The following information was provided by SANS and discusses IT Security Awareness. It was last updated in 2015.

By completing this module and the quiz, you will receive credit for CW 170, which is required for all employees every two years.
One of the most important things to understand is that you are a target. Many people mistakenly believe that cyber attackers only target our databases or web servers. In reality they also target individuals like you. While these attackers use a variety of sophisticated tools, they have learned that the simplest way to hack into an organization like ours is by targeting people like you.

Let’s take a look at how a group of cyber attackers might hack into our organization.
While the following story did not happen, it illustrates common methods used to hack into an organization like ours.

Several months ago, a team of cyber attackers decided to target our organization. We are not sure what their motivation was. Perhaps they wanted to steal our sensitive information, make a political statement, or gain access to one of our partners. All we know is that they began searching our website several weeks ago, learning everything they could about us. This included who we are, how we operate, and the identities of employees and staff.
They then began to harvest employees’ personal information from websites such as Facebook, YouTube, LinkedIn, Instagram, and public forums. Unfortunately, several employees had posted too much information about themselves and our organization.

As a result, the hackers were able to build a complete picture of our organization and learn details about key members of our staff. Armed with this information, they launched their attack.

Seven employees at our organization received emails that appeared to come from a package delivery service we commonly use.
While these emails appeared to be legitimate, they were actually phishing emails sent by the attacker. Each message contained an infected email attachment designed to bypass our anti-virus software and silently infect our computers. Unfortunately, two of the targeted employees fell victim to the phishing emails by opening the attachments.

And since their computers were not patched, they were quickly infected, giving the cyber attackers complete control.
The attackers then installed key-logging software on the computers, enabling them to capture all of the employees’ keystrokes. On one of the hacked computers, an employee was using a login and password they had shared with their coworkers.

The attackers quickly harvested this information and were able to log into other systems throughout our organization. Because the attackers were using stolen, legitimate passwords, our security team did not detect the attackers.

Over the next seven days, the attackers scanned the hard drives of numerous compromised systems, stealing every document, spreadsheet, and presentation they could find. They soon transferred over 150 Gigabytes of confidential information out of our organization, including a key project we had been working on for over three months.
Fortunately, an alert employee noticed several suspicious programs running on their computer and reported it.

As a result, the attackers were finally detected and blocked from causing any more harm.
While this is only an example provided for illustrative purposes, it demonstrates why we have security policies and controls.

They are carefully designed to protect you and our organization, while also ensuring that we are compliant with important standards and regulations. This is also why it is so important that you understand and follow our security policies.
You may not realize it, but you are even under attack when you and your family connect to the internet at home. To help protect yourself, your family and our organization, always remember some core principles:

- Always be cautious and assume you are a target. You may not think you or your information has value, but it does.
- Attacks are a constant threat on the internet. If something seems suspicious or too good to be true, it most likely is.
Now, let’s learn how cyber attackers compromise our computers and steal our information. One of the main techniques they use is called social engineering, which is also known as the art of human manipulation.

This is when attackers pretend to be someone or something you know or trust, such as your bank, a government organization, or even a friend or coworker. They then leverage that trust to get what they want, often by simply asking for it.

Let’s take a look at a real world example of such an attack.
You receive a phone call from someone claiming to be from a computer support company. They explain that your computer is behaving strangely, doing things like randomly scanning the internet, and they believe it is infected.

They tell you they have been tasked with investigating the issue and helping you secure your computer. They then use a variety of technical terms and take you through confusing steps to convince you that your computer is infected.

For example, they may ask you to find specific files on your computer and explain how to find them. When you locate these files, the caller will explain that they are a sign that your computer is infected.

In reality, these files are just common files found on every computer.
Once they trick you into believing your computer is infected, they will pressure you into going to a website and buying their security software.

However, the software they are selling is not really security software. It is actually an infected program that will give them total control of your computer.

In the end, not only have they fooled you into giving them control of your computer, but you just paid them to do it.
Social engineering attacks like these are not just limited to phone calls. Attackers can use almost any technology to fool you, including email, instant messaging, or text messages, and can even do it in person.

Remember, social engineering is nothing more than an attacker building trust with you, then abusing that trust to get what they want.

If you get an email, message, or phone call that seems odd, suspicious, or too good to be true, it may be an attack.

Common indicators of a social engineering attack include:
• People asking for information they should not have access to
• Using a lot of confusing or technical terms
• Creating a sense of urgency
If you believe someone is attempting to trick or fool you, simply hang up the phone or ignore the email and immediately contact the ITS help desk or information security team (ISO).
Email is one of the most powerful weapons in the cyber attacker’s arsenal, simply because so many people depend on it for their daily lives.

With email, an attacker can easily pretend to be someone or something you trust, such as your friend or your bank.

These attacks, often called phishing, work by tricking you into doing something seemingly harmless, like clicking on a link or opening an attachment.

For example, here is a phishing email pretending to be a well-known bank. The email is very professional looking, including the bank’s logo. The email says there is a problem with your account and that if you do not update your account immediately, it will be deactivated. It then requires you to click on a link and log into a website.

If you click on this link you are taken to a website controlled by the cyber attacker, who silently hacks into your browser, infects your computer, and takes control of it.
Alternatively, attackers will send emails with infected attachments instead of links. Here’s an example of what appears to be an email from a legitimate organization.

However, the attachment would silently infect your computer if you opened it.
In addition to general phishing attacks that can target anyone, attackers can utilize a more specialized attack called spear phishing. This is a highly targeted attack where only a few emails are sent to specific individuals within our organization. These emails appear very realistic, often with a subject that is relevant to the victim's job or appear to come from individuals that the victim highly trusts. Spear phishing attacks are harder to detect, but also require more work and research by the attacker.
Finally, there is Messaging. Just like email, almost any type of messaging can be used for phishing attacks, such as those on Facebook, Skype, Twitter, or your smartphone. Always be careful of messages, regardless of what technology you use.

In most cases simply opening an email or reading a message is safe. For most attacks to work, you have to do something after reading the message, such as opening the attachment, clicking on the link, or responding to the request for information. To protect yourself, keep the following in mind. Just because a message appears to come from a friend or someone you know does not mean the message is safe. Cyber criminals may have infected their computer, hacked their account, or spoofed the “From” address. If you are suspicious about a message from someone you know, call the person to verify if it they really sent it.
Be suspicious of any email directed to "Dear Customer" or some other generic salutation.

Be skeptical of any message that requires "immediate action", creates a sense of urgency, or threatens to shut down your account.

Be suspicious of messages that claim to be from an official organization but have grammar or spelling mistakes. Most organizations have professional writers and do not make these mistakes.
Before you click on a link, hover your mouse cursor over it, this will display the true destination of where the link will take you. Confirm that the destination displayed matches the destination in the email and make sure it is going to the organization's legitimate website. Even better is to type the proper website into your browser. For example, if you get an email from your bank asking you to update your bank account, type your bank's website in your browser, then login to the website directly.

On a mobile device? No problem. Simply hold your finger down on the link and you should see the true destination in a pop-up window.

Be careful with attachments and only open attachments you were expecting. Many of the infected attachments sent today can bypass most anti-virus programs.
Remember, sometimes you are the greatest risk to your email. Always double check that you are emailing the correct person before sending one, especially when sending something sensitive.

For example, with email features like auto-complete, you may try to email someone in finance but accidentally end up emailing an old friend.

Safely using email and messaging is ultimately about common sense. If a message sounds suspicious or too good to be true, it is most likely an attack. Simply delete the message.

If you get a message and you are not sure if it is an attack, contact your help desk or information security team (ISO).
Browsers are one of the primary ways we interact with the internet. We use them to read the news, shop online, and watch movies. But browsers also provide a window into our computers and are one of the most dangerous applications we use.

Cyber attackers have developed numerous techniques for attacking your browser. A common technique they use is to place tools designed to hack into your browser on websites that you might visit. The malicious tools then silently probe your browser and launch multiple attacks when you visit the site.

If your browser or any of your plugins are outdated or vulnerable, your computer will most likely become infected.
Unfortunately, there is no simple way to tell if a website is safe or not, so it important to take some simple precautions.

First, most browsers maintain a list of known malicious websites that intend to cause you harm. If you accidentally visit one of these known websites, your browser will post a warning like you see here. If your browser warns you against visiting a website like this, do not connect to it.

Always use the most current version of your browser and ensure it is up to date. This prevents attackers from exploiting known weaknesses and is one of the most effective ways to protect yourself. Do not install plug-ins or add-ons for your browser unless you absolutely need them and have prior approval. Plug-ins make it easier for attackers to hack your computer.

If you do have plug-ins installed, make sure they are as up-to-date as your browser.
Be sure your connection is encrypted whenever you connect to sensitive websites, such as online banking. Look for signs of encryption, like the website address starting with https and a padlock icon in the status bar.
Finally, always be sure to scan any files you download with anti-virus.
Mobile devices, such as smartphones and tablets, have become incredibly powerful. Not only can you call anyone in the world, but you can watch movies, read your email, bank online, and even install apps.

These combinations of factors make mobile devices very useful. However, it also can put you at great risk.

To protect yourself, we recommend the following:

Just like with your computer, install only apps that you need and make sure you download them from trusted sources. Criminals can create apps that look real, but are actually malicious programs designed to quietly take control of your devices.

In addition, do not install apps that request excessive permissions, such as the ability to silently send text messages or copy your address book.
Just like with your computer, backup your mobile device on a regular basis. This way, if something happens to the device, your information is not lost.

Make sure you update your mobile device and apps on a regular basis. Cyber attackers can more easily exploit your devices if you are running outdated software.

If your mobile device is old and no longer supported, consider purchasing a new one that can support the latest version of the operating system and security updates.

Never jailbreak or hack your own mobile device. Not only may your mobile device no longer be supported, but this usually cripples or disables many of the security features designed to protect you and your information.

If you have security software installed, such as anti-virus or a firewall, then make sure they are enabled and updated with the latest version.
Remember that many of the attacks you find in email can also happen via texting on your mobile device.

For example, cyber criminals can text messages asking you to connect to malicious websites, download infected apps, or ask you for private information such as your bank account.

If a text massage seems suspicious or too good to be true, simply delete it.
Be careful when using Wi-Fi. Many mobile devices will automatically connect to Wi-Fi networks without asking you, putting your device at risk. Disable Wi-Fi if you are not using it.

Attackers can also take advantage of your Bluetooth capabilities. Just like Wi-Fi, disable Bluetooth when you are not using it.

It is also important to turn off Bluetooth discoverable mode features.
Do not access or store work email or other data from our organization on your mobile device unless you’ve been authorized to do so and the appropriate security safeguards are in place.

Finally, when you lose a mobile device anyone can access all of your information including your emails, pictures, or contact lists, unless it is protected. Protect your devices with a hard-to-guess password or PIN.

If your device supports encryption, we recommend you use it.

Also, consider enabling remote wiping if available. This means, if your mobile device is lost or stolen, you can erase all your information remotely.

If you lose a device issued to you by the university or a device that contained any organizational information, notify the help desk or information security team (ISO) immediately.
Once someone knows your password they can steal your identity or access all of your personal information. Let’s learn what makes a good password and how to use them securely.

There are two key points to good passwords.
First, you want passwords that are hard to guess. This means do not use passwords such as 123456, your pet's name, or your birth date.

Second, use passwords that are easy to remember. If you keep forgetting your passwords they are not very helpful.

The problem is cyber criminals have developed sophisticated programs that can to guess or brute force your passwords, and they are constantly getting better at it. This means they can break into your accounts if your passwords are not strong enough. To protect yourself you want your password to be as long as possible. The longer your password is, the stronger it is.

In fact, instead of using just a single word as your password, use multiple words. This is called a passphrase.
For example, your passphrase could be something simple like: time for chocolate! To make your password even more secure, do the following:

- Use a number in your passphrase
- Have at least one lower case and one upper case letter in your passphrase
- Use a symbol in your passphrase

Let’s take our passphrase and make it even more secure by replacing some of the letters with numbers and symbols, as we just discussed.
First, notice how at least one of the words starts with a capital letter. Then we can replace letters with numbers or symbols. For example we can replace the letter 'a' with the '@' symbol, or replace the letter 'o' with the number '0'. In addition, we can add symbols by using common punctuation, such as spaces, a question mark, or an exclamation point. As a result we now have a strong password that is very difficult for cyber criminals to compromise, yet is simple to remember and easy to type.
In addition to strong passwords, you must protect how you use them.

Be sure to use different passwords for different accounts. For example, never use the passwords for your work or bank accounts as your personal accounts, such as Facebook, YouTube or Twitter. This way, if one of your passwords is hacked, the other accounts are still safe.

If you have too many passwords to remember, consider using a password manager. This is a special program you run on your computer that securely stores all your passwords for you. The only passwords you need to remember are the ones to your computer and the password manager program.

Check with your supervisor, the help desk, or the information security team to see if a password manager is an option you can use.

Never share your password with anyone else, including a fellow employees. Remember, your password is a secret; if anyone else knows your password it is no longer secure.
Do not use public computers, such as those at hotels or libraries, to log into a work or bank account. Since anyone can use these computers, they may be infected with malicious code that captures all your keystrokes. Only login to your work or bank accounts on trusted computers or mobile devices you control.

If you accidentally share your password with someone else, or believe your password may have been compromised or stolen, be sure to change it immediately.

Be careful of websites that require you to answer personal questions. These questions are used if you forget your password and need to reset it. The problem is the answers to these questions can often be found on the Internet, or even your Facebook page. Make sure that if you answer personal questions you use only information that is not publicly known.
Many online accounts offer something called two-factor authentication, or two-step verification. This is where you need more than just your password to log in, such as codes sent to your smartphone.

When possible, always use these stronger methods for authentication.

Finally, if you are no longer using an account, be sure to disable or delete it.
Encryption is a process that protects your information by making it unreadable or unusable by anyone that does not have your key. For example, encryption protects the information on your laptop in case you lose it or secures your credit card information when you make a purchase online.

When information is not encrypted, it is called plain-text, like you see here. This means anyone can easily read or access it.

You should encrypt sensitive information to protect it. This converts the information into a non-readable format called cipher-text.

Encryptions use mathematical formulas called algorithms, and a unique key to convert your information into cipher-text. The key is what locks or unlocks your information, just like a key can lock or unlock a door.
A common example of a key is a password, and only people who have that key can decrypt and unlock your information.

To protect your encrypted information you need to protect your key.

Examples of things that can be encrypted include the following:
• Mobile devices, such as your laptop, smartphone, or USB sticks
• Communication protocols, such as Voice over IP or Instant Messaging
• Electronic files or folders
• Your browser’s connections to websites, such as online banking, social networking sites, or online shopping

To learn more about encryption and how to use the different encryption technologies we support, contact the help desk or information security team (ISO).
Just like your work computer, your personal computer is also a target.

To protect yourself and your family, we recommend you take the following steps to protect any personally owned devices:

- Always be sure your computer or mobile devices have the latest patches installed and are running the latest versions of any installed software, such as your word processing software.

The simplest way to do this is to enable automatic updates on your computer and mobile devices.

In addition, some programs or mobile apps may have their own automatic updating options. If so, be sure they are enabled.

If you are no longer using a program, remove or uninstall it.
In addition to programs, you should ensure your browser and browser plugins or add-ons are up-to-date.

Every plugin you add to your browser becomes another potential avenue for attack. Only install browser plugins you absolutely need and delete them if you are no longer using them.

Consider using your browser in private mode to help protect your online privacy. This is a common feature that most browsers support.

When your browser is in privacy mode, it does not record what websites you visit, it does not cache website content, and usually wipes any cookies stored on your system.
Make sure your computer’s firewall is enabled and you are using updated anti-virus. However, you need to understand that anti-virus only detects and stops known malware. Attackers are constantly developing new malware variants that anti-virus cannot detect.

As such, having anti-virus installed does not mean your computer cannot be infected.
Finally, be sure you are doing regular backups of your information, such as family pictures or valuable documents.

If your computer does get hacked, often the only way you can recover it is by reinstalling your operating system and recovering your personal files from a backup.

Ultimately, you are your own best defense for your computer and mobile devices. Always use common sense. If something seems odd or too good to be true, it may be an attack.
Unfortunately, cyber criminals are extremely persistent. Sooner or later you may be compromised.

In this section we are going to show you what to look for and how to respond when you have been attacked. Remember, the faster you notice that you’ve been attacked, and the faster you notify someone to respond, the less damage cyber criminals can do.

Unfortunately, there is no simple way to determine if you are hacked.
Often when your computer or your account is compromised, cyber criminals take steps to make it difficult for you to find out.

Your computer may be reprogramed to lie to you, to tell you everything is okay.

However, here are some things you can look for as indicators that you have been attacked.

First, your anti-virus generates an alert. Your anti-virus software should scan your computer every time you save, open, or run a file. If it finds a virus on your system, your computer may have been hacked.
Second, your browser is taking you to unwanted websites or random websites open on your screen and you cannot close them.

Sometimes cyber criminals will reprogram your computer to take you to websites that you do not want to go to.
Third, your passwords no longer work.

Cyber criminals will often change your password after hacking your account so they maintain control of it.

Fourth, your friends or co-workers tell you they are receiving odd messages from your Facebook, Twitter, or email accounts that you know you did not send.
Finally, you believe you may have accidentally installed suspicious software. Sometimes you may click on software you did not mean to install, and now you believe you may have infected your computer.

If you believe your computer, mobile device, or work account has been compromised, do not attempt to fix the problem yourself. Instead, stop using it and contact your help desk or information security team (ISO) immediately.

Play it safe. It is far better to report a system that is not compromised, than it is to fail to report a system that is compromised.
We hope you have enjoyed the presentation.

We have covered who is targeting you, how you are being targeted, and what you can do to protect yourself. Some key lessons from this training include:

• Remember you are a target; cyber criminals are attempting to compromise your computers, mobile devices, accounts, and information
• Be suspicious. If an email or phone call seems too good to be true, it may be an attack.
• Always ensure your computer, mobile devices, and applications are updated and running the latest version
• Always protect our organization’s confidential information. Ensure our data is securely stored and only share it with authorized people who have a need to know.
Remember, our goal is not to scare you from using the internet. Technology is a tremendous tool that enables you to accomplish amazing things.

Our goal is for you to leverage the latest technology while protecting yourself, your family, and our organization.

If you have any additional questions about information security, please contact your help desk or information security team (ISO).
Unless given other instructions by email, follow these directions to receive credit for this class:

- Close this document and go back to the Training Library.
- Then open the “Review” document for CW 170.
- When you finish the paper quiz, please return to University Compliance Services.