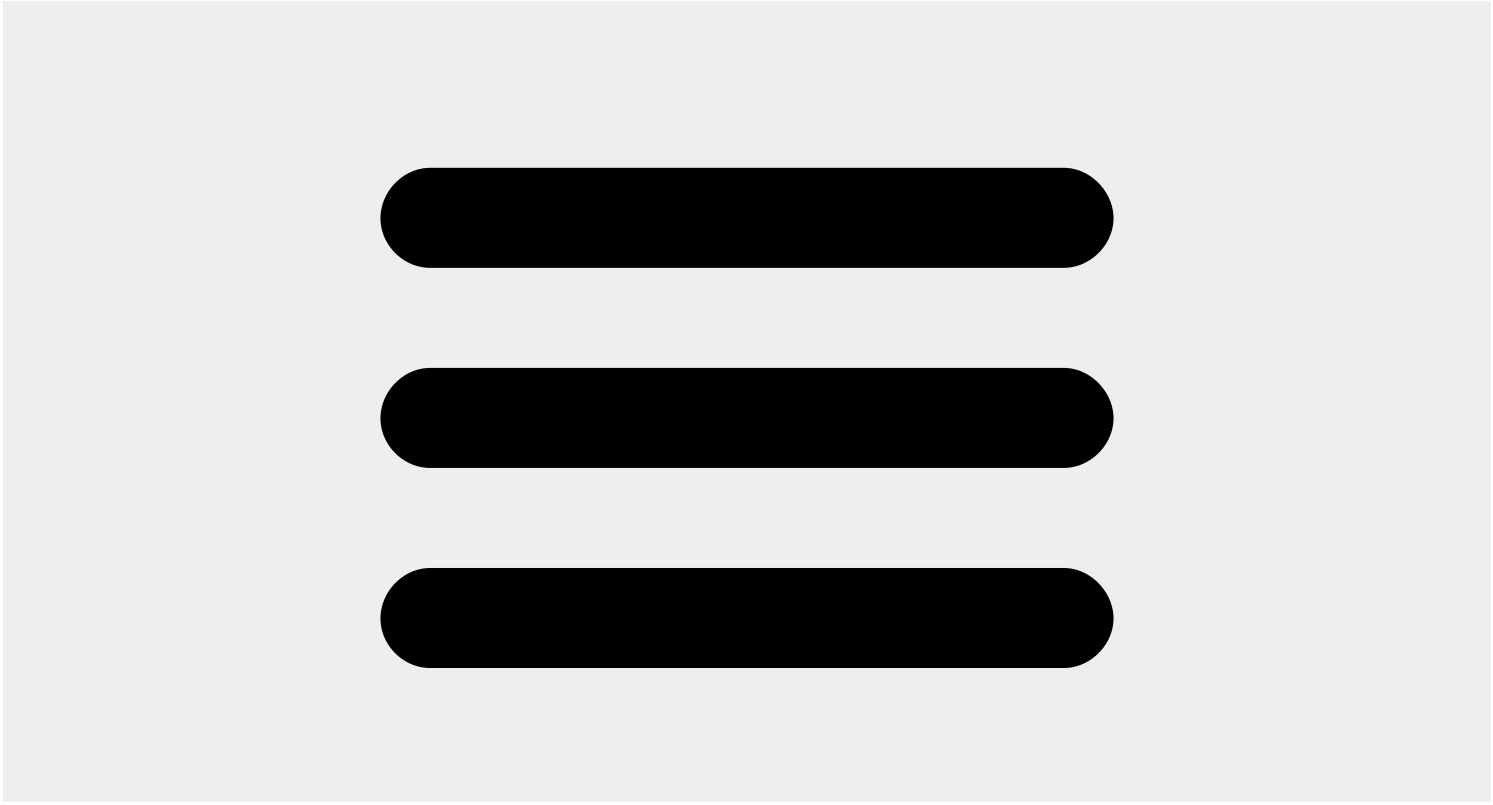
SOCIAL ENGINEERING: THE ART OF HACKING YOUR MIND

Posted on February 12, 2022 by Marina Tovar



Social engineering constitutes a severe threat to users' online safety, as it is an effective means to attack information systems and access users' data. Fortunately, most security vulnerabilities can be fixed through patches and strengthened security channels. Nevertheless, even security-enhancing methods are often powerless when users become victims of manipulated social engineering (Krombhloz et al., 2015). Social engineering is an incursion technique that relies on human error to access private information (Kaspersky, 2021). Thus, social engineering attacks target the ways in which individuals think and act.

Social Engineering Attacks: Methodology

It has to be noted that there is no specific methodology on how hackers prepare for this particular type of attack. Nevertheless, psychology and user's online interaction play an essential role in the ease in being targeted. The most prevalent typology of social engineering attacks has been shown to involve phones (Granger, 2001). Hackers analyze the target's online interaction to gather background information such as name, interests, and personal data, including email, LinkedIn and/or other social media platform connections. Once the hacker has acquired a complete picture of the target, they will most likely attempt to establish and create a relationship with that individual.

Once hackers have initiated the first interaction, they will attempt to exploit the target's weaknesses and advance the attack. For example, the interaction could occur from an email sent from a mailing address containing the name of an old friend or a connection request on LinkedIn of a previous acquaintance that the target had followed on Instagram. The victim in that email could click on a link and spread malware or a Remote Access Trojan (RAT) throughout their respective network. The hacker may opt to act as a familiar friend or associate and then inquire about the personal information that will allow the perpetrator to impersonate the victim. According to Krombholz et al. (2015), social engineering can also be elevated to a higher level and be easily automated and, therefore, be performed on a larger scale.

Why is Social Engineering so Successful?

"Security is about trust, and trust in protection and authenticity" (Granger, 2001). Unfortunately, social engineering techniques tend to rely on psychological methods to bypass personal security and take advantage of natural human willingness and vulnerabilities that humans tend to have. According to Peltier (2006), hackers use persuasion and influence through either direct or indirect routes. The attacker will ask for the information (direct route) or trigger the victim by making a statement that elicits a strong emotion like fear or excitement to acquire the information in a moment of vulnerability (indirect route). In addition, hackers rely on human error, as it is commonly a major option for illicit intrusion into technological devices, where individuals are often considered the weakest link (Abraham & Chengalur-Smith, 2010).

After a thorough investigation, the suspect will select a victim by scouring the target's networks for vulnerabilities to detect weaknesses and proceed with the attack. By studying the shortcomings of the target's systems and practices, the attacker can identify a pattern or a vulnerability that the victim is not cognizant of and attack that location. This technique is based on observation and the use of psychological methods, such as the principle of similarity or reciprocity, which serves to manipulate the victim and force that individual to undertake what the defrauder wants. The principle of similarity is a technique where victims will identify with people familiar or comparable to them. The principle of

reciprocity allows the perpetrators to utilize this sense of enforced indebtedness to evoke an unwise action from the victim. Therefore, comprehending how psychological triggers work in social engineering will help set the proper multi-level, effective defense and raise awareness (Gragg, 2003). Individuals still rely on a series of cognitive and social heuristics to make choices that provide suitable enough results, but sometimes these actions can lead to decision-making errors. Alternatively, these two principles are based on the use of techniques that do not involve a manipulation of the victim but lie in principles of apparent solidarity or similarity, that create short-cuts in the rationality of thought.

Conclusion

Social engineering ultimately is a means to an end, which involves obtaining the desired information or gaining access to critical resources, such as bank accounts, files with confidential information, or files that could prove harmful to the victim. Thus, it involves a methodology present in variant forms, like phishing or baiting, which combine observation, information gathering and psychological techniques to manipulate the target to achieve a final and illegal objective.

The critical element to protect against social engineering attacks is to identify the vulnerabilities, weaknesses, and threats individuals or employees might face and defend against those risks (Gragg, 2003). Detection, together with prevention, fulfills a transcendental role in handling such critical situations. Detecting suspicious emails, SMS, or communications that do not come from official channels can constitute the first step to identifying this type of intrusion. Prevention can be achieved through verifying these messages and comparing them with the information on official pathways or by using only trusted devices or identified secure methods of communication.

Bibliography

Abraham, S. and Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), pp.183-196.

Gragg, D., 2003. A multi-level defense against social engineering. *SANS Reading Room*, *13*, p.15.

Granger, S., 2001. Social engineering fundamentals, part I: hacker tactics. *Security Focus, December*, *18*.

Huber, M., Kowalski, S., Nohlberg, M. and Tjoa, S., 2009, August. Towards automating social engineering using social networking sites. In *2009 International Conference on Computational Science and Engineering* (Vol. 3, pp. 117-124). IEEE.

Kapersky (2022). *What is social engineering*. Available

at: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering (Accessed 17 January 2022).

Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, pp.113-122.

Peltier, T.R., 2006. Social engineering: Concepts and solutions. *Information Security Journal*, *15*(5), p.13.

Featured Image: *DAVID BISSON*

About the Author: *Marina Tovar is a Junior Researcher at IACS. She is a last-year International Relations and Law student at the Autonomous University of Barcelona, Spain. Her areas of interest are terrorism, hybrid threats, gender, and the Middle East.*