312-814-DoIT

DoIT.HelpDesk@illinois.gov

Why is using the Phish Alert Button important?

When you submit via Phish Alert, you receive a notification acknowledging your submittal. Later, you will receive an automated email with details on your submittal. Because of the behind the scenes analytics, the Security team is able to report if the submittal is:

- Clean email/legitimate
- Possible threat and needs more investigation
- A malicious email
- Spam
- Part of an automated pro-active phishing training campaign.

If you bypass the Phish Alert tool, then it takes more time to evaluate the suspicious email.

Knowledge Check

An agency executive receives a suspected phishing email. What is the best course of action for that executive to take?

- A. Call the Help Desk
  - A is a good answer but not the best answer. The Help Desk will advise you to submit to Phish Alert.
- B. Contact the head of security immediately via call or email
  - B is not the best answer. While contacting the head of security or the agency CIO might feel natural to the executive, it allows for the spread of the email within the network. That CIO or head of security doesn't always see their email in a timely manner. It could be hours versus seconds for them to loop in the Security Operation Center.
- C. Forward to DoIT.Security and cc: others
  - C is a good answer but not the best answer. It does not allow for the quickest response possible.
- D. Click on the Phish Alert button to submit
  - Correct: D! This is the fastest course of action for a suspicious email to be evaluated. Even though that official is a high value target, if the email is found to be malicious, the analysts can quickly take action to scan the network for instances of this email. Remember, the Phish Alert button is a direct link to the Security Operation Center.

Knowledge Check

Sam received an email from a group they sometimes do business with. After clicking on the invoice, Sam is prompted to enter their username and password. After doing so, Sam is confused about the invoice as it does not seem relevant to their job. What is their BEST course of action?

- A. Sam should only report the email using the Phish Alert Button (PAB)
  - A is not the best answer. There is a better answer. While submission using the Phish Alert Button will take report of the spread of the potentially malicious email, it does not address the incident of the user's account being compromised.
- B. Sam should only call the Help Desk
  - B is not the best answer. There is a better answer. Calling the help desk enables the user to report an incident and change their username and password. The incident report goes to the operation center for the team to look at your account and make sure no malicious actions has been taken against your account using your compromised credentials. If they don't report the potentially malicious email, it could be received by more users and take longer to notify the security team. These are separate but equally important actions.
- C. Sam should only call his supervisor

- C is not the best answer. While they can alert their supervisor so they can keep an eye open for suspicious emails from the compromised account. This answer does not address the issue of alerting the security team OR create an incident to resolve the account being compromised.

◦ D. Sam should submit the email to Phish Alert and call the help desk

- Correct: D! Sam potentially gave up their username and password. They should both contact the Help Desk and submit to Phish Alert. Submitting to Phish Alert will allow the analysts to immediately review the email and threat, but this alone does not tell the Security Operation center about the compromised credentials. Calling the Help Desk will allow for immediate password reset and initiate an account investigation. Cover your bases and do both.

Categories of Threats

Think about the threat categories below as possible launch ramps for potential cybersecurity breaches, incidents, and disasters.

1. **Natural Threats** - Disasters such as tornados, hurricanes, floods, and electrical storms.
2. **Malicious Outsiders** - Foreign Nations, criminal groups, hackers, spammers, industrial spies, etc.
3. **Malicious Insiders** - Disgruntled employees or vendors, spies, activists, unhappy customers, etc.
4. **Accidental Insiders** - Any employee or other person with access to your information or information systems.
5. **Non-Malicious Insiders** - Any employee who intentionally breaks policy but without the intent to cause harm.

What is an Insider Threat?

An insider threat could be someone who works for or who has authorized access to an organization's networks, systems, or data. These individuals can use their access either maliciously or unintentionally in a way that could negatively affect the organization.

A key takeaway of this course is that a person does not need to have malicious intent to pose as an insider threat. Accidents happen, and they can be costly in terms of money and loss of reputation.

Types of Insider Threats

People commonly categorize insider threats as either 'malicious' or 'accidental', but a third category has emerged in recent years. Non-malicious insider threat was added about three years ago to the list. It seems the same as an accidental insider but there is a subtle difference.

- Malicious insider threat
- Accidental insider threat
- Non-malicious insider threat

Malicious Insider Threat

Just as it sounds, the malicious insider threat is defined by the intent of the individual to harm the organization or expose data. Some examples of malicious actions include:

- Intellectual Property theft
- IT sabotage
- Fraud
- Espionage

Accidental Insider Threat

Where a malicious insider has the intent to harm or cause exposure of sensitive information, the accidental insider threat is defined by a "failure in human performance" according to US-CERT. This is a nice way of saying that human error is involved in causing harm to the organization. A classic example is when an employee falls for a phishing attack and clicks on a suspicious link in an email. (aka "Social Engineering" covered earlier in the course)

The human factor is a major reason phishing attacks are still so prevalent - they often work.

Examples of Accidental Insider Threats

Common examples of accidental insider threats include:

- Accidental disclosure of information, such as sending sensitive data to the wrong email address
- Physical data release, such as losing paper records
- Portable equipment loss, which includes not only losing laptops, but portable storage devices as well

Cyber training programs increase employee awareness and provide practice recognizing social engineering. This is often achieved through the following:

- Proactive Phishing campaigns
- Policy reviews
- Awareness training

The Non-Malicious Insider Threat

The non-malicious insider sounds just like accidental insider, but it is slightly different. A non-malicious insider threat is an individual who intentionally breaks policies, but without the intent to do the organization harm. The difference between a malicious insider and non-malicious insider is the intent. One wants to harm it or cause information to be leaked (malicious) and the other does not (non-malicious). The main difference between an accidental insider and non-malicious is the intent to break organizational rules, which put the organization at risk.

Knowledge Check

Sam works for a large state agency. They are trying to finish an annual report and want better fonts to make it look more creative. They download a free font program from the internet, even though it was against policy to do so. The next day, they run into some computer issues and encounter a black screen. Later, it is discovered they downloaded a malicious file which compromised the computer and network. The computer had to be completely wiped and re-imaged along with several other computers at the agency.

What type of threat category did this scenario BEST represent?

- A. Malicious Outsider
  - A is not the best answer. There is a better answer. Their intent was not malicious, and they are not an outsider.
- B. Accidental Insider
  - B is not the best answer. There is a better answer. Their intent was not malicious, and they were not accidental
- C. Non-Malicious Insider
  - Correct: C! This is the best answer as they were installing unapproved software on their work computer, which is against policy. While they did not intend to cause harm, they knowingly circumvented policy.
- D. Malicious Insider
  - D is not the best answer. There is a better answer. Their intent was NOT malicious.

Knowledge Check

Sam works for small state agency. They received an email from the IT Department asking them to click on a link and verify their

username and password. Sam quickly responded and provided the information. What most likely just occurred?

- A. The IT department was doing an annual check of credentials.
  - A is not the best answer. There is a better answer. An IT department would not need to ask your username and password. Users update their own username and passwords. If help is needed, IT can reset a username and password without needing that information from the user.
- B. A malicious outsider has stolen the credential of an accidental insider.
  - Correct: B! This is the best answer because they accidentally fell for phishing email which could allow a malicious outsider to harvest their credentials to use later. They did not circumvent policy knowingly. They were tricked.
- C. A malicious insider has introduced malware into the system
  - C is not the best answer. There is a better answer. Nothing in this scenario indicates that they had malicious intent.
- D. A malicious outsider has stolen the credentials of a non-malicious insider.
  - D is not the best answer. There is a better answer. They did not intentionally circumvent a policy or rule.

Physical Security

Physical security might make you re-think what you consider "polite" office etiquette. What does that mean? Here are some examples:

- Holding the door for someone seems to be polite, but security means they need to use their badge for proper access.
- Closely related to holding the door, is tailgating. This is when someone comes in the door right behind you and does not badge in. You need to call their attention to it or report to building security.
- Shoulder surfing is sometimes necessary when collaborating, but you can still ask for privacy when entering passwords and logins.
- Don't be afraid to ask for identification (i.e., an employee ID or a visitor's badge) or to report anyone who appears to be somewhere they should not be.

Securing your Workstation

Securing your workstation is an important component of physical security and is often overlooked. It is easy to become too comfortable or even complacent at our workstations. Below are just a few of the reasons why you should keep your workstation locked when you are not present:

- Laws and policies require the safeguarding of sensitive data. These include but are not limited to requirements pertaining to Personally Identifying Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), and Criminal History Information. In some cases, there may be penalties for not following proper handling protocols.
- Confidential information could be leaked or stolen.

When you leave your workstation, you need to LOCK it. This can be done different ways.

1. Press CTRL/ALT/Delete and then selecting "Lock"
2. Hit the Windows key + the "L" key
3. Open the windows menu, selecting your user profile, clicking "Lock"

The Clean Desk Concept

- Maintain a "clean desk" and keep your workspace secured by locking up any sensitive files and information.
- Don't leave documents unattended on the printer, copier, or in other areas.
- Remove papers and clean white boards when finished using conference rooms.
- Lock desks and filing cabinets when you leave.
- Shred or otherwise destroy sensitive documents when discarding them.

Security Quick Tips

The following tips help you navigate technology and cyberspace faster and safer. Help yourself by:

- **Using the Phish Alert button (PAB)** - While easy to use for reporting, you also receive feedback when you submit. You will get an automated email from security letting you know whether the email was safe, spam, malicious, or proactive phishing. This helps you spot phishing in your personal life.
- **Updating your devices and software helps plug security flaws** - Using devices or software that is not kept up to date is equivalent to never changing the oil, adding wiper fluid, or checking the gas level in your car. It is not "if" your car quits working, but "when" your car quits working without proper maintenance. Same principle applies to updates. Keep your devices and software updated.

Security Quick Tips, continued

- *** Recognizing legitimate IT notices -** How does your agency notify you that your password is expiring? If DoIT is your IT service provider, it looks like the picture to the right. You will receive an email notification of your upcoming password expiration. You will also notice in the lower right hand of your screen, a message that pops up to give you a countdown on how many days until your password expires. Know how to reset your own password and do it in a TIMELY manner. If you know what the legitimate reminder looks like, you will be less likely to fall for scams. You are given multiple reminders.

Security Quick Tips, continued

- **Being Wi-Fi smart** - Do not auto-connect to open Wi-Fi networks, like those available at stores, restaurants, hotels, or airports. For security purposes, it is better to use data than unsecured Wi-Fi. On your personal phone, NEVER log into banking or other secure accounts when using public Wi-Fi network.
- **Being proactive versus reactive** - Think about creating a folder in Outlook dedicated to communications from IT. (Department of Innovation and Technology or other IT related messaging) File emails from these trusted senders in that folder. Why? Because now you have a reference of what legitimate messages from your IT department look like. Also, when large changes are being made to your programs, software, or other significant IT changes, you are generally sent a notice or directions ahead of time. If you file it, you can refer back to it when you have questions.
- **Stopping giving up your credentials** - The Help Desk staff have elevated privileges and can access your account without needing your password. This is the same for your personal life. Amazon does not need you to verify your account credentials in an email. They don't need your account credentials to help you. Only you need them. Consider any other requests for your username and password to be malicious.

Knowledge Check

Sam works in an office where they must scan their badge before entering the building. It is the start of the workday, so there are a lot of people coming into the building. As Sam is starting to badge into the office, a person they vaguely recognize is coming to the door with their arms filled with boxes. If Sam is wanting to be polite AND follow security procedures, what is their BEST course of action?

- A. Sam should badge in and hold the door open for the person.
  - A is not the best answer. There is a better answer. While it is certainly polite to hold the door for someone, everyone must scan their badge before entering.
- B. Sam can just ignore the person and enter the building without helping them.
  - B is not the best answer. There is a better answer. While this is an option, the question is asking what the best course of action is to be polite AND secure.

- C. Sam tells the person that after they scan their badge, they will hold the door for them.
  - Correct: C! This is the best answer for being polite AND secure. Everyone must badge in so the fact that Sam waits until the person badges in and then hold the door open for them is the best course of action.
- D. Sam should pretend they left their badge in the car and run back to get it to avoid potentially awkward social interaction.
  - D is not the best answer. There is a better answer. The person trying to access the building WHILE Sam is trying to be polite AND secure. It isn't polite to fake an excuse to get out of an activity they would have otherwise done.

Scenario

Sam receives an email with the following message:

Your Outlook Web Access Domain Password expires in less than 24 hours. You can change the password using the self-service password reset website. The link is below:

Self-Service Password Reset Page

Your new password will need to meet password complexity requirements:

- at least 8 characters long and cannot contain your name
- it must contain at least one uppercase and one lower case character and a number

If you have any questions or need further assistance, please click the link above and click the Help button. Please DO NOT reply to this email. It is not a monitored account.

Source: Email Security Team

Knowledge Check

Based on the previous scenario, what is the best course of action for Sam?

- A. Click the link and reset their password before they lose access to their accounts and must call the Help Desk.
  - A is not the best answer. There is a better answer. The statement "less than 24 hours" implies a sense of urgency. If this is the first Sam has heard about this, then it is most likely fake.
- B. Sam should delete the email.
  - B is not the best answer. There is a better answer. If Sam had received this email at home, this would be the best course of action. At work, they should submit using the Phish Alert Button (PAB).
- C. Sam thinks this is a scam and is irritated. They reply to the sender and tells them they are wasting time and they were not fooled. Then they delete the message.

- C is not the best answer. There is a better answer. While not giving up their username and password, they have just indicated to the malicious outsider that their account is susceptible to interacting with would be phishing campaigns.

◦ D. Sam clicks on the Phish Alert button.

- Correct: D! Sam is suspicious because this is not how they have historically received password expiration notices. Bonus: the alleged "urgency" of the email was a flag.

Machine Learning and AI

Some popular terms have popped up over the course of the past year and you may have heard or read terms such as "AI Driven" or "Artificial Intelligence" in regards to digital products. This topic is hotly debated for various reasons but for this course we want you to realize that in most consumer cases these are just buzz words meant to make the latest product seem "cutting edge". It would be more accurate to call these products generative software (e.g. Generative Writing, Generative Art, Generative Music) vs "AI writing, art, and music". It's not creating new content, it's taking information collected from a database, in many cases the world wide web, and producing an output that it thinks someone is requesting. It doesn't validate information for accuracy. If you use any "AI tools" check that it's what you want, that it's not copyrighted material, and that it's accurate before using it (especially in a professional setting). Because these tools are becoming more ubiquitous, attackers are able to use these tools to create convincing messages, videos, and audio recordings that sound like they may be from a trusted person. Always think before you click and follow proper reporting protocol!

Usernames and Passwords

It is no secret that sales of usernames and passwords occur every day on the dark seas. The best advice regarding credentials is:

- Use a strong password- Current authoritative sources believe that a longer password with complexity is best but this is a hotly contested topic. Variables that help determine what is a good password include: system type, data, organization, compensating security controls, etc.
- Do not share your passwords with anyone- Again, a help desk does not need your password. They have other means to help you restore your account.
- Use Multifactor Authentication (MFA)- This strengthens the security of accounts should credentials be compromised.
- Do not store your password in written form.

MFA - the New Normal

By now everyone should be familiar with multifactor authentication (MFA). MFA is a method to prove who you say are by two or more factors. Those factors can be:

1. Something you know - like a username and password
2. Something you have - like a code or notification sent to a device you have
3. Something you are - like a fingerprint or face scan

State employees currently use MFA to log into Office 365 when not on a state network. Pretty soon, it will be standard procedure in more places. If you have not made the choice to enable MFA on your personal accounts, you should. While you may see it as an inconvenience, it is even more inconvenient to lose your identity, money, or your reputation.

Be Shore To Be Safe!

Everyone has seen a sharp rise in suspicious emails, texts, and calls. It cannot be stressed enough to be on guard.

If you receive an e-mail or text asking you to update your information or check a delivery status, your safest course of action is to go to the actual site associated with your account directly instead of clicking the link in the e-mail or text. This is equally true at work and in your personal life. You are more likely to see these events more in your personal life as you only have limited number of accounts for work AND a security team to actively intercept threats.

Think about it...

How often do you get emails that look to be from Amazon, PayPal, and other vendors that say your account needs updating or there is suspicious activity, and you need to click "here" to remedy?

These events occur daily. The hardest time of year is near the holidays when you are legitimately ordering more online and are receiving numerous delivery notices. It also makes sense with the added activity on your bank cards, you are more likely to get suspicious activity notices from banks and credit cards. Do not react in haste. No need to click the link, simply go to the actual website to check your order status or call the number on the back of your bank cards if you get a suspicious activity text, call, or email. Be proactive versus reactive.

Moral of the story?

1. If it seems off, report it! **Phish Alert Button (PAB)** is your reporting mechanism for emails. Everything else security related, contact **DoIT.Security@illinois.gov**
2. Slow down and think before you click or enter your credentials. If you think you clicked or gave your credentials in error, report it! It cannot hurt you to just be safe.
3. The faster something is reported to security, the faster it can be mitigated.
4. On your personal accounts at home, if in doubt - DELETE IT!

Information - Concepts, Rules, and Types

Frequently the following sections tend to get skipped over and clicked through. Please put your **public servant hat** on and read through the next several sections carefully and think about how it could be relevant to your work at the state. Then re-read the sections as a **private citizen**.

You are both a public servant and someone who interacts with the state in your personal life. Think about the duties you have in protecting information given to you while serving the public as well as how you would want your own information handled by public servants. The next sections are focused on information types and some rules and concepts that govern the handling of different types of information.

Privacy

Privacy is a set of fair information practices to ensure:

- personal information is accurate, relevant, and current;
- all collections, uses, and disclosures of personal information are known and appropriate; and,
- personal information is protected.

In the State of Illinois, we remain committed to protecting the privacy of our clients and staff as stated in our privacy policy and the Personal Information Act (815 ILCS 530). Rules and regulations regarding Privacy were developed to give people rights to control, manage, access, or even delete information about them that is collected and used by certain organizations.

The Illinois Identity Protection Act

The Identity Protection Act (IPA) requires each local and State government agency to draft, approve, and implement an

Identity Protection Policy to ensure the confidentiality and integrity of the Social Security numbers (SSNs) agencies collect, maintain, and use. Remember:

- Confidentiality refers to the concept of preventing unauthorized access.
- Integrity is the concept of protecting the reliability and correctness of the data.

The Illinois Identity Protection Act continued...

Agency, employees, and contractors shall NOT:

- Publicly post or publicly display in any manner an individual's SSN;
- Print an individual's SSN on any card required for the individual to access products or services;
- Print an individual's SSN on any materials that are mailed to the individual;
- Use, or disclose a SSN from an individual, unless: required to do so by state or federal law, or there is a documented need;
- Require an individual to use his or her SSN to access an Internet website;
- Use the SSN for any purpose other than the purpose for which it was collected.

Agency, employees, and contractors SHALL:

- Redact SSNs from the publicly accessible information or documents before allowing the public inspection or copying of the information or documents;
- Ensure only employees who are required to use or handle information or documents that contain SSNs will have access.

The Identity Protection Act Exceptions:

- Disclosure to another governmental entity if necessary, to perform their duties.
- The disclosure of Social Security numbers pursuant to a court order, warrant, or subpoena.
- The collection, use, or disclosure of Social Security numbers in order to ensure the safety of State and local government employees.
- The collection, use, or disclosure of Social Security numbers for internal verification or administrative purposes.
- The disclosure of Social Security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.
- The collection or use of Social Security numbers to investigate or prevent fraud to conduct background checks, to collect a debt, or to obtain a credit report.

Social Security Administration

The Social Security Administration (SSA) requires each employee, contractor, or agent who views SSA-provided information to understand there are potential criminal and administrative sanctions or penalties for unlawful disclosure of SSA provided information and the potential for criminal and/or civil sanctions or penalties associated with misuse or unauthorized disclosure of SSA-provided information.

Did you ever wonder?

Did you ever wonder why you receive numerous papers in your insurance statements or bank statements that tell you about their privacy policy? (Hint: It tends to be the "extra" papers in your statement you disregard and throw away)

This is because there are stiff penalties for not informing customers what information is being collected, how it is being used, and how it is being secured.

Regulation Requirements and Penalties

There are numerous other legislative requirements beside the Illinois Identity Protection Act and the Social Security Administration when it comes to regulated data type and privacy. In general, the requirements of these laws provide that the regulated organizations comply with the following:

- Inform their customers of their privacy policy.
- It is important that the organization provide their customers a copy of their privacy policy. Although the details and internal procedures of the policy do not necessarily need to be communicated, it is important that they convey the general nature and outline of the policy and how it affects the customer.
- Report to the customer what information is collected and how it is collected. Customers have the right to know what information is collected about them and the methods used to collect it. Collecting information is done in many different ways. The customer provides much information through forms, interviews, documentation provided for service, inquiries, and other communications. Information is also often collected from other organizations providing things such as credit reports, medical record transfers, or inquiries on the customer's behalf. It is also a common practice for some organizations to purchase customer information for purposes such as marketing. Most of this latter information is usually public information but should be protected, nonetheless.

Regulation Requirements and Penalties continued...

- Store, manage, and /or transmit the information in a secure manner.
- Being custodian to customer information also bears the responsibility of maintaining it securely. The organization must comply with using, storing and transmitting the information in a secure manner. Security policies and user training such as this tutorial are a key to the success of compliance with this requirement. Some legislation may even

go as far as defining the minimum levels of encryption to be used for storage or transmission of information.

- Maintain accurate and up to date information.
- The information that is maintained should be accurate and up to date. This can be very important in different industries such as healthcare and financial services. Medical treatments or financial decisions may be based on some of this information.
- Inform their customers how the information will be used.
- Most organizations collect information about their customers for specific purposes. It is important to the customer relationship that the organization communicates to the customer how they will use any information related to them. This includes providing services to the customer, marketing to them, sharing the information with affiliated or non-affiliated entities, and more.

Regulation Requirements and Penalties continued...

- Report to their customers with whom the information might be shared and why a customer should be informed of any potential situations that may lead to the sharing of their information. They should be told what information may be shared and what their options are for controlling this process. This might include consent, non-consent, or authorization on a situational basis.
- Inform their customers how to access the information maintained about them. Customers must be told how to access the information maintained about them. They should also be told how to request corrections to factual errors about them.
- Communicate the rights provided for the customer.
- Customers should be informed of the rights provided to them relating to the information an organization maintains about them.
- Many of these acts provide for sizable financial penalties to organizations that do not comply with the regulations or are found in violation of their customers' privacy.

Specific Types of Information

As mentioned, a few slides back, there are numerous types of regulated data in your workplace. Depending upon where you work, you may be required to take specific training based upon your organization's data. Data that requires specific classifications and training includes, but is not limited to:

* Criminal History Information (CHI)

* Personally Identifiable Information (PII)

* Personal Health Information (PHI)

* Federal Tax Information (FTI)

* Payment Card Information (PCI)

PII and You

What is PII? PII stands for Personally Identifiable Information. The National Institute of Standards and Technology, or NIST, defines PII as:

Information which can be used to distinguish or trace the identity of an individual **alone, or when combined** with other personal or identifying information which is linked or linkable to a specific individual.

PII is any information about an individual maintained by the State of Illinois, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's birth name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Just like your DNA makes you yourself in the physical world, PII makes you yourself in the digital world. In short, PII refers to any info that can be used to identify, contact, or locate a specific individual.

Examples of PII include, but are not limited to:

- Name, such as full name, birth name, mother's birth name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number;
- Address information, such as street address or email address; and
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry).

Protecting Personally Identifiable Information

Breaches involving PII can be hazardous to both individuals and organizations.

Harm to individuals may include:

- Identity theft (including financial losses);
- Embarrassment; and/or
- Blackmail.

Harm to our organizations or agencies may include:

- Loss of public trust;
- Legal liability; and/or
- Remediation costs.

Please check your agency policies for any additional requirements for handling personally identifiable information. Agencies often have additional protections, rules and guidelines they must follow to be compliant with state and federal laws.

Information Spillage (ACA Program)

Information spillage in the context of the ACA program refers to instances where sensitive information (e.g., Personally Identifiable Information [PII] or infrastructure configurations) that is inadvertently placed on, subsequently shared with, or distributed to personnel or information systems that are not authorized to process such information.

Information "spillage" incidents should be reported to DoIT.Security@illinois.gov as soon as possible.

State of Illinois IT policies

Each agency, board, or commission has different rules regarding the acceptable use of IT resources. Some are more restrictive than others. The reasons for these discrepancies are varied but a few examples of why some organizations have more restrictive policies than others are:

- The different types of data or information they work with. (FTI, PII, Criminal History, PHI, etc.)
- Differing regulatory authorities (IRS, Social Security Administration, FBI, Payment Card regulations, etc.)

For those agencies who have the Department of Innovation and Technology as a service provider, the base level policies regarding information technology can be found on the policy page. The Acceptable Use policy is also located on the webpage. The goal of the Acceptable Use policy is to establish minimum appropriate and acceptable practices and responsibilities regarding the use of IT Resources, which will protect proprietary, personal, privilege, or otherwise sensitive data. It establishes minimum guidelines for acceptable use. Your agency policy may be more restrictive, and to that extent will supersede the minimum requirements of the Acceptable Use policy.

Your Responsibility

It is your responsibility to help protect our organization's information and technology resources.

YOU are the front line of defense and are the easiest way for cyber criminals to gain access to information.

Privacy and data incidents can result in:

- Inability of your organization to fulfill its mission
- Disruption of day-to day operations
- Damage to the State of Illinois reputation
- Harm to individual's health or financial status

Reporting

Employees who suspect a security incident or possible compromise of data has occurred, should immediately contact Security. All suspicious emails should be submitted using the **Phish Alert button (PAB).**

If the phish alert button is not available or you have another security concern, contact:

DoIT.Security@illinois.gov

IF IN DOUBT - REPORT!

Completion & Certification

Please **sign below** to certify that you have carefully read and reviewed the content of, and completed, the **Security Awareness Training** as mandated by the Illinois Data Security on State Computers Act (20 ILCS 450/25). I understand that compliance with the State's statutes, policies and regulations is a condition of employment/appointment and that it is my obligation to read, understand, and remain current with any new or amended statute, policy, rule, directive or regulation. I further understand that a violation of any State statute, policy, rule, directive or regulation may result in disciplinary action, up to and including discharge or removal.

I UNDERSTAND THAT NO STATEMENT IN THIS TRAINING SUPERSEDES THE PERSONNEL CODE OR ANY NEGOTIATED CONTRACT, NOR DOES THIS TRAINING CONSTITUTE OR IMPLY ANY CONTRACTUAL OBLIGATIONS

Printed Name:_____

Signature:_____ Date: _____