Security Awareness 2025

Introduction

Cybersecurity attacks against information technology (IT) infrastructure persists every week. Why are there so many cyber-attacks? Part of the answer is that IT is targeted for attack because it supports every facet of our lives; from working, to shopping, and everyday life activities. This includes paying bills and filing taxes. The work we do to serve the public is reliant upon our ability to safely use the systems, devices, and data entrusted to us.

This is an awareness level cybersecurity course. 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 of the IT world. Just like navigating physical landscapes will have dangerous elements that you must be on the lookout for, the cybersecurity threat landscape has threats that malicious actors will attempt exploit to cause harm, damage, or destruction. These exploits can be found in systems, codes, processes, procedures, and even human behavior. The approach for this course is to keep it as simple as reasonably possible.

Ransomware

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.

Here's an example of how a ransomware attack can occur:

1. A user is tricked into clicking on a malicious link that downloads a file from an external website.
2. The user executes the file, not knowing that the file is ransomware.
3. The ransomware takes advantage of vulnerabilities in the user's computer and other computers to propagate throughout the organization.

4. The ransomware simultaneously encrypts files on all the computers, then displays messages on their screens demanding payment in exchange for decrypting the files.

Common ways ransomware can hit you:

1. Email - phishing emails can trick you into clicking on an attachment ("Urgent Invoice") that allows the malicious software program to take over your computer.
2. Malware - if your network or software is vulnerable , a cybercriminal can sneak in and plant malicious code. It might sit unnoticed for a period of time, allowing the bad guys time to access files and steal data, then finishing up with unleashing ransomware so you can't see the damage.

Don't assume your organization is too small to get hit. The nature of ransomware is that the cybercriminals work to ensure their malware spreads as widely as possible, infecting the computers of individuals and businesses of all sizes.

Social Engineering

What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

- Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as
- Natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- Epidemics and health scares (e.g., H1N1, COVID-19)

- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays

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 and including discharge.

---

5 Signs 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. (NIST, 2024) Please scroll through the entire list. The scroll bar is on the right hand side of the screen.

Clue	Explanation
Errors	Errors in grammar and spelling are very often a great way to identify a potential phishing email. Errors in ANY portion of an email could identify a potential phish attempt. This could include but is not limited to the subject, body, sender, or recipient.
Technical indicators	This can include unfamiliar or unknown senders. It can also include domains that are external to the organization. Some other technical indicators include, but are not limited to mismatched hyperlink in an email, or an attachment that doesn't match your job or the context of the email.
Visual Presentation Indicators	Inspect emails for outdated, mismatched, or text that redirects to an URL that doesn't match the content (You should manually navigate to sensitive sites, such as bank or work login pages.)
Language and content	Skilled cyber criminals use human emotion as a crowbar to break past cyber security. If your first response to an email is to worry, hurry, or fury just take a moment before you click or react in any way. Take a moment to review the content and never click in the email unless there is absolutely no other option. Consider calling the sender if you have their contact information.

Clue	Explanation
Common tactics	Common tactics include using cunning communication to legitimize their attack, creating a perception of need, building false trust, and using emotional manipulation. Skilled cyber criminals are trying to get you to act BEFORE you think. You can counter them if you remember to THINK before you act.

5 Types of Phishing Emails

The full number of differing types of Phishing emails can vary from one organization dictionary to another. The one trait ALL phishing attacks share is the attempt to exploit individuals through social engineering to compromise the security and bypass digital security measures.

Name	Description
Spear Phishing	Spear phishing is a targeted phishing method that cybercriminals use to steal your information by impersonating a trusted source. If they get the information they want, they may use it for malicious purposes such as identity theft. Unlike some other forms of phishing, spear phishing targets a specific individual.
Phishing	Phishing is when a cyberattacker sends you an email pretending to be someone else in hopes that you'll reply with the information they requested. Once you've given the attacker what they want, they may use your information for criminal activities or even sell your information on the dark web.
Vishing	Vishing, which is short for "**voice** phishing," is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them.
Smishing	Smishing is phishing through some form of a text message otherwise known as **SM**S.
Whaling	A whaling attack is a phishing or spear-phishing attack that targets a senior executive or other High Value Targets (HVTs). These individuals often have deep access to sensitive areas of the network, so a successful attack can result in access to valuable info.

Example of Phishing

Read the sample email below. Try to spot potential flags or warning signs to the receiver. 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 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)
    a. This icon is located in the upper right hand corner of Microsoft Outlook and will look like the icon shown on this slide.
2. If you can't find the Phish Alert button, simply forward to DoIT.Security@illinois.gov with the original email added as an attachment.

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

Sam was recently hired as an agency executive and received an email addressed to them by name and title. The email appeared to be an email from a vendor congratulating them on their role and to register their account with them, however when Sam hovered over a link in the email. It did not match the URL listed. Sam immediately reported the email via the Phish Alert Button (PAB) and it was confirmed malicious. What type of attack was attempted?

- A. Cyber-Pincer attack
  - A is not the best answer. The "Cyber-Pincer attack" is not a standardized name for an attack type.
- B. HTML Barrage
  - B is not the best answer. The "HTML Barrage" is not a standardized name for an attack type.
- C. Whaling
  - Correct: C! Whaling is the correct answer, Sam was most likely targeted due to their position as an agency executive, plus being new to the organization the attackers likely suspected that Sam would not recognize a legitimate threat or be familiar with reporting procedures. Sam's position affords them a high level of access to very sensitive data over a wide range of systems making them a VERY High Value Target.
- D. SMishing

- D is not the best answer. Sam was attacked as a High Value Target AND was NOT targeted through text messages.

Knowledge Check

Sam's entire office was sent an email with an invoice for approval. The invoice appeared to come from a trusted web platform that manages digital signatures. But after logging in, Sam noticed the URL is completely different and does not contain the invoice they were expecting. What type of attack just occurred?

- A. Malicious Insider attack
  - A is not the best answer. A Malicious Insider is not a type of phishing attack. It is a descriptor for a specific type of threat.
- B. Vishing
  - B is not the best answer. Sam did not receive a voice call for the attack. They received an email
- C. Phishing
  - Correct: C! Sam and many others in the office were included on the email, even though a message of that nature should have only gone to appropriate personnel.
- D. Spear-Phishing
  - D is not the best answer. Sam was not the only user to receive the email. This was more of a broad "wide-net" style of attack.

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.

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. Here in the following slides are some, but not all, the ways to identify each type of insider threat

- 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 is working on new content for a report and submitted a request to have new software installed. The request was declined as the requested software had not been thoroughly vetted and was deemed an unnecessary security risk. Sam found a work around for installing the unauthorized software and did so. Sam's device was communicating on the network to a known address that is used for malicious deployment of ransomware and was immediately isolated on the network. Which title best describes Sam for this scenario?

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 receives a phone call from someone who claims to be their boss, while the voice sounds vaguely familiar the caller ID shows an unfamiliar name and number. The caller is asking for them to send them iTunes gift cards for a raffle basket. How should Sam proceed?

- A. Sam should go ahead and purchase the gift cards and send them since their boss is asking for it.

- A is not the best answer. There is a better answer. Sam has not authenticated the request or the requestor and runs the risk of losing their own money or worse, state funds.

◦ B. Sam should call the Illinois State Police to report an imposter.

- B is not the best answer. There is a better answer. Sam cannot say with certainty that this is an imposter at this time. While the name and phone number do indicate unusual activity there is a possibility that there is a legitimate reason for this method of communication and request.

◦ C. Sam should follow up with the requestor after the phone call, using a known good point of contact, or even in person (if feasible) to authenticate the request. Additionally, If the request is not authentic, then Sam should send an e-mail to DoIT.Security@illinois.gov.

- Correct: C! This allows Sam the opportunity to make sure they are not being manipulated into giving money to a cyber criminal while also being to provide clarity to the situation and report it if appropriate for the scenario.

◦ D. Sam should yell at the caller and berate them for their unreasonable request.

- D is not the best answer. There is a better answer. Sam cannot say with certainty that this is an imposter at this time. While the name and phone number do indicate unusual activity there is a possibility that there is a legitimate reason for this method of communication and request.

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.
- If someone drops, places, or leaves a storage device (e.g. flash drive or portable hard drive) in a public area report do NOT insert into your computer until the storage media has been checked and cleared for use on devices.

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.

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

- **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 is walking to their office building from their vehicle and they notice someone placing USB drives throughout the parking lot. Which of the following actions should Sam **NOT** do?

- A. Sam should notify the security desk.
  - A is not the best answer. There is a better answer. This is something Sam SHOULD do.
- B. Sam should send an email to DoIT.Security@illinois.gov.
  - B is not the best answer. There is a better answer. This is something Sam SHOULD do.
- C. Sam should pick up a flash drive to use on their computer so they can store a secure document.
  - Correct: C! Sam should NOT use any storage device that could potentially be used to cause harm or exploitation of the Information Technology Systems they interact with.
- D. Sam should notify their supervisor about the incident with the storage.
  - D is not the best answer. There is a better answer. This is something Sam SHOULD do.

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!

Knowledge Check

Sam used a popular Generative Writing web application for a public facing project. What is something Sam does NOT need to check before publishing the project.

- A. Copyright material. Because Sam used the web application, Sam has no responsibility to verify that the content is covered/protected by Copyright laws.
  - Incorrect. A is not the best answer. There is a better answer. Even while using a web application. Sam is responsible for all content they publish.
- B. Accuracy of Material. Sam used artificial intelligence. it couldn't possibly give bad information.
  - Incorrect. B is not the best answer. There is a better answer. While the information provided may be convincing and often times sounds plausible. Generative Writing is still dependent on the quality of the information it receives. You should ALWAYS double check the accuracy of any and all claims made by an AI tool.
- C. The date content was generated.
  - Correct. C is the best answer. When content is generated is irrelevant, as long as the content is not protected, is accurate, and is consistent with what you are trying to use it for then. When the content was created isn't an urgent factor if it's still true and accurate information.
- D. Content Relevance
  - Incorrect. D Is not the best answer. Just like when having a conversation with a human. Generative software can "misunderstand" what it is we are really asking. Especially if we use unclear or imprecise terms.

Usernames and Passwords

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

- Use a strong password.
- Variables that help determine what is a good password include: system type, data, organization, compensating security controls, etc.
- Do not share or reuse your passwords with anyone - A help desk does not need your password. They have other means to help you resolve issues.
- Use Multifactor Authentication (MFA)when available.
- 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 your credentials 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.

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.

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.

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.

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!

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!

Completion & Certification

I certify that I 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 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.

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

I certify and Acknowledge the above statement. *(Please type your name and date in the fields below.)*

Name:

Date: