Social Engineering

Now, social engineering is any act that manipulates users into revealing confidential information or performing other actions that are detrimental to that user or the security of our systems. Now, there's lots of different types of social engineering. There's things like pretexting, malicious insider threats, diversion theft, phishing, hoaxes, shoulder surfing, eavesdropping, dumpster diving, baiting, piggybacking, and watering hole attacks.

Demo: Pretexting

Alright, so that's the basic idea of a pretexting call. I didn't know anything about the organization, but giving this receptionist some kind of likely facts, like the fact that she's running an HP system or a large printer in the copy room, which most businesses have, then I can trick her into giving me some kind of information. Now, if you've ever gotten one of those calls that says, "Hey, this is John from Microsoft and your Windows machine has been reporting that it's been infected with malware. I'm calling you to help clean it up. I just need you to do step one two and three," this is a pretexting call. In fact, this is one of the more common pretexts out there. The reason why I even use this example of a Windows machine calling out with Malware is because I had the conversation with my mom earlier this week.

And so, we want to make sure we train our employees to not fall for pretext and don't fill in the gaps for other people when they're calling you or even if they're doing it in person, because pretexting is a way that we give some amount of information that seems true so that you'll give us more information to fill in the gaps.

Insider Threat

An insider threat is simply somebody who works for your organization, but they have ulterior motives and they want to do something negative to your organization.

And so, you have to keep an eye on that and there's lots of ways to do that. One of the ways we talked about before was DLP, Data Loss Protection, right? You install Data Loss Protection and it will keep track of all the files that are being copied and

downloaded so you can go back and figure out, was that person really stealing from you or were they just doing their job?

Phishing

Phishing has become very commonplace. Basically, a victim is contacted by email, telephone, text message, or some other method posing as a legitimate organization. Now, when you see the word **phishing** on the exam, I want you to think of email because they have a distinct difference for telephone and text messages. Telephones are called **vishing** and text messages are called **smishing**.

Spear Phishing

Well, with spear phishing, I really want to focus on creating a message tailored to a specific person.

Whaling

Well, whaling is focused on spear phishing, but specifically at a high-level executive. So, these are your CEOs, your CFOs, your CIOs, your CSOs, or other chief-level executives.

Smishing

Now, the next thing we want to look at is smishing, or SMS phishing. This is short message service. It's text messages.

Vishing

Now, vishing, this is voice phishing. Voice phishing is phishing that occurs over a telephone.

Pharming

If we try to do it, we're trying to trick somebody to go to a different website. (usually by modifying hosts file)

Motivation Factors

1. Now, the first one is **authority**. People are much more willing to comply and do what you tell them to if they think it's coming from somebody who's in authority.

2. Now, the next one that we have is what's called **urgency**. And urgency is all about the fact that people know that we're in a rush a lot of the time, we're busy these days, right? And people want to help others by nature. It's just in our human nature.

3. The next one we have is **social proof**. Let's say that I put up a website out there that was fake and scammy, right? And I was trying to phish people to get them to go there. Well, if I can get some social engineering done through Facebook or Twitter where I get people to like that site or share that site for me, that starts showing social proof and people are more likely to click on it, right? People are much more likely to click on things that have a lot of likes, a lot of shares, and a lot of their friends doing it.

4. The next one we have is **scarcity**. Now, scarcity is when you use a technique to get people to act quick, much like urgency, but the difference here is that usually, you're going to do it through like an email campaign or phishing, right? You go sign up now, supplies are limited. We only have five spots left, you've got to sign up right now if you want to get part of this, right? And so, you'll get this email and you'll be like, wow, this is a really good deal on a new MacBook computer.

5. The next one we have is **likability**. People want to be and interact with people they like. Social engineers are some of the most friendly and likable people you will ever meet. You don't have these crusty, angry people as good social engineers. It just doesn't happen. You have friendly people, you have pretty people. One of the things that a lot of my pentesting teams like to do is they will take a very pretty woman and put her on the team because a lot of the people who work in IT are men.

6. Now, the last one we have here is **fear**, and fear is a great motivator if used properly. In fact, ransomware and any virus scans, they live off fear, right? It's if you don't do this, then this other bad thing is going to happen. It's a threat or a demand.

More Threats

Diversion Theft

Diversion theft occurs when a thief tries to divert a shipment and take responsibility for it, and send it to a different location. So, for example, maybe I call up FedEx because I know you have a new laptop being shipped to your office today, and I pretend that I'm you and say, "Oh, I'm not at my office, I'm actually at my house. It's at 123 Main Street." And now, FedEx brings that over to me, that was a diversion theft.

HOAX

Now, a hoax is an attempt at deceiving people into believing something is false even if it's true, or making them believe something is true, even if it's false. Basically, there's an idea of like a virus hoax. I might send an email out to all of my friends and say, "Hey everybody, there's a virus going around. To protect yourself from it, go to your C drive and delete your boot.ini file." Now, there really was no virus, but if they delete that boot.ini file, they can mess up their systems and prevent it from booting, causing them a problem, right? The hoax was I made them believe there was something there and made them take action into it.

Shoulder Surfing

That’s when you’re sitting at the office working, and somebody comes up behind you and uses direct observation to obtain authentication information. So, for example, as you're sitting there logging into your computer, if I look over your shoulder and watch your fingers, and see you type in "P-A-S-S-W-O-R-D," "password," I now know your password, right? That's the idea here with shoulder surfing.

Eavesdropping

The next one we have is eavesdropping. Maybe I'm going to stand around while you're talking with your boss, and overhear you telling him some information that I want to get. By listening in and doing that direct observation through my ears, I'm able to listen in to that conversation and get the information I want.

Dumpster Diving

This is when a person actually scavenges for personal or confidential information in garbage or recycling containers. Yes, I know it sounds dirty, but guess what? Hackers are willing to do it.

Baiting

The next one we have is baiting. Baiting is when a malicious individual leaves behind a malware-infected thumb drive or USB drive or a CD someplace around that somebody might have curiosity to pick up and insert into their computer. One of the ways that you do baiting if you're not inside the organization is you can walk through their parking lot and drop a nice 64-gigabyte thumb drive in there.

Piggybacking

The next one we have is piggybacking, and we talked about this back in physical security. This is going to occur when an unauthorized person tags along with an authorized person to gain access into a restricted area. For example, let's say I have a server room door that's protected by a combination lock or a cipher lock. I'm authorized because I'm assistant administrator. If I go in there and I PIN in and open the door, and somebody walks in behind me, that's called piggybacking.

Watering Hole Attack

Finally, we have a watering hole attack. Now, watering hole attack we've mentioned before, as well. This is when an attacker figures out where your users like to go, like a common website, they attack that website, embed their own malware, so, next time when you go to that website, you download the malware and again, get access. Because you're trying to trick a user here into doing something you want, it also falls into this larger area of social engineering.

Fraud & Scams

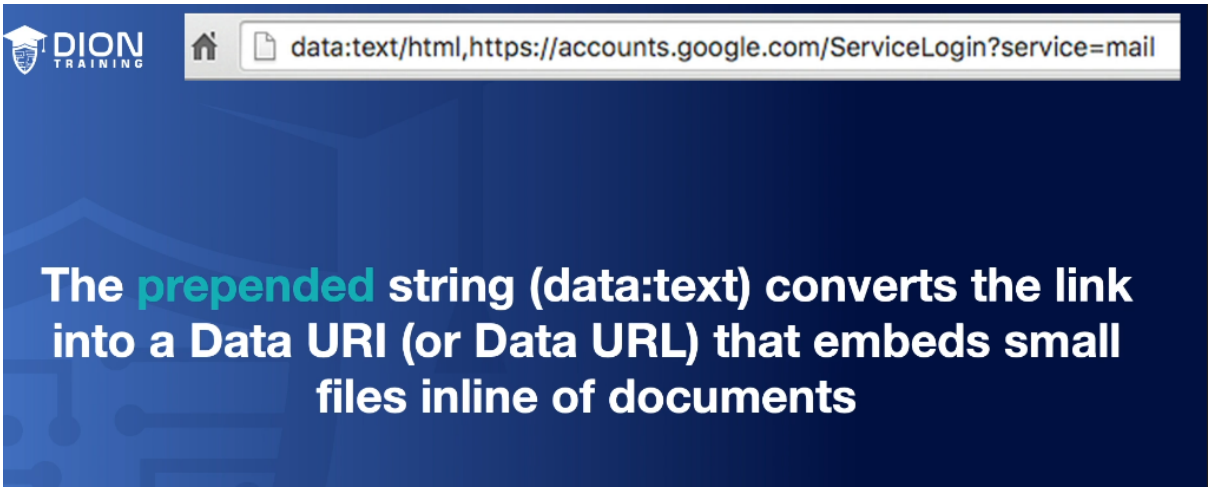
Fraud

Well, when you're dealing with a fraud, you're dealing with the wrongful or criminal deception intended to result in financial or personal gain. So, if I'm trying to commit fraud against you, I'm trying to essentially steal from you in some way. But I'm not really stealing like picking your pocket, you're actually giving it to me because I'm going to trick you into doing it. And that's why this is part of social engineering. Now, one of the most common frauds that we deal with inside of cybersecurity is identity fraud. Identity fraud is the use by one person of another person's personal information without their authorization to commit a crime or to deceive or defraud that other person or some other third party. Really, what this sounds like is identity theft, right? We hear that term a lot these days. When we talk about somebody who stole your social security number, or your date of birth, or your personal information, or where you were born, all of that information can be used to steal your identity. Now, when somebody commits identity theft, they're actually stealing another person's identity and using it as their own. So, they're going to actually become you. They want to take your social security number, and they're going to apply for new credit as if they're you. They're taking over your identity. That's the idea with identity theft. Now, often, we hear identity fraud and identity theft being used interchangeably. Now, there's really a misconception here because there is a difference between identity fraud and identity theft. With identity fraud, I might just take your credit card number and then go make charges as if I'm you. That's not technically identity theft, that's just identity fraud. But these days, most people will use both terms interchangeably and more commonly, you'll hear identity theft as the term.

Scam

Well, a scam is a fraudulent or deceptive act or operation. That's it. It's really simple. Essentially, it's somebody trying to deceive you into doing something. Now, I can do that in a lot of different ways, but the one that we are most worried about as cybersecurity professionals is what's known as an invoice scam. This is because it is commonly used against small businesses, medium-sized businesses, and large businesses. When we talk about an invoice scam, this is a scam in which a person is tricked into paying for a fake invoice for a product or service that they did not actually order.

Prepending



Influence Campaigns

Now, when I talk about influence operation, this is a collection of tactical information about an adversary, as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent. Now, that's a really nice fluffy way of saying you want to take information and use it against someone. That's what influence operations is all about. Now, influence operations is really the military term, but in the CompTIA objectives, they use the term influence campaign instead. An influence campaign is one small part of a larger influence operation, but we're going to use these terms interchangeably throughout this lesson.

Hybrid Warfare

Now, as I said, influence operations are something that's often done by militaries. And it's a form of hybrid warfare. When we talk about hybrid warfare, this is a military strategy that employs the full spectrum of warfare. It's going to use political warfare and blending conventional warfare like dropping bombs and shooting guns. It's going to use a regular warfare like special operation teams and even cyber warfare. And when you're doing cyber warfare, you can use influencing methods, things like putting out fake news, things like using diplomacy or foreign electoral intervention.

There's lots of things you can do as part of this hybrid warfare, and under hybrid warfare, influence operations is part of the grander military strategy.
Now, you may be wondering, why are we talking military strategy in a class on cybersecurity? Well, it's because it's being used in the cyber realm and it's being used inside our corporate networks. For instance, some of our large companies out there like Facebook and Twitter have been used to do these influence campaigns. If you look back to our 2016 election in the United States, there has been proof that the Russians were running an influence campaign. According to the New York Times, the Russian influence campaign on social media in the 2016 election made an extraordinary effort to target African-Americans and used an array of tactics to try to suppress voter turnout among those democratic voters and unleashed a blizzard of activity on Instagram that was actually higher or exceeded the amount of posts on Facebook.

User Education

The problem is, users are our number one vulnerability in the network. As a security professional, I can install all the technology I want, but if I don't fix the user, it's all going to be for nothing. I can put firewalls and intrusion prevention systems, and host-based security systems, and all sorts of other stuff to protect my network, but if the user clicks okay or accept and lets the bad guy in, it's just going to go right through all of it, right?

- Never share auth info
- Clean desk policy
- Log events
- Encrypt emails and VoIP
- Never use unknown usb/media
- Shred unused physical paper
- Follow data policies
- Track shipments
- Teach good web security
- Whitelist over blacklist