A Primer on Social Engineering Threats

Paul Chin[*] & Lim Thong Soon[**]

Abstract: Social Engineering Attacks are a form of deception using communication or media network whereby the victim is tricked into revealing usernames, passwords or other sensitive information to a hacker, parting with a sum of money, or performing some insecure acts. It is not limited to computer systems and can also be done through normal telephone calls or face-to-face communication. World renowned computer hacker Kevin Mitnick who evaded the authorities in the 1990's was the world's first hacker known to widely employ social engineering attacks above all else as the main medium of attack. Such attacks became more prevalent as people began to rely more and more on social media and social networking services. Among all the hacking incidents, the basic principles employed in social engineering attacks have not changed much over the years, as in this attack the hacker targets vulnerable users by psychological manipulation. It has been said that a chain is only as strong as its weakest link. More so when it comes to security. A security system is only as strong as its weakest link - which is the human user. Social engineering attacks lead to loss of finances, intellectual property, private data and consumer credibility. This paper examines the anatomy and execution of the attack and also presents a survey of the various notable frameworks to study such attacks and concludes with some mitigation countermeasures to deal with the threat.

Keywords: Social engineering, social media, social network, phishing, security awareness

[*]Paul Chin, School of Applied Creative Arts and Design, Han Chiang University College of Communication. Email: paulchin@hju.edu.my
[**]Lim Thong Soon, School of Applied Creative Arts and Design, Han Chiang U niversity College of Communication. Email: limthongsoon@hju.edu.my

INTRODUCTION

Social Engineering Attacks are a form of deception using communication or media network whereby the victim is tricked into revealing usernames, passwords or other sensitive information to a hacker, or, to perform some insecure acts (Kumar et al., 2015). It is not limited to computer systems and can also be done through normal telephone calls or face-to-face communication. World renowned computer hacker Kevin Mitnick who evaded the authorities in the 1990's highly advocates social engineering attacks above all else as a medium of attack (Zheng et al., 2019).

MEDIUM OF ATTACK

Among all the medium of attacks, social engineering is the least technical of all as it can take the form of a simple phone call at the very least. Other forms of attack include sending fake emails, SMS, fake websites, fake login pages and fake software downloads also known as trojans. An organisation may install the best firewalls, antivirus and intrusion detection systems. These may be the cutting-edge technology, but, one thing that organisations usually overlook is the human factor. It has been said that a chain is only as strong as its weakest link. More so when it comes to security. A security system is only as strong as its weakest link - which is the human user (Mitnick & Simon, 2002).

A TYPICAL ATTACK SCENARIO

Selamat Sdn Bhd (Selamat) is a high-tech company boasting of its latest cutting-edge firewall and intrusion prevention systems. Its staff consist of highly skilled workers knowledgeable in IT and security and also some administrative staff. One of the administrative staff, Miss Harimau is a social media freak and frequently hangs out on Facebook. One fine day, she receives a friend request from a handsome gentleman, Mr Skywalker. Delighted and taken in by his good looks and trusted profile, she immediately accepts the friend's invitation. Over the next few weeks, the online chats became more and more intimate. Then, one fine

day, Mr Skywalker emailed her an intimate picture of himself as an attachment. Unknown to Miss Harimau, the picture file not only contains a picture but also a hidden program. She threw caution to the winds and immediately opened the picture file on her office PC. While she was looking at the photos, the hidden program evades all antivirus and installs itself as a hidden backdoor which allows Mr Skywalker to take control of not only Miss Harimau's PC but also as a launchpad to escalate attacks against the internal network of Selamat Sdn Bhd.

ANALYSIS OF THE ATTACK

Mr Skywalker bypassed the perimeter defence firewall and intrusion prevention systems and managed to get into the organisation by deceiving a human user. He did not attack the high-tech equipment, he attacked the human users - the weakest link in the security (Mitnick & Simon, 2002). Prior to the attack, he had managed to find out the staff names from the company profiles on the Internet. A deep search using data mining tools like Maltego (Al-khateeb & Agarwal, 2019) revealed some facebook accounts. After filtering some names, he chose the most gullible one - Ms Harimau. Putting out some fake photos of himself and creating fake profiles and posts, he managed to befriend Ms Harimau. He then proceeded to gain the trust and friendship patiently over the course of the next few weeks. Then, he crafted a new backdoor program from scratch and also used encryption so as to avoid all antivirus detection (Tasiopoulos & Katsikas, 2014). The program was written to show a revealing picture of himself when clicked. This fake file is also known as a Trojan. He altered the extension of the picture file to masquerade as a jpg photo using the RTLO exploit (Tasiopoulos & Katsikas, 2014). He then emailed it to Ms Harimau's corporate email to ensure it bypassed the firewalls and intrusion prevention systems. When Miss Harimau opened the attachment, her Antivirus did not detect it as a malware because it was a (sic) picture file and also because it was a newly created program - also known as zero-day malware (Tasiopoulos & Katsikas, 2014).

In this scenario, the social engineering took place:

1. When she accepted Skywalker's friend request on Facebook.

2. When she continued to develop the friendship and the trust over the ensuing weeks.
3. Having trusted Skywalker and also unable to contain her inquisitiveness, she opened the email attachment that Skywalker sent her.

ANATOMY OF A SOCIAL ENGINEERING ATTACK

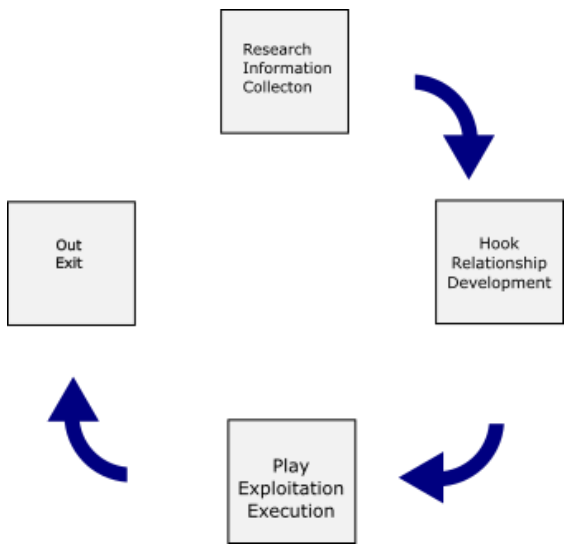


Figure 1: Anatomy of a social engineering attack (Salahdine & Kaabouch, 2019)

1. STAGE ONE: INFORMATION GATHERING

It starts off with information gathering where the hacker finds out as much information about the target as possible. He would use automated social engineering attack tools like Maltego to map out hidden paths and relationships between the organisation and its employees, friends, mentors, affiliations, schools, relatives and everything related to all the people connected to the target. This wealth of information can be used to lend credence to the attack, eg if the hacker knows that Miss Harimau likes certain food or engages in certain hobbies, he could send her things related to what she likes. Furthermore, the hacker could also spoof the email sender's name and email to masquerade as one of her friends. This is typically done in phishing attacks where a hacker pretends to be from a

Bank and sends an email pretending to be from the said bank complete with fake bank email sender's address and a letter head with convincing logos and a design which looks identical to that coming from the bank. This attack is also known as Spear Phishing (Gupta et al., 2017). In the body of the letter, the hacker would give fake warning messages saying that the account needs to be re-validated for security reasons and it provides a fake link to the (sic) bank's website where the user can re-enter her credentials to re-validate her account (Lohani, 2018). In such a scenario, the gullible victim would trust the email because she would indeed have an account with such a bank. The hacker knows this from the information gathering which was done at the outset (Al-khateeb & Agarwal, 2019).

2. Stage Two: Hook Relationship Develoment

In stage two, the hacker builds up the relationship with the objective of gaining the trust of the target. In the case of Harimau, the facebook relationship deepens over the days with Mr Skywalker gradually building up the trust (Zheng et al., 2019) .

3. Stage Three: Play Exploitation And Execution

In this stage, the hacker, would attack the user by using deception in order to cause the victim to perform a security-flawed action, eg, open an email attachment containing a trojan, or click on a link in an email message to go to a fake website to key in her password, or to make some money payment or transfer. This attack works because of the trust which was built from Stage Two of the attack.

4. Stage Four: Exit

In this final stage, the hacker, having obtained the fruits of his labour would either silently leave the scene, or, keep a low profile whilst maintaining a backdoor access to the system, depending on the initial objective of the attack. If the initial objective was to bypass the perimeter defence and enter an organisation's network, then he would continue to maintain a low-profile whilst wiping out all traces of the attack. On the other hand, if the initial objective was to cause a sum of money to be transferred, then he would silently leave the scene without a trace. If a

facebook account was used as the medium of attack, the owner would be untraceable as he would have used VPN and Tor networks to hide his location and IP address when creating a fake facebook or email account and posting or emailing his victims (Sardá et al., 2019).

Social Engineering Framework Models

Two types of social engineering framework models exist in the literature. The first is a conceptual model and the second is phase-based model. The former involves what is called key-entities in a social engineering attack, whilst the latter employs the actual attack process (Zheng et al., 2019). A large number of the phase-based models involve a life-cycle type of attack, also known as the Kevin-Mitnick social-engineering cycle of attack (Mitnick & Simon, 2002).

Kevin Mitnick Social Engineering Cycle

This is the most common of all the Social Engineering Attack Cycles and is depicted in Figure 2, which bears some similarities to the anatomy of an attack as referred to in Figure 1.

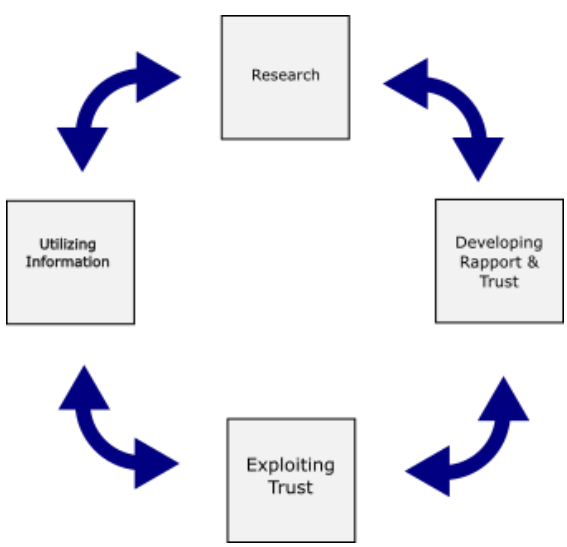


Figure 2: Kevin Mitnick's Social Engineering Cycle

The difference is that in Kevin Mitnick's cycle, the phases repeats itself like a clock-face going clockwise from Research to Developing Trust to Exploiting to Utilising Information and then back to Research. Not only that, the cycles can go backwards, i.e anti-clockwise. For example, if during the Exploiting Trust phase, if the objectives are not met, then the hacker can go back to the previous phase, viz. Developing Rapport and Trust. Then, once, more trust has been established, he can proceed to Exploiting Trust again. Similarly, in the Utilising Information phase, new data may emerge. This can then lead to the next phase, which is Research, and the cycle repeats itself.

RESEARCH PHASE

The Research Phase is where the attacker collects information from the web, articles, news, magazines, observations and subtle queries either through emails, phone calls, or social network interactions.

DEVELOPING RAPPORT AND TRUST PHASE

This is where the attacker tries to develop intimacy, friendship and trust with the target. He may use insider information, citing people known to the target, plea for assistance, or faking some authority.

EXPLOITING TRUST PHASE

In this phase, the attacker could fake the requesting of assistance from the victim to perform some action. This could be information or physical actions like transfer of file, money, or, access to some protected service, or building. Another tactic is to psychologically influence the target to seek assistance from the attacker. From the information gathering research phase, the attacker could know that the target may be in need of something. He could then take advantage of this knowledge to tacitly give the impression that he could provide what the target is seeking.

UTILISING INFORMATION PHASE

In this phase, the attacker could already have achieved the objective. If it is part of a bigger objective, then the attacker would repeat the cycle or revert back to an earlier phase in the cycle and repeat until the final objective is achieved.

EVOLUTION OF SOCIAL ENGINEERING ATTACKS

Other phase-based models are developed from Kevin Mitnick's cycle. All of them have Kevin Mitnick's basic cycle and are only differentiated in detailed sub-phases. Apart from this, there are also conceptual models. These models are purely academic as they focus on the ingredients of each phase, eg. Janczewski and Fu, (2010) proposed a conceptual model where the elements of social engineering attacks are extracted into attacking methods, vulnerabilities, consequences and defences. One drawback of the conceptual model is that it is not intuitive and does not provide a clear picture of how an actual attack unfolds in real life. To meet the shortcomings of these social engineering attack models, Zheng et al. (2019) proposed a model consisting of SED and SES. SED stands for Social Engineering Dialogs whilst SES is an acronym for Social Engineering Session. One complete attack from commencement to completion where the goal is achieved is called an SES. And each SES can be broken down into small logical sections called SED (Social Engineering Dialogs). This is analogous to strategy and tactics. The long term objective and plan of attack is strategy and is comparable to SES, whilst the short term objective of each stage is the tactics, which is analogous to SEDs. The SES model consists of three stages:

1. Preparation of the attack;
2. Implementation of the attack; and
3. Attack gain

Each stage can be implemented using one or multiple SEDs. An SED typically includes the required elements, eg, physical objects, resources, players and script dialog.

TYPES OF SOCIAL ENGINEERING ATTACKS

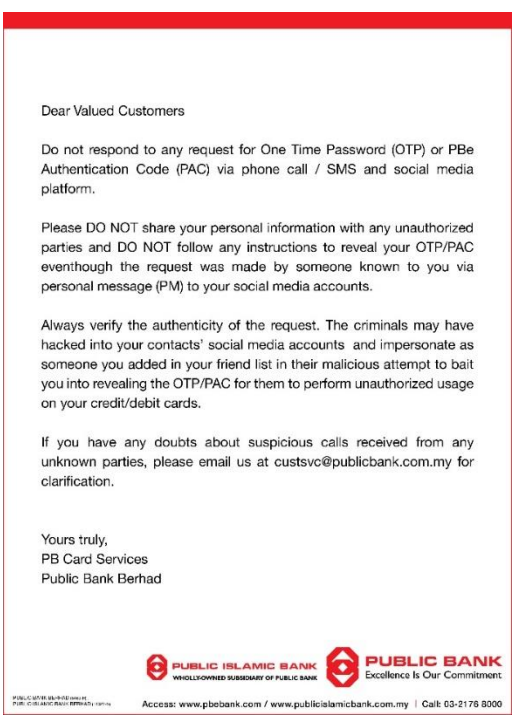
Figure 3 summarises the various types of attacks that exist (Salahdine & Kaabouch, 2019). Each of them can be technical based or human based, or a mix of the two.

Figure 3: A chart showing Social Engineering Attacks
(Salahdine & Kaabouch, 2019)

PHISHING

This is the most prevalent of all social engineering attacks (Gupta et al., 2017). The attackers' goal is to acquire personal information via emails, telephone calls, sms, social media and websites. Examples include fake emails asking a victim to reactivate his/her bank account by visiting a fake bank login website provided via a link in the email. Another example is a fake message to the victim informing the latter of

some prize money won and requiring the latter to perform some further action to claim the money. Phishing attacks can be sub-divided into Vishing, Business Email Compromise, Whaling, Interactive Voice Response and Spear Phishing. Among these phising sub-categories, the deadliest of them all is Spear Phishing. This is because the victims are attacked apparently from the inside, eg, a phone call from your bank informing you that someone has used your Identification Card to apply for a credit card and has swiped a sum of money with it. The caller is able to confirm your full name, Identification Card number, address and other details. This makes it difficult to detect the fake caller from a legitimate call from a bank. All these elements combine to make it the phishing attack with the highest success rate (Gupta et al., 2017). Spear Phishing is also known as credential spear phishing as it invariably uses the victim's credentials to exploit the trust mechanism to manipulate the user into performing insecure actions. Figure 4 shows an advisory from a bank alerting customers about a spear phishing attack.



Dear Valued Customers

Do not respond to any request for One Time Password (OTP) or PBe Authentication Code (PAC) via phone call / SMS and social media platform.

Please DO NOT share your personal information with any unauthorized parties and DO NOT follow any instructions to reveal your OTP/PAC eventhough the request was made by someone known to you via personal message (PM) to your social media accounts.

Always verify the authenticity of the request. The criminals may have hacked into your contacts' social media accounts and impersonate as someone you added in your friend list in their malicious attempt to bait you into revealing the OTP/PAC for them to perform unauthorized usage on your credit/debit cards.

If you have any doubts about suspicious calls received from any unknown parties, please email us at custsvc@publicbank.com.my for clarification.

Yours truly,
PB Card Services
Public Bank Berhad

PUBLIC ISLAMIC BANK
WHOLLY-OWNED SUBSIDIARY OF PUBLIC BANK
PUBLIC BANK
Excellence Is Our Commitment

Access: www.pbebank.com / www.publicislamicbank.com.my | Call: 03-2178 8000

Figure 4: An advisory from a bank on phishing attack

MITIGATING SOCIAL ENGINEERING ATTACKS

Apparently, one way to prevent such attacks is through creating more awareness among netizens of how such attacks are executed. In order to make good locks, one must first know how to break locks. This is where the media can play a pivotal role in disseminating information effectively. Nevertheless, even today with so many fraud and social engineering cases already reported in the media, people still fall easy prey to scams and deception. This is because the social engineering hacker exploits human nature's innate tendency to trust one another. This trust mechanism is not only used by hackers but also exploited by seasoned marketing professionals to sell products and services. The burning question that remains is how do we create this awareness of social engineering attacks.

Companies and organisations should take the lead. They should make addressing social engineering attacks part of corporate risk management strategies (Osuagwu et al., 2015). Some of the measures that can be taken include reporting hacking incidents, keeping confidential information safe, orientating new employees to secure best practices, sharing list of blacklisted emails, promoting security workshops, educating employees on dangers of social media and communication networks (Foozy et al., 2011). Fake phone calls can be detected by consulting contact lists, avoiding performing actions from unsolicited calls, interrogating callers with answers only known to the recipients and requesting to call back to a publicly-verified telephone number instead of the given one (Kaushalya et al., 2019). Companies could organise discreet practical simulations of phishing attacks where employees take part (Chothia et al., 2019). This practical training would expose employees to what it feels like to be psychologically manipulated in a real attack and as such prepare them to identify future attacks. Ho et al. (2010) proposed a reliable system which would apply a set of scoring criteria on communications based on certain established attacker anomalies to determine whether it is a spear phishing attack. Trojan-based attacks may be thwarted by disallowing others to use your computer, and also using USB scanners and also warning users about the dangers of using picked-up USB devices. Email attachments from suspicious sources should also not be opened.

Of all the counter-measures proposed, only one of them focuses on the crucial element – the human user. Better insight could be gleaned by looking directly at a human user's personalities and traits that make users more vulnerable. Such an approach is in fact advocated by Albladi and Weir (2016). The researchers propose studying the reasons people become victims so easily to psychological manipulation. We need to identify the factors that make people susceptible and build profiles to identify human weaknesses. Once we know how to identify vulnerable groups, training and education could be used to upgrade their awareness and skills to defend against such attacks. As such, a user-centric framework should be created to investigate highly susceptible user profiles. Bakhshi (2018) did a research in which USB sticks marked 'confidential' were strewn about near the office building entrance. It was found that 60% of the office workers who picked up the 'confidential' USB sticks would actually plug it into their office computers to see what was inside. A hacker could deliberately drop trojanised USB sticks outside the entrance of the building or office carparks of the target organisation. We can count on 60% of the employees to pick them up and plug them into their office PCs, thus, giving easy access to hackers from outside the organisation. As such, any kind of user-centric profiling of vulnerable users need to include such human traits.

Another refreshing approach to dealing with social engineering attacks was proposed by Algarni et al. (2016). The researchers did a study on one of the most fertile grounds for social engineering attacks, viz. social networking sites, eg. Facebook. They found that attacks executed in Social Networking Sites had high success rates due to the following factors:

1. Perceived Sincerity
2. Perceived Competence
3. Perceived Attraction
4. Perceived Worthiness

The above four factors combined together increase the source credibility of attackers, hence eliciting high levels of trust. One of the prominent features of Facebook is the Mutual Friends parameter. If a user

sees that a new friend requester has many mutual friends, then she is more inclined to trust him.

Kevin Mitnick also provided a Security Awareness Online Training (Mitnick, 2019). This is a web-based interactive training using live demonstration videos, short tests and scenarios. Topics covered include the major social engineering attack vectors, including spams, general phishing, spear-phising and ransomware.

CONCLUSION

Social Engineering Attacks are here to stay. Despite all the technological advances in computer and network security, systems are still vulnerable as hackers will continue to attack the weakest link – human users. This is compounded by the lack of initiative among companies and organisations to take a pro-active role to tackle this issue. With the advent of Internet innovations and the growth of Social Networking Sites, we can expect to see not a decrease, but rather an increase in such attacks as social networking sites will always be fertile hunting grounds for hackers. A core need for humans is the need to interact and to communicate with fellow humans. Each day, more and more resources are being channeled into linking people together – thus unwittingly increasing the attack surface manifold. Needless to say, social engineering attacks will continue to evolve and grow as there will never be a shortage of people whose daily lives are intimately connected to social media and social networking services.

REFERENCES

Al-khateeb, S., & Agarwal, N. (2019). *Social Cyber Forensics (SCF): Uncoverin g Hidden Relationships*. https://doi.org/10.1007/978-3-030-13690-1_4

Albladi, S., & Weir, G. R. S. (2016). Vulnerability to social engineering in social networks: A proposed user-centric framework. *2016 IEEE Internationa l Conference on Cybercrime and Computer Forensic, ICCCF 2016*. http s://doi.org/10.1109/ICCCF.2016.7740435

Algarni, A., Xu, Y., & Chan, T. (2016). Measuring source credibility of social engineering attackers on Facebook. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2016-March*, 3686–3695. https://doi.org/10.1109/HICSS.2016.460

Bakhshi, T. (2018). Social engineering: Revisiting end-user awareness and susce ptibility to classic attack vectors. *Proceedings - 2017 13th International Conference on Emerging Technologies, ICET2017*, *2018-Janua*, 1–6. h ttps://doi.org/10.1109/ICET.2017.8281653

Chothia, T., Paiu, S.I., & Oultram, M. (2019). Phishing Attacks: Learning by Doi ng. Retrieved October 18, 2019, from https://www.cs.bham.ac.uk/~tpc/ LearnToPhish/ website: www.cs.bham.ac.uk/

Foozy, C., Ahmad, R., & Abdollah, M. (2011). Generic Taxonomy of Social Eng ineering Attack. *Malaysian Technical Universities International Confer ence on Engineering Technology MUiCET 2011 (2011)*, (MUiCET), 52 7–533. Retrieved from http://ftmk.utem.edu.my/zaki/VolumeII/PENUL ISAN DAN PENERBITAN/4.1/Antarabangsa/Prosiding/4.1.9b/muceit2 011cikferesa.pdf

Gupta, S., Singhal, A., & Kapoor, A. (2017). A literature survey on social engine ering attacks: Phishing attack. *Proceeding - IEEE International Confere nce on Computing, Communication and Automation, ICCCA 2016*, 537 –540. https://doi.org/10.1109/CCAA.2016.7813778

Ho, G., Sharma, A., Javed, M., Paxson, V., & Wagner, D. (2010). Detecting Cre dential Spearphishing Attacks in Enterprise Settings. *Proceedings of the International Multiconference on Computer Science and Information T echnology*. Retrieved from https://www.usenix.org/conference/usenixse curity17/technical-sessions/presentation/ho

Janczewski, L. J., & Fu, L. (2010). Social engineering-based attacks: Model and New Zealand perspective. *Proceedings of the International Multiconfer ence on Computer Science and Information Technology, IMCSIT 2010*, *5*, 847–853. https://doi.org/10.1109/imcsit.2010.5680026

Kaushalya, S. A. D. T. P., Randeniya, R. M. R. S. B., & Liyanage, A. D. S. (201 9). An Overview of Social Engineering in the Context of Information Se curity. *2018 IEEE 5th International Conference on Engineering Techno logies and Applied Sciences, ICETAS 2018*. https://doi.org/10.1109/ICE TAS.2018.8629126

Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social Engineering Threats and Awareness: A Survey. In *European Journal of Advances in Engineerin g and Technology* (Vol. 2).

Lohani, S. (2018). Social Engineering: Hacking into Humans. *4th International Conference on Cyber Security (ICCS) 2018*. https://doi.org/10.0000/PA PERS.SSRN.COM/3329391

Mitnick, K. (2019). Kevin Mitnick's Security Awareness Training. Retrieved Oc tober 19, 2019, from https://www.mitnicksecurity.com/shopping/kevin-mitnick-security-awareness-training website: https://www.mitnicksecuri ty.com/shopping/kevin-mitnick-security-awareness-training

Mitnick, K. D., & Simon, W. L. (2002). *THE ART OF DECEPTION Controlling the Human Element of Security*. Wiley.

Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015). Mitigating social engineering for improved cybersecurity. *CYBER-Abuja 2015 - International Conference on Cyberspace Governance: The Imperative for National and Economic Security - Proceedings*, 91–100. https://doi.org/10.1109/CYBER-Abuja.2015.7360515

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Sardá, T., Natale, S., Sotirakopoulos, N., & Monaghan, M. (2019). Understanding online anonymity. *Media, Culture & Society*, *41*(4), 557–564. https://doi.org/10.1177/0163443719842074

Tasiopoulos, V. G., & Katsikas, S. K. (2014). Bypassing Antivirus Detection with Encryption. *Proceedings of the 18th Panhellenic Conference on Informatics - PCI '14*, 1–2. https://doi.org/10.1145/2645791.2645857

Zheng, K., Wu, T., Wang, X., Wu, B., & Wu, C. (2019). A Session and Dialogue-Based Social Engineering Framework. *IEEE Access*, *7*, 67781–67794. https://doi.org/10.1109/ACCESS.2019.2919150