**Social Engineering**

Module 13 | Activity 1



**Introduction**

Security professionals recognize that their responsibility to protect their organization or employer is not limited to the eight hours they spend at the office, working behind a virtual platform.

The reason why social engineering attacks are often so powerful is because they strike in unpredictable yet simple ways. Try thinking of a few methods we covered back in the slideshow.

* A person holding boxes of donuts is welcomed into a building without being questioned
* Pretending to be on the phone while getting into an elevator that required a badge to work.
* Scamming somebody over the phone while maintaining a tone of urgency and frustration on your end so as to create pressure.

As we can see, even the most simple methods that prey on people’s emotions and psychology can yield effective results.

**Getting Started**

In this activity you will practice recognizing warning signs of an impending social engineering attack before it is too late. Security professionals know how to remain vigilant at all times and they are able to recognize when something feels off.

If you recall, there was one page in the slides that talked about social engineering during the cyber defense competition. Hopefully the competition is held in person at Iowa State during Spring ‘22. So a lot of more social interaction is able to take place for the social engineering portion.

The competition leaders and the red team come up with something a little different every year in an attempt to trick you but the principle remains the same. Keep your eyes peeled.

The following scenarios will allow you to practice how you would react in the real world. And while there is no exact perfect answer the ultimate goal, as you might know is to protect your team and its assets. Pair up for this activity if you aren't already.

Scenario 1: You get a phone call...

During the cyber defense competition you and your school will assume the role of a blue team that is trying to ward off attackers, while maintaining essential services running for whatever company/organization that you are representing.

For example, one year the blue team was helping out the police department. Another year it might be a small online marketplace.

Sometimes the red team has phones, for the competition.

Let’s assume that in whatever scenario you may end up competing in, the day of the competition has arrived. You are setting up some of the services on your machines and then you receive a phone call from somebody claiming to be tech support. And they are there to help you resolve an issue. You realize that you have been struggling a bit with setting up some of your services and decide to keep talking to the person on the phone.

* What went wrong in this situation?
* Name a few things considered red flags.
* How else could you have handled this situation?
* Should you give the person on the other end any information?
* Why would you feel the need to give in and talk to this person?

One of the first things you should do when you get an unexpected phone call like this is to question the person on the other end. Who do they work for? What do they want? How do they benefit from helping you? Or simply just keep them on hold. A real scammer will stop being friendly after you question their motives and waste their time. Whereas a real service representative would understand why you might be suspicious.

As a final note on this scenario, don’t forget to document this call in your notes. As it is part of your final score during the competition, how well you are able to document all of this information.

Scenario 2: A strange email…

Your team returns from a short break and you come back to find a strange email or correspondence that you discover shortly after getting your email server running.

You open it because the subject line got your attention but you are still unable to verify where this email came from. The email body seems to have been written in a rush. And it is asking you to act quickly in order to receive an Iowa State Cyber Defense Competition T-Shirt. “Fill out the following survey!”, it reads. “Please provide your shirt size and your ISELAB credentials”, it says.

Given this information, there are a few things to consider. Namely...

* Is this an official email? Who sent it?
* Why didn’t anyone mention anything about a free t-shirt before?
* Can I trust the survey?
* Name a few other red flags.
* Should you give the person on the other end any information?
* In what way are they trying to bait you and is the risk worth the reward?
* Let’s say that you decide to not put yourself at risk. Especially since you already filled out another form in paper, earlier in the morning for you to provide your shirt size. But that one DID NOT ask for your credentials. What will you do to properly handle the situation, after you find out that it is indeed a scam?

Many cyber attacks are more likely to succeed if they are supplemented with a good “dose” of social engineering. This is because humans are not computers, our behaviour is unpredictable in most given situations. Social engineering attacks prey on one or more of the following three attributes: fear, curiosity, helpfulness. An attacker might try to blackmail you with some unflattering pictures on your social media. Or try to get to you by trying to lure you in by taking advantage of your curious nature. They might even give you something for “free”, like a gift card to make you more susceptible to try and give something back, such as information, in order to repay the favor.

Scenario 3: There's something about this person...

In this scenario you are approached by a very charismatic person at the grocery store in the hummus aisle. They begin to ask you for your opinion on various flavors of the delicious chickpea-based paste. So you decide to chat for a few minutes.

During your conversation you cover a range of topics. You talk about your dog, your weekend plans and some of your favorite books.

After you part ways you don’t think too much about the interaction. Once you get home you begin to realize that this is not the first time you have seen this person. So you decide to be on the lookout for anything suspicious in the next few days.

At work the next morning you share your encounter with this person with a coworker and they mention that something similar happened to them a few months back. The same profile of this character was even described.

* What exactly could be going on here?
* Why do the sort of questions the stranger asked, matter?
* How could this simple information then be used against you?
* In what ways can this scenario apply to the cyber defense competition?

If this was a one time occasion then the stranger was probably just being friendly and presented no real danger but most of the time when people approach you and they are a little over the top, it is because they want something from you. In this case, your coworker had a similar experience.

Social engineering experts are great at extracting information from seemingly insignificant questions. They can use what they learned about your dog and try to use it as your password. Or send you a phishing email from a “bookstore” that you would be tempted to open. They might even go as far as to break into your house if you mentioned that you would be absent over the weekend.

The Five Qualities of Highly Effective Scams

We have talked an awful lot about social engineering attacks and scams that people may use against you. Sometimes they are blatant and obvious, such as the good old, “your extended warranty has expired” phone call. But most of the time professional criminals are experts at hiding their intentions and great at manipulating people, so much so that they don’t even have to break into your house to steal your things because more often than not, their victims willingly hand over what they want.

So how can we become better at spotting these types of schemes? What are some of the main characteristics indicating that something fishy might be going on? As a side note and as one of the two authors of this curriculum I can admit that I have been scammed before, many times. Especially when I visit big cities. But each time I learn something and it usually doesn’t happen again. Anyway, here are the five things that point to a social engineering attack or a scam of some kind:

* A heavy sense of urgency is evident
* You are being asked to take actions that goes against protocol
* The attacker is being overly curious, pushy even aggressive when you fight back
* The attacker’s vernacular is confusing and hard to follow
* You get a sense of something being too good to be true

Manipulation is not limited to these qualities and there may as well be numerous other pointers that give away something is about to go south.

What do you make of these five points? Did we miss anything? Were any of them surprising to you? How can we make sure we learn from our past mistakes and head into the future as wiser and more mature individuals?

In any case, if you feel as though you’re in the middle of a social engineering attack. Stop what you are doing, including the sharing of information with the attacker and notify your security team of everything that has occurred so far.