FORTINET
NSE Training Institute

Lesson 1: Bad Actors

Every day, every hour, people of all ages, all over the world, are at risk of consequence from cyber threats.

While you're watching this video, I find many ways to trick people into telling me their account names and passwords directly. This is what I call phishing. And here's, how it works.

First, I set up a web server with a login page that looks identical to the one I want to break into. Then, I'll redirect their browser to the real login page where they can log in and think that everything's OK. Then, I send a specifically crafted email that looks like it was sent by the real system that will include a handy link.

However, that link doesn't take them to the real system; it takes them to my special web server that is masquerading as the real system.

By the time they get into the real system, I have their credentials and can log in as them. And the best part, most of the people will never know.

And this is just the beginning.

Who are we? Simple. We're the ones motivated by political, social, or moral outrage representing things we collectively don't agree with.

I'm the guy who sends bogus network requests to our victims, to attack what is known as a distributed denial of service attack. While we get millions of computers worldwide.

How do we get all those computers? Easy, we set up a botnet. A command and control server accessible on the internet, that through a malware installed on some unsuspecting computers will wait patiently for instructions from the command and control server.

But a common method is to put a software installer as an attachment to spam email. Let's say, a bank error in your favor. By the time they open the attachment to find out more and realize that it isn't real, we already installed a botnet software on their computer.

And the best part, they have no idea.

Our ideology intimidate and strike terror into the hearts of our enemies by causing disruption, mayhem, and damage. Do you know who we are? Yes, we are cyber terrorist.

A group not usually well-funded, but with a lot of ingenuity to attack our enemy high profile targets, capable to disrupt internet services with DDoS attacks, infiltrate systems to steal sensitive data, or expose the personal data about people we want harmed. We also threaten to corrupt critical information, hoping to throw entire industries into disarray.

But how can we accomplish all this with few resources?

Easy, through spear phishing, a simple technique where we send emails only to specific people we want to target. Once we've infected the computer that they use, we know that we can get to the more serious stuff. Which in the end, is what we really want.

Our motivation? What moves the world? Money. And what do we do?

Though our presence is purely online, we utilize existing malware to target point of sale credit card terminals. Yes we are cyber criminals, and here is what we're capable of doing.

Getting into a network and stealing the credit card data, we can sell that info to any number of buyers. Or even use those credit cards ourselves.

Once we're inside that network, we can also grab the personal information about other customers.

Then, there's ransomware. This allows us to extort money directly from the owners of infected computers, holding their data for ransom.

Usually it means infecting a computer with software, that will encrypt a computer's hard drive and display a message demanding the payment of some amount of bitcoin in trade for the encryption key to get their data back.

The best part, the more computers that get infected, the more money we make.

Our missions include espionage, extortion, and embarrassment.

Using targeted cyber weapons, to disrupt, damage, or destroy critical infrastructure. We are cyber warriors, and we're a well-funded group that act in the national and military interests of our country's government. And have the resources to not only use any exploit method that exists, but also develop new ones on our own.

Have a seat, and just watch what we are capable of doing.

Our well-known methodology, is to leverage unmatched vulnerabilities in common operating systems and applications. You can call it zero day. Because you have just learned of the cyber threat, and the solution to fix it has not been created.

Hopefully, we are the only ones who know about the vulnerability.

If it comes time that we have to launch an attack that uses an exploit of an unpatched vulnerability, then most likely it won't be long until someone figures out how that attack worked.

Then the software vendor will almost always issue a patch right away, that's why once we use one, it has a pretty short shelf life before it's no longer usable again.

Like I said, this is why we keep it a secret.

Now that we know the risks, we can be more careful and better prepared. We live in a connected world, and it is everybody's job to make it safe.

Lesson 2: Data Security Perspectives

Hi. I'm Chloe. Welcome to the InfoSec-Awareness Series (IAS): Data Security lesson. Let's talk about your role as an internet user, and how cyberthreats affect your experience whether at home, at work, or traveling.

Information Security, also known as InfoSec, is important to people of all ages. It's a team sport and we each have a role to play. As technology continues to rapidly change in this Information Age, we have a shared responsibility to make cyberspace a more secure environment for ourselves and for future generations.

While a lot of training and education content is geared towards security for organizations, we want to provide suggestions for how individuals can be safe on the internet. Whenever you're online, you're vulnerable, and thwarting evolving cyberattacks demands constant vigilance. We like to think of it as becoming a human firewall. It's common sense. You can outsmart attackers with security awareness. By learning what actions you can take as an individual user, you can reduce your risks online. Let's start!

For data protection, security and privacy go hand-in-hand. Data privacy relates to business policies that define appropriate data management such as collection, retention, and deletion. Cybersecurity comprises methods for protecting networks, devices, and data from unauthorized access, and ensuring the confidentiality, integrity, and availability of all that information. Information Security includes cybersecurity and physical security.

Here are a few important terms to help you understand some of the risks:

- Vulnerabilities – are flaws in software, firmware, or hardware that an attacker can exploit to perform unauthorized actions in a system. Attackers take advantage of these errors to infect computers with malware or perform other malicious activity.
- Attackers – seek to exploit vulnerabilities in software and computer systems for their own gain, and their actions are typically in violation of the intended use of the system. Threats range from mere mischief to stealing or altering information.
- Attack surface – is any exposed place in your environment that a bad actor can use to gain entry to, or extract something valuable, the places that you want to protect. After gaining initial access to a network, adversaries traverse the allowed communication paths between network devices to gain deeper access. Therefore, it's the goal of cybersecurity professionals to identify all the attack surfaces, reduce their size, and decrease the risk of attack.
- Malware – is an unwanted file or program that can cause harm to a computer or compromise data stored on a computer. Examples of malicious code classification include a virus, worm, botnet, Trojan horse, DDOS, and ransomware. Malicious data files are non-executable such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file that exploits weaknesses in the software program used to open it. Attackers frequently use this to install malware on a victim's system, commonly distributing the files via email, social media, and compromised websites.
- Social engineering – is extremely lucrative because people are deceived into believing it's legitimate. The goal of a social engineer is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or another entity, and giving them access to your network. Threat actors prefer the path of least resistance —why waste an expensive zero-day when social engineering works— they hack the psyche of targets, who rarely realize the disguises, as well as rely on publically available intelligence and interactions to generate victim profiles. These scams lure victims by appearing trustworthy, and they leverage emotional triggers, such as curiosity, urgency, and intimidation.

Nowadays, it seems that everything relies on the internet: email, smartphones, video games, social media, applications, online shopping, medical equipment and medical records. The list goes on. The downside is that cyberthreats pose a serious risk to your business as well your personal data. For example, malware can erase your entire system, an attacker might break into your system and alter your files, a cybercriminal can use your computer to attack others, or an attacker might steal your credit card information and make unauthorized purchases. There is no guarantee that even with the best precautions, some of these things won't occur. However, there are steps you can take right now to minimize the chances. The first step is to recognize potential cyber risks.

Just as technology continues to move forward, making our lives easier and more connected, cybercriminals use sophisticated techniques to compromise technology and online habits. Attackers like to exploit social media content, even our vacation plans, because these activities require you to provide sensitive information online. Always remember, highly sensitive and private information requires vigilant protection. For example, your personally identifiable information (PII) includes anything that can distinguish you, such as your full name, your birthday, biometrics, your passport, ID, credit card, or phone numbers, and your home or email address. You must also protect your company proprietary data. Sharing sensitive information online presents a huge opportunity for cybercriminals to commit credit card fraud, identity theft as well as compromise your access to company proprietary resources, simply put: data is the new gold. That’s why it is imperative to follow privacy and data protection laws at work.

For each business role, the acceptable level of risk to cybersecurity and privacy must be documented. Industry-recognized security practices must be incorporated, and appropriate safeguards implemented to protect personal information as well as data, systems, activities, and assets of an organization. The goal is to create a security-minded workforce.

Cybercrime is a global threat with no borders. Consequently, regulatory industries and governments, such as the General Data Protection Regulation (GDPR) in Europe, as well as the USA, Australia, Japan, and China have prioritized the security of information with new laws and compliance standards. Remember to be the protector of your information. Human error accounts for nearly all data breaches! Be wary of suspicious requests, unknown attempts at contact, and unsolicited information that comes to you in any form of communication. Ask your company’s Privacy Office if you have any questions. They are there to help you navigate these risks and can provide recommendations on how to be cyber safe.

Let’s review why attackers have such a high success rate. Malicious attacks are constantly increasing. Research shows that 91% of cyber incidents that occur inside an organization are caused by some form of human error such as inadvertently clicking a spearphishing email. Privileged access abuse is linked to an estimated 80% of data breaches. In a world where the odds are heavily tipped in favor of cyber adversaries, data security must take precedence.

When it comes to cybersecurity, knowledge is power and that’s why, by implementing actions you can take, you can avoid common traps. Be cyber safe out there!

Thank you for your time, and please remember to take the quiz that follows this lesson.

Lesson 3: Password Perspectives

Hi. I’m Steve. Welcome to the InfoSec-Awareness Series (IAS): Password lesson. Let’s talk about your role in protecting sensitive data by using a unique and strong password.

First, if you keep your password written down on a note under your keyboard, please stop. Dispose of it today, and do not place that note in the trash. Shred it! In addition, keeping default credentials on any device is the very worst kind of password because it makes it so much easier for attackers. Hackers maintain databases of common credentials, especially for targeted systems that are connected to the internet. For example, here’s a list of the most commonly used, really bad passwords. Don’t use them!

- 123456789
- 12345678
- 1234567
- 123456
- 12345
- 123123
- 111111
- 666666
- 654321
- Qwerty
- qwerty123
- Abc123
- Aa123456
- !@#$%^&*
- Passw0rd
- password1
- admin
- charlie
- Donald
- football
- iloveyou
- monkey
- Password
- Princess
- sunshine
- welcome
- zzxxccvvbb

Remember, the best password is a strong passphrase with a different combination of random uppercase and lowercase letters, numbers, and special characters that is difficult to guess, even for someone who knows personal details of your life. Do not make it easy for hackers to compromise your accounts by using a bad password. To sum it up, passwords are like your toothbrush: you want to choose a good one, never share it, and replace it at least twice a year. Always change default passwords and make sure all your passwords are different for each account. That way, if an attacker breaks into a system they will only have the password for that one account. All the remaining accounts will still be inaccessible to them.

Now, I know what you're going to say: I can't remember all these passwords, and that's understandable. Fortunately, there are password manager applications that will create and save strong passwords for you, and then securely let you retrieve them when needed. We recommend you chose a reputable password manager. Ask around, do some research, find one that works for you, and make sure your master password is strong. If you are installing an application onto a mobile device, remember to download it from the official app stores. Just one suggestion though, be careful where the password manager stores your passwords. If it's in the cloud or an off-device storage, then any attack on that storage will possibly give the bad guys all your passwords.

This brings us to multi-factor authentication or MFA where the system requires at least two separate elements to allow access. In most cases, this consists of something you know, like a password, along with something you have, which can take different forms, such as a physical token that shows a number that quickly changes. To use a token, you look at the display and enter the number string that it says in the logon prompt along with your password. The hardware token is synchronized with the system that you're logging into so that even if your password is compromised, an attacker won't be successful without the hardware token, and because it’s constantly changing, even if an attacker sees what you enter from the token, it’s likely no longer valid.

Another option is a software token, which often takes the form of an application loaded onto your smartphone. They work the same as a hardware token but you use your smartphone to call up the code. Alternatively, some systems simply issue a one-time code to allow you access, and it is transmitted to you in a secure way that is set up in advance. The recommendation here is, if a vendor has an MFA option, it's going to be more secure than just the password alone. Truthfully, no matter how strong your password is—a breach is always possible. All it takes is for just one of your accounts to be hacked, and your important information can become accessible to cybercriminals. Bottom line: continuously prioritize protection for all accounts with elevated privileges, remote access, and high value assets by enabling MFA. That way, you ensure the only person who has access to your account is you for email, banking, social media, and any other service that requires logging in.

Here's a topic that we all know about, and don't want to think about. Backups. I hope everyone knows that to protect your data, you must back it up regularly. Don’t forget, to defend against a data disaster it is crucial to also password protect your data backups. If something happens, like a ransomware attack, having recent backups available will help you to restore your valuable data without worrying about paying the ransom. We're not going to recommend any particular backup solution, just make sure that whatever you choose allows you to restore from any particular point in time in the past, plus integrates encryption as an extra layer of data protection. If your sensitive data is accidently compromised, it is rendered useless. Also, be careful with where your backups are stored. Some ransomware attacks will also encrypt the back-up drive if it is physically attached to your computer 100% of the time.

While not particularly a security topic, it might also be a good time to think about archiving your very important files and documents, such as photographs for future generations.

When it comes to cybersecurity, knowledge is power and that’s why, by implementing actions you can take, you can avoid common traps. Be cyber safe out there!

Thank you for your time, and please remember to take the quiz that follows this lesson.

Lesson 4: Internet Security Perspectives

Hi. I'm Chloe. Welcome to the InfoSec-Awareness Series (IAS): Internet Threat lesson. Let's talk about your role as an internet user, how cyberthreats affect your experience, whether at home, at work, or traveling, and the stakes involved.

In our lifetime, technology has exploded with digital ones and zeros that drive nearly every facet of our existence. Emerging technologies, such as artificial intelligence (AI), machine learning, 5G, quantum computing, and evolving technologies, such as cloud, autonomous vehicles, and connected devices in the internet of things (IoT) are targets that must be safeguarded against compromise. In fact, every second more than a hundred new IoT devices are connected to the web. As this cyberthreat landscape continues to increase, we must expand our security awareness. Cybersecurity is a shared responsibility. We each have to do our part to keep the internet safe.

First, be vigilant! Criminals rely on social engineering to compromise systems simply because it works. Therefore, we must understand the myriad of social engineering scams. Social Engineers, also called Threat Actors, try to influence behavior, and human error accounts for nearly all data breaches. The goal of a social engineer is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or another entity, and giving them access to your network.

Here are examples of social engineering:

- Juice Jacking – compromised public charging station that installs malware when a portable device plugs in from public areas, such as an airport, train station, or conference arena
- Phishing – weaponized email that masquerades as reputable, lures targeted groups into taking an action, and only requires one victim to be successful
- Ransomware – malware payload that prevents access to computer systems, demands a sum of money to be paid to retrieve the data, and email is the predominate attack vector because it relies on a single click to circumvent controls
- Spearphishing, Whaling, CEO Fraud, and Business Email Compromise (BEC) – fraudulent, weaponized messages that target a specific role or person and is often financially motivated

Bait happens. Alternatively, when you become a human firewall, you make it harder for an attacker. Simply use common sense and awareness whenever something feels even remotely suspicious.

Now let's talk about mobile security. Most of us keep our mobile devices with us throughout the day. We check them frequently, and even keep them at very close range while we sleep because these devices enable access to information anytime from anywhere. Today, they conduct more than half of all internet traffic, and the distinction between a mobile device and a PC is hazy. Because your portable device can contain vast amounts of sensitive information, they are very attractive targets, and provide lucrative opportunities for criminals that are intent on exploiting them. With enticing data from mobile app activities, such as banking, social networking, emails, maintaining calendars and contacts, mobile e-commerce, as well as GPS information, a multitude of vulnerabilities exist. For example, vulnerabilities in the technology layers of a mobile device, as well as SMS, MMS, Bluetooth, and the synchronization between computers and mobile devices are potential attack vectors that extend the capabilities of malicious actors.

Cybercriminal activity targeting mobile devices can have dire consequences, including stealing critical data, tracking users, and denying access to their devices. Your mobile device can also be used as a launching pad for more lucrative attacks aimed at enterprise systems, social networks, and cloud platforms.

To help mitigate threats affecting these vulnerabilities, secure your Wi-Fi network. Technically, the term Wi-Fi stands for wireless fidelity, and your wireless router is the primary entrance for cybercriminals to access all of your connected devices at home. Always secure your digital devices. Before connecting to any public wireless hotspot, such as on an airplane, in an airport, hotel, or café, confirm the name of the network and login procedures with appropriate staff to ensure the legitimacy of the network.

Public hotspots are always a security risk. To protect against the threat of juice jacking, think twice before using a seemingly convenient charging station at the hotel, airport, or train station. Instead, invest in your own portable charger. Those free charging ports might be loaded with malware that will infect your device and give attackers easy access to all your data. If devices on your network are compromised, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.

We all want to do the right thing. So let’s develop good traveling habits for protecting our portable devices, such as:

- Avoid joining unknown Wi-Fi networks
- Use Multi-Factor Authentication (MFA)
- Back up your data
- Avoid opening files, clicking links, or calling numbers from unsolicited messages
- Change the factory-set default username and password on every device
- Delete all information stored in a device prior to discarding it
- Disable features not currently in use, such as Bluetooth infrared, or Wi-Fi
- Encrypt all sensitive data and communication paths
- Enable screen lock, using a strong password or personal identification number (PIN)
- Follow your company policies and data handling guidelines
- Maintain up-to-date software and operating systems
- Never leave your portable device open and unattended
- Power down your device or put it in airplane mode prior to storing it
- Set Bluetooth-enabled devices to non-discoverable
- Turn off automatic connections when not in use

Now, let’s talk about email. We spend a big part of our day dealing with our inbox. In fact, 300 billion emails are sent across the globe every single day. Email is the number #1 infection vector for all kinds of malware, including ransomware. A common form of malware transmission is via attachments. If you receive an email with an attachment, and the email is from someone you don't know, you probably should not open the attachment.

Let’s back up, and talk about how your received these emails in the first place. No matter if it's classic spam or phishing, someone has your email address and it's been passed around amongst the spammers. While it’s difficult to keep your email address completely secret, there are ways to make your email address seem less valuable to spammers. One of the more effective ways is to configure your email client to not display downloaded graphic images. With spam, the mere act of downloading images tells the spammers that there's a person actually looking at the email. This increases the value of your email address as a target. Most email clients that support this option will allow you to download the images for legitimate email messages. That way, they look well formatted and easier to read. Generally, spam doesn’t request an action, and to prevent further messages from the sender, simply mark that email as junk and block the sender.

Let’s delve into Phishing, Spearphishing, Whaling, CEO Fraud, and Business Email Compromise (BEC). Cybercriminals craft legitimate-looking emails that encourage people to take an action, such as clicking a link or opening an attachment, which at first glance looks like it is from an authentic financial institution, e-commerce site, government agency, or any other service or business. These attacks collect personal, proprietary, and financial information, and can infect your machine with malware and viruses. Often, hackers use domain-spoofing techniques. They masquerade as coming from a sender that you may know, in an effort to get you to supply sensitive information, such as your login credentials, account numbers, credit card numbers, and money transfers. Because these emails look as if they legitimately come from sources you trust, it can be very hard to tell that they are fake.

Cybercriminals rely on email to launch attacks because it continues to work. They are appealing and believable because the email looks similar to a real request. To be successful, it must trick users. To protect yourself, be suspicious of any communication that directs you to take an action, no matter how official it appears. Remember to pause and look for clues to determine if it is fake. For example, does this bait look “phishy” to you? It’s an infamous example of a high-profile person receiving an urgent email that said he must change his password, and well, he clicked the link in this email:

Now, if you remember only one single thing in this entire video, it’s this: Stop, and hover over every link before you click! If you take a moment to hover the mouse over a link, you will see the true destination of that link. This is a significant clue to determine if an email is legitimate.

For example, if you get an email that appears to come from your bank saying there’s a problem with your account and you must log into a website to correct the problem by clicking a link, do not click. Instead, open an up-to-date browser and manually type the website address (URL) to see what’s happening.

If you receive an email that requests the movement of money, such as payment of an invoice, even if it’s from someone you know, we recommend that you use another form of trusted communication to verify that the message is legitimate before taking action. Also, carefully check the email address. Just because a message says it’s coming from the name of a person you know or trust, it does not mean that it truly is that person.

Phishing attacks are sent to a wide audience whereas Spearphishing, Whaling, CEO Fraud, BEC, and even Vishing are directed towards specific individuals or business roles. Research shows these attacks are effective 91% of the time. If an attacker is interested in breaking into a particular organization, they might use a personally-crafted email or a targeted phone call, seemingly from a source internal to that organization or from a vendor that the organization does business with and is trusted. Many times these fake communications appear as a direct message from your boss or a C-suite executive. If you’re suspicious, even if the details appear accurate, do not respond.

Hover your mouse over links to check their true destination, and check for spelling or grammar errors. To be safe, never transfer money, divulge sensitive information, or grant special access without first double-checking to confirm from an alternate trusted source.

Social engineers are experts at impersonating legitimate sources, manipulating human nature to trigger an emotional response, and enticing you to skip normal security protocols. Don’t fall for it!

When it comes to cybersecurity, knowledge is power and that’s why, by implementing actions you can take, you can avoid common traps. Be cyber safe out there!

Thank you for your time, and please remember to take the quiz that follows this lesson.

Lesson 5: Insider Threat Perspectives

Hi. I’m Steve. Welcome to the InfoSec-Awareness Series (IAS): Insider Threat lesson. Let’s talk about your role as a trusted insider at work, the stakes involved, as well as demonstrate how common sense is crucial to preventing a security incident.

Security threats come from everywhere, all over the world, 24 hours a day, 7 days a week, and 365 days a year. Moreover, human error is the root cause of almost every single data breach.

To make it simple, here’s a list of helpful tips to build cyber resilience and increase your physical security awareness while at your place of business.

- Always follow company policy and data handling guidelines. If you are not sure about a policy, please ask. There are no dumb questions.
- Back up sensitive and critical information on an encrypted device with a strong password.
- Be aware of shoulder surfing or people who hang around your desk and act suspicious. They might be looking for confidential information or watch you enter passwords.
- Do not write or leave passwords on notes posted on or under your desk, computer, or keyboard.
- Keep your desk free of any proprietary or confidential information, and securely lock private information away in a desk drawer when you leave your workstation for an extended period, and at the end of the day.
- Lock your computer screen and cell phone every time you step away to prevent anyone from seeing or manipulating confidential information on your device.
- Report broken doors, windows, and locks to your security personnel as soon as possible.
- Report suspicious activity in or near your facility’s entry and exit points, loading docks, parking areas, garages, and immediate vicinity, and always remember to lock your car.
- Report suspicious packages, and do not open or touch them.
- Shred and destroy all documents that contain sensitive personal or organizational information rather than tossing them in the waste bin.
- Treat all devices, such as your computer, DVD, CDROM, USB drives, and laptop as sensitive if they contain proprietary and sensitive data. Never share it with an unauthorized person, which includes your family members.
- Use your badge to enter your workplace and do not allow tailgaters. Check for identification and ask lingering individuals to identify the purpose of their visit to your workplace.

Now, let’s talk about insider threat. Most insiders are loyal, hardworking employees who do meaningful work for their company, and at the end of the day go home to their family, friends, and/or beloved pets. Moreover, we may think of cyberthreats as coming from an anonymous criminal who is far away and behind a computer screen, and that cybersecurity measures at our place of business need to focus only on external threats. Unfortunately, an insider threat can be detrimental to an organization, its data, and its brand reputation. Both current and former employees possess valuable knowledge about a company, and are capable of committing crimes that may cause irreparable harm to the organization.

Let’s define it. An Insider has authorized access to company resources, such as critical information, personnel, equipment, facilities, networks, and systems. An Insider Threat is the risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization.

Typically, an insider threat is a well-intentioned employee that ends up doing something accidental and puts the company at risk, such as clicking a phishing email or something negligent, such as a privileged user not following company policy in order to complete their work faster, which can result in some form of security compromise albeit unwittingly. On the other hand, a malicious insider threat is connected to the organization, and wittingly targets it for an attack. They perform deliberate actions, such as malicious exploitation, theft, destruction of data, or the compromise of information technology resources. Research shows this person could be a present or former employee, contractor, a board member, or anyone who has or had authorized access to the office building, networks, systems, or sensitive company information.

Insider threats are one of the most challenging attack vectors to manage because the trusted users who must have legitimate access to critical data, networks, and resources, are also the very same users who may cause damage to those assets.

People are at the center of every insider threat. Therefore, putting people first is always essential. Life happens, and we all must deal with unexpected challenges and obstacles that life sends our way. It is also human nature to make a mistake. What's really important is to learn from it and not be negligent. Then again, research shows that truly malicious acts are seldom impulsive. Something happens that contributes to a trusted insider evolving into a malicious insider. To help mitigate this risk, ensure all critical assets have been identified and securely protected.

Most insider threats are unintentional, hence our focus on training awareness. We must be vigilant. If you see something or hear something concerning, then say something. For example: Who did you see? What did you see? When did you see it? Where did it occur? Why is it suspicious? It doesn't matter how big or small it seems, such as a secure door is ajar, or a confidential document is left on the printer, or a piece of equipment is acting oddly. Report any suspicious activity to your manager and your organization's information security team.

When it comes to cybersecurity, knowledge is power and that's why, by implementing actions you can take, you can avoid common traps. Be cyber safe out there!

Thank you for your time, and please remember to take the quiz that follows this lesson.