Putting the best foot forward against fraud

The advent of digital communications has helped to bring people from across the world closer together. However, the same technologies used to propel this shift have also created new opportunities for fraudsters to exploit through so-called, 'social engineering' attacks.

Temps de lecture : minute

20 October 2022

This form of scam has been on the rise across Europe in recent years, and now poses a real and direct challenge to businesses and individuals alike. Thankfully, there are some simple steps that can be implemented to mitigate the threat.

In this article, we'll discuss what these steps look like in practice, and explain how they can be used to provide a strong barrier against fraudsters. We'll also highlight the many different forms that social engineering attacks can take, focussing on several key variants that are most common across Europe. Finally, we'll detail the potential damage that can be caused by a well-executed social engineering attack and provide examples of additional solutions, which can be leveraged to help halt attacks in their tracks.

What is social engineering?

Before all that however, let's start with the basics; what is a social engineering attack? It's a term that is used within a few different fields, but increasingly associated with the murky world of cybercrime. Simply

put, a social engineering attack normally refers to any scam that tries to manipulate an individual into making security mistakes or giving away sensitive information. These attacks can be used against either an individual, or a business, and can take place online, or in-person.

Take for example baiting, which is a form of social engineering scam that's very common across Europe. Baiting occurs when an individual is pushed to commit a specific action, either through a physical or virtual prompt. A common baiting tactic is to leave a USB drive on the desk of an unsuspecting individual in the hope they may insert it into a computer. If this happens, the USB then launches malicious software, which can extract sensitive data from the computer, or network of computers that it's now connected to.

The form of social engineering attack which is usually most recognised by individuals is catfishing. Catfishing has been documented across several TV and film projects in recent years, but despite this awareness it remains a big threat. Catfishing is when a fraudster creates a fake social media, or dating site profile to start a friendship, or romantic relationship with an unsuspecting victim. Next, fraudsters will look to use this relationship to manipulate sensitive data out of an individual, which can then be used for monetary gain.

To close out this section, we'll discuss the most used form of social engineering attack across Europe - phishing. Phishing occurs when a fraudster tries to trick an individual into revealing sensitive information, often using a fake email message, or phone call in the process. At one point in time phishing scams were very easy to spot, but this is no longer the case. Nowadays, sophisticated fraudsters are able to create incredibly hard to detect phishing scams.

Simple steps to help

It's important to remember that there are other forms of social engineering attacks outside of baiting, catfishing, and phishing. Unfortunately, scammers now have a vast array of tools and tactics at their disposal, which individuals and businesses must be weary of. Therefore, if you're looking to keep you and your business safe, then it's essential to be able to recognise some of the tell-tale signs of a social engineering scam. While this won't ensure your total safety, it will provide an important first line of defence.

To do this, individuals must further familiarise themselves with the different varieties of social engineering scam out there. Reading this article is a great first step, but don't be scared to go further in your research as it will all help. Raising awareness around social engineering attacks is similarly important within a business setting. To this end, it's never a bad idea to invest in some training sessions that help staff members to be more confident in identifying, and ultimately mitigating social engineering scams.

In a similar vein, it's also critical to establish effective security protocols for the handling and storage of sensitive data, both in your personal and business life. Broadly speaking, people should always be highly weary when asked to share personal information, either online, or over the phone. For example, if you receive a call that you're not sure about, simply hang up and call the company back on a phone number listed on their official website. A similar process can be followed for suspicious looking emails too.

The price of protection

The previously discussed recommendations are some fantastic first steps for businesses to take in their fight against fraud, however they probably

won’t hold off committed fraudsters forever. Thankfully, companies also have the option to invest in technologies that can provide more long-term solutions to the problem. For example, by hiring a social engineering prevention company, businesses can have their websites, or platforms checked for any vulnerabilities by a team of dedicated security experts.

Businesses should also look to leverage ID verification technologies within their systems, which allow email addresses and phone numbers to be checked for any of the tell-tale signs of fraud. Solutions, such as the one produced by *SEON*, allow companies and individuals to assess social and digital footprints in order to make highly accurate fraud decisions. With these systems in place, businesses and individuals alike can be more confident that social engineering attacks will be stopped in their tracks.

The time to act has come

From everyday consumers to huge multinational corporations, nobody is safe from social engineering attacks. However, from a monetary perspective, fraudsters have more to gain from targeting companies, which makes them an increasingly sought-after target. For those in the C-Suite, the challenge is to find measures that can limit the effectiveness of such attempts as they happen. Fundamentally, education around the topic is a huge part of the battle and is the starting point for change.

Sadly however, it’s almost impossible to prevent some social engineering attacks from succeeding. The good news is that the broader fraud prevention ecosystem is now becoming better at recognising when stolen information is being used. This more holistic approach to the challenge is certainly a step forward, but still can’t be relied on to wholly eradicate the problem. Particularly for businesses, the risk remains too great to ignore, which is why companies across Europe must remain focused on tackling the increasing challenge of advanced fraudulent activity.

Tamas Kadar is CEO and cofounder of *SEON*.

Article by Tamas Kadar