HRD 2018 - Cyber Security Awareness Training 2018 C28547 Transcript (by Training Module) and Acknowledgement

# You are the Shield

Welcome to Security Awareness training. The purpose of this training is to build your cyber security defenses and make you stronger. Cyber attackers have learned that often the easiest way to get what they want is to bypass technical defenses and target people. They do this by attempting to trick or rush you into making mistakes, such as opening an infected email attachment, sharing your passwords, or giving them sensitive information they should not have access to. These attacks are happening every day. However, the good news is cyber security’s actually not that hard. Once you understand the basics, it becomes easy to protect both yourself and our organization. In addition, many of the lessons you will learn can also be used to protect you and your family at home. Thanks for doing your part to keep us all safe and secure.

# Social Engineering

Social engineering attacks are everywhere. They are one of the most common types of attacks because they are so simple and effective, and technology alone cannot stop them. Social engineering is the art of human manipulation. Attackers trick you into doing something you should not do, such as opening an infected email attachment, sharing your password, letting a stranger into a physically secure area, or sending sensitive information. Because these attacks can take any form, including phone calls, text messages, emails, social media, or even in person, you need to be on alert. Let’s take a look at two examples of social engineering. You receive an urgent text message from your bank. The message informs you that your bank account has expired and your account will be locked. It then gives you a special phone number to call to update your account. When you call the phone number, it’s an automated system that first asks you a series of personal questions to prove who you are. However, this is not really your bank, nor is the system trying to determine your identity. Instead, this is an automated attack by cyber criminals who are attempting to record and steal all your information, including your birth date, credit card or bank numbers, home address, and phone number. Their goal is to steal your identity and financial information. Here is a more advanced social engineering attack. You receive an email that appears to be from your boss. The email is short and urgent. It says that law enforcement is conducting a secret investigation of our organization and that people may have to go to jail. The email then states that you will receive a phone call in 15 minutes from our legal team, and that you are to answer any questions they ask. However, the email is really not from your boss, it’s a fake. The person that calls you 15 minutes later is not really from our legal team, but the same cyber attacker pretending to be a lawyer. They are simply attempting to get you to give up as much sensitive information as possible. So how can you protect yourself from social engineering attacks? Spot them before they happen. Some of the most common clues include someone: Creating a tremendous sense of urgency, often through fear, intimidation, a crisis, or an important deadline. They are trying to rush you into making a mistake. Requesting you to bypass or ignore our security procedures or policies. Asking you for information they should not have access to: Using confusing or technical terms to trick you into taking an action; something too good to be true. (No, you did not actually win the lottery.) If you feel you are under such an attack, simply hang up the phone or ignore the message and contact the help desk or information security team right away.

# Email, Phishing, and Messaging

You get an email in your inbox or a message on your phone. There is a problem with your bank account and details need to be updated right away. All you have to do is click on a link. Before you click, stop and think: this may be a phishing attack. Phishing is a type of social engineering attack that uses emails or messaging the same way bait is used to catch a fish. Cyber attackers send thousands, if not millions, of emails in hopes that someone will take the bait. These emails attempt to fool you into taking an action, such as clicking on a link, opening an attachment, or completing a form. The cyber attackers are not sure who exactly gets these emails, but taking any one of these seemingly harmless actions can get you hooked. So how do you know if an email or message is a phishing attack? Here are some signs to look for: Messages directed to “Dear Customer” or some other generic greeting. The bad guys don’t know who you are; they just try to phish as many people as possible. Messages creating a strong sense of urgency or curiosity. Messages claiming to be from an official organization, such as your bank, but have grammar or spelling mistakes, or the email comes from a personal email account, such as @gmail.com. The From email address is an official organization, but the Reply-To address is someone’s personal email account. Messages requesting highly sensitive information, such as your credit card number or password. You receive a message from someone you know, but the tone or message just does not sound like him or her. Remember, it is easy for a cyber attacker to create an email that appears to be from a friend or coworker. If you receive an email or message with any of these signs, or a suspicious message, report it right away. In addition, before clicking on a link, hover your mouse cursor over it. This will display the link's true destination, so that you can confirm if you are being directed to a legitimate website. On many mobile devices, pressing and holding the link will also show you the true destination. Even better, instead of clicking on the link, type the website's address directly into your browser. For example, if you get an email from your bank asking you to update account details, ignore the emailed link. Simply type your bank’s website address into your browser and log in as usual. When messages have attachments, only open those you were expecting. You are the best defense we have against infected attachments, as anti-virus solutions may not detect all versions of malware. In addition to phishing, take care to not accidentally expose sensitive information when using email or messaging. Email features, such as auto-complete, make it easy for you to accidentally email the wrong person. For example, you may try to email someone in human resources, but because of auto-complete, accidentally email a friend. Remember that once an email is sent, it is no longer under your control. Finally, be careful with the email Reply-All feature. In an email thread with many people, it is all too easy to accidently reply to everyone, when you only want to contact the original sender. It’s everyone’s job to be on alert to phishing and other email and messaging dangers.

# Browsing Safely

When you go online to shop or read the news, you are most likely using a browser. Browsers are one of the primary ways we interact with the Internet. As a result, browsers are a target for cyber attackers. Keep your shield strong against browser attacks by always using the latest version of your browser. Updated browsers have the latest security patches and are much harder to hack into. Not sure if you have the latest browser update? Contact the help desk or the information security team to confirm. Here are some other tips to stay safe online. Stay safe online by not connecting to websites when you receive a warning. Modern browsers can recognize certain malicious websites designed to cause you harm. If your browser warns you that the website you are about to visit is dangerous, close it and find the information you need on a safer website. Before sending sensitive information online, such as submitting your credit card number for online shopping, make sure your browser is using HTTPS, which is a sign of encryption. Encryption scrambles the information passed between your computer and the destination so only the authorized website can read it. Look for signs of encryption, such as the website address starting with HTTPS and a padlock icon in the status bar. Plug-ins or add-ons are small pieces of software added to browsers that are used for additional features, such as playing games, watching movies, or text editing. Every plug-in that is installed in your browser potentially adds additional vulnerabilities. Only install plug-ins or add-ons in your browser if you absolutely need them and you have prior approval. Once installed, just like with your browser, always use the latest version of the plug-in. Finally, when you are finished visiting a website, be sure to log off. This removes sensitive login and password information before closing the browser. Remember, safe browsing behaviors work to strengthen your shield.

# Social Networks

Social networking sites and apps are amazing tools that help us share information and communicate with others from around the world. Unfortunately, these tools also come with unique dangers. Shield yourself by protecting each account with a strong password and always use a different password for each account. In addition, always enable two-step verification whenever possible. Strong passwords are one of the most important things you can do to protect your social networking activity. Here are some other things you can do to stay safe. When posting information, assume anything you post will eventually become public. Privacy controls help, but these controls can be confusing, change often, and may not fully protect you. If you do not want your family or boss to see it, you probably should not post it. Track what your friends, coworkers, and contacts share about you. Ask them to be considerate of your privacy. If you feel a post is inappropriate, ask them to remove the content or report it to the website’s abuse department. In return, be considerate of what you post about others. Just like email and messaging, cyber attackers may attempt to fool you through social networking. A common method cyber attackers use is hacking into a person’s social networking account and then posting messages pretending to be that individual. If you receive any odd or suspicious messages from a friend and you want to confirm if it was really them that sent it, contact him or her in a separate email or phone call. Never respond directly to the post; you could be responding to the cyber attacker. Finally, to keep our organization secure, do not post or share any confidential information about our organization. If you have any questions about what you can or cannot post or share about work, please ask your supervisor.

# Mobile Devices

Mobile devices, like smartphones and tablets, store a great deal of personal and sensitive information, such as your contacts, photos, text messages, and online activity. Protect these devices like you protect your computer. First and foremost, keep track of your mobile devices at all times. You may not realize it, but you are far more likely to lose a mobile device than have it stolen. Always protect each device with a screen lock, such as a strong password, finger swipe pattern, or your fingerprint. This way, if your device is lost or stolen, no one can access the information on it. In addition, enable remote wiping if possible. Remote wiping allows you to erase information if your device is lost or stolen. How else can you keep your devices safe? Always use the latest operating system for your device and keep it updated. Vendors are constantly fixing known vulnerabilities or adding new security features. If your device is old and no longer supports the latest operating system, consider buying a new device. Choose mobile apps from only trusted sources and only install the apps you need. Before downloading, check how many people use an app and its reviews. If an app is new, has few reviews, or lots of negative reviews, then choose a different one. This helps protect you from criminals who distribute mobile apps that look legitimate, but are really programs that infect your devices. When choosing apps, carefully review the permissions. If an app requires excessive permissions, either don’t install it and find a different app to meet your needs or disable those features. Once installed, just like your device’s operating system, always keep your apps updated and current. Never jailbreak or root your mobile device. Not only may your device no longer be supported, but this cripples or disables many of the security features designed to protect you and your information. You may also void the warranty for the device. Disable Wi-Fi and Bluetooth when these services are not in use. Not only does this protect your mobile device from automatically connecting to potentially dangerous networks without you knowing it, it helps improve your device’s battery life. Do not access or store work email or other work data on your mobile device unless you are authorized to do so and security safeguards are in place. Finally, if either a device belonging to the organization or a personal device that has organizational information on it does get lost or stolen, report it immediately.

# Passwords

A weak password is like an open door to cyber attackers. Each of us has a responsibility to shut the door and lock it with a strong password and to use our passwords safely. Keep your shield strong by following these tips for secure password creation and use. Create a strong password by making it long. Every character you add makes it stronger and more secure. Also, make sure your passwords are hard to guess. Avoid using information that is publicly known about you, such as your birth date, pets’ names, or anything you may have shared on social media. Using a passphrase is one of the simplest ways to ensure that you have a strong password. A passphrase is nothing more than a password made up of multiple words, such as the sentence “We need a vacation,” or a collection of random words, such as “happy-quiet-summer-rain.” These examples are strong because they have many characters, yet are easy to both remember and type. In some cases, you may be asked to also include a mix of symbols, numbers, or upper and lowercase letters in your password. Just remember to always use a different, unique password for each account. That way, if one of your accounts is hacked and your password is compromised, your other accounts are still safe. If you have too many passwords to remember, consider using a password manager. This is a special program that securely stores all of your passwords; you only need to remember the password to your password manager. Check with your supervisor or the help desk to see if this is an option. Your password is a secret. Never share your password with anyone else, including coworkers or your supervisor. If anyone else knows your password, it is no longer secure. Protecting your password also means not using public computers to log in to online accounts, such as checking email at hotels or libraries. Since anyone can use these computers, they may be infected with malware. Only log in to accounts from computers or mobile devices that you trust. Some websites use security questions for your accounts. You supply answers to personal questions in case you forget your password and need to reset it. Here’s the challenge: some of these questions or answers can be found online or on your social network accounts. Only use information that is not publicly known about you, or simply make up answers to questions. Finally, some accounts offer something called two-step verification, also called two-factor authentication or multi-factor authentication. While this sounds complex, it is really quite simple. This requires a one-time code in addition to your password to log in. For example, a unique code is generated in a special app on your smartphone that is used with your password to log in. Whenever possible, enable two-step verification so that your accounts are protected by more than just a password by itself. Weak or compromised passwords are one of the most common ways cyber attackers break into organizations or online accounts. If you accidentally share your password with someone else, or believe your password may have been hacked or stolen, be sure to change it immediately and contact the help desk or information security team right away.

# Data Security

Data security is keeping sensitive information protected, whether you are accessing, processing, transferring, archiving, or even destroying it. Protecting our data ensures we maintain our reputation, as well as stay compliant with the numerous regulations and standards. Here are the ways that you can help keep our data safe. We expect you to be able to identify the sensitivity of the information you are working with and the required steps to protect that information. Only use authorized systems to handle sensitive information. Do not copy or store anything to an unauthorized system or account, such as your personal laptop or personal email account. Keep our systems secure by only using authorized and licensed software. Using or installing unauthorized software creates risk for our systems and data. Cloud services, such as Dropbox, Apple iCloud, or Google Drive, are not to be used for storing or sharing sensitive information unless you have prior approval. Always secure sensitive information found in physical form, such as storing sensitive documents in a locked cabinet or drawer when leaving. Use a screen lock on your computer when leaving for lunch or at the end of the day, as this prevents unauthorized personnel from accessing it. If someone calls or emails you asking for sensitive information, authenticate the person first using approved procedures. You are an important gatekeeper; authorize access before sharing sensitive information. When sending or transmitting sensitive information, use secure methods like encryption. It is important to remember that any communication you send needs to comply with our standards for communication. In addition, before you send an email or text message, pause and ask yourself how it would appear if it were displayed in a legal or public setting. Only use mobile media, such as USB drives, with prior approval, and encrypt any sensitive data with approved encryption software. Protect these devices at all times, as they can easily be lost or stolen. If you have privileged access to a system, always log in to that system first with your unique, non-privileged user ID, then elevate your privileges. Do not engage in risky behavior, such as browsing the Internet, while using elevated privileges.

# Personally Identifiable Information (PII)

Our organization handles a special type of information called Personally Identifiable Information, or PII. PII is any information that can be used to identify a specific individual, such as your medical records, bank accounts, and credit cards. It also includes your driver’s license, passport, or national ID cards, like a Social Security number. In the video Data Security, you learned steps for protecting sensitive information. The same steps apply to protecting PII. In addition, PII is a special category of sensitive information. Be aware that single pieces of information can be combined or linked together to create PII. For example, if you pay a medical bill with a credit card, that bill is now linked to your medical record. Your medical record also links your name to other forms of PII, such as your Social Security number. Cyber attackers work to link each piece of information, and this can lead to identity theft or a breach of sensitive information. You can help us protect PII by recognizing the sensitivity of the information you use or access. Only collect PII that you absolutely need. Be on the lookout for files or records containing PII so that they can be secured properly. If you need to share PII, such as sending a copy of a file containing Social Security numbers, find out if the recipient really needs all the information. When possible, remove all PII that you can and then use a secure, approved method to send the remaining information. Another way to protect PII is separating out how information is sent. For example, if you need to share bank account information, send the person’s name, address, and general information through secure means, such as encrypted email. Next, telephone the recipient and share the bank account numbers over the phone. In addition, evaluate whether or not the entire account number is necessary. For example, shorten the data shared and give only the last four digits. When handling PII, be sure you know and follow our policies and procedures for how to securely store, access, and transmit PII. If you have any questions about how to securely handle PII, contact the help desk, privacy, or security team. Finally, help us to improve and update our policies to protect PII. We continually look for secure ways to handle data and protect the data in our care. The people who rely on us are thankful that you guard their PII. You would expect others to do the same with your sensitive information.

# Hacked

Most of the time, you can keep yourself secure by following the simple steps we have covered in this training. Steps such as always keeping your computers and devices updated or always using a strong, unique password for each account. However, cyber attackers are persistent; sooner or later you may be hacked. The important thing to remember is that this can happen to anyone. The faster you recognize the signs of a hacked system or compromised data, and the faster you report it, the more you help to protect us. Here are some of the most common clues to look for. Your anti-virus program has triggered an alert that your system is infected, particularly if it says that it was unable to remove or quarantine the affected files. You get a pop-up message stating that your computer is now encrypted and you must pay a ransom to recover it, or that your computer is infected and you must call a tech support phone number to fix it. Your browser is taking you to unwanted or random websites and you cannot close them. Your password no longer works when you try to log in to your system or an online account, even though you know your password is correct. Cyber attackers will often change your password after hacking your account so they maintain control of it. Your friends or coworkers tell you they are receiving odd messages from your accounts, messages that you know you never sent. You believe you may have accidentally installed suspicious software. Sometimes, you may click on software you did not mean to install and believe it may have infected your computer. If you believe a computer, device, or work account has been hacked, report it right away and do not attempt to fix the problem yourself. Trying to fix a hacked system can cause far more harm than good and corrupt valuable evidence needed by our security team. Instead, stop using the compromised system and contact the help desk or information security team immediately.

# Conclusion

We hope our training has made you more confident defending yourself against today’s cyber attackers. While technology can help protect you, you are ultimately our best defense. Some key things to remember from your training: Cyber attackers use a variety of social engineering methods to trick their victims. If an email, message, or phone call seems odd, suspicious, or too good to be true, it may be an attack. Always use a long, unique passphrase as your password for each of your accounts. In addition, use two-step verification whenever possible. Secure passwords are key to protecting yourself and our data. Ensure your laptop or mobile device has a screen lock enabled. That way, if it’s lost or stolen, the data on it is still protected. Make sure you are always using updated, current software and apps on your computers and mobile devices. Cyber attackers are constantly finding new weaknesses in technology. By always using the latest version, you make it much harder for cyber attackers to break in. If your system supports anti-virus, be sure it’s enabled and running the latest version. Finally, always understand the sensitivity of the information you access or handle and the steps to protect that information, to include how to safely share it with others. If you have any questions about information security or concerns about a security incident, please contact the help desk or information security team right away.

**Proceed to next page – Employee Acknowledgement**

# Employee Acknowledgement

By signing below, I acknowledge that I have read, understand, and agree to abide by the provisions set forth in the ***Cyber Security Awareness Training***.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Print Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Signature                                                       Date