Google IT Support Specialization

Course 5: IT security

01 Understanding security threats

Table des matières

[1 Understanding IT security threat 2](#_Toc14375870)

[1.1 Introduction to it security 2](#_Toc14375871)

[1.1.1 Course introduction 2](#_Toc14375872)

[1.2 Malicious software 3](#_Toc14375873)

[1.2.1 The cia triad 3](#_Toc14375874)

[1.2.2 Essential security terms 3](#_Toc14375875)

[1.2.3 Malicious software 4](#_Toc14375876)

[1.2.4 Malware continued 5](#_Toc14375877)

[1.3 Network attacks 6](#_Toc14375878)

[1.3.1 Network attacks 6](#_Toc14375879)

[1.3.2 Denial of service 6](#_Toc14375880)

[1.4 Other attacks 7](#_Toc14375881)

[1.4.1 Client-side attacks 7](#_Toc14375882)

[1.4.2 Password attacks 8](#_Toc14375883)

[1.4.3 Deceptive attacks 8](#_Toc14375884)

# Understanding IT security threat

## Introduction to it security

### Course introduction

Before we get going on the next course, I want to say big congratulations. You've made it all the way to the final course of this program. It's been quite a journey, but look at the progress you've made. You've learned all the fundamentals of IT. We're now at the last course, the one that will round out your foundational knowledge. I'm talking about security. Without it, all of the processes you've learned so far can fail, and no IT girl or guy wants that. Before we dive in, I'd like to reintroduce myself. We met way back in the first course when we talked about the history of the Internet and the Internet of Things. My name is Gian Spicuzza, and I'm the Program Manager in Android Security. I help protect Androids, two billion plus devices, by managing and driving new security features for each Android design release or versions of Android. As early as I can remember, I've loved technology. I've worked in IT since I was 16-years-old, and I'd fill my time reading books about new tech and building servers from old computer parts down at my parents basement. I was never a very good test-taker, and my grades definitely reflected that. But I didn't let it stop me from pursuing my career. I worked as the one person IT crew for three non-profits while I was getting my education. It was really stressful being responsible for everything, from configuring and administering databases to showing new employees how to access email and internal tools. Now, looking back, this experience was invaluable, and of course, security was an essential part of my IT work. Now, I work directly with hardware manufacturers, app developers, and engineering teams within Google to create the most secure experiences for our users. For many of them, their cell phone is the only connection they have to the Internet, and I feel such a sense of fulfillment knowing that my work can have a major impact on people all over the world who rely so heavily on their devices. To be successful at cybersecurity, sometimes you need to put yourself in the mindset of an attacker and always be one step ahead. So, are you ready to do good by thinking bad? Let's jump right in. In this module, you're going to be learning all about security, how people attack it and how do we defend against these attacks. By the end of the module, you'll be able to define and recognize security risks, vulnerabilities, and threats. You'll also be able to identify the most common security attacks. Finally, you'll understand how security revolves around the CIA principle and what the CIA principle is. When you think of security, what's the first thing you think of? It's probably physical security, stuff like making sure your belongings are safe from potential thieves, locking your front doors at night, and putting your valuables in a safe place. But in today's digital world, your money isn't just in your wallet, your cash is also stored inside online bank accounts accessible with the right password. Some of us don't carry credit cards at all, and those who do, don't just have them in their wallets. They're stored on their favorite websites so that they can make purchases more easily. It's not just money we care about. Most of our entire personal world lives on mobile phones. Our text messages, photos, personal data, application logins, and more are all kept right inside the devices we have in our pockets. Unfortunately, we live in a world where there are people and organizations that try to steal data from companies, from governments, and even from people like you and me. Don't let movies warp your perception of these digital thieves. They aren't as glamorous or professional as you may think. Digital thieves don't have a team of hackers and dark hoodies furiously typing into computer terminals all day hoping to break into multi-billion dollar companies. That's not to say that doesn't happen because we all know it does. But most of the time, the average Internet attacker is someone who looks just like you and me, a regular person who happened to stumble upon a hole in your security system and then took advantage of it. It could have been something as simple as figuring out that you use your dog's name as your password. When the only thing securing your bank account is the word Fido, you're in trouble. But just like we have physical security alarms to deter potential burglars, we also have many methods to prevent our digital security from being compromised. By the end of this course, you'll gain a deeper understanding of computer security. You'll learn how to prevent the most commonly used computer attacks. You'll understand the various security protocols and mechanisms that we use on our machines in the web and on our networks. You'll also learn more about cryptography, authentication, and access mechanisms, which are important skills for any IT support specialist. We'll wrap up the course by giving you the necessary tools to assess the security of an organization and decide on the best security preventative measures. Today, just about every business or industry relies heavily on technology to conduct day-to-day business, can you imagine a company, large or small, operating without email, without functional computers or Internet access. Take the case of a small company. It needs some technology if it wants to be able to access credit cards. Recent attacks like the WannaCry cryptoworm and large scale attacks using the Mirai botnet highlight the scope and scale of how security affects us all. It's something we need to take seriously. Because of our widespread dependence on technology, digital security is more important than ever before, and it's going to continue to have a growing impact on all industries and aspects of our lives. So let's make sure you're armed with the right tools to keep yourself and your future clients safe.

## Malicious software

### The CIA triad

Throughout this course, there'll be one key acronym to keep in mind, the CIA. No, I'm not talking about the U.S. Central Intelligence Agency, although they do have a lot to do with national security. When I say CIA, I'm talking about confidentiality, integrity, and availability. These three key principles are the foundation for what's widely referred to as the CIA triad, a guiding model for designing information security policies. These three principles will help you develop security policies in the workplace and for your own personal environments. Let's start with confidentiality. Confidentiality means keeping things hidden. In I.T., it means keeping the data that you have hidden safely from unwanted eyes. One particular method of confidentiality that you probably use everyday is password protection. Only you, maybe your partner, should know the password to gain access to your bank account online. For confidentiality to work, you need to limit access to your data. Only those who absolutely need to know how to gain access, should. The I in CIA stands for integrity. Integrity means keeping our data accurate and untampered with. The data that we send or receive should remain the same throughout its entire journey. Imagine if you downloaded a file off the Internet, and the website you're downloading it from, says the file is three megs. Then, when you download it, it turns out to be about 30 megs. That's a red flag. Something happened during the download, something potentially unsafe. An unwanted file may now be living on your hard drive. As you'll learn in a later lesson, this happens all too often. Last but not least. Let's look at the A in CIA, which stands for availability. Availability means that the information we have is readily accessible to those people that should have it. This can mean many things, like being prepared if your data is lost or if your system is down. Security attacks are designed to steal all kinds of things from you, time, material things, your dignity. Some steal the time that you'll need to spend to get services back up and running. Some security attacks will hold your system hostage, until you pay a ransom for it. Sounds scary and it is but that's why you're here, to learn how to stop these types of attacks from happening. Going through this course, you'll see how every aspect of security revolves around these three key principles: confidentiality, integrity and availability.

### Essential security terms

Before we dive into things like bringing down digital thieves, let's get some of the terminology out of the way. We'll be using these terms throughout the entire course. So you should know them inside and out before we get started.

The first one is Risk. The possibility of suffering a loss in the event of an attack on the system. Let's say that you buy a new phone. One security measure you can take to protect your device, is to set up a screen lock using a password or pattern that you add to prevent others from accessing your info. A screen lock is a security feature that helps prevent unwanted access by creating an action you have to do to gain entry. If you choose not to add a screen lock to your phone, the risk that you take is that someone could easily gain access to your phone and steal your data. Even adding something as simple as a passcode or a screen lock can help you protect your personal or company data from getting into the wrong hands.

Next up is the term Vulnerability. A flaw in the system that could be exploited to compromise the system. Vulnerabilities can be holes that you may or may not be aware of. Maybe you go away for a long vacation and lock every door and window in your house before you leave. But you forget to lock the bathroom window. That bathroom window is now a vulnerability that burglars can use to break into your house. Another example is when you're writing a web app and enable a de-bug account for testing during development but forget to disable it before launching the app. You now have a vulnerability in your app that an attacker can potentially discover. There's a special type of vulnerability called a 0-day vulnerability or zero day for short. Which is a vulnerability that is not known to the software developer or vendor, but is known to an attacker. The name refers to the amount of time the software vendor has had to react to and to fix the vulnerability, zero days.

Another key term is Exploit. Software that is used to take advantage of a security bug or vulnerability. Attackers will write up exploits for vulnerabilities they find in software to cause harm to the system. Let's say the attacker discovers a zero day vulnerability. She decides to take advantage of the previously unknown bug and writes a zero day exploit code. That code will specifically target and take advantage of this unknown bug to gain access and cause damage to systems. Not cool. The next term to know is Threat. The possibility of danger that could exploit a vulnerability. Threats are just possible attackers, sort of like burglars. Not all burglars will attempt to break into your home to steal your most prized possessions, but they could, and so they're considered threats.

Next up, Hacker. A hacker in the security world is someone who attempts to break into or exploit a system. Most of us associate hackers with malicious figures. But there are actually two common types of hackers. You have black hat hackers, who try to get into systems to do something malicious. There are also white hat hackers who attempt to find weaknesses in a system, but also alert the owners of those systems so that they can fix it before someone else does something malicious. While there are other types of hackers, these are the two main ones and the most important for us to understand right now.

The last term to know is Attack. Which is an actual attempt at causing harm to a system. It's super important to be aware of possible threats and vulnerabilities to your system so that you can better prepare for them. The sad reality is that there will always be attacks on your system. But before you start searching for an underground bunker to spend the rest of your days in, remember that there are ways that you can detect and mitigate attacks and we're here to help you learn how to do just that. In this module, we'll be talking about some of the common attacks that you will encounter at home and in the workplace.

Throughout the course, you'll learn how to harden your systems against these attacks. Turns out, there are hundreds of ways that your system can be attacked. But there are also hundreds of ways that you can prevent them. We won't talk about all of them, but we will cover the major ones. So abandon the bunker idea and prepare to dive in because things are about to get real. Real secure.

### Malicious software

Malware is a type of malicious software that can be used to obtain your sensitive information or delete or modify files. Basically, it can be used for any and all unwanted purposes. The most common types of malware you'll see are viruses, worms, adware, spyware, Trojans, root kids, backdoors, botnets, my, I know, I know, it's a long list, but we'll go into detail about each of these and even learn about some real-life cases. But for now, let's talk about the most common forms of malware. Viruses are the best known type of malware, and they work the same way that viruses in your body work. When you get sick, a virus attaches itself to a healthy cell in your body, then replicates itself and spreads to other healthy cells in your body, until bam! You're sneezing and wheezing and you're a mess. In a computer virus, the virus attaches itself to some sort of executable code like a program. When the program is running, it touches many files, each of which is now susceptible to being infected with the virus. So, the virus replicates itself on these files, does the malicious work it's intended to do, and repeats this over and over until it spreads as far as it can. Scary, right? Well, hold on tight, we're just getting started. Worms are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network. One case of a famous computer worm was the ILOVEYOU or Love Bug which spread to millions of Windows machines. The worm would spread via email. Someone would email a message with a subject line of I Love You, and an attachment that was actually the worm disguised as a love letter text file. The techs file was actually an executable file that when opened would execute many attacks like copying itself to several files and folders, launching other malicious software, replacing files, and then hiding itself after it was done. The worm spread by stealing e-mail addresses that were in the victim's computer and chat clients. It then proceeded to send that email out to everyone in the address book. The Love Bug spread across the world and caused billions of dollars in damage, not so lovely. This was just one of the many reasons why you should never open email attachments that you do not recognize. Adware is one of the most visible forms of malware that you'll encounter, most of us see it every day. Adware is just software that displays advertisements and collects data. Sometimes we legitimately download adware. That happens when you agree to the terms of service that allows you to use free software in exchange for showing you advertisements. Other times, it may get installed without your consent and may do other malicious things than just display advertisements. In Greek mythology, there's a famous tale of the invasion of the city of Troy. The Greeks, who had been trying to gain access into the walled city, finally decided to hide themselves in a giant wooden statue of a horse under the guise of a gift. The Trojans allowed the gift inside, then in the dead of night ,the Greeks broke out of the statue and attacked the city. In computer security, we have malware that functions like a Trojan horse, and it's named after this exact thing. A Trojan is malware that disguises itself as one thing but does something else. Just like how the historical Trojan horse was accepted into the city by the citizens of Troy. A computer Trojan has to be accepted by the user, meaning the program has to be executed by the user. No one would willingly install malware on their machine, that's why trojans are meant to entice you to install them by disguising themselves as other software. Spyware is the type of malware that's meant to spy on you. Which could mean monitoring your computer screens, key presses, webcams, and then reporting or streaming all of this information to another party, it's not good. A keylogger is a common type of spyware that's used to record every keystroke you make. It can capture all of the messages you type, your confidential information, your passwords, and even more. Ransomware is a type of attack that holds your data or system hostage until you pay some sort of ransom. Remember the availability principle we learned about in the first video? Does this attack sound like a way to decrease the availability of our security? Bingo! That's because it is. A recent case of ransomware was the WannaCry ransomware attack in May of 2017. The malware took advantage of a vulnerability in older Windows systems, infecting hundreds of thousands of machines across the world. Most notably, the attack shutdown the systems for the National Health Services in England, causing a health-related crisis. The WannaCry ransomware attack devastated systems around the world. These types of attacks are becoming more common and we need to be ready to fight them, so let's soldier on.

### Malware continued

Let's pick up where we left off with Malware. So far, we've covered some of the major types of Malware that can be found in the system, including Malware, Viruses, Worms, Adware, Spyware and Ransomware. What if our attackers could not only do malicious things like steal our data, but they could also steal our computers resources like the CPU? Well, I'm sorry to tell you that actually exists. There is Malware out there that can utilize someone else's machine to perform a task that is centrally controlled by the attacker. These compromised machines are known as Bots. If there are a collection of one or more Bots, we call that network of devices a Botnet.

Botnets are designed to utilize the power of the Internet-connected machines to perform some distributed function. Take mining Bitcoin, for example, mining Bitcoin requires a machine to perform some computation that takes up your machine's resources. At the end, you may be rewarded with some amount of Bitcoin. A popular attack has been creating Botnets to do stuff like mine Bitcoins. So instead of having one computer run computations, attackers can now have a thousand computers running computations and raking in more and more Bitcoin. A backdoor is a way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers. Backdoors are most commonly installed after an attacker has gain access to your system and wants to maintain that access. Even if you discovered your system has been compromised, you may not realize that a backdoor to your system exists. If it does, you need to lock it up before more damage can be done. Another form of Malware that can be particularly problematic is a rootkit. A rootkit by its name is a kit for root, meaning a collection of software or tools that an admin would use. It allows admin level modification to an operating system. A rootkit can be hard to detect because it can hide itself from the system using the system itself. Sneaky little sucker. The rootkit can be running lots of malicious processes, but at the same time those processes wouldn't show up in task manager because it can hide its own presence. A logic bomb is a type of Malware that's intentionally installed, after a certain event or time has triggered, it will run the malicious program. There's a popular logic bomb case that happened in 2006, wherein unhappy systems administrator at a bank, set off a logic bomb and brought down a company's services in an attempt to drop their stock prices. The former employee was caught and charged with fraud, then sentenced to eight years in prison. Not the most logical Logic bomb.

## Network attacks

### Network attacks

A network attack that is simple in concept, but can cause a lot of damage is a DNS Cache Poisoning attack. You probably remember from the bits and bytes of computer networking course, that DNS works by getting information about IP addresses and names to make it easier for you to find a website. A DNS Cache Poisoning attack works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server. It then feeds you fake DNS addresses when you try to access legitimate websites. Not only that, DNS Cache Poisoning can spread to other networks too. If other DNS servers are getting their DNS information from a compromised server, they'll serve those bad DNS entries to other hosts. Several years ago, there was a large scale DNS Cache Poisoning attack in Brazil. It appeared that attackers managed to poison the DNS cache of some local ISPs, by inserting fake DNS records for various popular websites like Google, Gmail, or Hotmail. When someone attempted to visit one of those sites, they were served a fake DNS record and were sent to a server that the attacker controlled, which hosted a small java applet. The user would then be tricked into installing the applet, which was actually a malicious banking trojan designed to steal banking credentials. This is an example of the real world damage DNS Cache Poisoning attacks can pose. You can learn more about it in the next supplementary reading. A man-in-the-middle attack, is an attack that places the attacker in the middle of two hosts that think they're communicating directly with each other. It's clearly a name that needs some updating, men aren't the only hackers out there. The attack will monitor the information going to and from these hosts, and potentially modify it in transit. A common man-in-the-middle attack is a session hijacking or cookie hijacking. Let's say you log into a website and forget to log out. Now, you've already authenticated yourself to the website and generated a session token that grants you access to that website. If someone was performing a session hijacking, they could steal that token and impersonate you on the website, and no one wants that. This is another reason to think about the CIA's of security, you always want to make sure that the data that you are sending or receiving has integrity and isn't being tampered with. Another way a man-in-the-middle attack can be established is a rogue access point attack. A rogue AP is an access point that is installed on the network without the network administrator's knowledge. Sometimes, in corporate environments, someone may plug a router into their corporate network to create a simple wireless network. Innocent enough, right? Wrong. This can actually be pretty dangerous, and could grant unauthorized access to an authorized secure network. Instead of an attacker having to gain access to a network by plugging directly into a network port, they can just stand outside the building and hop onto this wireless network. A final man-in-the-middle method will cover is called an evil twin. It's similar to the rogue AP example but has a small but important difference. The premise of an evil twin attack is for you to connect to a network that is identical to yours. This identical network is our networks evil twin and is controlled by our attacker. Once we connect to it, they will be able to monitor our traffic. I wonder if Fred Weasley ever did this to George, probably not, they were wizards. They could just magic their way out of problems. Must be nice.

### Denial of service

A Denial-of-Service, or DoS attack, is an attack that tries to prevent access to a service for legitimate users by overwhelming the network or server. Think about how you normally get on a website. Most major websites are capable of serving millions of users. But for this example, imagine you have a website that could only serve 10 users. If someone was performing a Denial-of-Service attack, they would just take up all 10 of those spots, and legitimate users would have been denied the service, because there's no more room for them. Now apply that to a website like Google, or Facebook. DoS attacks try to take up those resources of a service, and prevent real users from accessing it, not a pretty picture. The Ping of Death or POD, is a pretty simple example of a DoS attack. It works by sending a malformed ping to a computer. The ping would be larger in size than what the internet protocol was made to handle. So it results in a buffer overflow. This can cause the system to crash and potentially allow the execution of malicious code. Another example is a ping flood, which sends tons of ping packets to a system. More specifically, it sends ICMP echo requests, since a ping expects an equal number of ICMP echo replies. If a computer can't keep up with this, then it's prone to being overwhelmed and taken down. Not cool ping flood, not cool. Similar to a ping flood is a SYN flood. Remember that to make a TCP connection, a client sends a SYN packet to a server it wants to connect to. Next, the server sends back a SYN-ACK message, then the client sends in ack message. In a SYN flood, the server is being bombarded with the SYN packets. The server is sending back SYN-ACK packets but the attacker is not sending ack messages. This means that the connection stays open and is taking up the server's resources. Other users will be unable to connect to the server which is a big problem. Since the TCP connection is half-open, we also refer to SYN floods as half-open attacks, sounds messy, right? It is, the DoS attacks we've learned about so far only use a single machine to carry out an attack. But what if attackers could utilize multiple machines? A much scarier scenario, they'd be able to take down services in greater volumes and even quicker rates. Even scarier, attackers can absolutely do that. A DoS attack using multiple systems, is called a distributed denial-of-service attack or DDoS. DDoS attacks need a large volume of systems to carry out an attack and they're usually helped by botnet attackers. In that scenario, they can gain access to large volumes of machines to perform an attack. In October of 2016, a DDoS attack occurred the DNS service provider, Dyn was a target of a DDoS. Fake DNS look up requests along with SYN floods that botnets to performing overloaded their system. Dyn handled the DNS for major website like Reddit, GitHub, Twitter, etc. So once that went down, it also took down its customers, making those services inaccessible. Don't get between people on the Reddit threads or Twitter feeds, I know from experience, it's not pretty.

## Other attacks

### Client-side attacks

We've talked a lot about security attacks that target victims directly, but they aren't the only type of attacks that occur in the web. One day, you may find yourself in software development or software engineering. And you'll need to know about these other types of attacks in order to ensure the security of your work. A common security exploit that can occur in software development and runs rampant on the web is the possibility for an attacker to inject malicious code. We refer to these types of attacks as injection attacks. So how do injection attacks work? Great question. For simplicity's sake, we won't get into the details of the code implementation, but imagine a car. You keep your car running by putting gas in it. Now, consider someone who wants to do something malicious to that car. That person could inject your gas tank with a strawberry banana milkshake. While that may sound delicious, it could also ruin your car. So how do you fight against that? A hypothetical method to prevent this is adding a mechanism to your car that only accepts gasoline and no other liquids. Injection attacks in websites work the exact same way, except without the mouthwatering strawberry banana milkshakes, and without having overly complex solutions. Injection attacks can be mitigated with good software development principles, like validating input and sanitizing data. Is anyone else getting hungry? Milkshake break? No? Okay, we'll move on. Cross-site scripting, or XSS attacks, are a type of injection attack where the attacker can insert malicious code and target the user of the service. XSS attacks are a common method to achieve a session hijacking. It would be as simple as embedding a malicious script in a website, and the user unknowingly executes the script in their browser. The script could then do malicious things like steal a victims cookies and have access to a log in to a website. Mm, cookies. Another type of injection attack is a SQL, or S-Q-L, injection attack. Unlike an XSS that targets a user, a SQL injection attack targets the entire website if the website is using a SQL database. Attackers can potentially run SQL commands that allow them to delete website data, copy it, and run other malicious commands. Now that that's out of the way, it's snack time.

### Password attacks

There is no getting around it, passwords are the most secure common safeguards we have to prevent unauthorized account access. Unfortunately, our passwords may not be as secure or strong as they should be. A common attack that occurs to gain access to an account is a password attack. Password attacks utilize software like password crackers that try and guess your password. And they work extremely well, so don't try to reuse that fido password. It didn't secure your bank account and it's not going to work here. Okay, moving on. A common password attack is a brute force attack, which just continuously tries different combinations of characters and letters until it gets access. Since this attack requires testing a lot of combinations of passwords, it usually takes a while to do this. Have you ever seen a CAPTCHA when logging into a website? CAPTCHAs are used to distinguish a real human from a machine. They ask things like, are you human, or are you a robot, or are you a dancer? In a password attack, if you didn't have a CAPTCHA available, an automated system can just keep trying to log into your account until it found the right password combination. But with a CAPTCHA, it prevents these attacks from executing. Another type of password attack is a dictionary attack. A dictionary attack doesn't test out brute force combinations like ABC1 or capital ABC1. Instead, it tries out words that are commonly used in passwords, like password, monkey, football. The best way to prevent a password attack is to utilize strong passwords. Don't include real words you would find in a dictionary and make sure to use a mix of capitals, letters, and symbols. Without any fail-safes like CAPTCHAs or other account protections, it would take a typical password cracker application about one minute to crack a password like sandwich. But substantially longer to crack something like what you see here, spelled s, @, n, capital D, w, h, number 1, c, then another h. See how that's the same but also way harder to crack?

### Deceptive attacks

Get ready because we're about to dive into one of the least technical but most disturbing attacks that can be done, social engineering. Social engineering is an attack method that relies heavily on interactions with humans instead of computers. You can harden your defenses as much as you want. You can spend millions of dollars on State of the Art Security Infrastructure. But if Susan the systems administrator has all the access to your system, and gets tricked into handling over her credentials, there's nothing you can do to stop it. As we've learned from the greatest sci-fi movies, humans will always be the weakest link in life, and in your security system. Social engineering is a kind of con game where attackers use deceptive techniques to gain access to personal information. They then try to have a user execute something, and basically scam a victim into doing that thing. A popular type of social engineering attack is a phishing attack. Phishing usually occurs when a malicious email is sent to a victim disguised as something legitimate. One common phishing attack is an email, saying your bank account has been compromised. And then, gives you a link to click on to reset your password. When you go to the link, it looks like your bank's website but it's actually a fake website. So you're tricked into entering your current password and credentials in order to reset your current password. Another variation of phishing is spear phishing. Both phishing schemes have the same end goals, but spearfishing specifically targets individual or group. The fake emails may contain some personal information like your name, or the names of friends or family. So they seem more trustworthy. Another popular social engineering attack is email spoofing. Spoofing is when a source is masquerading around as something else. Think of an email spoof. This is what happens when you receive an email with a misleading sender address. You can send an email and have it appear to come from anywhere you want, whether it exists or not. Imagine if you open that email you thought was from your friend Brian. Brian's real email address is in the front part and the email says that you have to check out this funny link. Well, you know Brian. He's pretty awesome and he always said super funny emails, so you click on the link. Suddenly, you have malware installed. And you're probably not feeling so awesome about Brian right now. Not all social engineering occurs digitally. In fact, one attack happens through actual physical contact. This is called baiting, which is used to entice a victim to do something. For example, an attacker could just leave a USB drive somewhere in hopes that someone out there will plug it into their machine to see what's on it. But they've just installed malware on the machine without even knowing it. Another popular attack that can occur offline is called tailgating, which is essentially gaining access into a restricted area or building by following a real employee in. In most corporate environments, building access is restricted through the use of a keycard or some other entry method. But a tailgater could use social engineering tactics to trick an employee into thinking that they're there for a legitimate reason like doing maintenance on the building, or delivering packages. Once a tailgater is in, they have physical access to your corporate assets. Pretty scary stuff we've covered so far huh? I bet you didn't realize that there were so many ways to compromise security. Hopefully, you've gained a better grasp on the common attacks out there, and signs and what to look for. Now that you've been exposed to the fundamental types of security threats, we'll dive deep into best practices for security and how to create technical implementations for secure systems. But first up, we're going to test your knowledge with a quiz covering the different attacks we've talked about in this module.