Interdisciplinary Term Paper

Myrna Santiago

College of Cybersecurity, Old Dominion University

IDS 300W: Interdisciplinary Theories and Concepts

Dr. Peter Baker

November 24, 2024

INTRODUCTION

Social Engineering, in Cybersecurity, is the use of deception to manipulate individuals into divulging important information that can be used for illegal purposes. In contrast, ethically done, social engineering can produce positive results for individuals. The people that use these techniques are known as threat actors, if done illegally, and ethical hackers, if done legally. These individuals have either gain or security in mind. It can be financial, espionage or bragging rights gain for the threat actors and protection, and security for the ethical hackers. In the last two decades, the study of social engineering has multiply exponentially, especially after the pandemic of 2020. Nefarious individuals have used psychological techniques to undermine people's ability to protect themselves, talking them out of important information, like Personal Identifiable Information, security passwords, or other information that can be used to exploit systems, that in any other case will be secure. For Cyber professionals, the weakest link in the cybersecurity chain is the end-user and for years studies have been conducted in the techniques and solutions have been put in place, all of which address security of networks and infrastructure, and education of the end-user. One thing that has been lacking is the effect that social engineering, done illegally or legally, has on individuals and how they are psychologically, socially and economically affected after the attack?

An analysis of social engineering can be studied from multiple disciplines points of view. Disciplines that can study the benefits and drawbacks of social engineering are Ethics, Economics, Psychology, Sociology, Information Technology, Cybersecurity, and Philosophy. For this research, we will concentrate on the disciplines of Psychology, Sociology, and Economics, because they provide interesting views on the topic.

Literature Review

According to Psychology, one of the reasons social engineering attacks are successful is fear of authority from employees. People behave a certain way if they know they are observed. It is believed that in an ethical social engineering attack that has been openly announced people tend to behave more cautiously if they know the exact date and time of the test. In her review, Washo (2021) argues that even when ethical social engineering was performed, employees received education and knew about the test they were more likely to provide help to the attacker, if it represented an authority figure. When this happens, individuals feel shame and insecurity, making like a regular social engineering attack.

Montañez et al. (2020) in contrast argue that people with higher education, higher awareness and higher exposure to attacks are less susceptible. This means that if they know can identify what is happening, they can avoid manipulation. They feel empowered and have increased participation in changing behaviors positively. Even after an attack these kinds of people feel the need to educate themselves instead of dueling in what ifs.

Another insight of Montañez et al. (2020) is that people are unlikely to consciously think about social engineering attacks unless they become a habit. Which means that if a person is not trained in cyber hygiene, they are more likely to suffer from social engineering attacks and their post attack effects.

In their study, Siddiqi et al. (2022), it points that people may align with equal thinking individuals and adopt similar behaviors. These types of behaviors can produce different reactions depending on the type of attack. If the attack affected the whole group, they tend to close ranks and be distrustful of outsiders. If the attack was to an individual, that person's feelings of shame

tend to make the person isolate themselves from others. Anxiety and fear of mockery can affect the group as a whole or individually. In a work environment, the group or individual can suffer from anxiety and stress due to fear of repercussions from administrators and colleagues. They fear losing trust, being reprimanded or fired, or being passed for a raise or promotion because of their mistake. Similarly, individuals suffer from stress, anxiety and depression if the attack can create problems with spouses, family members and friends, even in ethical social engineering cases.

Another thing that Siddiqui et al. (2022) noted was the fear of scarcity by individuals. People are more likely to fall for social engineering techniques if they perceive that they are missing out on something valuable, exclusive or that can be considered vital. An example of this is the scarcity of hygiene products during the pandemic of 2020. This type of fear can spill over an individual's health and make them more susceptible to health issues. People who like to be prepared for worst case scenarios are less susceptible to this type of attack and can even recover faster in this type of situation.

In Sociology, Montañez et al (2022), provide an insight into social engineering effects, which can be affected by cultural and societal norms. In a society where privacy and awareness are constantly taught, an individual is less likely to suffer from social engineering attacks. These types of societal teachings empower and educate individuals, promoting a healthier environment.

One observation of Kumar et al. (2024), is that to overcome the effects of social engineering the individual need group support. They also observe that public perception of online security depends greatly on the available programs that any individual has at their disposition.

Michael (2023) argues that to promote a change in the effects of social engineering an empathic social culture needs to be fostered and promoted in the work environment. He said to help a person move from an attack an environment of transparency, consent, self-forgiveness and acceptance of mistakes need to be fostered. An empathic culture can help a person overcome negative feelings and seek help.

Many experts argue that the social effects are great, including but not limited to manipulation of public opinion that can affect adversely, social or political movements, erosion of trust that can affect the ability of create and maintain relationships, and privacy concerns among others.

Klimburg-Witjes et al, (2021), observed that individuals who are victims of a simulated attack were often see as naïve and dumb, creating a social culture of distrust. This culture generally creates a toxic environment and affects performance and productivity. The form of speech and approaches to respond to an individual that has suffered from social engineering are impactful. If an administrator uses derogatory language to describe an individual that has suffered through a social engineering attack, ethically or not, another victim is less likely to come forth and seek education. If the administrator provides a human approach more people will be willing to admit mistakes and seek help.

In terms of Economic impact, most experts agree that people tend to be reckless after an attack. According to Berg et al. (2022), this tendency is in response to bank responses. Many people that have their credit card compromised and the problem resolved by the bank tend to be careless in their handling of their information because subconsciously they know that the bank will solve their problem. This carelessness often goes beyond credit card information, and they

get into bigger problems. They also argue about the shame and anxiety approach that victims are very fearful of banks and other financial institutions after a social engineering attack and tend to hide valuables from everyone including family and friends, being distrustful of everyone that surrounds them.

Common Ground

The evidence on Psychology shows that while the initial feelings after a social engineering attack were mostly negative, like anger, frustration, stress and anxiety, the people that were higher educated in the topic were more likely to overcome the feelings and educate themselves. They were faster in accept their mistakes and move to a place of learning, even those that were ethically social engineered. Others worried about being victim of manipulation and worried about loss of autonomy. These people responded by an increase in stress and anxiety, which could lead to depression. They were more likely to develop health problems and trust issues. Both points of view are valid but to move them to a more positive outcome there should be techniques that use the educative and acceptive principles of those that were able to overcome the effects to help those that could not.

Socially speaking the evidence shows that fostering a culture of empathy and understanding could provide a positive outcome. Feelings of being understood and listened to were more likely to trust others after a social engineering attack. In the other hand feelings of shame and anxiety were observe in individuals that did not have a positive environment at work and home. These individuals were more likely to fear repercussions from administrators and colleagues at work and spouses or family members at work. They suffered in silence and were more likely to isolate themselves. Social programs and support were very important to overcome

the problems that social engineering cause. If a person feels safe in an environment they are more likely to seek help, especially if they feel understood or they can identify with someone else situation. Social support decrease feelings of isolation. Social understanding decrease anxiety and depression.

Economically speaking, social engineering attack fostered a culture of recklessness due to bank responses to credit card fraud. People were more likely to trust others because subconsciously they taught that banks could solve any financial problem that could arise. They were more likely to make uninformed investments, increase consumption of unnecessary items or services, and need to participate in the latest economic trends. On the opposite side we saw how some individuals went to extremes of not trusting financial institutions to the point of keeping their money and valuables in a place they considered safe. These two extremes were both bad, in terms of financial security and economic health. People need to see and understand how financial security works, as well as understand the consequences of unhealthy decision making after a traumatic experience. Institutions need to educate consumers in how the products work and how they can benefit or be affected according to the decisions made.

Conclusion

While many experts agree that social engineering, even ethically done, can create psychological, social, and economic problems. They agreed that there are solutions that can be implemented to help individuals. To do this we also need to address situations that can be detrimental to these solutions. Some of those adverse situations are taboos surrounding mental health discussions, shaming a person for a mistake, fear of repercussions and authority, and environments that impact the morale and trust of individuals.

Even in ethical social engineering, people can make mistakes. Fostering communication between individuals can help address the problems of low morale and trust in a work environment. Similarly fostering communication in relationships can help a person overcome the negative feelings after a social engineering attack. If a partner or friend provides a shoulder or ear without judgement, a person is more likely to open about their feelings and seek help. Psychologically speaking therapy is a good response to those feelings. People will more likely seek recovery and take the situation as a learning experience if they are supported.

A social empathic environment either at work or outside can provide a more effective way to address the feelings of isolation and shame after an attack. If people are attuned to the victim, they will see the change in the person's personality and will try to help even if they do not know the problem. While people tend to isolate themselves after a social engineering attack a close coworker, family member or friend will try to engage the person and provide silent support.

In economics, education of the public is key. Institutions need to educate the consumer after they acquire a product, and after they suffer a social engineering attack. Developing educational products that are easy to understand by individuals, not experts, is paramount to reduced social engineering that target individuals economically. If a person understands that not all financial products are secure and protected against social engineering attacks, they will be more careful about their financial decisions. Similarly, educating a person about the risks of having every valuable item or money in one place can be risky and dangerous, because they can become targets of attacks by people they know.

Social engineering needs more research in other disciplines that are not related to technology and cybersecurity, to understand long term effects and possible solutions that mitigate and resolve

satisfactorily these attacks. Especially in situations that force social isolation like the pandemic of 2020. Even ethically done social engineering can be detrimental for society and its individuals and more needs to be done before concrete answers are provided.

References

Berg, S., and Thorvik, T. (2022). Social Engineering attacks in the light of security economics. *NTNU.* file:///C:/Users/mecgs/OneDrive/Desktop/ODU/Fall%202024/IDS%20300W/no.ntnu_inspera_107093487_30161437.pdf

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. *Science, Technology, & Human Values, 46(6), 1316-1339*. https://doi.org/10.1177/0162243921992844

Kumar, R., and Tiwari, S. (2024). Social Engineering: Its Significance and Implications for Future Research. *International Journal of Research Publication and Reviews, 5(1), pp 4255-4263.* https://doi.org/10.55248/gengpi.5.0124.0324

Michael, T. (2023). *Beyond Checkboxes: The Human Element of GRC.* EXCELMINDCYBER LLC.

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in psychology*, *11*, 1755. https://doi.org/10.3389/fpsyg.2020.01755

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, *12*(12), 6042. https://doi.org/10.3390/app12126042

Washo, A. H. (2021). An Interdisciplinary view of social engineering: A call to action for research. *Computer In Human Behavior Report, 4, 100126.* https://doi.org/10.1016/j.chbr.2021.100126