# Security Awareness Training 2018-2019

## Introduction

Cybersecurity has become a top priority across the nation. It is a proven fact that most data breaches are the direct result of end user error.  No matter what our skill level is, all of us are considered "end users".  Completing this awareness level course helps us to better secure the state's information and data entrusted to us, while providing some typical tactics we can use to protect our personal information, as well.

## Course Topics

Technology and the threats to our information, systems and networks are ever evolving, yet there are some basic measures we can take to protect ourselves and our organizations better.

## What does information security mean to you?

The National Institute of Standards and Technology defines Information Security as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

To put the above definition in perspective, think about all the information you and/or your organization have access to, collect and are responsible for. Making sure that information is safe is every employee's job.

## Various forms of Information

In today's work environment, many information systems are electronic but information (or data) comes in many different formats and must be protected. The following are all forms in which data can be distributed:

- Electronic
- Paper
- Oral

## "Cybersecurity"

Cybersecurity is a frequently heard buzzword. It is defined in a variety of ways but the National Institute of Standards and Technology (NIST) defines Cybersecurity as:

"The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."

## Information Security vs. Cybersecurity

Remember, information security is concerned with all information no matter the format, storage or mode of transmission (electronic, paper or oral). The term "Cybersecurity" has a digital or computer implication.

For the purpose of this course, the central focus is trying to protect the information, the technology that carries information and information systems in your care.

**FUN FACT**: The spelling of Cybersecurity vs. Cyber Security vs. Cyber-Security is a hotly debated topic and is often used interchangeably. According to a post by GovTech, the single word has been used in more government circles and news sources are using it instead of the other renditions.

## Goal of Information Security

When we hear the phrase "protecting information", most of us think of keeping specific information and details a secret. The goal of Information Security is not to create and keep secrets but, rather to protect the confidentiality, integrity, and availability of information and information systems.

The following 3 elements are all included in the overall goal of Information Security:

- Confidentiality
- Integrity
- Availability

## Example

Your bank account is a good example of an information system that must be confidential, available, and have integrity.

Imagine the following scenarios:

- Your account was not kept confidential and someone else was able to access it when they approached the ATM. How much damage could be done?
- Every time you went to the ATM, the balance it displayed was inaccurate. How could the poor integrity of your balance information affect your budgeting and spending decisions?
- Your bank's ATM was rarely available when you needed it. Would you continue to use that bank?

## Knowledge Check

Now that you understand the 3 key elements of information security, you are ready to learn about threats to information security and your role in protecting that information.

What is the goal of information security?

a. Ensure that employees have proper identification

b. Protect the confidentiality, integrity, and availability of information and information systems

c. Protect file cabinets with keys and cable locks

Correct Answer is B!  The goal of information security is to protect the confidentiality, integrity, and availability of information and information systems.

# Physical Security

## Things to consider when in the workplace...

Physical security is an important Information Systems safeguard. Limiting authorized personnel's access to Information Systems and infrastructure diminishes the likelihood that information will be stolen or misused.

- Avoid "Tailgating"-Never allow anyone to follow you into the building or secure area without his or her badge. One way to handle the situation is to ask them if you could be of some assistance with a simple, "May I help you?"
- Do not be afraid to challenge or report anyone who does not display a visitor's badge.
- Do not allow anyone else to use your badge for building or secure area access.

**Report any suspicious activity to the Building Security Personnel**

## Securing your workstation

Securing your workstation is an important component of physical security and is often overlooked as we become comfortable or even complacent at our work stations.

Below are just a few of the reasons to lock your workstation:

- Rules regarding the safeguarding of sensitive data including, but not limited to: Personally Identifying Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Criminal History Information. Each have consequences for not following proper handling protocol
- Prevent leaking of confidential information
- Prevent insider Threat (Malicious or Accidental)- *to be covered later in course*

**Lock your workstation anytime you leave it by pressing CTRL/ALT/Delete- Lock**

## Other Physical Security Tips

- Only store and transport removable media such as CDs/DVDs, flash drives, and external hard drives when approved and in a secure manner.
- Maintain a "clean desk" and keep your workspace secured; i.e., lock up any sensitive files and diskettes.
- Don't leave documents unattended on the printer, copier or fax machine.
- Do not throw any confidential documents in your trash bin. Instead, properly dispose of the information using a shredder.
- Remove papers and wipe boards clean when finished using conference rooms.
- Lock filing cabinets when you leave.
- Shred or otherwise destroy sensitive documents when discarding them.

## Portable Media

Portable Media refers to items that store information but are not physically part of a computer. This would include CD-ROMs, DVDs, USB flash drives, among others.

Be sure to only used portable media in compliance with your policy.

Portable media options are great inventions and make moving data from one computer to another very convenient. However, without a secure network connection, portable media could introduce malware to your computer and information systems. Portable media also face a higher risk of being lost or stolen.

***As this training is provided for a wide number of organizations with different IT service departments, it is not possible to cover all portable media and media protection policies and procedures.**

## Put Down that Thumb Drive: You don't know where it has been!

- USBs and Thumb Drives pose an enormous risk to organizations. Using a thumb drive or USB to carry files back and forth between personal devices and state devices can introduce viruses or malware to state resources.
- Don't risk the security of your private devices and information. Not only can accessing information from a foreign thumb drive damage your organization's technology and information but, it can also cause serious damage to your own resources.
- If you come across a thumb drive or USB device laying around, do not insert into any device. Again…you don't know where it has been!

## Flash Drive Experiment

In 2015, two experiments were conducted separately by researchers at the University of Illinois and CompTIA, an IT industry association. Both groups dropped between 200-250 flash drives on the U of I campus and in four cities:

- In the University of Illinois study, more than 45 percent of people picked up the drives and plugged them into their computers.
- In the CompTIA experiment, nearly 1 in 5 people picked the drives up and plugged them into their computers.

**What if that flash drive were infected?**

Depending on what was put on the drive, files could be locked, sensitive data lost, and possible malware could infiltrate your network and shut down your organization.

## Knowledge Check

Ava needs to leave her workstation to ask her coworker a question. What should she do before leaving her workstation?

A. Lock her workstation by pressing CTRL/ALT/Delete- Lock

B. Turn off her monitors

C. Log out of her email

The best answer is A.

# Passwords

## Passwords = Target

Passwords are a frequently targeted vulnerability in any system. A strong password for your network account and other applications is a basic protection mechanism.

Creating a simple or generic password is easy but **not secure**.

Systems and websites have varying minimum standards for passwords. Do NOT follow the minimum!

## Tips for creating better passwords

- Do not use familiar names.
- Avoid using common or easily researched facts about yourself (birthday, pet names, etc).
- Avoid dictionary words Why? Because software "cracking" programs can be easily purchased online. Simply exchange letters for special character or numbers. Example: F00t6@11 instead of "Football".
- Length and complexity of the password make a big it sufficiently more difficult for a hacker.

## More on Password Length and Complexity

Did you know that an 8 character password can be cracked instantly if it only contains numbers? It can take weeks to crack a more secure password containing numbers, upper/lowercase letters as well as special characters like $,%,&, etc. A combination of numbers, upper/lowercase letters and special characters makes a password more "Complex".

Although it is difficult for us to remember multiple passwords, refrain from using the same password for more than one site. Using the same password on multiple accounts is simply giving away the key to potentially all of those accounts.

**Did you Know?? A password containing 16 characters including numbers, upper and lowercase letters, and special characters can take up to 193 Trillion years to crack?**

## Protecting your Passwords

Not only is it important to create strong passwords but those passwords must be protected. Below are just a few tips for protecting your passwords:

1. **Do not share your passwords**- Your Help Desk does not need to know your password as they have access to other means to help you restore your system. Consider any email or phone call requesting your password a scam.
2. **Do not write down your password and store it at your workstation**- Did you know that some companies will hire security firms to try and find passwords left by employees in their workstation to test their security policies and training?
3. **Passwords should not be stored in a computer file.**
4. **Do not reuse the same password on multiple systems or sites.**

## Remember!

Remember, most systems will require you to change your password at various intervals, but you should do the same for your personal accounts. Your money, identity and credit card information are tempting targets and are under constant attack. It is a hassle to remember to change the passwords and have unique passwords for all accounts, but if you have ever been the victim of identity theft or had money stolen, it is worth the effort.

Set a calendar reminder for yourself!

## Knowledge Check

Which of the following passwords is most secure?

A. Jenny!18

B. B1@ckH@wksRule!!

C. ChicagoBears2018

D. 1234567891011123

B is the correct answer because it is 16 characters AND is complex (numbers, upper and lowercase letters and special characters.

Choice A has complexity but it is only 8 characters long.

Choice C has length but no complexity. Uses both dictionary words and numbers only.

Choice D has length, but it is only numbers. It can be cracked in a matter of seconds.

## Social Engineering Explained

## What is Social Engineering?

Simply put, social engineering is the art of tricking people into divulging personal information or other confidential data. It is an umbrella term that includes phishing, pharming, smishing, vishing and other types of manipulation. The term "social engineering" sounds innocent enough but it is a malicious act and a topic all Internet users should understand. This is where YOU become the weakest link in your organization's security perimeter. You are a target at home and at work.

- Social engineering attacks are more common and more successful than computer hacking attacks against the network.
- Unlike hacking, social engineering relies more on trickery and psychological manipulation than technical knowledge. For example, a malicious user may send you a "phishing" email that says you need to reset your username and password for a specific website. The email may appear to be legitimate, but if you click the link in the message, it may direct you to a fake website that captures your information.

## False Alerts on Websites

Another common type of social engineering uses false alerts on websites. For example, when you open a webpage, you might receive a message stating your computer has a virus and you need to download a specific program or call a phone number to fix it.

In most cases, these alerts are auto-generated and are completely false. If you follow the instructions in the alert message, you may end up downloading spyware or giving away personal information over the phone.

It is wise to be skeptical of any message, email, or website that asks you to share personal data - especially if the request is from an unknown source. You can often verify the legitimacy of a message by checking the URL address of the website.

## Social Engineering Explained

Social Engineers want any information that will give them access to government systems or facilities. Common targets are:

- Passwords
- Security badges
- Access to secure areas of the building
- Smart phones
- Wallets
- Employee's or Client's personal information

## Phishing

Do not confuse **phishing** with **fishing**! They are similar but instead of trying to capture bass or catfish, a phisher attempts to "catch" your personal information.

Phishers will send out e-mails that appear to come from legitimate websites or banking institutions.

The e-mails state that your information needs to be updated or validated. It will then ask that you enter your username and password, after clicking a link included in the e-mail. Some e-mails will ask that you enter even more information, such as your full name, address, phone number, social security number, and credit card number.

**Giving away your username and password could give the "phisher" access to other accounts if you reuse passwords.**

## Phishing Advice

Phishing e-mails often look surprisingly legitimate, and even the Web pages where you are asked to enter your information may look real. However, the URL in the address field can give you some clues as to whether it is a scam or not.

Let's pretend the name of a popular retailer you frequently do business with is "Discount.com".

- "http://www.discount.com" and "http://cgi3.discount.com" are valid Web addresses,
- **BUT** "http://www.discount.validate-info.com" and "http://discount.login123.com" are false addresses, which may be used by phishers.

If you receive an e-mail that asks you to update your information and you think it might be valid, go to the website by typing the URL in your browser's address field instead of clicking the link in the e-mail.

****Please note:** The examples used are not actual phishing sites and are merely used to illustrate the concept.******

## Phishing DON'Ts

If you are suspicious of an email:

- Do NOT click on the links provided in the email
- Do NOT open any attachments in the email
- Do NOT provide personal information or financial data
- Be suspicious of any email that:
- Requests personal information
- Contains spelling and grammatical errors
- Asks you to click on a link
- Is unexpected or from an organization with whom you do not have a relationship

## Report Phishing

As the audience for this training is diverse, not all users have the same reporting methods or abilities.

Look for a phishing reporting tool used by organization's email service provider.

*If you don't have that option, report the message to your IT security team and then delete the email!

**IF IN DOUBT- DELETE!** Never give your Password to **ANYONE** in an Email or over the Telephone!

## Phishing Example #1

**From**: XXXXX.XXXXX

**Sent**: Tuesday, March 24, 2015 8:30 AM

**Subject**: Important Notice

Important notice from the helpdesk.  Your E-mail box has reached its maximum limit of 20 GB of storage and Your account will be disabled if you do not upgrade now.

For your own good, you are to provide your correct information to enable us carry out your email account upgrade and remember without your correct information your email account will be closed.

To upgrade your email account today,

**CLICKHERE**

Your account will remain active after we have confirmed your email account successfully.

## Phishing Example #2

**From**: XXXXXXXX@gov.bm

**Sent**: Thursday, December 10, 2015 6:00 AM

**Subject**: Suspended Account (Help Desk)

Attention,

Your Password Expires in 2hour(s) You are to change your Password below via ACCOUNT MANAGEMENT PAGE.

Click on **CHANGE PASSWORD**

If Password is not change in the next 2hour(s) Your next log-in Access will be declined. If you do find difficulties in Change Password, to upgrade your email account today, quotas, accessing files or missing files please contact the ITS Helpdesk (itshelpdesk@webmail.org/XXXXX).

Regards,

IT Services

## Spear Phishing Explained

Spear phishing is an attempt to manipulate a targeted individual who possesses information the hacker wishes to gain access to. The attacker may have one or more pieces of inside information that they will, generally, use for leverage when attempting to extract information from the individual.

**Always verify requests before sending any confidential or sensitive information**

## Spear Phishing in Action:

**Step 1** - An attacker obtains the name of someone in Human Resources.

**Step 2** - Armed with the above information and the name of the company president, the attacker sends an email (spoofed to look like it came from the president of the company) directly to the person in HR.

**Step** 3 - In the fake email, the president asks for all of the payroll information for everyone that worked at the company for the previous year.

**Step 4** - The HR employee complies with the request

**Step 5** - Once the information has been sent, the HR person may not even realize that it went to the wrong email address. All that information just went to the attacker.

## Other Phishing Buzzwords

**"Smishing"** - A phishing scam carried out by text messaging

**"Vishing"** - A phishing scam carried out via a telephone call

The FBI's Internet Crime Complaint Center (IC3) warns that attempts as cyber-crimes are not solely limited to computers. Both work or private phone lines are susceptible "smishing" and "vishing".

## Example of Smishing and Vishing

Criminals set up an automated dialing system to text or call people in a particular region or area code. The victims will receive messages like: "Your account has encountered a problem," or "Your ATM card needs to be reactivated," and are then directed to a phone number or website asking for personal information. Armed with that information, criminals can steal from victims' bank accounts, charge purchases on their charge cards, create a phony ATM card, etc.

## More Examples of Smishing and Vishing

- Smishing with text messaging using a problem scenario: "Credit Union. Please call 1-800-555-1212 about a transaction on your credit card".
- Smishing with text message using a notification scenario: "Bank. Your account balance exceeds $5,000. Please call 1-800-555-1212".
- Vishing with phone using impersonation: "Hey Jim, This is mike in shipping. I forgot the account number for buying supplies. Can you help me out?
- Vishing via telephone using compassion: "I need this application submitted by 5 pm or I will be fined $100. I don't know my account number, but it hasn't changed since last year. Can you tell me my account number from last year's application?"

## Knowledge Check

A phishing email...

A. Is a type of social engineering attack

B. Can be from an organization that you recognize, like a professional association

C. Contains a link to a web site that asks you for personal information

D. All of the above

Choice D is the best answer.

## Identity Theft

## Identity Theft overview

The Federal Trade Commission (FTC) estimates that 9 million people have their identity stolen each year.

Identity thieves use names, addresses, Social Security numbers, and financial information of their victims to obtain credit cards, loans, and bank accounts for themselves.

If you believe you are a victim of identity theft:

- Contact the three credit reporting companies (Equifax, Experian, and Trans Union) and place a fraud alert on your report.
- Inform your bank, credit card issuers and other financial institutions that you are a victim of identity theft.
- If you know who stole your information, contact the police and file a report.

## Combatting Identity Theft

- Be extremely cautious when providing your Social Security number. Know how and why it will be used.
- Review credit card and bank statements at least monthly for unauthorized transactions.
- Use strong passwords for your home computer and web sites you visit, especially email accounts and financial institutions.
- Leave your Social Security card and passport at home. Never leave them in your purse or wallet unless necessary.
- Shred sensitive documents and mail containing your name and address.

## Security On-the-Go

## On-the-Go tips:

- Always maintain possession of your laptop and other mobile devices.
- Ensure wireless security features are properly configured. Use WPA/WPA2 to secure your Wi-Fi. WEP is incredibly weak and should never be used.
- Do not auto-connect to open Wi-Fi networks like at a hotel or airport and NEVER log into banking or other secure accounts when using a free, public Wi-Fi network.
- Make sure your mobile device is Password Protected (and hard to guess - complex). Also, make sure your laptop has encryption enabled.
- Report a loss or theft of your laptop or other government furnished device immediately.

## Wireless Security

In our on the go society, people and organizations rely on wireless network technology for data sharing and connectivity.

A wireless network has all of the same security issues as a wired network plus more.

To help mitigate the risk of using wireless devices, it is important that you have a basic understanding of how they work and what you should do to safeguard your organization's information resources as well as your own private information resources.

## Wireless Vulnerabilities

Using a wireless network creates a number of vulnerabilities that must be addressed for secure communications. Those vulnerabilities are:

- Intruders can attempt to connect to networks via wireless access points.
- Wireless communications can be intercepted.
- Wireless devices can be accessed if not physically secured.
- Wireless devices are typically small and easily stolen.
- Other network resources may be attacked if an intruder gains access through an unsecured wireless device.
- Viruses can be introduced, and other malicious attacks can be attempted on the wireless signal.

## Using Wireless Networks Securely

Much of the responsibility for network security falls on your IT staff. However, the use of wireless devices puts some of the responsibility on you as well. Tips for securing your wireless communications:

- Protect the wireless device from physical theft.
- Wireless devices should not be connected to both external networks and our organization's networks at the same time.
- Install a personal firewall on wireless client devices.
- Use current anti-virus protection on all wireless client devices.
- Disable file sharing on wireless client devices.
- Wireless client devices containing sensitive information should be encrypted.
- Keep software patches for wireless devices up to date.

## Mobile Devices

The use of mobile devices in the workplace can be a great security concern. Today's mobile devices are capable of storing and processing large amounts of data. This makes them an ideal target for cyber-criminals. Theft, loss or even the unauthorized use of mobile devices can lead to loss of an organization's information, unauthorized data access and malware infection.

**Consult your policies on the use of mobile devices to help protect our information resources and assets.**

## Mobile Device Security Best Practices

A majority of data loss with mobile devices is a result of security failures. Following the guidelines below will help protect information:

**Passwords** - Password protect your devices.

**Encryption** - Encryption can be crucial to protecting the data stored on a mobile device in the event of theft or loss. Make sure that you use an approved encryption tool, especially if there is sensitive data involved

**Malware** - A simple click on the wrong link can lead to malware infection of any device. Mobile devices are becoming a popular target for malware authors. Malware can be presented as links on web pages, within phishing e-mails and even through apps for mobile devices.

## Mobile Device Security Best Practices...continued

**Physical Security** - Mobile devices are the ideal target for information theft. They hold a lot of data and can be easily concealed and transported. Never leave your device unsecured or unattended.

**Wireless Connections** - Always use trusted and secured wireless connections, if possible. Free public wi-fi connections are often targeted by cyber-criminals looking for new victims.

# 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.

***Be aware that depending upon where you work, you may be required to take specific Privacy training.**

# What is confidential Data?

Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to citizens, clients, and your organization, our providers and partners. Examples of Confidential Data include: data protected by state or federal privacy regulations, data protected by confidentiality agreements, and other information deemed Confidential by the Department. There are additional security and privacy controls that must be applied to Confidential Data.

# Confidential Data

Confidential data includes, but is not limited to:

- Criminal History Information (CHI)
- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Individually Identifying Health Information (IIHI)
- Federal Tax Information (FTI)
- Social Security Administration (SSA)
- Office of Child Support Enforcement (OCSE),
- National Directory of New Hires Data (HDN)
- Educational Information (FERPA)

****Be aware that depending upon where you work, you may be required to take specific training based upon the above types of data.****

# Threats

## Categories of Threats

When you think about threats to information systems and data you can break down the threats into 4 general categories:

1. **Natural** - Disasters such a tornados, hurricanes, floods and electrical storms can cause damage to IT systems
2. **Malicious Outsiders** - Foreign Nations, criminal groups, hackers, spammers, industrial spies, and etc.
3. **Malicious Insider** - Disgruntled employees or vendors, spies, activists, unhappy customers
4. **Accidental Insiders** - Any employee!

## What can you do?

Obviously you cannot control **natural disasters** and threats, but as an employee or private citizen you can make sure that important information and systems are backed up and secured in the event of a disaster.

Protecting yourself from **malicious outsiders** starts with not falling for phishing scams, using strong passwords and surfing the internet wisely.

## The Insider Threat

The **Malicious Insider** makes a conscious decision to deliberately cause harm to an organization; they are fully aware of their actions and recognize the damage or impact it can have on the organization. Some are tech savvy users who react to challenges. They use their knowledge of weaknesses and vulnerabilities to breach clearance and access sensitive information.

The **Accidental Insider** could be anyone. We all have the potential to be an **Accidental Insider**. **Accidental Insiders** often metaphorically "open the door" to **Malicious Insiders** by leaving sensitive data and passwords around or leaving their workstation unlocked.

## Insider Threat continued...

**Accidental Insiders** are how **Malicious Outsiders** gain entry to our information systems or data. The Accidental **Insider** clicks on links in emails or gives away user ids and passwords in phishing scams.

An **Accidental Insider** could be someone who exposes data accidentally - such as an employee who accesses company data through public WiFi without the knowledge that it's unsecured.

**AVOID being an ACCIDENTAL INSIDER!**

## Reporting and Seeking Assistance

## Information Security is EVERYONE'S responsibility

In the event data is lost, stolen or misused, it is important to respond appropriately. Common security incidents and questions include but are not limited to:

- A suspected virus
- Missing file
- Corrupted data
- Inability to connect to a server or workstation
- Lost or stolen laptop
- Lost cell phone
- Confidential information sent to an unauthorized recipient by accident
- Confidential information sent in an unprotected manner

## Your Responsibility

As an employee or contractor, 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 our organization to fulfill its mission
- Disruption of day-to day operations
- Damage to our organization's reputation
- Harm to individual's health or financial status

## Help Desk/Service Desk

Your help desk will NEVER send emails that require you to send personal information via email, external web sites, links or pop-up windows. Any unsolicited request for account information you receive through email, web sites, links or pop-up windows should be considered fraudulent.

## Who do you call?

Employees who discover a security incident or concern must notify their supervisor who then must notify their Help Desk.

****The audience for this training is diverse, so the contact information for the Help Desk or Security department varies. Find the contact information for your organization now and keep it handy in the event of a problem.****

If you are unable to contact your supervisor, you should contact your Help Desk directly.

## IF IN DOUBT - CALL TO REPORT!

## The End!