The Weakest Link

CONCEAL
Detect. Defend. Isolate.

This year, 82% of breaches involved the human element. This puts the person square in the center of the security estate with the Social Engineering pattern capturing many of those human-centric events. Here are a few of the top social engineering attack types:

PHISHING

Cybercriminals attempt to lure users to click on a link or open an attachment from an email or malicious website that infects their computers, creating vulnerability to attacks.

BAITING

Cybercriminals promiss an item, commodity, or reward to attract victims, infect their system with malware, and steal their sensitive information.

QUID PRO QUO

Cybercriminals scam by targeting an individual with an offer to pay for a service that seems legitimate for financial gain.

PRETEXTING

Cybercriminals will present a false scenario, or “pretext”, to gain the victim’s trust and offer a deal that is too good to be true or try to gain sympathy to scam a victim.

TAILGATING

Cybercriminals attempt to ‘piggyback” off an employee to gain access to an area of an organization’s space that they are not privy on their own.

BY THE NUMBERS....

In 2021, **83%** of organizations reported experiencing phishing attacks.

Cybercriminals use social engineering in **98%** of attacks.

There are **75** times as many phishing websites as malware sites.

With **241,342** successful incidents, phishing was the most common cybercrime in 2020.

Change the Narrative

Strongest Link

Training can potentially help improve security behaviors, in both day-to-day (such as Don’t Click ... Stuff, and using a password keeper) as well as in design (such as secure coding, lifecycle management, etc.). Unfortunately, while getting training is easy, proving it’s working is a bit harder. Here are some pointers for changing the narrative:

The goal of training must be to change human behavior, not just to train.

The training program must have an outcome driven approach.

36% of Organizations Report Implementing At-Scale Cyber Security Awareness and SecOps Cross-Training

Employees’ Understanding of Phishing dropped **15%** over 2021

Training must directly relate to the trainees role and responsibilities.

Motivation and incentive for trainees must be meaningful and purposeful.

54% of employees would spend more time studying if they were given specific course recommendations to assist them in achieving their professional objectives

Ensure employees feel like they are an important part of the security mission and the most important aspect of the security stack.

To remain employed, **74%** of workers are eager to learn new skills or retrain

Sources:
https://www.thesslstore.com/blog/19-security-awareness-statistics-you-should-know-before-offering-training/
https://webtribunal.net/blog/social-engineering-statistics/#gref
https://www.crowdstrike.com/cybersecurity-101/social-engineering-attacks/
https://www.verizon.com/business/en-gb/resources/reports/dbir/

CONCEAL
Detect. Defend. Isolate.