Social Engineering: What Is It? Types of Social Engineering Attacks and How to protect yourself from them

With human error being the top cause of data breaches in all kinds of organizations, it isn't surprising that a type of cyber attack that **exploits human psychology** would be **one of the most common threats to enterprise security** we see.

When we recently wrote about history's most famous hackers, we mentioned Kevin Mitnick, who predominantly used social engineering tactics to earn the title of "the world's most famous hacker." Since then, the techniques used in social engineering attacks have become even more sophisticated and more dangerous. Today, we'll explore what **social engineering is, exactly, as well as the most common types of social engineering attacks in use**, and how we can protect ourselves from this constant threat.

What is social engineering?

Social engineering attacks usually exploit human psychology and susceptibility to manipulation to trick victims into uncovering sensitive data or breaking security measures that will allow an attacker access to the network. Something that makes social engineering attacks one of the most dangerous types of network threats is the general lack of cybersecurity culture. In an organization, **employees are the first line of defense** — and they're all too frequently the weakest link, so much so that all it takes is one employee clicking on a suspicious link to cost the company tens of thousands of dollars.

Here's an example of a social engineering attack: An attacker approaches its target using social media, and gains his/her trust. Putting faith into that trust and confidence, the target forms a relationship with the attacker, who tricks him/her into giving away sensitive information that will allow the attacker access to bank account information.

That's just one example. Now let's look at all the different types of social engineering attacks one can encounter.

Types of social engineering attacks

Hackers are constantly developing clever tactics to trick employees or individuals into divulging their sensitive data. **Getting familiar with the types of social engineering techniques they use gives you a better chance of staying safe**.

Phishing

Phishing is not only the leading type of social hacking attack, but also of all types of cybercrime in general. Attack vectors commonly used for phishing include **email, SMS, social media, and more, with email-based phishing campaigns being the most frequent**.

Here's a common scenario involving a phishing email: An attacker impersonates a legitimate company such as a bank or a major corporation, and the email will almost always feature a call to action that gives a sense of urgency to the target. It might tell them that they need to change their password due to detection of suspicious activity on their account, or even that they've won a prize, and they're required to input their private information to claim it.

All phishing tactics follow the same pattern: **tricking the target into clicking on a malicious link that will take them to a website that may or may not impersonate a legitimate one, asking them for their credentials, then injecting malware or viruses or leading their target to a ransomware attack where they'll be asked for money to unlock private data.**

Phishing tactics often include a large target list, with all entries getting the identical email so email providers can easily mark them as spam to help protect us. But, there are still other forms of phishing campaigns, some more dangerous, than others.

Spear phishing

As opposed to “traditional” phishing campaigns, spear phishing is **highly targeted toward either one specific organization, a specific sector within an organization, or even just one employee**.

Spear phishing does require more effort from the attacker’s side, as he needs to perform a full OSINT investigation on the victim(s), perform extensive research about everything surrounding them and **customize the email**, which makes it much harder to distinguish from a legitimate email and ups the attacker’s chances of succeeding.

We often see spear phishing targeting financial departments for financial gain, or newer employees as they’re easier to trick into giving away private information and credentials.

Whaling

Whaling attacks are **another subcategory of phishing**. What distinguishes it from phishing and spear phishing is its choice of targets. **In whaling, the target holds a higher rank in organizations — such as CEO, CTO, CFO and other executive positions**.

Otherwise, they use similar tactics to steal sensitive information, gain access to restricted systems, and any data with high financial value. **Whaling is often aimed at government agencies or major corporations**.

The name “whaling’ alone indicates that bigger fish are targeted.

Vishing

As you may have noticed, phishing is mostly done over email, but that's not the case for this type of phishing — called "vishing."

Vishing **uses phone calls** to trick people into giving away their private data. The attacker creates a fake phone number, calls an individual posing as a bank or some other service provider, and asks for their credentials or bank account details. As it's quite frequent that we get calls from our bank it's no wonder attackers have used this to their advantage.

For more details on phishing, check out our blog post which also examines this type of cyber attack.

Baiting

In movies we've often seen that bit of comedy with someone finding a dollar bill on the floor, then, trying to reach for it with the bill constantly getting yanked farther and farther away. This eventually leads the unwitting soul face-to-face with the pranksters who then laugh at such susceptibility. Well, the digital world also has its own version of baiting.

Baiting involves a **digital or physical object** that is alluring to its target, and will either ask for their credentials or inject malware into their system. When it comes to **physical bait**, we often see attacks using USB flash drives that are left 'laying around' for a curious individual to pick up and insert into their machine. This infected USB drive will then inject malicious software into the victim's machine and allow attackers access to it.

With **digital bait**, we often see a download link to popular music, movies or even sought-after software that is actually a malicious link in disguise, one that will install malware in the victim's computer.

Quid pro quo

If you saw the movie Silence of the Lambs or know a little Latin, you've heard the phrase "Quid pro quo."[2] **It means an exchange of goods or services, essentially, an exchange of "something for something."**

Quid pro quo is often regarded as a **subcategory of baiting** but what differentiates it from regular baiting is that the **attacker offers something to the target in exchange for divulging private data, or any other specific action that will get attacker what they want.**

The most common scenario we see with a quid pro quo attack involves an **attacker posing as technical support or a computer expert who offers the target assistance with a real problem, while asking for their login credentials or other private data.**

This type of attack can also include any action or service the hacker will offer to the target either in exchange for sensitive information or with a promise of a material prize. Leveraging on people's love of (seemingly) affordable or even **free gifts and services**, quid pro quo attacks can be quite successful.

Pretexting

Pretexting may be hard to distinguish from other types of social hacking attacks. What really sets it aparts is that **it can be performed using different attack vectors, including email, phone calls or even face-to-face communication.**

In a pretexting attack, **the attacker poses as a person of trust**, such as a family member, someone from the target's organization like a member of the IT department or a manager, **or any other individual holding authority over the target.**

By impersonating someone known and trusted, it's easy for the attacker gain private information from the target or even ask for money directly. This type of attack can also be used to uncover security vulnerabilities or backdoors into an organization's infrastructure.

Because it exploits some of the most human vulnerabilities — including trust and familiarity — pretexting can be extremely dangerous. **It's important to double-check the sender or caller who seems too direct regarding what they need from you**.

Tailgating

Tailgating, also known as piggybacking, is a type of social engineering attack that's a little different from the others because **it's almost exclusively physical in its attack vector**.

This type of attack involves an **attacker asking for access to a restricted area of an organization's physical or digital space**. A common scenario we see in tailgating is an attacker **asking an employee to "hold the door" to a restricted area because they forgot their access or identity card, or even merely asking an employee to borrow their machine.**

This attack may be quite useful in large organizations where employees aren't likely to know all of their co-workers. They're often easily tricked into yielding access.

Scareware

With the growing fear culture surrounding cybersecurity, scareware is a very successful form of social hacking. **It appeals to people's anxiety and fear to get them to install malicious software**.

Scareware is often seen in pop-ups that tell the target their machine has been infected with viruses. They can convincingly appear as though they're coming from a legitimate antivirus software company. **These**

pop-up ads always have a sense of urgency in telling you to quickly download their software if you want to get rid of the virus that has, unbeknownst to you, infected your computer.

Besides pop-ups, scareware can also present itself as emails informing you that your computer is under threat (and that you need to install their software ASAP). This software will of course cost you some money, so you'll need to input your bank credentials. Once you have fallen victim to this type of attack and installed their "antivirus" software, your computer will then get infected with malware, giving attackers access to even more of your private information, on top of the bank information you've already given them for that fraudulent software purchase.

5 WAYS TO PROTECT YOURSELF FROM SOCIAL ENGINEERING ATTACKS

Because social engineering exploits basic human behaviour and cognitive biases, it's hard to give foolproof tips to steer clear of its dangers. It might even take a lot of self-help to stay unharmed through many of these threats. That's why we've compiled a list of 5 ways you can, at the very least, harden your inner and outer defenses against social engineering attacks.

1. Be a skeptic. ALWAYS

Never let anyone tell you that you're too paranoid when it comes to security. Crackers actually want to exploit your emotions, often leveraging your fear and trust, so you need to be on alert whenever someone attempts such an attack.

If you ever sense that someone is asking you questions regarding the topics commonly used as added protection to your accounts, such as your mother's birth name, your first pet's name, your birthplace, etc., make sure you really know this person and verify that he or she is truly a person of trust.

Should you receive any suspicious emails from a distant relative or a member of your staff, always verify that's really the person you're talking to and make sure he or she is authorized, even on a personal level, to ask you for private information as appropriate.

It's never bad to be a skeptic. And when it comes to social engineering, it may be your best bet.

2. Educate yourself and your staff

As we mentioned, **the lack of cybersecurity culture in many organizations is one of the biggest reasons behind the success of social engineering attacks.** For that reason it's important to train your staff and familiarize them with all these different tactics.

Besides your staff, you yourself need to understand social engineering in its many forms. Because social engineering is designed to play with human nature, you as a member of an organization's staff are also a potential target for cyber criminals.

3. Update, update, update

As we've seen, some types of social engineering attackers **will try to find any loopholes or security backdoors in your infrastructure.** That's why it's crucial to keep all of your software up to date.

Staying on top of **all newly released security patches** can help you mitigate plenty of attacks, even if you don't stick exclusively to those related to social engineering.

4. Prioritize

To really know what to protect, you need to get into the minds of cybercriminals. This will be done most efficiently by **having a red team in your line of defense**. If you, for some reason, don't have a red team then you'll **need to work on discovering your most critical assets that are likely to give power to possible attackers.**

Organizations will often give importance to the information they deem most critical to their **financial and commercial gain, but that's just what the attackers want you to think**. This is why you need to rethink what are really the most valuable assets to your organization, those that hold the key to uncovering the depth of your sensitive data and protect it the best you can.

5. Keep your professional and private accounts safe

In some of these social engineering attacks, we mentioned that an attacker will conduct extensive OSINT and offline research on your life, behaviour, habits and patterns. **For this reason, it's very important that we keep all of our professional and private accounts safe.**

It's not unusual that an attacker will raid our Facebook and LinkedIn profiles to find answers to common security questions, or to examine everyday behaviour. With so many social media platforms in use, it can seem difficult to keep track of all those different passwords — but it's crucial if we want to stay safe, both online and offline.

Use security questions with answers you don't divulge on any other platforms, employ 2FA and always use the strongest passwords you can think of. And, we know those notebooks specially designed for you to input your passwords may appeal to your "aesthetic" but you really don't want to keep your safety, and the safety of others, so easily accessible.

Conclusion

When attackers use human emotion as a point of contact, it's easy for any of us to fall victim to them. Whether you're an individual, an employee or part of the higher management of an organization, it's important to **always keep your guard up — you never know when malicious actors can strike**.