Preventing Social Engineering Attacks

Tristan Irvin

ICTN 4040

Dr. Lunsford

East Carolina University

April 15, 2019

Abstract

Social engineering plays a key role in information security. Many attacks are social engineering attacks, and they can cause significant damage to a business – whether indirectly or directly. Social engineering attacks attempt to steal private information and use it maliciously. In this paper, the different methods of attacks are discussed. After learning the different ways social engineering attacks are conducted, we look at how to prevent them. Preventing social engineering attacks is an important aspect of information security because these attacks are considered one of the easier attacks. By preventing these attacks, the sensitive data that attackers are attempting to gain won't be of easy access. A one hundred percent prevention rate is difficult to achieve, and some social engineering attacks are successful; however, there are ways to save important information from being leaked when an attack is successful. By learning the different attack methods and how to prevent them, the threat of social engineering attacks can easily be dramatically decreased.

Preventing Social Engineering Attacks

INTRODUCTION

Social engineering is defined as "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes", ("Social engineering | Definition", n.d.). The Oxford Dictionary defines social engineering in two ways, with the aforementioned definition being directly related to information security. Many organizations do not take the necessary precautions to protect against social engineering attacks. Since this issue is overlooked so much, it opens up another vulnerability in an organization, (Indrajit, 2017). It is assumed that social engineering attacks are random and have no structure; however, there are consistent behaviors that prove otherwise, (Indrajit, 2017). As stated earlier, these attacks aim to steal confidential information and then use it in a fraudulent way; many times, the confidential information stolen is passwords. Once passwords are stolen, they can be sold or even used to steal other confidential information that is protected by the compromised passwords. This is one example of the things attackers are looking to steal from their victims when they conduct one of these attacks. In this paper, we dive into the way social engineering has evolved, different ways social engineering attacks are conducted, and ways to prevent the attacks. Preventing social engineering attacks in a business is a difficult task due to humans being naïve in nature. After understanding the different techniques used, that difficult task can become much easier. Although completely eliminating social engineering attacks is quite impossible, this paper aims to provide a good understanding of social engineering attacks with the hope that the audience no longer is a potential victim of this kind of cyber-attack.

EVOLUTION OF SOCIAL ENGINEERING

When it comes to the evolution of social engineering, the concept has not necessarily changed. Rather, the way it is used has changed significantly. It started out as just trying to get people to gain confidence in you, (Hebert, 2018). Once someone had confidence in you, it was pretty easy to get whatever information you needed or wanted. That concept is still accurate in today's society; however, instead of manipulating someone face-to-face, most social engineering attacks happen on a computer of some sort. Whether it be a desktop computer, laptop, tablet, or cell phone, all these devices are potential platforms for a human to be socially engineered. The main way social engineering has evolved is through the medium in which an attacker gains its victims. Along with other forms of cyber-attacks, social engineering has been evolving to be a critical piece of cybersecurity today.

TYPES OF SOCIAL ENGINEERING ATTACKS

There are numerous ways that social engineering attacks could be conducted. The types that are focused on in this paper are directly related with information security that put people and business's at risk. The top three types of social engineering attacks are phishing, vishing, and impersonation. There is a fourth type that has started to become relevant in today's society, smishing, which is derived from one of the other types already mentioned. With these types of attacks identified, we will look at how each of them is conducted. The first type we will investigate is a phishing attack. Phishing attacks have been happening for quite sometime now, and even more so since email is so widely used. The way attackers conduct phishing attacks is by attempting to get someone to click on a malicious link or email attachment, (Hatfield, 2018). The reason why phishing attacks continue to be successful is because the attackers do two things: they pretend to be legitimate users that are in need of certain information, and they have become very talented at making their emails look just like a legitimate email, (Hatfield, 2018). Sometimes people are in a

rush and don't pay close attention to small details that would give away a malicious email, or sometimes someone may just be naïve and click on the malicious link. Some phishing attacks can be very sophisticated to where even highly trained IT security professionals are tricked into providing confidential information. One recent example of this was in 2016 when Hillary Clinton was running for President. Clinton's Chairman for her campaign was sent an email to his Google account that stated someone from Ukraine attempted to login to his account. The email included a link that he could change his password at to avoid his account being compromised. His IT security team investigated the email and told him that it was legit and told him to go ahead and use the link to change his password, (Hatfield, 2018). Well, he input the information into a malicious site and was the victim of a social engineering attack even though he had a security team investigate the email first. This is just one example of how sophisticated phishing attacks can be, and why it is important to learn about them. The next type of attack we will discuss is a vishing attack. Vishing attacks occur when someone attempts to steal information over the phone. These attacks happen by someone spoofing their phone number to pretend to be someone of importance, such as tech support, ("The Official Social Engineering Portal", n.d.). Some attackers that are conducting a vishing attack take extra precautious measures and use voice changers to protect their identity, ("The Official Social Engineering Portal", n.d.). There are a few techniques that vishing attackers use to successfully gain sensitive information. One of the more recent techniques vishing attackers have been using is to pretend to be someone from the IRS. The attackers would make the call claiming to be from the IRS and that the person needed to pay immediately or face consequences such as jail time, ("The Official Social Engineering Portal", n.d.). There have been several people within the last few years that have fallen for this attack simply because they get frightened by the threat of jail time. Millions of dollars have been stolen due to this type of attack

by the victims giving up credit card information. Vishing attacks are the most successful attacks when it comes to gaining information, because these attacks have been responsible for over $46 Billion lost annually, ("The Official Social Engineering Portal", n.d.). The third type of attack that we are going to look over is impersonation. Impersonation is when an attacker pretends to be someone that is of legitimate importance to their victim. Usually, the two main impersonation techniques used are an attacker trying to impersonate a delivery driver or someone from tech support, ("The Official Social Engineering Portal", n.d.). The reason delivery drivers are so easy to impersonate is because they have simple uniforms and their job is easy to do. Another thing is why they are so successful is because delivery drivers are usually trusted by a business, ("The Official Social Engineering Portal", n.d.). Once a delivery driver has gained that trust, usually they can go wherever in a building to make a delivery, which can lead to them having access to parts of an organization they shouldn't have access to. The same would go for someone attempting to impersonate tech support. They are usually already trusted, so they would just have open access to steal whatever information they wanted to. There are several other cases that someone could use to impersonate to gain information, these two are just some very common techniques that are used for impersonation attacks. The fourth type of attack that we will discuss is smishing. Smishing is when the attacker uses an SMS text message to attempt to gain information, ("The Official Social Engineering Portal", n.d.). These attacks are very similar to a phishing attack, except these attacks happen with text messages instead of through an email. The attacker usually tries to get a victim to click on a malicious link to input confidential information. Now that we have covered some different types of attacks, we see that they all have some things in common, like an attacker trying to be someone they are not. Whether it be via email, phone call, in person, or via text message, the attacker wants you to believe they are of importance to you. They are

trying to gain trust in you so that you will give up valuable information. In one example that we saw, even trained professionals can be victims. It is important to learn about how the attacks are conducted so that we can look at how prevent you from being the victim of one of these attacks.

PREVENTION METHODS

The main lesson that this paper aims to teach is how to prevent social engineering attacks. Since the people of a business are considered the weakest link in the organization, preventing against these attacks is very important. It can be one of the toughest tasks that has to be tackled, but these tips are to hopefully make the task easier. The first thing that needs to happen is the organization needs to have policies and procedures in place that protect against social engineering, (Schaab, Peckers & Pape, 2017). Such policies should be that employees cannot give out their username and password to anyone for any reason. Not only should there be these policies, but also there needs to be enforcement of the policies to make sure that employees take the policies seriously. On top of these policies, the employees need to be provided with security training and awareness programs that teach these facts about how attacks are conducted, (Schaab, Peckers & Pape, 2017). These programs should also teach the employees about the policies and the importance of them and how they protect the organization. By giving this detailed information, it makes the employees more likely to be extra cautious because they see the purpose in why they have to do something a certain way, (Schaab, Peckers & Pape, 2017). Another thing that should be taken into consideration is who receives what training. All employees should have the basic knowledge of how these attacks work, but another thing to look at is which employees are going to be attacked by a more sophisticated attack. For example, an executive of an organization would more than likely receive a very sophisticated attack because they have access to more sensitive information, so executives may require more in-depth training to make sure they understand how

to not fall victim to these attacks, (Aldawood & Skinner, 2019). The different levels of an organization may require different levels of training, but the important thing is that everyone is on the same page to make sure sensitive data is protected when it comes to social engineering attacks.

CONCLUSION

Social engineering attacks have proven to do damage to organizations. These attacks are normally successful due to the lack of knowledge and training that is provided to employees. Providing the necessary training and knowledge to employees is critical to ensure they are prepared for social engineering attacks. It goes beyond just having policies in place, but also enforcing those policies. Employees need to have sufficient knowledge of how social engineering attacks work because then they will be more likely to pick up on them when they are occurring. Along with having the sufficient knowledge of the attacks, employees need to know the importance of protecting against them as well. Knowing the importance will improve their efforts towards being cautious with information and who they give it to and will also make them more aware of emails they reply to and links they click on. Even though social engineering attacks can never be one hundred percent eliminated, taking these necessary steps can greatly decrease the likelihood of someone in your organization to fall victim to a social engineering attack.

References

*Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet,11*(3), 73. doi:10.3390/fi11030073

*Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security,73*, 102-113. doi:10.1016/j.cose.2017.10.008

Hebert, T. (2018, August 15). What is Social Engineering? The Human Confidence Game. Retrieved April 14, 2019, from https://www.globalsign.com/en/blog/what-is-social-engineering-the-human-confidence-game/

*Indrajit, R. E. (2017). Social Engineering Framework: Understanding the Deception Approach to Human Element of Security. *International Journal of Computer Science Issues,14*(2), 8-16. doi:10.20943/01201702.816

*Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information and Computer Security,25*(2), 206-222. doi:10.1108/ics-04-2017-0022

Social engineering | Definition of social engineering in English by Oxford Dictionaries. (n.d.). Retrieved from https://en.oxforddictionaries.com/definition/social_engineering

The Official Social Engineering Portal. (n.d.). Retrieved from https://www.social-engineer.org/