Social Engineering: It's not just email anymore

WHAT IS A SOCIAL ENGINEERING ATTACK?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity.

If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

WHY IS SOCIAL ENGINEERING SO DANGEROUS?

One of the greatest dangers of social engineering is that the attacks don't have to work against everyone: A single successfully fooled victim can provide enough information to trigger an attack that can affect an entire organization.

Over time, social engineering attacks have grown increasingly sophisticated.

Not only do fake websites or emails look realistic enough to fool victims into revealing data that can be used for identity theft, social engineering has also become one of the most common ways for attackers to breach an organization's initial defenses in order to cause further disruption and harm.

HOW TO DEFEND AGAINST SOCIAL ENGINEERING?

While psychological attacks test the strength of even the best security systems, we can mitigate the risk of social engineering with awareness training.

Consistent training of employees is highly recommended. This should include demonstrations of the ways in which attackers might attempt to socially engineer employees.

Training helps teach employees to defend against such attacks and to understand why their role within the security culture is vital to the organization.

Establish a clear set of security policies to help employees make the best decisions when it comes to social engineering attempts.

STAY ALERT!

The rise of AI has significantly expanded social engineering in recent years. Whereas cybercriminals once focused mainly on phishing via email, they now exploit a wide range of channels: phone calls (vishing), text and chat messages (smishing), social media, and even fake helpdesks or WhatsApp messages. Attacks have also become increasingly personal and convincing using the use of publicly available information and AI. Below are examples of channels employees use on a daily basis channels that cybercriminals actively exploit.

PHONE CALLS | VISHING

AI-generated voices mimic trusted individuals to extract sensitive information

TEXT MESSAGES | SMISHING

Fraudent SMS messages prompt clicks on malicious links or requests for perosonal data.

SLACK AND TEAMS

Cybercriminals infiltrate chats, posing as team members to share harmful links or requests.

ZOOM AND VIDEO CALLS

Deepfake technology enables impersonation during live meetings, leading to unauthorized actions.

QR CODE ATTACKS

Physical and digital QR codes redirecting to credential harvesting sites

LINKEDIN INMAIL

Professional networking messages delivering credential theft links.