OUCH! October 2022

The Monthly Security Awareness Newsletter for You

Emotional Triggers – How Cyber Attackers Trick You

Overview

Cyber attackers are constantly innovating ways to trick us into doing things we should not do, like clicking on malicious links, opening infected email attachments, purchasing gift cards or giving up our passwords. In addition, they often use different technologies or platforms to try to trick us, such as email, phone calls, text messaging, or social media. While all of this may seem overwhelming, most of these attacks share the same thing: emotion. By knowing the emotional triggers that cyber attackers use, you can often spot their attacks no matter what method they are using.

It's all About Emotions

It all starts with emotions. We, as humans, far too often make decisions based on emotions instead of facts. There is, in fact, an entire field of study on this concept called "behavioral economics," led by researchers such as Daniel Khaneman, Richard Thaler, and Cass Sunstein. Fortunately for us, if we know the emotional triggers to look for, we can successfully spot and stop most attacks. Listed below are the most common emotional triggers for which to watch. Sometimes cyber attackers will use a combination of these different emotions in the same email, text message, social media post, or phone call - making it that much more effective.

Urgency: Urgency is one of the most common emotional triggers, as it's so effective. Cyber attackers will often use fear, anxiety, scarcity, or intimidation to rush you into making a mistake. Take, for example, an urgent email from your boss demanding sensitive documents to be sent to her right away, when in reality it is a cyber attacker pretending to be your boss. Or perhaps you get a text message from a cyber attacker pretending to be the government informing you that your taxes are overdue and you have to pay now or you will go to jail.

Anger: You get a message about a political, environmental, or social issue that you are very passionate about — something like "you won't believe what this political group or corporate company is doing!"

Surprise / **Curiosity**: Sometimes the attacks that are the most successful say the least. Curiosity is evoked with surprise; we want to learn more. It is a response to something unexpected. For example, a cyber attacker sends you a message that a package is undelivered and to click on a link to learn more, even though you did not order anything online. We are enticed to learn more! Unfortunately, there's no package, just malicious intent on the other side of that link.

Trust: Attackers use a name or brand you trust to convince you into taking an action. For example, a message pretending to be from your bank, a well-known charity, a trusted government organization, or even a person you know. Just because an email or text message uses a name of an organization you know and their logo, does not mean the message actually came from them.

Excitement: You get a text message from your bank or service provider thanking you for making your payments on time. The text message then provides a link where you can claim a reward–a new iPad, how exciting! The link takes you to a website that looks official, but asks for all of your personal information, or says that you need to provide credit card information to cover small shipping/handling costs. This is a cyber attacker who is simply stealing your money or your identity.

Empathy / Compassion: Cyber attackers take advantage of your good will. For example, after a disaster appears on the news, they will send out millions of fake emails pretending to be a charity serving the victims and asking you for money.

By better understanding these emotional triggers, you will be far better prepared to spot and stop cyber attackers, regardless of the lure, technology, or platform they use.

Guest Editor

My-Ngoc Nguyen is the CEO/Principal of Secured IT Solutions. With 20 years of experience, she has deep experience with managing and maturing cyber security and risk management programs for both the federal government and private sector. She brings this experience as a Certified Instructor regularly teaching MGT512. https://www.linkedin.com/in/menop, My-Ngoc Nguyen | SANS Institute @MenopN.

Resources

Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Phone Scams: https://www.sans.org/newsletters/ouch/vishing/
Social Media Scams: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Messaging Scams: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Phishing Attacks: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/