VICTORIA UNIVERSITY OF WELLINGTON TE HERENGA WAKA

Wellington Faculty of Engineering Te Wāhanga Ahunui Pūkaha

Ethics and Sustainability Symposium

Creating a Code of Ethics for Social Engineering in Cybersecurity: A Case Study

Abraham Alfred

Abstract

The world of cybersecurity is fast growing and has the need of more competent social engineers who can train staff and improve training further in the industry. They can engage with people if they were to either get information out of them or to educate them on their own. They can then further educate their workplace's cybersecurity posture towards social engineering attacks such as phishing, raising awareness about spyware, and teaching new personnel about the importance of upholding a professional standard while out on client engagements.

Keywords: Social Engineering; Penetration Testing; Code of Ethics; Spyware.

1. Introduction

Social Engineering is an art of subliminally manipulating a person to collect vital information. Information can come in different forms such as to gather intelligence, gain unlawful access to personal details and physical access to buildings or items or virtually into accounts, and persuade a person to perform an action they would not otherwise perform. This form of practice is often used within information security which is now widely referred to as cybersecurity. Cybersecurity is not limited to "ethical hacking", "cyber defense", "data analytics", etc. but more than that. Hatfield states cybersecurity is not limited to confidentiality, integrity, and availability of data within a computer's network, but it is also concerning broader aspects such as access to buildings, computer hardware, and remote (virtual) access via the internet [1].

The importance of social engineering in regular and intimate parts of our daily lives necessitates the need for this art to adhere to a code of ethics. The CEO of Social-Engineering LLC Chris Hadnagy states "*leave others feeling better for having met you.*" [2] as his company's core value motto. As practitioners we must practice professionalism while performing an engagement exercise on client premises [3]. Therefore, practitioners of the art of social engineering must always govern their actions through a strict code of ethics.

1.1. Objective

This paper analyses issues within and present recommendations for the creation of a code of ethics for social engineering. The scope is narrowed to a selection of pertinent issues to specifically address social engineering within penetration testing regarding information security/cybersecurity. The recommendations from this study should be seated within a more general code of ethics for social engineering. This is intended for any professional practitioner within the industry, enthusiasts interested in cybersecurity especially penetration testing, or anyone studying information security/cybersecurity.

2. Literature review

2.1. Manipulation of an individual and the importance of training

The most common social engineering attacks are the ones performed in-person. These attacks often use the Cialdini principles of persuasion and manipulation [5]. Persuading an individual through an in-person approach is considered the most important aspect for social engineering. Aldawood and Skinner state that individuals often lack personal motivation to be trained on a regular basis [6]. A vital flaw within human nature is the trustworthiness an individual has which is the point of manipulation for a threat actor. The other main flaw is that individuals usually lead very busy lifestyles within their employment as well as outside of their employment, therefore fatigue plays a large role.

Aldawood and Skinner [6] also mention that organisations often have strong security policies to force training on their employees, but it is often not grasped well by employees due to other stress within their work hours such as meeting deadlines [6]. This causes issues in terms of learning how to evade such types of attacks on a day-to-day basis. Although this can be an issue for most, other individuals often are reluctant to receive training for social engineering awareness and mitigation. This is due to the lack of interest in security within the organisations they are employed at.

The concept of security often falls upon deaf ears despite the common occurrence of personnel being attacked for information and data gathering relating to the individual's role professionally and personally [6]. Awareness training is important because threat actors often target employees who hold a low profile at a workplace. Sometimes, this is not ideal for the threat actor, but it allows leverage for them to privilege escalate during their information gathering attacks as they move up in the chain for a wider attack surface.

2.2. Use of technology within Social Engineering

The use of technology plays the biggest part in the realm of social engineering. Threat actors use attack vectors such as phishing. Phishing is a term for spoofing emails, text messages on a cellular device, social media messaging service messages, fake popup ads on webpages, and so forth [4]. It has many other names which are spear phishing, whale phishing and vishing phishing [4]. These special attack names are often used in terminology towards higher ranking targets such as important military and government personnel, journalists etc. These types of attacks are often done by nation state sponsored actors to commit cyber espionage and siphon vital information from high-ranking personnel. Often carried out via email attachments, these are carefully conducted operations by threat actors. The most well-known attack in current year was done through a spyware known as Pegasus [7].

Developed by an Israeli cyber weapons firm going by the name NSO Group, developed this state-of-the-art cyber weapon for the purpose of the collection of data of specific individuals listed as major criminals [8]. This cyber weapon was later used by the Saudi Arabian government to track a Saudi journalist named Jamal Khashoggi [12]. Pegasus was used to track and hunt down the journalist which later led to the torture and murder of the journalist by the Saudi Arabian government. A forensics investigation led by Amnesty International uncovered that Pegasus used a "zero-click" tactic to launch its attacks [9].
A zero-click attack is where the user does not need engagement with a notification, application, or webpage they come across. If the Pegasus payload is sent to the victim, it unleashes itself on the user's device without interaction [9]. In the independent peer review carried out by Marczak, Scott-Railton, Anstis, and Deibert from Citizen Lab on July 18, 2021, have stated that the spyware known as Pegasus was indeed being used maliciously towards the death of the Saudi journalist [10].

Pegasus worked as a spear-phishing tool as an investigative journalist called Carmen Aristegui was targeted by this spyware. Her son was a collateral target as the spyware was used to send fake notifications about his mother and other fake notifications [11]. Carmen was sent urgent work-related messages which were of serious nature. Some messages contained notifications of kidnappings of her colleagues and defamation lawsuits [11].

3. Code of ethics

The appropriate code of ethics is deemed to be the code which is used by Social Engineer LLC, designed by their CEO. The following are the sections which are applicable:

1. **The social engineer must always respect the public and take ownership of their actions.**
   "Respect the public by accepting responsibility and ownership over your actions, and their effects on the welfare of those in, around, and involved with the engagement" [2].
2. **The social engineer must always avoid illegal activities at all costs.**
   "Avoid engaging in, or being a party to, unethical, unlawful, or illegal acts that negatively affect your professional reputation, the information security discipline, the practice of social engineering, others' well-being, or the parties and individuals in, around, and involved with the engagement" [2].
3. **The social engineer must never cause grief or harassment of any kind to the person they are targeting within an engagement.**
   "Reject any engagement, or aspect of an engagement, that may make a target feel vulnerable or discriminated against. This includes, but is not limited to, sexual harassment, offensive comments (verbal, written, or otherwise) related to gender, sexual orientation, race, religion, or disability, stalking, or following, deliberate intimidation, or harassing materials. Additionally, lewd, or offensive behaviour or language, which may be sexually explicit or offensive in nature, materials or conduct, language, behaviour, or content that contains profanity, obscene gestures, or gendered, religious, ethnic, or racial, slurs are all to be avoided. Employing any of these tactics reduces the target's ability to learn and improve from the engagement" [2].
4. **The social engineer must always train new personnel learning the art of social engineering in a way that their actions leave a good impact on the client and people in general.**
   "When training future social engineers, consider that training will leave a lasting impact on your students and the methodology with which you train will echo through all students' future engagements. Provide students with the knowledge and tools to create positive learning environments and productive scenarios for their future engagements and clients" [2].
5. **The social engineer must also train the new personnel with realistic scenarios to perform professionally during engagements.**
   "Ensure the social engineering practices of yourself and your students include conscientious, thoughtful, and considerate ways to escalate engagements to eventually emulate real-world attack vectors. Recognize our clients are seeking ways to improve their security posture and work with them to increase the difficulty of realistic attack vectors" [2].
6. **The social engineer must never expose vulnerabilities unless told to do so by their employer or the client.**
   "Respect that social engineering engagements involve human vulnerability and avoid publicizing vulnerabilities, whether through a blog, social media, or other medium, that result in harmful effects, emotions, or feelings for your client and the individuals and parties in, around, and involved with the engagement" [2].
7. **The social engineer must always do their best to represent the firm which they work for and the cybersecurity industry to the best of their ability.**

> “Do not misrepresent your abilities or your work to the community, your employer, or your peers. Ensure you have the experience and knowledge promised to your clients and stakeholders” [2].

3.1. Wider approaches

3.1.1. Principle i

For the first code, a wider approach is that the social engineer must strictly take ownership of their actions while on a wider engagement. This will prevent any mistakes in the future from the social engineer. It also allows the engineer to respect the public and not abuse their social manipulation talent. This can be applied to day-to-day engagements with clients or whilst out in public.

3.1.2. Principle ii

For the second code, a wider approach is that the social engineer must avoid any illegal activities. This can be applied to the social engineer avoiding abusing their ability as mentioned above. It can also prevent the social engineer from staying away from being unlawful and abusing their ability to gain information by illegal means.

3.1.3. Principle iii

For the third code, a wider approach is that the social engineer must always avoid any act of harassment. If the consequences of their engagement could potentially result in harassment in a pre-planning stage of any public or private engagement, it must be avoided at all costs.

3.1.4. Principle iv

For the fourth code, a wider approach is that the social engineer needs to train new onboarding staff within their company to represent good morals while out on an engagement and think critically just in general as well as within a cybersecurity perspective.

3.1.5. Principle v

For the fifth code, a wider approach is that the social engineer needs to train new onboarding staff within their company with new training tactics and provide realistic scenarios from which they can learn from. Realistic scenarios will be comprised of any cold call tactics such as vishing. Vishing is voice phishing which uses lying to an individual by means of impersonation of another person [1].

3.1.6. Principle vi

For the sixth code, a wider approach is that the social engineer must never expose any vulnerabilities found to the public unless told to do so by a client or their employer. This is because of any legal issues the client, or their employer could face. They must always ask for permission before making any decisions such as vulnerability exposure.

3.1.7. Principle vii

For the seventh code, a wider approach is that the social engineer must always represent their industry and employer to the best of their ability. This is because they are representing just more than themselves and their skills out in the field during engagements. They must always take pride in the industry they work in and the employer they work for. This shows professionalism and an excellent work-ethic which attracts clients as well as making yourself well known in the industry for your set of skills.

4. Case study

The specific case study this paper focusses on is of social engineering being used in penetration testing within cybersecurity. Within penetration testing, social engineering can be used for engagements. A small to medium sized enterprise (SME) which has a team of six hackers who are given a task to breach a local well known law firm within Wellington, New Zealand.

The law firm has employees who are from different cultural backgrounds and the company is culturally diverse. Some of the staff are university students working as a law clerk on their university holidays and majority of staff are female. They are tasked with getting information out of everyone who works at the law firm. They are sent out for the engagement within said law firm and find that the law firm have previously been a part of many other vulnerabilities and are continuing to use bad practices within their workplace.

4.1. Principle i

The first code states that the social engineer must always respect the public and take ownership of their actions. In the scenario listed above, the hackers must always treat everyone equally and with respect. They must never abuse the power they behold as social engineers. They must treat the staff at the law firm with the respect the employees deserve and never overstep their boundaries. Overstepping boundaries relates to gathering information unnecessary to the task at hand and over engaging with one of the law firm's employees.

4.2. Principle ii

The second code states that the social engineer must always avoid illegal activities at all costs. The hacker accidentally might leak information that they have uncovered during their engagement at the law firm. If they were to perform any unethical activity such as misuse of data after gaining access through social engineering tactics, it is deemed illegal and the hacker could defame the cybersecurity industry, the company they work for, lose their employment at the cybersecurity firm which they work for, face jail time, etc. This can be prevented by keeping to a strict code of conduct such as avoid storing information on any non-corporate device. This can be the hacker's personal cell phone etc.

4.3. Principle iii

The third code states that the social engineer must never cause grief or harassment to any person. The hacker must never discriminate a person while at the law firm. A hacker could potentially be biased towards focusing on vulnerable people such as people of different racial heritages. Often, there is a language barrier which is easy to manipulate. However, this can be considered harassment as the person being engineered potentially might not understand the hacker if the hacker is a fluent English speaker and provide the hacker with any information with ease to avoid hassle. This must always be avoided at all costs as it is not appropriate to prey on easy targets even if it is tempting.

4.4. Principle iv

The fourth code states that the social engineer must train new personnel in a way their actions leave a good impact. The hackers mentioned in the case study must train all new staff to the best of their abilities that they reflect their mentors in the end of their training phases by making good and moral choices. They must make sound decisions while on an engagement with a high-ranking client such as the law firm mentioned above. If staff was not trained correctly, this could result in the client (in this case the law firm) losing trust in the cybersecurity firm which could lead to a loss of a contract and a termination of any future engagements within that law firm.

4.5. Principle v

The fifth code talks again about training new personnel but with new tactics and realistic scenarios to help them perform professionally during an engagement. This will avoid any issues previously mentioned in above principles as well as give new personnel the best approach on how to gauge a situation and plan an attack accordingly and then act upon that decision made by them.

4.6. Principle vi

The sixth code talks about not exposing any vulnerabilities. As mentioned in the case study, the law firm have quite a few vulnerabilities. The vulnerabilities are not directly related to social engineering, but they were successfully found due to the tactics of social engineering. These can easily be mitigated by better staff training within the law firm.

4.7. Principle vii

The seventh code states that the social engineer must always do their best to represent their firm and the industry. This must be upheld to the highest standards while on an engagement. This is because the hackers are representing their firm and its capabilities by acting as a unit of highly skilled professionals. Therefore, a very strict policy must be followed to carry out successful engagements.

5. Conclusion and recommendations

Social engineers who are working in the field must consider better training techniques to train new staff within their team as well as training client staff and other employees within their own workplace. The lack of security awareness is the biggest flaw, making matters worse as well as the lack of willingness to learn is another flaw which must be tackled by professionals within the industry.

The best way to approach both situations would be to offer training sessions which are flexible with employee workloads. Holding conferences which capture the person's interest is the best step forward in terms of educating them about threats like social engineering. Enriching people's knowledge about common social engineering tactics will make the person learning feel as if they were a social engineer themselves.

References

[1] J. M. Hatfield, "*Virtuous human hacking: The ethics of Social Engineering in penetration-testing*," Computers &amp; Security, vol. 83, pp. 354–366, 2019. [Accessed: 20 April 2022].

[2] "*Social Engineering Code of ethics*," Security Through Education, 11-Jun-2021. [Online]. Available: https://www.social-engineer.org/framework/general-discussion/social-engineering-code-of-ethics/. [Accessed: 20 April 2022].

[3] "*It is important to have ethics in social engineering*," Social, 31-Dec-2020. [Online]. Available: https://www.social-engineer.com/it-is-important-to-have-ethics-in-social-engineering/. [Accessed: 22 April 2022].

[4] F. Salahdine and N. Kaabouch, "*Social Engineering Attacks: A survey*," Future Internet, vol. 11, no. 4, p. 89, 2019. [Accessed: 22 April 2022].

[5] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "*Advanced Social Engineering attacks*," Journal of Information Security and Applications, vol. 22, pp. 113–122, 2015. [Accessed: 18 April 2022].

[6] H. Aldawood and G. Skinner, "*Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues*," Future Internet, vol. 11, no. 3, p. 73, 2019. [Accessed: 10 April 2022].

[7] "*Massive data leak reveals Israeli NSO spyware used to target activists, journalists, and political leaders,"* Amnesty International, 07-Jan-2022. [Online]. Available: https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/. [Accessed: 25 April 2022].

[8] "*Scale of secretive Cyber Surveillance 'an international human rights crisis' in which NSO Group is complicit*," Amnesty International, 07-Jan-2022. [Online]. Available: https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso/. [Accessed: 25 April 2022].

[9] "*Forensic methodology report: How to catch nso group's pegasus*," Amnesty International, 26-Apr-2022. [Online]. Available: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/. [Accessed: 25 April 2022].

[10] B. Marczak, J. Scott-Railton, S. Anstis, and R. Deibert, "*Independent peer review of Amnesty International's forensic methods for identifying pegasus spyware*," The Citizen Lab, 19-Jul-2021. [Online]. Available: https://citizenlab.ca/2021/07/amnesty-peer-review/. [Accessed: 25 April 2022].

[11] J. Scott-Railton, B. Marczak, B. A. Razzak, M. Crete-Nishihata, and R. Deibert, "*Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware*," The Citizen Lab, 10-Nov-2021. [Online]. Available: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/. [Accessed: 25 April 2022].

[12] "*Jamal Khashoggi: All you need to know about Saudi journalist's death*," BBC News, 24-Feb-2021. [Online]. Available: https://www.bbc.com/news/world-europe-45812399. [Accessed: 25 April 2022].