KCS Group Europe

The subtle traps of sophisticated social engineering

January 2024

Social engineering is on the rise. Increasingly sophisticated attacks are testing our ability to recognise scams and challenging businesses' cybersecurity protocols. Orchestrators of such schemes exploit psychological vulnerabilities, targeting the human element of security systems rather than relying on conventional technological tactics. Their methods involve manipulating individuals so that they inadvertently reveal confidential information that enables fraud.

Social engineering is a deception technique that is rooted in ancient times. However, it has evolved and adapted to the digital landscape. The increasing dependence we have on social media and data has enabled perpetrators to refine their practice, resulting in a relentless cat-and-mouse challenge of safeguarding systems against human vulnerabilities.

Understanding the psychology behind social engineering

The list of psychological principles used by social engineering experts is extensive: for example, the principle of *authority* which relies on the fact that humans are more likely to comply with requests that are perceived as authoritative. The *liking* or *honeytrap* principle exploits the tendency to be influenced by those we are attracted to. Other tactics include the concept of *social proof* where humans mimic or follow the opinion of others (for example, a phishing email where an offer is endorsed by reputable, maybe familiar, professionals).

The principle of *scarcity* or *fear of missing out* is employed in the form of a limited time offer in an email or phone call requiring immediate action, perhaps to provide credentials before it's too late.

Skilled perpetrators gain a target's trust by appearing credible or implying shared common interests. They then manipulate the natural human desire to be helpful or avoid conflict or exploit an ignorance of security protocols. The opportunities and techniques are endless.

Identifying remote and physical social engineering attacks

There are two main methods of remote social engineering attacks. The first technique is *phishing* where the attacker sends out large volumes of fraudulent emails to random addresses in the hope that an individual will divulge confidential data. Most people have been on the receiving end of this type of attack. In *spear phishing*, bespoke emails are targeted at a specific individual, for example, offering legitimate products and services relevant to the sector the victim operates in.

When it comes to physical rather than remote attacks, *pretexting* is the act of fabricating a scene, environment, or identity to acquire confidential information from a victim under false pretences. An unnecessary or forceful sense of urgency is often applied alongside the request to divulge information. Another which capitalises on the human tendency to trust is *tailgating.* An unauthorised individual follows an authorised member of staff into a restricted area, exploiting politeness and distraction principles.

Baiting is the term given to the strategic placing of malware-infected devices and cables. Items such as USB drives or phone charger adapters can be strategically placed in corporate carparking spaces, toilets, recreational areas and business lounges. A USB drive may be labelled 'Confidential' or 'Bonus Payroll Report' to lure the curious. When the malware USB is put into a computer – or a charging adapter is used in a phone – the device is compromised in a matter of seconds.

Dumpster diving involves a perpetrator looking through a victim's rubbish bins to find carelessly discarded documents or hardware, revealing a surprising amount of useful information. *Shoulder surfing,* as the name suggests, is simply a social engineering specialist being nosy – taking the opportunity to observe bank balances, passwords used for computers or PIN numbers used at bank ATMs.

Famous social engineering case studies

In 2017, perpetrators posing as construction workers targeted a spear-phishing attack on MacEwan University in Canada, successfully convincing the accounts department to redirect payments totalling CAN$11.8 million to a fraudulent account. In 2020, the famous Twitter Bitcoin scam emerged. Hackers acquired password access to Twitter's network via social engineering employees and high-profile user accounts were then used to endorse a Bitcoin scam.

More recently, in 2021, a significant ransomware incident occurred in the Colonial Pipeline in the United States. Perpetrators successfully breached the Pipeline's networks, using a compromised password obtained from a staff member through bribes and threats. The hacking group known as DarkSide managed to shut down the largest pipeline in the US, causing huge shortages along the East Coast. A ransom of 75 bitcoin or US$4.4 million was paid and the pipeline network was restored.

It is widely reported that over 80% of cyberattacks due to social engineering methods are successful, exploiting human vulnerabilities rather than attempting to penetrate firewalls remotely. Why? Because it's easier.

Preventing social engineering attacks

Safeguarding against social engineering attacks requires discipline, technical acumen and constant vigilance. Businesses must enforce strict protocols, routinely update software patch vulnerabilities and control access to sensitive areas such as business meeting rooms and computer server rooms. Employees should use two-factor authentication and adopt robust password practices (for example, incorporating a sentence-style mix of upper- and lower-case letters, symbols and numbers – such as OrangeTomatoesWallsBlue?23).

The future of social engineering

Social engineering continues to evolve, with tactics and techniques being driven by advancements in technology and social media online habits. AI is used to engineer sophisticated spear phishing campaigns and Deepfake technology manipulates targets through convincingly altered video and audio pretexts.

As people become increasingly aware of email phishing, the concern now is that social engineering actors will develop approaches exploiting vulnerabilities in new social media platforms and communications methods.

Security professionals anticipate a rise in targeted and sophisticated social engineering attacks, with spear-phishing focusing on high-value targets with access to critical information (known as a 'whaling attack'). The interconnectedness of the Internet of Things (IoT) inevitably presents opportunities for exploitation. In addition, as people continue to work remotely, attackers are expected to exploit the reduced physical and technological security measures typical of home networks. These tactics will exploit both local and global events, such as health pandemics or political upheavals, to manipulate the thoughts of individuals and organisations.

Conclusion

Social engineering is, by its very nature, a more unpleasant side of cybercrime. Unlike the non-people-facing keyboard coding criminals, these perpetrators use human psychology to manipulate others to do their bidding which can, of course, involve blunt tactics like threats of violence.

Individuals who work in IT security departments of large companies stand out as clear targets, as do individuals who have access to confidential and valuable business critical information. Unsolicited introductions, discussions in public and excessive compliments all create a context for social engineering attacks. Maintaining vigilance and awareness of potential threats is vital.

'One who deceives will always find those who allow themselves to be deceived.' —Niccolò Machiavelli.