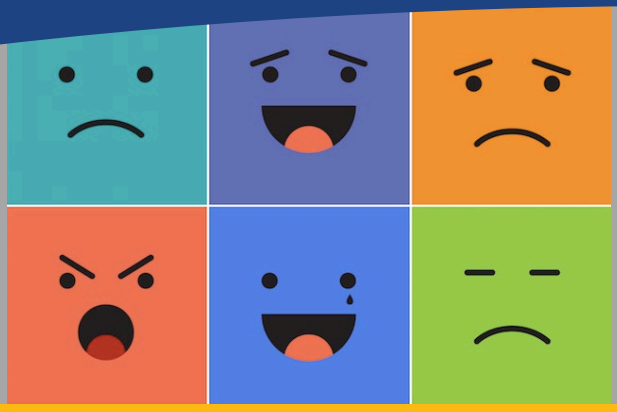
ISSUE
6
July
2023

Security Awareness Bulletin



In this issue

Cybersecurity: When the hack is in your head, not your computer!

Overview

Cyber attackers employ an assortment of strategies to dupe us into acts we should generally avoid: clicking on harmful links, opening malware-infected email attachments, making unwarranted purchases, or even surrendering our passwords. They cunningly leverage diverse platforms like emails, phone calls, text messages, and social media to launch these deceptive maneuvers. While the variety of their tactics can be daunting, a common thread linking most of these attacks is emotion. By understanding the emotional triggers cyber attackers exploit, we can discern their assaults, regardless of the method or platform they employ.

Decoding the Emotional Game Plan

The starting point of these attacks is always emotion. Humans are prone to making decisions on an emotional basis rather than considering facts. Behavioral economics, a field pioneered by scholars like Daniel Khaneman, Richard Thaler, and Cass Sunstein, dives deep into this phenomenon. If we familiarize ourselves with the emotional triggers attackers leverage, we are well-equipped to discern and counter most cyber threats. Here, we outline the most frequently exploited emotional triggers:

Instant Response: A Clever Ploy

Attackers exploit the sense of urgency effectively. They induce fear, anxiety, scarcity, or intimidation to pressure you into making hasty decisions. For instance, you may receive an email supposedly from your boss, demanding immediate dispatch of confidential documents. In reality, a cyber attacker could be masquerading as your boss.

Outrage: A Manipulative Technique

A message about a cause you ardently support, like a political, environmental, or social issue, can trigger anger and make you susceptible to cyber attacks.

Surprise and Curiosity: A Double-edged Sword

Often, the most effective attacks are those that reveal the least. Attackers evoke our curiosity with surprises, making us yearn for more information. For example, you might receive a message about an undelivered package prompting you to click a link, leading you straight into a cyber trap.

Trust: A Fragile Shield

Attackers feign association with a trusted name or brand to induce you to act. Just because a message uses the logo or name of an organization you recognize, it does not necessarily mean the message originates from them.

Excitement: A Deceptive Bait

Attackers capitalize on our excitement. You may receive a text from your bank or service provider appreciating your timely payments and offering a reward. The link, while appearing official, is merely a facade to steal your money or identity.

Empathy/Compassion: A Soft Target

Attackers exploit your goodwill. Post a disaster, they may send out countless emails pretending to be a charity and soliciting donations. They'll play on your emotions, your desire to help those in need, taking advantage of the confusion and desperation that often follow disasters. Always verify the legitimacy of the charity and the email before donating.

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.