Security Awareness

This course is intended for those who need to take annual Security Awareness Training.

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 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 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 hiking trails for beginners. Just because you have hiking boots (computer), a packed rucksack (Wi-Fi) and a hiking trail (Internet). Just because you have these resources for your hike, that does not automatically make you a safe and experienced hiker who is ready to navigate the cyber-trail. The goals of this course are to:

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

The "Threat Landscape"

Threat Landscape is a popular phrase describing the dangers lurking in the information technology world. Just like a mountain landscape has dangerous elements that you must be on the lookout for, the cybersecurity threat landscape has threats that exploit possible weaknesses that can 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. Try not to get hung up on semantics and true technical jargon.

What Is Lurking Out There?

Short answer? A lot!

This security awareness course takes you along a cyber-trail to identify some hazards including suggestions on how to avoid those hazards while working for organizations of all shapes and sizes and even apply them to your own personal cyber-trails.

Remember – Sensitive networks, systems, assets, and data are irresistible for those with bad intentions.

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. Which one of the following outcomes depends upon what the "bad actor" 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 an employee, you need to understand that while using work resources, the most common way a computer is infected by ransomware is through social engineering. Upcoming pages 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 do not have a 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

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 "door and windows" 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, report it in accordance with your organization’s security practices and directions.

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.

If in doubt…throw it out.

Common Traits of Phishing Emails

Phishing is one of the most common attack methods used by cyber criminals. Fortunately, there are often signs to help determine if the email is a scam. This list is a good reference for both your work and personal life. Please read through the entire list.

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 (but don't click!) 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, includes spelling errors 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.
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 Red Flags

Read the sample email below. Try to spot potential red flags or warning signs to the receiver. The next five sections will focus on different ways to look for red flags in emails. Red flag = something that should trigger suspicion.

From: hr@outsideorganization.znet

To: you@yourorganization.net

Date: Tuesday, December 3:00 AM

Subject: Survay

Hi User,
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!

Red Flags – Look at the 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.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like micorsoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.

Red Flags – Look At The Date And Who It Was Sent To.

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.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

Red Flags – Look At The Subject And Any Attachments

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

- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?
- 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.)
- I see an attachment with a possibly dangerous file type.

Red Flags – Look At Any 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 address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known website. For instance, www.bankofarnerica.com - the "m" is really two characters - "r" and "n."

Red Flags – Review The Content Of The Email

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?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

What To Do When You See A Red Flag Or A Suspicious Email?

If your office or place of work has a reporting process in place, always report it! As this course is written for a diverse audience with different reporting protocol, take this as an opportunity to discover your organization's reporting protocol. Post it somewhere near your workstation so you are not looking for it when the need arises. Make sure you know the answer to these questions:

1. What is the contact number for my help desk or IT department?
2. What is the protocol for reporting suspicious emails?
3. What is the protocol if I think I have fallen for a scam?

Categories Of Threats

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

1. Natural Threats - Disasters such as tornadoes, hurricanes, floods, and electrical storms. (You will notice when large disasters occur, the scams surrounding these incidents increase as well.)
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 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 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 two 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 the United States Computer Readiness Team (USCERT). 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 user awareness and provide practice recognizing social engineering. This is often achieved through the following:

- Simulated 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 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.

Physical Security

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

- 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.

- Confidential information could be leaked or stolen.

When you leave your workstation, you need to LOCK it. This can be done different ways. (Please note the following commands are exclusively for windows. If you use a Mac or Linux based OS, please look up the instructions for those Operating systems on how to lock your machine).

1. Press CTRL/ALT/Delete and then selecting "Lock"
2. Hit the Windows key + the "L" key

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

- 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.
- Recognizing legitimate IT notices - How does your work/organization notify you that your password is expiring? 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.
- 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 or if you must, use a VPN to protect sensitive information.
- Being proactive versus reactive - Think about creating an email folder dedicated to communications from legitimate sources. File emails (or setup email rules) from these trusted senders in that folder. Why? Because now you have a reference of what legitimate messages from these senders look like. Also, when large changes are being made to your programs, software, or other significant changes, you are generally sent a notice or directions ahead of time. If you file it, you can refer to it when you have questions or refer to the program owner’s website for more information and patch notes.

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- 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!
- Use Multifactor Authentication (MFA)- This strengthens the security of accounts should credentials be compromised.
- Do not store your password in written form at your workstation or personal computer
- Utilize Password Managers to generate unique and complex passwords and store them securely so that you don't have to rely on your memory or weak and reused passwords.

MFA - The New Normal

By now, hopefully, you 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

It's Dangerous To Go Alone - Take This (Knowledge)!

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.

Think About It...

How often do you get emails or texts 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 or delete it!
2. Slow down and think before you click or enter your credentials. If you think you clicked or gave your credentials in error, update your password!
3. On your personal accounts at home, if in doubt - DELETE IT!

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.

Types of Information

* Personally Identifiable Information (PII)
* Personal Health Information (PHI)
* Federal Tax Information (FTI)
* Payment Card Information (PCI)

Fun Fact

People frequently read the previous list and ask, What about HIPAA data? HIPAA is not a type of data.

HIPAA stands for Health Insurance Portability and Accountability Act. HIPAA privacy rules protect the privacy of individual identifiable health information, called protected health information (PHI). HIPAA stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and generally prohibits healthcare providers and healthcare businesses, called covered entities, from disclosing protected information to anyone other than a patient and the patient's authorized representatives without their consent. Specific HIPAA training that goes into far greater detail than these few sentences is provided to many agency staff who work in the health, family, and human service organizations.

The same is true of Federal Tax Information (FTI). The Internal Revenue Service mandates certain agencies must take special FTI training, entitled Information Safeguard Training. At least 6,000 State of Illinois employees must take specialized FTI training annually.

PII

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 an entity, 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).