Locked24

Everything You Need to Know About Social Engineering

locked24.com

Everything You Need to Know About Social Engineering

Every day, billions of people across the globe receive even more billions of spam messages. Most of these emails from someone claiming to be someone they're not. Whether they're in the form of emails, texts, phone calls, you've no doubt received them yourself.

These messages might be from fake companies claiming you won fake prizes, or from government entities warning you your Social Security Number has been frozen unless you pay $500 in Amazon gift cards. These are the obvious spam messages (though millions of victims fall for them), but there are more nefarious scams at play too.

Have you ever received an email or phone call from someone claiming to be from your company that just didn't feel right? It might look legit on the surface, coming from a spoofed but real-looking internal email address complete with signature and images, but something's phishy.

If this has happened to you, either personally or at work, there's a high likelihood that it was a social engineering attempt to gather personal or company information.

What's Social Engineering?

Social engineering, in its broadest definition, is any act that influences someone to do something that is not in their best interest. It is the art of manipulating people to do what you want.

Some common scenarios and targets of social engineering include the following:

- HR or payroll asking for your banking information or your SSN
- IT asking for your username and password
- A coworker or manager sending you an unexpected attachment with little to no explanation
- A manager or executive asking for help or a favor, usually involving you buying gift cards and emailing them the card numbers and PINs

Social engineering can happen to anyone at any time, but it's particularly dangerous in an office setting where multiple people with the same information mean multiple opportunities to exploit.

Humans are gullible creatures. The average person will believe just about anything if you pitch it to them right. Hackers and cybercriminals use social engineering to great effect in all kinds of different attacks. According to Cybint, 95% of cybersecurity breaches involve social engineering and/or human error.

In this quick eBook, we'll outline the 6 key principles and 4 major threat vectors of social engineering attacks. We'll also discuss the best countermeasures to keep you, your employees, and your business safe.

6 Key Principles of Influence for Social Engineering Attacks

Based on the Theory of Influence by Robert Cialdini, Regents' Professor Emeritus of Psychology at Arizona State University

Reciprocity

Have you ever gotten a free sample? It's because marketers know people are apt to return favors. So do social engineers. They will make it seem like they're doing you a favor, and you'll eventually return in kind.

Commitment & Consistency

If you state a goal orally or in writing, you're more likely to follow through on it—even if the incentive is then removed. Social engineers will try to get you to commit to something knowing you're more likely to do what they ask.

Social Proof

People tend to follow the crowd and do what they see others doing. Social engineers will make it seem like they've helped your friends or team members or hundreds of other customers hoping you'll follow suit.

Authority

We respect those in authority—even if they only seem important. Social engineers will pose as a manager or executive, an IT technician, security, or anything like that to get you to play along.

Likeability

You're more likely to listen to someone you like, and social engineers may try to sweet talk you into believing something or acting on something not in your best interest.

Scarcity

The laws of supply and demand are at work here. If you think supply is low, you're more likely to act on something more spontaneously. "Exclusive" offers to call now are an example of this. Social engineers will try to create a sense of urgency to get you to bite.

4 Major Social Engineering Vectors

Phishing

One of the most common forms of social engineering, phishing refers to emails sent out en masse and betting on a small percentage—but a still large number—of bites on their bait. Here are some common indicators of a phishing attempt:

- Suspicious sender's address
- Generic greetings and signatures with no contact information
- Spoofed hyperlinks
- Poor spelling and layout
- Suspicious attachments

Vishing

You'll notice a pattern here, but vishing is voice phishing done over the phone to gain access to private information. You've no doubt received voicemails saying your SSN is flagged for fraud and yada yada yada. That's vishing.

Smishing

And smishing is SMS phishing to get you to act on information from an SMS text message. You'll see these a lot with texts claiming you won a prize, or that there was a problem with a nonexistent shipment, asking you to log in and verify information.

Impersonation

Not much explanation is needed here. Social engineers may try to gain entry into a secure area by pretending or pretexting to be someone important. You can get into almost anywhere with a high-vis vest, hard hat, and a clipboard.

How to Combat Social Engineering

Social engineering is a major concern for many businesses, but you can take steps to mitigate the risk of human error. Make sure you and your employees practice these safe steps to avoid falling victim to social engineering attacks:

- Be wary of any unsolicited calls, visits, or messages from people who want information about the business or its employees
- Don't give out information that isn't publicly available
- Don't send sensitive information over the internet or through email (unless it's properly encrypted)
- Install and maintain antivirus, spam, and firewall software
- Conduct periodic social engineering tests on employees

Now that you know the principles and vectors of engineering and how to combat malicious attempts to access sensitive information, you can begin to put plans in place to minimize the risk of that information falling into the wrong hands.

A professional assessment from Locked24 will ensure that all your vulnerabilities are addressed, including educating your employees and providing ongoing education.

Locked24 is here to help

Social engineering is just one of many ways hackers will try to access your secure systems, and good employee training on social engineering is a huge first step towards good cybersecurity.

Don't let unknown security vulnerabilities be the downfall of your business. Talk to our security experts for a free security inspection and assessment. We'll give you the best recommendations based on your needs and resources.

Call us today at 866-714-LOCK
or
send us a message online here!