Introduction to Social Engineering

Brought to you by Assemble You.
It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

What does "Black Friday" mean to you? For millions of people, it's the biggest shopping day of the year. But it's also a very clever piece of marketing. We all fall victim to the time pressure that 24-hours-of-low-prices thrusts upon us, and many of us save specifically for it. This 24-hour time pressure is not the only strategy deployed by marketers, either. There are always news stories and viral videos showing people camping outside stores to get inside first and desperate people physically fighting over flat-screen TVs. But this colossal fear of missing out on amazing deals is artificial and very much intentional. Creating a fear of missing out - or FOMO as it's often shortened to - is a specific, deliberate strategy.

Black Friday is an example of what's called "social engineering." It is the art of manipulating human behavior to get someone to do something.

In cybersecurity specifically, though, social engineering implies something more menacing.

In his book *How to Hack a Human: Cybersecurity for the Mind*, security expert Raef Meeuwisse defines social engineering as

> *...the act of constructing relationships, friendships or other human interactions for the purpose of enticing the recipient to perform an inadvisable action or reveal secret information.*

In cybersecurity terms, this means preying on our emotional responses to make us voluntarily compromise our own security.

Today, we'll learn about social engineering attacks, the standard techniques used in them, and how we can protect ourselves against them.

Security vendor PurpleSec claims that 98% of cyber attacks use social engineering. Hackers need a vulnerability to start their security breach - most frequently a human. In *Secrets and Lies: Digital Security in a Networked World*, Bruce Schneier writes that

> *People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.*

Bad actors exploit people by tricking them into doing something they want them to do using various methods. Once a barrier is removed via social engineering, hackers have a way into a system or a network to steal confidential and sensitive information.

A prominent example of successful social engineering is the US Department of Justice's data breach in 2016. 200GB of confidential data was exposed after a hacker successfully impersonated a staff member. A compromised internal email address and some basic deception allowed the attacker to convince other staff to provide full access to internal files.

This is an excellent example of how damaging even the simplest social engineering techniques can be.

The DOJ example seems laughable, but it's easy to be misled. Have you ever received a text or email claiming that "your parcel was undeliverable" which included a code that looked legit? Delivery scams are big business - Caleb Barlow, vice president for IBM Security says it's a $445 BILLION scam.

Maybe you've received an email stating that your bank account is locked because of various unsuccessful login attempts. The email also contains a link to unlock the account or reset the password. When an email scam is well-designed, most of us would simply click on the link that the hackers wanted. When we visit the website, a perfect replica of the actual bank website, we enter our credentials. The hackers on the other side receive your login credentials. Alternatively, clicking on that link can drop malware onto your system, which can pass on a lot of information from your system to hackers. That's their successfully executed first step. This is an example of a specific technique - **trust** - in action.

It's not the only technique. So, let's quickly learn about some more.

The next is **authority**.

With this, the hacker pretends to be someone with authority, such as a police officer. They use that authority to get information from the target. For example, the hacker pretending to be a police officer may call the CEO's assistant and ask for the CEO's mobile number and email address. If the assistant refuses, the hacker can pressurize and threaten consequences for non-cooperation until the receptionist eventually complies.

Another technique is **urgency**.

With this approach, the hacker creates a sense of urgency for the target. It's done via email or through a phone call, and the target is given no choice to think but instead forced to act quickly. For example, the hacker may call a target to get their user credentials under the pretense of helping them to reset their password. The hacker can inform the target that the organization's user accounts have been leaked, and before any user account is compromised, the passwords need to be reset. The target may simply reveal the password, as they're under the illusion that the clock is ticking.

The final technique we'll discuss is **intimidation**. Suppose your boss had a presentation to prospective investors coming up, and you received a phone call. On the other end, someone claiming to be with your boss says his files - including a confidential revenue file - are corrupt, so you need to email them immediately. Perhaps you'd decline initially, but the bad actor could intimidate you by saying something like, "Look, if you want to be responsible for this six-figure opportunity falling through, that's okay. I'll tell him you refused to help." The hacker has created a situation where you feel trapped and afraid of the consequences.

Using one of these techniques, hackers conduct various attacks in social engineering. We need to understand each type to differentiate between them, as they all have unique characteristics. So, let's take a look at them, starting with phishing.

Phishing is considered the most common type of social engineering attack. It is performed via email with spoofed email addresses containing a specific message in the body text. For example, it can talk about a locked bank account or the recipient winning a million-dollar through a lottery. The email body also contains links to trick the recipient into providing personal information, such as a credit card or social security number. The email might even ask you to reset your password by clicking on a link.

So, why do hackers rely so heavily on phishing to conduct security breaches? The answer is simple – they only need an email address to send out a phishing email, and email addresses can be easily acquired with ea. Astonishingly, in 2020, **75% of companies** globally were phishing victims.

Recent data on hostingtribunal shows that 60% of the companies lost data in phishing. In comparison, 52% had been compromised with the user credentials. Another 29% ended up with malware infection, which damaged their networks.

Next up, the whale phishing.
It is a type of phishing attack. Think of catching the big fish in the ocean – this is what symbolizes the whale phishing attack. The hackers go after the top executives in an organization to get confidential information. They use the same method of sending out a phishing email but only to the senior executives. For example, a spoofed email from the CEO is sent to the Chief Financial Officer (CFO) with the latest revenue and profit information.

Similar to whale phishing, spear phishing is another type of phishing attack. Whereas a normal phishing attempt may be sent to many email addresses, a spear-phishing attack is more targeted.

Another type of social engineering attack is tailgating, and it's a bit more old-fashioned.

Have you ever walked through a door behind someone without flashing your ID badge? The first person flashed the ID badge to unlock a door, but you conveniently followed your colleague right through the door. Well, this is tailgating. Tailgating relies on common courtesy and people's natural tendency not to challenge others.

Next up is baiting.
We have all seen the free giveaways via internet ads, emails, or even television ads. Hackers use baiting to exchange confidential information for something valuable. For example, a hacker may offer money or even a gift card to complete a survey hosted on a spoofed website. When we log on to this website thinking it's legitimate, the hacker captures the user credentials

The final type of social engineering attack is a honey trap.
A hacker convinces the victim about romantic feelings. When the victim is convinced, the hacker convincingly gains the information. According to the FBI, romance scammers defrauded Americans out of $1 billion in 2021.

So, now we know the different types of social engineering techniques and attacks, let's get onto how we safeguard ourselves.

It is nearly impossible to stop social engineering attacks from happening. However, several methods can significantly reduce the chances of falling victim to one.

The first method is **training**.
Everyone in an organization should undergo a basic level of security training. Employees should know about social engineering and specifically phishing attacks. Not everyone needs to be a security expert, but fundamental knowledge can prevent security breaches.

The next one is the **restricted access privileges**.

Users within an organization must be assigned permissions on a need-to-know basis. That way, even if the hacker can get into the system, though this method won't protect the data on the network, it will delay the process.

Two-factor authentication is another imperative measure we must take.
In most cases, hackers are after user credentials, which they later use to exfiltrate and steal information. With two-factor authentication in place -even if hackers get the user credentials of a target - they still require the second factor, be it a PIN, One-time Password, or even a smart card.

Another critical method is **security policies**.
Security policies are used to define the security posture of an organization. The security policies should focus on passwords, training, and infrastructure. For example, a password policy should drive the users to use complex passwords and change them after a certain number of days.

Last but not least, **social engineering campaigns**.
These are good to verify the knowledge of social engineering of the users within the organization. The outcome of a social engineering campaign can help you further train the users. You can also conduct a phishing simulation with the users and determine the number still falling for social engineering.

So, that's a lot of information to digest. But now is time to take action. This week, we'd like you to think about your passwords - are they easily guessable if somebody got to know you? Do you use Two-Factor Authentication? If not, we strongly encourage it.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] What is Social Engineering?
- [Video] The Science Behind Human Hacking (Social Engineering) - Christopher Hadnagy
- [Video] The Dark Arts of Social Engineering – SANS Security Awareness Summit 2018
- [Article] What is Social Engineering?, Kasperksky
- [Article] Social Engineering - It's Not Just About Phishing, K. Townsend
- [Article] Social Engineering Principles, D. Gibson
- [Infographic] Social Engineering and How to Win the Battle for Trust
- [Book] Secrets and Lies: Digital Security in a Networked World, B. Schneier
- [Book] How to Hack a Human: Cybersecurity for the Mind, R. Meeuwisse