# SecurityAwarenessNews

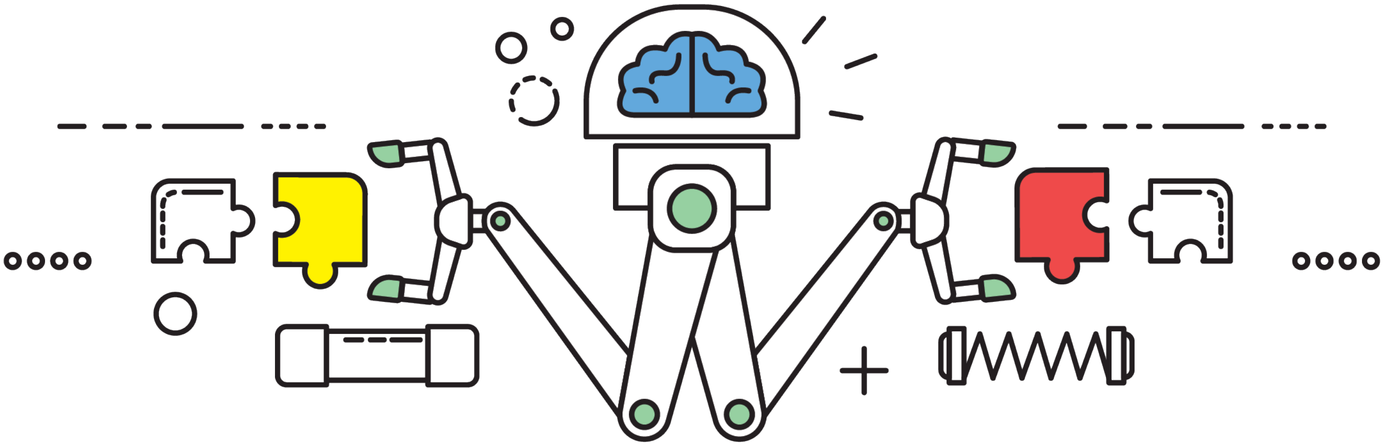
the security awareness newsletter for security aware people

# Hacking the Human

The Psychology of Scams

Reverse Engineering Social Engineers

You Clicked on a Phishing Link. Now What?



# The Psychology of Scams

In his book, *Influence: The Psychology of Persuasion*, Dr. Robert Cialdini explores six universal principles of influence that leverage human instincts:

1. **Reciprocation:** the desire to repay people.
2. **Commitment:** the work we put in to justify the choices we make.
3. **Social Proof:** the confirmation we seek from others that a decision was correct.
4. **Liking:** our tendency to agree with people we like and vice versa.
5. **Authority:** the increased likelihood of saying "yes" to anyone who we believe is an authority figure.
6. **Scarcity:** our desire to acquire something that has limited availability.

Each one helps explain the science behind how people successfully influence others and why some people fall for scams. In fact, we can easily find evidence of these six principles in social engineering, which is the art of manipulating and deceiving someone for nefarious purposes.

Consider, for example, how authority plays into business email compromise, or BEC. The scammer poses as an executive by setting up an imposter email account and sending requests for wire transfers of money to the executive's employees. The employees are likely to oblige because they believe the request came from their manager or boss—an authority figure.

Similarly, phishing attacks often create a sense of urgency. They might claim that an account has been hacked and that you need to log in immediately to update the password. The scammer in this case is leveraging the fictitious scarcity of time.

We could apply more examples to all six principles, but the key takeaway is that social engineers don't hack computers; they hack people through psychological manipulation. And by gaining an understanding of why scams work, we're better positioned to recognize when someone is trying to con us.

In short, when you receive requests to click on links or send money, always question if someone is attempting to leverage your human instincts. Ask yourself, "how logical is this? Is anything about the scenario different or odd? What would be the worst possible outcome, and how likely is it to occur?"

If you feel even a small degree of skepticism, don't take any action. Instead, follow organizational policies, and report the incident immediately.

# Reverse Engineering Social Engineers

Reverse engineering is a great way to learn how something works by examining or disassembling it. We already reverse engineered the psychology behind how scammers deceive people using the six principles of influence. Now, let's reverse engineer common ways social engineers and scammers manipulate emotions and learn how you can avoid falling for cons.

**Urgency:** Social engineers use persuasion techniques to short-circuit critical thinking. They want us to make a quick decision and take an action without considering the consequences.

**Prevention technique:** slow down, and use common sense. Carefully inspect all messages that urge you to take a quick action. Scrutinize the source, and question the logic of the situation.

**Fear:** Scare tactics, such as claiming that you owe money or must appear in court, are a great way to convince people to click on links or download attachments.

**Prevention technique:** relax and don't let your emotions drive your response. Ask yourself, "does this make any sense?" Or "What are the chances that this is a scam?" Again, slow down, and think critically.

**Desperation:** During stressful times—natural disasters, illness, financial pressure—people lose their ability to think clearly. Scammers attack those situations by offering unrealistic promises and get-rich-quick schemes.

**Prevention technique:** remember that if something is too good to be true, it's likely not true. This is especially the case with sudden, random offers of money.

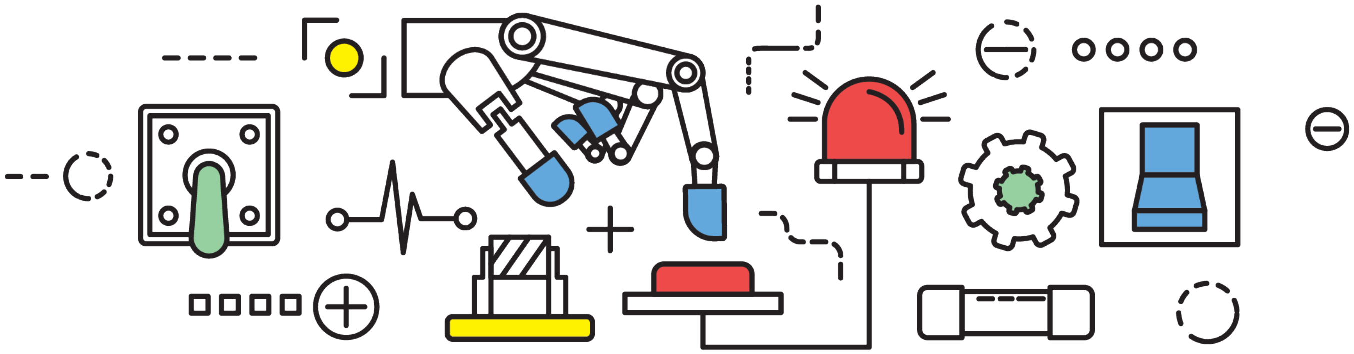
**Curiosity:** People are naturally curious. Social engineers know that when someone finds a random USB flash drive, they will be tempted to plug it in and view its contents—an easy way to infect computers with data-stealing malware.

**Prevention technique:** remain skeptical. Don't let intrigue convince you to plug in a random USB device or take any other potentially risky action, like clicking links or visiting suspicious websites.

**Sympathy:** Someone approaches an office entrance with their arms full of packages. The polite thing to do is hold the door open for them, right? Unfortunately, that sympathetic reaction could allow a social engineer access to a secured area.

**Prevention technique:** be firm but polite. Scammers know sympathy works. For example, they often ask for money using "woe is me" scenarios by sending messages that appear to come from people you know. Again, scrutinize the request, and never send money to anyone at random.

*Most social engineering cons can be foiled by slowing down, thinking critically, and never assuming someone is who they claim they are.*



# You Clicked on a Phishing Link. Now What?

Before covering the steps you must take if you click on a phishing link, let's establish an important caveat: phishing attacks come in many forms and yield many different results. Some attacks infect computers or devices with malware. Others send you to malicious websites. It's all about the intent and sophistication of the attacker. So the actions you take may vary by situation. Regardless, you should obviously avoid clicking on phishing links at all costs. But we're human, and bad clicks do happen. Here's what to do if it happens to you:

## At work or on a work device:

Stop what you're doing. Take no further action. Notify the appropriate party (IT helpdesk, for example) immediately. With timely reporting, you empower your organization to take swift action, review the event, and mitigate damages.

## At home or on a personal device:

- Disconnect the device from your network. This may help prevent any potential viruses or malware from spreading to other devices.
- Utilize antivirus and anti-malware tools. Run a deep scan that searches all files and folders; then follow the instructions if the software identifies a threat.
- Update passwords. Even though it can be tedious, update your passwords starting with highly sensitive accounts, like banking and insurance.
- Reboot and recover. In some cases, you may have to perform a full system reset, which will delete all files. If you have a reliable data backup, this step is less painful.
- Seek professional help. If none of the steps above fix problems with your device, you might have to seek help from a computer technician.

## Want to avoid all of this mess?

**Then don't overlook common warning signs of phishing attacks such as:**

- A sense of urgency. "Click now to immediately update your payment or lose service!"
- Threatening language. "Your loan has hit default and the bank has summoned you to court."
- Bad grammar. "Its without youre knowing that you accounts nolonger worked. Clicks here!"
- Generic greetings. "Dearest customer. We hope this email finds you most excellent."
- Unrealistic promises. "You won a lottery you never entered! You're now wealthy. Just click this link."
- Random requests for information. "Hello, I know we've never met but can you please send me all of your personal data?"

**Additionally, keep in mind that phishing is not limited to email. These attacks happen over the phone, via text message, on social media, and through any communication method you can imagine. So stay alert, treat requests for money or confidential information with skepticism, think before you click, and always follow organizational policies.**