WHAT IS SOCIAL ENGINEERING?

In the realm of cyber threat intelligence and information security, 'social engineering' involves employing deceptive tactics to influence individuals into revealing sensitive information or engaging in actions that may not align with their best interests.

KEY TECHNIQUES TO BE MINDFUL OF:

Phishing

A prevalent social engineering tactic where attackers deceive individuals into disclosing personal information by posing as a trusted contact. Email phishing is becoming increasingly sophisticated, with attackers disguising their email addresses to mimic reputable organizations.

Voice Phishing (Vishing)

This is over-the-phone social engineering to obtain personal and financial information. Scammers pretend to need information to confirm identity, often impersonating trusted figures like co-workers or bank officials.

Whaling Attack

A sophisticated phishing attack targeting high-value individuals like executives. Emails masquerade as critical business communications from legitimate authorities.

Scareware

Victims receive false alarms and threats, leading them to install useless or harmful software. Also known as deception software, rogue scanner software, or fraudware.

Spear Phishing

Attackers tailor messages to a specific audience, often within a particular business sector or company. They conduct research on the target, combining information from the organization, social media profiles, and other publicly available sources.

Smishing

SMS phishing involves sending text messages, pretending to be reputable companies, and encouraging victims to pay money, share information, or click on suspicious links.

Watering Hole Attacks

Attackers compromise trusted websites to infect victims' computers. They target websites the victim is likely to visit, such as suppliers' websites or industry journals.

Baiting

A widespread attack using online ads, websites, or physical items like USB drives with enticing offers. Victims are tricked into giving away personal information or downloading malware.

Quishing

Using malicious QR codes in phishing scams to compromise user logins. These deceptive attacks skillfully mimic official channels, such as legitimate company emails.

Business Email Compromise (BEC)

Exploits the reliance on email for business transactions. Attackers target organizations, sending spear-phishing emails or calls to convince victims to conduct seemingly legitimate transactions.

Diversion Theft

Professional thieves persuade victims, often transport or courier companies, to redirect goods to another location for easy theft. This can also occur online when attackers convince someone to send confidential information to an associate.

Tailgating

Attackers focus on getting physical access to restricted sites or buildings by following staff members with legitimate access. They may ask employees to hold doors open for them.

Think before you click

If it sounds too good to be true, it usually is

Know your next move

Immediately report suspicious activity to your IT department

CleanINTERNET®

Invest in CleanINTERNET® to shield 99.9% of malware threats, including Ransomware

Contact Us: **Website:** https://www.centripetal.ai/ **Email:** sales@centripetal.ai