SecurityAwarenessNews
the security awareness newsletter for security aware people

What Social Engineers Don't Want You To Know

Principles of Persuasion

Common Attack Methods

Building Your Cognitive Defense

Principles of Persuasion

Social engineering refers to attacks that use deception and manipulation to trick individuals into taking actions that are against their best interests. Nearly every successful attack has one thing in common: the targets don't know they're being scammed.

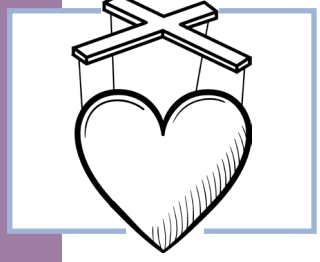
Attackers accomplish this by exploiting natural human tendencies and emotions. They use well-established principles of persuasion to trick people into revealing information or performing a dangerous action. Let's review a few common principles social engineers live by that they don't want you to know about.

Principle 1: Be a Good Storyteller

Attackers create believable scenarios to make their requests seem legitimate and logical. A compelling story can persuade someone to lower their guard and become more receptive to the situation. Getting people to buy into the social engineer's narrative is at the core of successful attacks.

Principle 2: Establish Authority

By impersonating a figure of authority, such as a manager, IT administrator, or government agent, social engineers attempt to exploit our natural tendency to follow a leader. People are far less likely to question or refuse a demand when it appears to come from someone in a position of power.



Principle 3: Strike at the Heart

Social engineers exploit powerful emotions such as fear, greed, curiosity, and the desire to be helpful. An emotional response bypasses logical thinking, causing people to react instinctively rather than critically analyzing the situation.

Principle 4: Push a Sense of Urgency

Attackers create a false sense of urgency to pressure people into making a quick decision. They will insist that a critical action must be taken immediately, or something bad will happen, such as losing access to an account or incurring additional fees due to an unpaid debt.

Principle 5: Gain and Abuse Trust

The end goal of many attacks is to gain someone's trust. Social engineers want to avoid suspicion and remove skepticism from any given scenario. They often accomplish this by first researching their targets via social media and other forums. This helps them gather useful intel that can make them appear trustworthy.

Common Attack Methods

Gaining an understanding of how social engineers launch their scams is one of the best ways to defend against them. There are many ways these attacks can materialize. Let's review a few of the most common.

Phishing Emails

Phishing attacks refer to attempts by scammers to get people to open malicious links or attachments, or reveal confidential information. The most common come in the form of fraudulent messages disguised to look like they are from a legitimate source, such as your bank or a popular online service. These emails often make alarming claims, such as "Your account has been suspended due to fraudulent activity!"

Phone Calls

Voice phishing attacks involve a scammer calling you and impersonating someone trustworthy, like a tech support agent, a bank's fraud department, or a government official. They create a fake problem that requires immediate action, pressuring you into revealing sensitive information, such as passwords or financial details, or even granting them remote access to your computer.

Text Messages

Similar to phishing emails, this attack uses deceptive text messages to lure you into opening a malicious link. These messages typically create a sense of urgency with fake package delivery notices, bank account warnings, or prize notifications, leading you to fraudulent websites designed to steal your personal information or passwords.

USB Flash Drives

Attackers have been known to leave malicious USB flash drives in public areas, hoping that someone's curiosity will lead them to plug it into their device. Although the flash drive appears normal, it's specifically designed to infect devices with malicious code that can steal confidential data.

Social Media

Attackers love to slide into people's direct messages with lucrative promises. This is commonly the case in investment scams, where the attacker assures you that you will make a substantial amount of money by investing in a form of digital currency. They will send you screenshots of the money they've made and promise that it's a foolproof way to earn large amounts of money.

Building Your Cognitive Defense

Social engineering targets human psychology by creating situations designed to induce feelings of pressure, fear, or even sympathy for the attacker. It's all a mind game, which is why it's vital for you to build and sharpen your cognitive defense.

This means training your mind to recognize and resist these psychological tricks. It involves developing a habit of pausing to think critically and allowing your logical reasoning to override an emotional reaction.

Here are a few ways to sharpen your cognitive defense:

Question Everything

Do I know you? Why are you contacting me? Why do you need this information? Is this link safe? With a small amount of effort, you could answer the biggest question of all: Am I being scammed?

Stay Alert

When handling requests for money or confidential information, pay close attention to the tone and context of the situation. Be extremely careful with any messages that contain links or attachments, even if they appear to come from someone you know. Never assume someone is who they claim to be.

Slow Down and Think

Remember, social engineers find success by manipulating human emotions. If you receive a message or phone call that evokes a sense of urgency, contains threatening language, makes unrealistic promises, or otherwise provokes your emotions, stop and think. Those are common warning signs of scams.

Prioritize Your Privacy

The more information a social engineer can gather about you, the easier it will be for them to appear legitimate and gain your trust. Limit what you share on social media and other forums. Consider setting your social profiles to private. Vet people before you connect.

Trust Your Instincts

Most scams can be thwarted by simply using situational awareness. Follow your instincts if something seems off or too good to be true. A little bit of skepticism could be all it takes to circumvent social engineering attacks. Utilize situational awareness both online and in real life.