SOCIAL ENGINEERING: A DIGITAL HYPNOTIZATION PLOY

Biraj Das[1]

[1]Assam Police, Guwahati, Assam, India.

DOI: https://www.doi.org/10.58257/IJPREMS32078

ABSTRACT

The term "hypnosis" is attempted to be captured in this document as a tactic for putting a person into a trance and eventually gaining his attention. Apart from folklore relating to "hypnosis", there are even some medical and therapeutic benefits as well, which are used by psychologists. The digital hypnosis, however, has emerged as a new concern to the society, particularly with the ever-growing emphasis on digitalization in financial and business sectors. There are various types of Attack Vectors, i.e., phishing emails, Trojans, SQL Injection, etc. But Social Engineering is one of the most widely used tactics to gain right-to-know authority from a target or a victim by a perpetrator, and subsequently, the target is being exploited. This is very analogous to "hypnosis". This can also be viewed as a demonstration of “destructive obedience”, which relates to an act of obeying a command from some unverified sources or unknown persons without bothering to confirm the validity, possibly as a consequence of having limited knowledge. Social engineering is merely a psychological operation. Usually, it is executed in four steps as indicated below.

Investigation: Identifying the target after knowing a bit of his background.

Hook: Trying to increase “proximity” either by means of indulging into some kinds of mutually interesting topics or provocation.

Play:: After gaining confidence, the perpetrator tries to expand his grip and starts exploiting, which can also be treated as the “Foot-in-the-door” technique.

Exit:: After the target has been exploited, the perpetrator exits, often without issuing any alarm to the victim.

Thus, the wicked mission of the perpetrator gets accomplished, and the victim may well become aware about the exact happening after some time, often several days. It would be pertinent to indicate here that, in this entire operation, the perpetrator doesn’t use any kind of hacking tools to gain access to the victim’s system. This is done completely through human-to-human interactions. The perpetrator exploits the psychological manipulation, i.e., “Coercive Persuasion” to have a propensity to compromise the victim's security protocols, and consequently, the exploited.

Keywords: social engineering, digital hypnosis, psychological operation

1. INTRODUCTION

The core objective of this document is to figure out a psychological solution to counter the Social Engineering Attack. Such attacks are very novel, and the perpetrators never use any kinds of cutting-edge hacking tools to breach the security protocols or access the victim's system to steal information or other resources. In this tactic, what the perpetrator does is simply carry out psychological operations to victimize their prey. Friedman & Hoffman, 200.

In this era of cutting-edge technology, the digital environment has become the custodian of most of the human assets or resources, which does not exclusively mean money, other intellectual property, etc. It has even started playing a significant role apart from political and academic careers in health, showbiz, and human dignity as well.

Bamakan Nezhadsistani, Bodaghi, & Qu, 2022 In such a scenario, a perpetrator always tries to access his potential victim’s information with malicious intent that is residing in the digital environment. The intention of the perpetrator is always malicious, but it's not exclusively stealing money alone, even though the majority of them do so. Some of them even do so to undermine his target victim, and there may be some other purposes as well, which would be definitely unethical.To gain unauthorized access to the digital environment (computer network or System), the perpetrators always adopt different procedures, which are technically called Attack vectors. The most common attack vectors are malware, viruses, attachments, web pages, messages, social engineering, etc. Alkhalil, Hewage, Nawaf, & Khan, 2021 Out of all these attack vectors social engineering is the most widely used tactics to gain right-to-know authority from a victim by a perpetrator for exploitation. It’s a broad range of malicious activities accomplished through human interactions. The most common social engineering attacks are phishing, whaling, baiting, honey traps, watering hole, etc. In the social engineering attack technique, the perpetrator doesn't use any kinds of hacking tools or technical techniques. He simply manipulates his target psychologically, which is analogous to hypnotization, so that his target naturally gets inclined to trust the attacker, and finally his security protocols get breached, such as when he himself provides his login credentials or pays money to the attacker. Since It’s a broad range of malicious activities accomplished through human interactions. Therefore, to mitigate the risk of social engineering attacks, psychologists can play a crucial role.

2. DIGITALIZATION

If an object is captured digitally, then its scalability goes to an infinite level. For example, if a picture of a man is captured digitally, the picture can be morphed up to any level. Using artificial intelligence, his picture can even be morphed according to his different age levels. (Bovik, 2009)

The quantum digitalization of human life has become such a phenomenon that even a baby, before being exposed to the physical world, gets exposed to the digital world. During an ultrasound prenatal test, the picture of the baby while it is in its mother's womb gets captured digitally and exposed to an electronic monitor for medical examination.

DIGITAL HYPNOTIZATION:

The term "hypnosis" is attempted to be captured in this document as a tactic for putting a person into a trance and eventually gaining his unabridged attention. Apart from folklore relating to "hypnosis", there are even some medical and therapeutic benefits as well, which are used by psychologists. Digital hypnosis, however, has emerged as a new concern for society, particularly with the ever-growing emphasis on digitalization in every aspect of human life and death. (Lynch, 2000)

Engineering is one of the most widely used tactics to gain right-to-know authority from a target or victim by a perpetrator, and subsequently, the target is being exploited. This is very analogous to "hypnosis". This can also be viewed as a demonstration of "destructive obedience", which relates to the act of obeying a command from unverified sources or unknown persons without bothering to confirm its validity, possibly as a consequence of having limited knowledge.

3. SOCIAL ENGINEERING

Social engineering is merely a psychological operation. Usually, it is executed in four steps as indicated below. (Fig A)

1. **Investigation**: Identifying the target after knowing a bit of his background.
2. **Hook**: Trying to increase “proximity” either by means of indulging into some kinds of mutually interesting topics or provocation.
3. **Play**: After gaining confidence, the perpetrator tries to expand his grip and starts exploiting, which can also be treated as the “Foot-in-the-door” technique.
4. **Exit** : After the target has been exploited, the perpetrator exits, often without issuing any alarm to the victim.

Thus, the wicked mission of the perpetrator gets accomplished, and the victim may well become aware about the exact happening after some time, often several days.

It would be pertinent to indicate here that, in this entire operation, the perpetrator doesn’t use any kind of hacking tools to gain access to the victim’s system. This is done completely through human-to-human interactions. The perpetrator exploits the psychological manipulation, i.e., “Coercive Persuasion” to have a propensity to compromise the victim's security protocols, and consequently, the exploited.

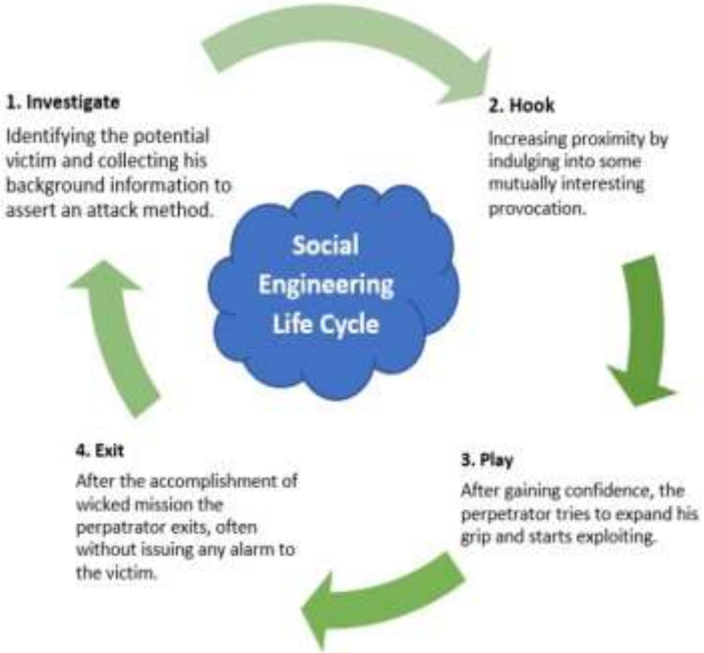
1. Investigate
Identifying the potential victim and collecting his background information to assert an attack method.
2. Hook
Increasing proximity by indulging into some mutually interesting provocation.
Social Engineering Life Cycle
4. Exit
After the accomplishment of wicked mission the perpatrator exits, often without issuing any alarm to the victim.
3. Play
After gaining confidence, the perpetrator tries to expand his grip and starts exploiting.

Figure-A

Coercive Persuasion:: It's a brainwashing tactic to get the potential targets to believe certain ideas that are set by the attacker. (Winn, 2000)

NEUROCOGNITIVE ASPECTS OF SOCIAL ENGINEERING:

In a social engineering attack, the cybercriminal largely exploits the weaknesses of the human limbic system or neurocognitive functions as a whole. The limbic system principally gets involved in humans behavioral and emotional responses, especially when it faces fight or flight responses.

The moot question is why netizens are vulnerable to social engineering attacks and what could be the defence mechanism to minimize or mitigate the damage. In these grave situations, psychology may play a critical role.

When the threat is fed to the prefrontal cortex from the amygdala, the prefrontal cortex takes an executive or rational decision, but it depends on the quantum of information fed to the prefrontal cortex. After receiving the potential threat, the amygdala takes some time to feed it to the prefrontal cortex, and this may vary from man to man for various reasons, such as his age, the effectiveness of his pineal gland, hippocampus, etc. (Blair, 2007)

Therefore, the enhancement of neurocognitive functions has become very essential to counter such cyberattacks, and psychologists can work out a kind of framework to thwart such attacks. Psychologically, it is evident that the Amygdala and Prefrontal cortex play a significant role in the central circuitry of emotion in the human brain. Even though the different functional divisions of the Prefrontal cortex viz. the dorsolateral, ventromedial, and orbital sectors, play a significant role in emotional regulation, the amygdala plays a critical role in sensing and capturing potential threats or anxiety, which is eventually fed to the Prefrontal cortex to play the role of emotional responses. (Kilpatrick & Cahill, 2003)

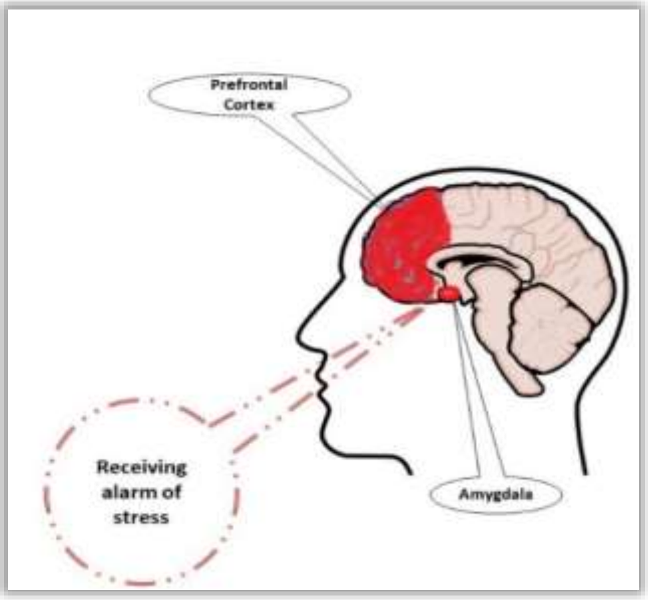

Figure-B

In an ideal situation, the amygdala captures the current environment, whether it is stress or a potential threat, etc., and feeds it to the prefrontal cortex to respond. Whereas the prefrontal cortex acts by synchronizing the intracellular signalling pathways that affect the effects of stress on the Prefrontal Cortex that controls the emotional responses to stress, (as shown in the pictorial Figure-B), like that of the CPU of a computer system.

Whereas the prefrontal cortex is responsible for initiating the process of thinking and rational or executive decision-making, and the decision depends on the available information processed in the mind. Psychologically, it is well established that emotion is important for the fundamental tasks of survival and adaptation, which modulate memory and facilitate decision-making.

However, in the case of a social engineering attack, the source of the threat is intangible in a manner that doesn't have a physical existence because the perpetrator is using cyberspace. To counter such a novel fight or flight situation, probably no extensive biobehavioural study has been initiated to date. In the Indian context, almost every day, a colossal number of people are victimized, as most of the perpetrators use social engineering tactics to dupe or victimize in another sense. The epicentre of cyber fraud is Jamtara, which is also nicknamed the phishing capital of India, and social engineering is the only tactic adopted by the fraudsters from this capital to compel their preys to breach the security protocols to get victimized. (Rajput, 2020)

4. SUGGESTIONS FOR FUTURE RESEARCH:

In this paper, the following comprehensive contributions are set to be put forward:

1. The social engineering attack is merely a psychological attack to breach the security protocols of the target or victim, and no hacking tools are utilized by the attacker.
2. A new chapter in the field of psychology can be thought of by researchers or thinktanks from the perspective of psychology, which may be termed cyber cognitive psychology. This new field of cognitive psychology will encompass the required cybersecurity requirements commensurate with the cybersecurity domain.
3. This effort will definitely pave the way for framing an effective defence mechanism against social engineering attacks.
4. The process will be faced with certain constraints, as the victims of such attacks will most likely consider the attacks legitimate and even be victimized. Therefore, this would be the vital challenge that needs to be neutralized at the very least, or else, without being neuro-linguistically programmed, the potential victims will hardly understand the grave situation.
5. While working on the framework, the quantitative representation for mathematically characterizing persuasion, which would be a core concept in the emerging Cyber Cognitive psychology, is paramount to having substantial domain knowledge to avail a better and more consistent outcome.
6. In addition, Researcher would also like to propose a spectrum of future research directions emphasizing quantifying the effect of model parameters such as the victim's short-term cognition factors, long-term cognition factors, long-memory, and attacker effort on the amount of persuasion experienced by the target.

7. CONCLUSION

In a nutshell, in this document, effort is being put into ensuring that in social engineering attacks, the perpetrator doesn't use any kinds of hacking tools or technical skills as well. Through psychological manipulation, the cybercriminal put his victim into a trance so that he could be manipulated for some kind of malicious purpose, similar to destructive obedience in psychological terms. However, in this odd circumstance, it would not be an exaggeration to say that the victim's limbic system momentarily gets crashed and his prefrontal cortex fails to make the requisite decision that the victim is under the influence of some kind of attack, for which he may commit some serious mistakes that may lead him to get victimized. Therefore, to overcome such a serious consequence or vulnerable situation, psychology as a whole can play a critical role in preventing netizens from becoming prey to such fraudsters.

8. REFERENCE

[1] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science,, 3, 563060.

[2] Bamakan, S. M., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. Scientific Reports,, 12(1), 2178.

[3] Blair, R. J. (2007). Aggression, psychopathy and free will from a cognitive neuroscience perspective. Behavioral sciences & the law, 25(2), 321-331.

[4] Bovik, A. C. (2009). The essential guide to image processing. Academic Press.

[5] Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. Information Knowledge Systems Management, 7(1-2), 159-180.

[6] Kilpatrick, L., & Cahill, L. (2003). Amygdala modulation of parahippocampal and frontal regions during emotionally influenced memory storage. Neuroimage, 20(4), 2091-2099.

[7] Lynch, J. J. (2000). A cry unheard: New insights into the medical consequences of loneliness. Bancroft Press.

[8] Rajput, B. (2020). Cyber Economic Crime in India. Springer International Publishing.

[9] Winn, D. (2000). The manipulated mind: Brainwashing, conditioning, and indoctrination. Ishk.