THE PSYCHOLOGY OF CYBER

How cybersecurity and psychology are intertwined

THIS MONTH'S TOPICS:

Security Fatigue
Staying alert online...

The Psychological Advantage
The mental side of cybersecurity

Scam of the Month:
Social engineering scams...

Cyber Zen Den:
Building a mental fortress

Psychology may be a field of its own, but it greatly impacts many different facets of life, even when it comes to cybersecurity!

Cybercriminals have been known to use psychological manipulation to trick users into giving up their information, as elements such as emotion, motivation, and fatigue can all impact an employee's ability to make the secure decision.

In this month's newsletter, learn how to combat security fatigue, spot social engineering, and get the psychological advantage over a cybercriminal.

SECURITY FATIGUE

Security fatigue refers to weariness or reluctance to make digital security a priority.

Users are more likely to reveal personal information or click a phishing link when they are tired or overwhelmed.

Using a password manager can help combat security fatigue that stems from trying to remember passwords.

Taking breaks, being cognizant of screen time, and turning off unnecessary notifications all help stop security fatigue.

32% of users do nothing upon notice of a breach.

This is the time to take action!

Change passwords and make all recommended changes if your data has been compromised.

The Psychological Advantage

Inevitable Threat

Due to the sheer volume of notifications and security risks, many users feel like there is nothing they can do to prevent cyber-attacks. While most users know there are threats, many also feel that breaches are inevitable.

Social Influence

The private nature of digital activity leads to many users not knowing what security practices others implement. Discussing security implications and solutions with friends and family helps drive action and create a positive connection with security.

Positive Habits

It has been found that consistent training is the best way to make security less overwhelming. When users know what to look for, they will feel confident about their security position. When good cyber decisions become a habit, the user has a psychological advantage.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Karen arrived home after a long day at work. She had just settled in on the couch to watch her favorite television show when she heard her phone ping.

She had a message from an unknown number that read, "Hi." Karen did not respond, she assumed they had the wrong number. A few minutes later, the number messaged her again saying, "It was great meeting you last week!" Karen decided to reply to let them know they had the wrong number.

"Just my luck," the person replied, "She must have given me the wrong number. Well, what's your name?" The person sent a picture of himself, as well. Karen felt bad for him and thought he seemed nice, so she continued to message him for the next few days.

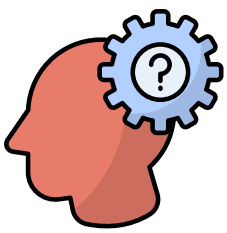
It turned out they had a lot in common. He sent Karen a few cool websites to check out. They kept in touch and after a few weeks, he asked her for a favor. He needed an expensive medical treatment and was wondering if she could help pay for it. Karen was worried about her new friend and wired him the money. What she did not know was that she had fallen for a scam.

Did you spot the red flags?

- Wrong number scams are on the rise. They often start with a text message to a "wrong number" and include a picture of an attractive young person.
- The scammer sent Karen many unsolicited links to websites that were likely malicious.
- An emotional story was used to request money via wire transfer. This is a common method of exchange used by cybercriminals.

Never send an unknown number money or personal details. Do not be fooled by a picture, as scammers often fake their identity.

Do not reply to text messages from unknown numbers. This will mark your number as "active" and will lead to an increase in calls and texts.



Social engineering attacks exploit human psychology. By relying on the natural tendencies of empathy, curiosity, trust, or even greed, cybercriminals are able to successfully carry out these scams.

Key Takeaways

Cybercriminals use psychology and emotion to carry out their scams.

Being aware of this fact, and knowing how to get the psychological advantage, will allow users to have the upper hand.

Combating security fatigue: Using password managers, limiting notifications, and taking breaks throughout the day are great ways to combat security fatigue.

Making cybersecurity social: Discussing with those around us allows for cybersecurity knowledge to spread. Be conscious of the risks but also confident that you know how to combat them.

Keeping emotions in check: It is hard to spot social engineering until it is too late. Whenever emotions begin to get involved in a situation online, stop and remember your training before moving forward.

Mental Fortitude

Mental fortitude involves having the emotional intelligence to use mindfulness in situations. It involves harnessing emotions.

How does this relate to cybersecurity?

Staying strong and being mindful of emotions while online can help users avoid scams that appeal to their emotions.

Now apply this concept to cyber-awareness.

In order to stay fully mindful in situations online, security fatigue must be avoided. Take breaks throughout the day to think about mental fortitude and be cognizant of your fatigue levels when working or browsing online.