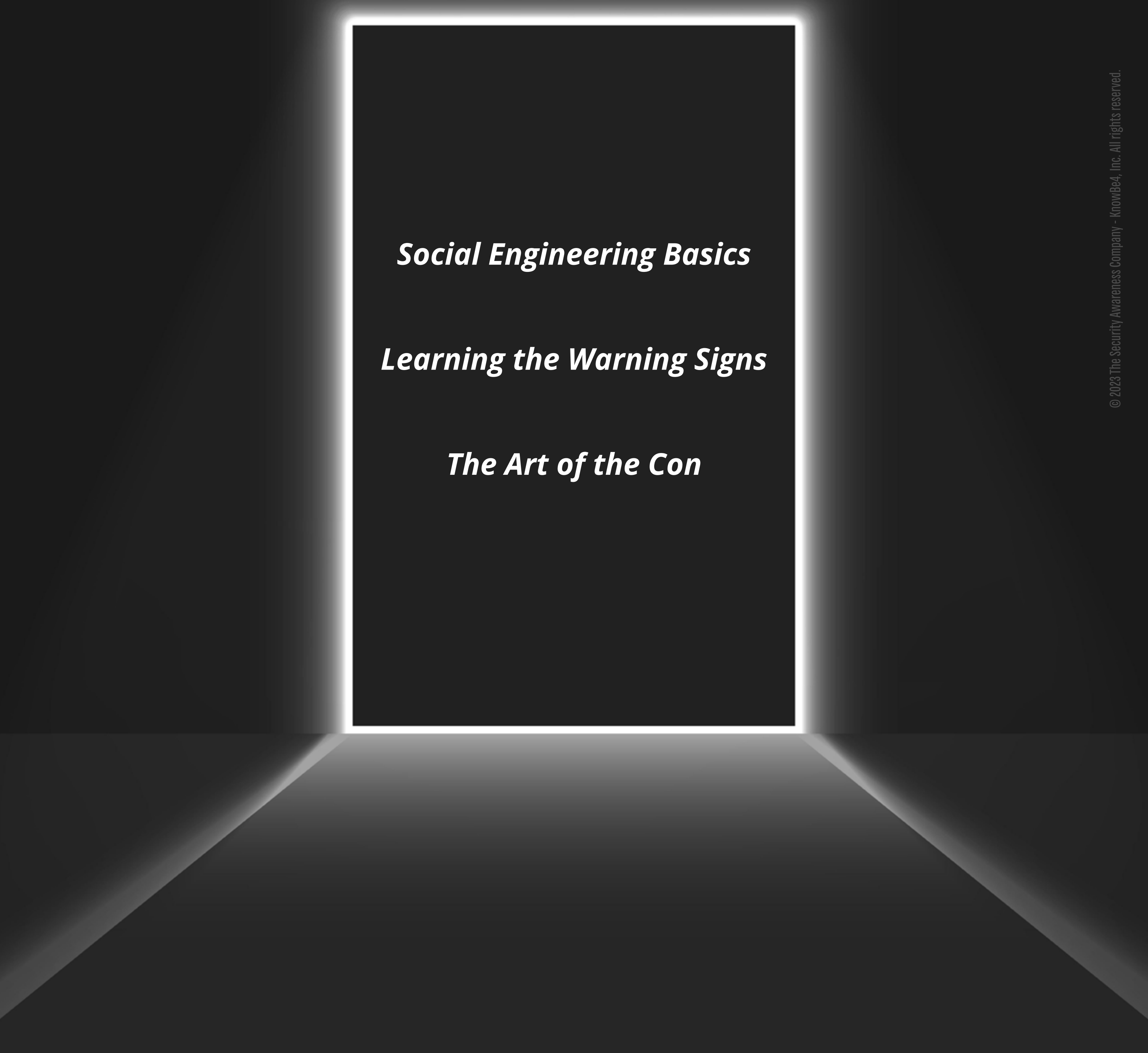
September 2023

SecurityAwarenessNews

the security awareness newsletter for security aware people

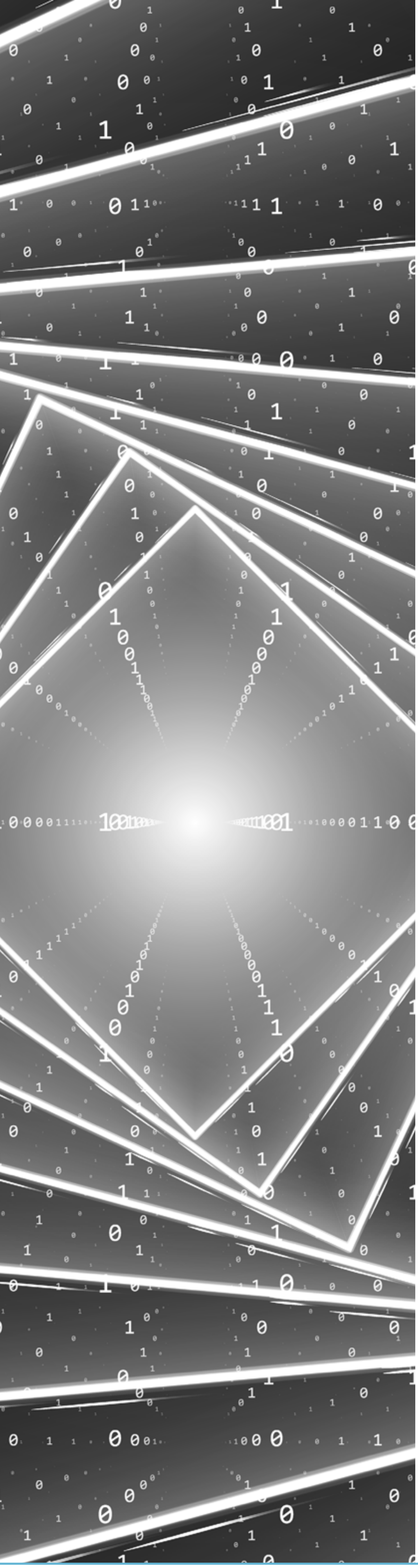
Fundamentals of Social Engineering



Social Engineering Basics

Learning the Warning Signs

The Art of the Con



Social Engineering Basics

Think like a criminal for a minute. You want to steal confidential information from an organization. What is the easiest way to accomplish that? One method is to spend years learning everything about networks, computing, and technology.

Or you could simply create a fictitious story that will trick someone into giving you the information you want. That's the fundamental basis of social engineering: hacking humans, not technology or devices. Let's review a few basics of this type of attack.

What is social engineering?

Social engineering is the use of psychological manipulation and deception to mislead people. Most social engineering attacks are carried out for a few reasons:

- ***Gain unauthorized access, both in the physical and digital realms***
- ***Convince people to divulge something confidential, like passwords***
- ***Scam people and organizations out of money***

How common are social engineering attacks?

Almost every scam involves some form of social engineering. In fact, the majority of security incidents at organizations worldwide are the direct result of these attacks. The reason is quite simple: it's easier to con people than it is to launch highly-sophisticated cyberattacks that involve complex technology or processes.

Why is social engineering so effective?

Social engineers are in the business of instigating and influencing human errors. Their top strategy involves creating fake yet believable scenarios that set emotional traps. Fear, love, curiosity, and urgency — as examples — are powerful ingredients social engineers use to gain and abuse someone's trust.

How can you protect yourself and your organization?

Slow down, think critically, and never make assumptions. Treat all requests for confidential information or money with skepticism. At work, follow organizational policies and report anything unusual immediately.

Learning the Warning Signs

While the attack methods of social engineers vary, let's focus on the main fundamental element needed to avoid becoming a victim: learning the warning signs. Here are five common signs of scams to stay alert for:

Fabricated Urgency

Social engineers make a living by convincing people to do something without thinking. That's why many scams feature a sense of urgency. Phishing attacks, which are any attempt to con people out of data or money, are especially known for setting an urgent tone. The goal is to make the target believe something bad will happen if they don't act immediately, like incurring additional fees because a payment is overdue.

Threatening Language

Fear tactics represent one of the most effective tools in the social engineer's toolbox. Creating scenarios that feature threatening language can quickly get the target's attention and scare them into action. Extortion is a prime example. The attacker will claim they hacked the target's webcam and recorded them doing something embarrassing. They will then threaten to release the video to all of the target's family unless a ransom is paid.

Impersonation

A great way to gain trust is by impersonating someone or some organization the target knows. For example, imagine getting a phone call from a bank representative who claims that there's an unusually large payment pending from your account. To block the payment, they need you to confirm your banking number and password. It may seem ridiculous that anyone would fall for this kind of scam, but it's unfortunately common.

Temptation

USB flash drives offer a lot of convenience for social engineers. They can use those handy items to spread malware (malicious software) without developing any sort of elaborate story to gain and abuse trust. Instead, this attack preys on curiosity by dropping USB drives in common areas. Many people will feel tempted to plug one in if they find it, which could then infect their device with malware.

Unrealistic Promises

Good news! You're owed a large family inheritance that will make you rich overnight. All you have to do is pay an upfront processing fee and the money is yours. Of course, the inheritance isn't real, and if you pay the upfront fee, you'll never get that money back. Similar to the banking impersonation example, it's hard to believe anyone would fall for the unrealistic promises of money and other things, but if they didn't work, scammers wouldn't even bother.

Stay alert for these common warning signs both at home and at work. They could be the difference between falling for a scam and protecting yourself and your organization.

The Art of the Con

Most people believe they'd never fall for a scam, including Carson and Riley.

They were hunting for a new apartment and couldn't believe their luck when they found the rental listing of their dreams that surprisingly fit their budget. They immediately responded to the listing and were thrilled when Taylor — the owner of the apartment — said it was still available.

After exchanging a few text messages, Taylor provided a day and time for them to check out the apartment in person. He was out of town for a few weeks, so he couldn't be there, but promised that the doors would be unlocked. "Just let yourselves in!"

The apartment looked just like the pictures online. In fact, it was even better. Carson and Riley joyfully texted Taylor that they were ready to move forward.

Within minutes, Taylor sent a request for the first month's deposit to hold the apartment. He said they could finalize the full application process when he returned from his trip. Without hesitation, they paid the deposit via an instant payment service.

A few days later, the couple invited friends to view their new home and check out the neighborhood. As they approached it, however, they noticed something strange. Someone was in the process of moving in.

They quickly learned that the apartment was already rented out to that person, who also informed Carson and Riley that the apartment was not owned by anyone named Taylor. Shocked, they immediately called and texted Taylor, who, of course, was unresponsive. They never heard from him again.

That's the art of the con: a seemingly trustworthy scenario that avoids suspicion and short-circuits logical thinking.

So what happened?

Carson and Riley are real people, and their story is something many others have experienced. It's known as a rental scam, where a social engineer lists a real property but isn't the owner of that property. Taylor likely broke into the home and unlocked the doors right before Carson and Riley showed up to view it.

How could it have been avoided?

While it may seem advanced, there were three major warning signs of a scam:

- ***The rental listing was too good to be true***
- ***Taylor was conveniently unavailable to meet in person***
- ***He immediately requested money before any lease was signed***

This example illustrates how important it is to stay alert for anything that might seem off or unusual. Never assume someone is who they claim to be, and don't ignore your instincts if you encounter a suspicious situation.