Alex Smetana

11/02/2022

CIS303

Assignment 03

The article *The Psychology of Social Engineering,* presents the idea of social engineering everyday use of it. The hypothesis of this article states “social engineering is the use of psychological, sociological, ideological tricks to manipulate people to get your own ways". Essentially, the argument is that humans exploit other humans, sometimes without the use of any code or a computer at all. Social engineering is very powerful tactic that is used every day in malicious and non-malicious ways.

The presenter in this article is Niall Merrigan, is the head of Cybersecurity Norway @ Capgemini. Based on his position and background, it is assumed that this is an individual who is aware of what he is talking about and that he is up to date on current events/cybersecurity training. His claims that he gives to the viewer is very clear and backed up with evidence. Based on that evidence, we can infer that the bias in this speech is very low.

One main message that the article describes, is how humans are the biggest vulnerabilities in any security system. In a system, a company might make great use of encryption, multi factor authentication, and have the best anti-virus software available, however all that it takes is a crack in the foundation for it to crumble, most commonly with the human

factor. It is very difficult to train humans to be secure due to the power of social engineering. Social engineering uses the power of human emotion to make an individual feel good about getting scammed. It is most notably done in marketing however, when applied with the use of malicious intent, it can have fatal results.

Overall, this article was written to educate the viewer on the effects of social engineering today. This topic is important because social engineering is used in your everyday life and most of the time it is not malicious. For example, companies use social engineering in marketing. The article gives the example of drink size prices. A standard drink size is small, medium, and large. The medium cup is almost irrelevant, it's just a placeholder between a to make a large look like a better deal because it is significantly more expensive than a small, however slightly less than a large. Ultimately, the goal of a drink is to get the most money out a consumer as possible, while using social engineering to make the consumer feel as though they have gotten a deal.

Let's make a hypothetical scenario demonstrating the use of social engineering in a malicious way. The scenario is how to gain access to a hotel room without the use of a hotel key. The first step into social engineering is providing some backstory to the person you are manipulating. For example, the scammer may call the front desk to set up ahead of time to establish a plausible story and build trust between the scammer and the victim. The scammer may tell the desk attendant that he will be out for the day and that his wife will be showing up later in the day and will be needing access to a card key. Although, this first step is not necessary, providing a call ahead helps build up trust between the scammer and victim.

Secondly, the scammer will begin their social engineering attack in person. Later in the day, the person claiming to be the guest's wife will show up at the front desk. She will mention

the phone call and provide details about the husband to further build trust with the desk attendant. Once trust is built up, the scammer will manipulate the desk attendant by creating a problem that didn't exist. For example, she may claim that she never received a card because her and her husband got in a domestic dispute resulting in her not having her card. She will reaffirm what was told in the phone call by telling the desk attendant that her husband is in a meeting a will not be available all day. She may throw in tiny details to make the victim feel bad. For example, she could tell her about the horrible day she was having and mention a ton of problems. She may throw in a bunch of unnecessary details to make the victim feel bad.

Finally, she will ask for access to the room. The front desk attendant will be more likely to comply with the scammer given more plausible the story. The scammers most goal is to try to maximize the odds that she will gain key card access. Overall, this is a basic social engineering scam has the potential to be effective based on how convincing the scammer is. Playing off human emotions while being convincing, is one of the most powerful techniques you can do to gain access to confidential information.

In conclusion, humans are the biggest weakness in any security system. Unlike security systems, humans must be trained and no matter how strong the security systems are, there will always be human error. A scammer may be able to gain confidential information without touching a computer. Social engineering is one of the easiest ways to gain information whether having malicious intent or not.

Citations

*The Pyschology of Social Engineering - Niall Merrigan*. (n.d.). Www.youtube.com. https://www.youtube.com/watch?v=wDY_SPfed7c