The Digital Forensics Challenges Of Social Engineering Forensics

# Abstract

The research paper looked into the field of digital forensics and discussed the challenges faced with social engineering forensics as well as discussing solutions to those challenges. The paper is significant because it educates the reader about the dangers of social engineering and provides them with solutions to reduce those dangers. The work is important due to social engineering attacks being on the rise and causing massive negative implications for stakeholders involved. There are solutions that can be said to be credible however more quantitative data needs to be done to prove their effectiveness. A case study from coinbase about an unsuccessful social engineering attack was used as the basis for the recommendations proposed. A breakdown of social engineering was given to inform the reader. A qualitative approach was used.

# 1.0 Introduction

With the emergence of digital forensics investigations,crime prevention agencies and task forces have been able to collect,store and transfer electronic data associated with cyber criminals so that sufficient evidence can be provided to link them to a cyber crime(Ieong, 2006). Because of this emergence, it has been harder for cyber criminals to hide their digital footprint. However, whilst there have been useful applications of digital forensics,there has also been an abundance of challenges that have made digital forensics a difficult procedure(Vincze, 2016).

**1.1 Motivation**

The motivation for this area of research is due to the increasing necessity to understand and distinguish the challenges associated with social engineering forensics. Social engineering is the practice of manipulating human individuals in engaging them to disclose classified information or perform unauthorised acts within an organisation(Mouton et al., 2016) . This demonstrated a threat towards cyber infrastructure. Bad actors taking advantage of human social interactions and the susceptibility of humans to breach security procedures, generates more reasoning as to why effective techniques for investigating and mitigating social engineering attacks require more attention within the broad field of digital forensics.

**1.2 Why People Should Care About Social Engineering:**

Social engineering attacks have been on the increase over the years(Venkatesha et al., 2021). These attacks can have heavily financial,reputational and security losses that can devastate organisations and individuals(Wang et al., 2020). Because of these extreme consequences,it lays the foundation for why members of society should be educated on social engineering in terms of its impact, and attack strategy. With this new profound knowledge,strategies for prevention,investigation and recovery can be developed and put into action.

**1.3 Research Question**

The aim of the paper was to highlight the challenges digital forensic analysts face when conducting social engineering forensics. The aim was to be achieved through evaluating existing solutions towards the problem and proposing new solutions to tackle the issue. Moreover, the elaborateness of social engineering attacks are explored along with the impact they impose on digital forensic investigations. The research question is what are the obstacles a forensic analyst faces when conducting social engineering forensics? And what strategies can be utilised to mitigate those challenges with desirable results?

**1.4 Methodology**

The approach chosen to tackle the research question was the qualitative approach. This approach was selected because it allows a researcher to review existing literature and case studies about the topic so that personal evaluations and inferences can be drawn to reach a new conclusion. From the analysis and evaluation of the challenges and current solutions, new insights are hoped to be reached that can aid in individuals or organisations protecting their intellectual property.

**1.5 Contributions**

The research conducted contributes to the wider topic of digital forensics as a whole because it discusses the challenges digital forensics analysts face when undergoing social engineering forensics. Moreover,solutions are proposed that forensic specialists can adhere to in order to make social engineering forensics easier to diagnose and assist in preventing social engineering attacks.

**1.6 Results**

Qualitative results are expected from the paper including social engineering forensic challenges being explored as well as a review of current solutions and new solutions being proposed. The aim is by the end of the research paper, readers will be more informed of the difficulties of social engineering forensics and have a higher awareness of the different strategies that can be utilised to combat the problems efficiently.

# 2.0 Related Work

Social engineering is the art of deceiving a person to make them reveal classified information or grant access to a computer system without proper authorisation(Hatfield, 2018). Social engineering is pivotal within the wider scope of digital forensics because it is an ongoing cyber threat that gives criminals a foothold within peoples security systems and information assets(alderwood & skinner, 2018). Because of this,digital forensics is required so that an understanding can be made about the attackers' tactics and vectors. With this new understanding,procedures can be implemented around it to prevent the same attack from happening again. There are different types of social engineering attacks a criminal can use against a target victim. There are as followed:

**2.1 Pretexting**

Pretexting is where a bad actor fabricates a persona or story towards a victim to appear as a trusted personnel so that they can get the victim to perform whatever the attacker requests(Alazri, 2015).

**2.2 Phishing**

Phishing attack is where the attacker sends a malicious email to a target pretending to be from a trusted source in order to either gain confidential information from the victim or to get the victim to download a malicious file attached to the email(Gupta et al., 2016).

**2.3 Dumpster Diving**

Dumpster diving is where a bad actor will search through the trash of organisations or individuals to find dashed items that could have confidential information which could lead to the compromise of the organisations cyber infrastructure(Krombholz et al., 2015).

**2.4 Historical Context Of Social Engineering**

Social engineering has seen a steady increase in complexity and impact towards individuals from its early days to current times. Within the early days of social engineering,attacks were normally carried out through the phone where attackers attempted to gain sensitive information from victims or get them to make financial transactions(marzuoli et al., 2016).

Social engineers would then take a more confrontational approach by impersonating trusted individuals face to face with victims(Algarni et al., 2014). With the emergence of the internet, phishing emails became part of a social engineering process with emails becoming more sophisticated and specific as time went by(Kirda & Kruegel, 2005). Now social engineering is incorporated in the majority of cyber attacks as an actor vector to increase the success rate of an attack launching(Gallegos-Segovia et al., 2017). Social engineering attacks retain a lot of psychological principles that exploit human aspects because of humans innate nature. For example humans have a natural tendency to want to assist someone who requires help. An attacker will use this to their advantage and pretend to be an employee at a company seeking access to a private sector of a building or requesting sensitive information that they should not be allowed to see(Ghafir et al., 2016). Another principle would be likeliness. Humans tend to be more willing to cooperate with someone who shares the same hobbies,beliefs and passions as themselves(Bullée et al., 2017). Attackers will use that human vulnerability to their advantage by reading up about the target and create a false personality that the target would admire.

Social engineering attacks are a prevalent cyber attack within modern society. 98% of cyber attacks reported involve some form of social engineering(PurpleSec LLC, 2021).within 2022, successful phishing attacks leading to financial losses increased by 76%(Proofpoint, 2023). It is estimated that organisations experience an average of 700 social engineering attacks year round(Greig, 2021). On average social engineering attacks cost companies £130,000 through stolen data or money(Partida, 2020). This figure can increase when you factor in recovery fees,fines and upgrading new computer infrastructure. Big worldwide organisations have been made victims of social engineering attacks, An example would be when attackers sent phishing emails to google and facebook employees to inform them to deposit money into fraudulent accounts for genuine services. From 2013-2015 the attackers cost google and facebook £100 million(Tessian, 2023). Another example of a devastating social engineering attack was in 2016 when attackers sent spear phishing emails to employees at a bangladesh bank. This granted them access to the bank's network and they were able to transfer £81 million to accounts in the Philippines(Kostic, 2023).

**2.5 Current Solutions**

Because of the prevalence and damage social engineering can cause, solutions have been developed to prevent them from being successfully launched. These solutions are both technical and non technical. In terms of non technical, the most common practice is training and awareness campaigns about social engineering, how to spot it,its impact and the procedures to follow if you encounter it(Almomani et al., 2013). This solution is important for employees and staff so that they understand the dangers of social engineering and how it can have catastrophic consequences for their organisation. In terms of technical solutions, email spam filtering is another widely adopted approach. This is where filters would be set up within peoples emails to distinguish between a legitimate email or a phishing email. If a phishing email is detected, it will be quarantined so it can not do any harm(Sanz et al., 2008). Another method is intrusion detection systems. This is a system that will monitor for any abnormal behaviours or patterns within a system that resembles signs of a social engineering attack(Liao et al., 2013) If any signs are detected it will be reported so that further analysis can be conducted. Multi factor authentication is another widely used technical solution. This is an additional layer of protection that requires a user to provide two or more authentication factors before being granted access to a system or account. These factors are either something you know,own or are(Henricks & Kettani, 2019).

**2.6 Effectiveness**

With the solutions that are currently available it is important to assess whether they are effective in deterring social engineering attacks. Education and awareness programs are shown to have a positive effect in reducing social engineering attacks in particular,self training is presented as the most effective in terms of different training categories(Heartfield et al., 2016). However, when doing an extensive search for quantitative data that shows the effectiveness of each of the solutions listed previously, there were no concrete sources found that showed a distinctive link. This suggests there is a lack of credible papers that clearly shows evidence that the solutions listed are effective when put into use. This will be a recommendation discussed in the future work section of this research paper.

**2.7 Limitations**

With the solutions presented previously, they each come with shortcomings that make preventing social engineering attacks more difficult. With email spam filtering systems there are instances where the system generates false positives or false negatives. False positives is when the system marks a legitimate email as spam or malicious. False negatives is when malicious or spam emails are marked as legitimate and are passed through(kumar trivedi & dey, 2016). Malicious emails being passed through can cause catastrophic damage so it's important that email spam filters are regularly tested so that false negative rates are as low as possible. The limitation of 2fa is it can still be bypassed by the attacker simply by targeting the user for the passwords or codes. The attacker can use another form of social engineering to retrieve it. Furthermore,when a 2fa code is requested, the service provider has no way to tell whether a legitimate user requested the code or the attacker.This coincides with the other limitation of a passive warning message. This is because if the service provider knew an attacker requested this code, they would be alerted to provide a specific warming message to the victim instead of a generic one that would make the victim aware that they are being manipulated(Siadati et al., 2017). Intrusion detection systems also suffer from false-negatives/false-positives. A lot of noise that is generated from harmless activity can disguise real attempts of social engineering. Coincidentally, normal system procedures for testing protocols could be perceived as active social engineering attempts and increase the rate of false-positives. Human factors can halt the effectiveness of training and awareness programs when it comes to tackling social engineering. One such example would be humans unwillingness to accept change or their overconfidence. One study saw how employees administered non compliant behaviours during training and showed overconfidence in identifying social engineering attacks(Aldawood & Skinner, 2019). This is a limitation as employees could overlook an early sign of an attack which would lead to extensive damage.

This section falls directly into the research question of what are the obstacles a forensic analyst faces when conducting social engineering forensics? As numerous challenges have been identified. As a summary the challenges identified were:

* Detection Difficulty

As demonstrated, social engineering mainly revolves around humans and psychological manipulation leaving hardly any digital footprint that can be analysed.

* Lack Of Quantitative Data

Because of the lack of quantitative data showing evidence that current solutions are effective, it makes it difficult for social engineering forensic analysts to assess whether the current solutions are advantageous in mitigating social engineering attacks.

* Human Factors

As discussed humans have many factors such as resistance to change their behaviour or overconfidence when it comes to social engineering training. Because of these human factors, it makes social engineering training programs less effective in educating humans about the threat of social engineering which in turn would make them less able to report social engineering attempts properly.

**2.8 Research Methodology**

For this research paper, the qualitative approach was chosen. More specifically, a case study was utilised. A qualitative approach was chosen because it allows for an in-depth understanding of a topic that has complex factors within it(Tetnowski & Damico, 2001). This is especially advantageous in the field of social engineering because there are a lot of variables that come into play when diagnosing an attack. A list of recommendations will be presented that are deemed to be universal recommendations that any organisation can implement with the result of it reducing social engineering attacks. A real life case study of a social engineering attack will be used as a template to demonstrate why the recommendations suggested are relevant. This approach has the advantage of being practically applicable because the context of the recommendations are based on a real world case study, demonstrating its value and applicability of the recommendations.

A demonstration of the effectiveness of the recommendations is possible as it can be showcased how they tackle forensic social engineering challenges.

# 3.0 Proposed Solution

The purpose of the proposed solution is to present relevant recommendations that have been drawn from the context of the case study and challenges mentioned in earlier sections. The case study being used is an unsuccessful social engineering attack that targeted the company coinbase. The attacker was unable to gain any direct system access or funds from the company despite efforts of social engineering. This is all due to Coinbase's robust security controls and procedures. These recommendations have been made with the aim to answer the research question of what strategies can be utilised to mitigate those challenges with desirable results? The case study used was from [Social Engineering - A Coinbase Case Study](https://www.coinbase.com/blog/social-engineering-a-coinbase-case-study)

**3.1 Recommendations**

* **Implement 2 Factor Authentication**

From the case study, the attacker was unable to gain access to the coinbase account because they did not have the correct multi factor authentication credentials. This prevented them from being able to access the system as deep as they were planning to. By implementing 2fa it will make it more challenging for the attacker to gain access to the system. This recommendation is an existing solution pointed out in the previous section.

* **Regularly Update Employee Training And Awareness**

The social engineering attack commenced in the first place because one employee responded to the sms text by clicking the link. Majority of employees however had ignored the urgent sms text. This demonstrated how it only takes one vulnerable person for an attack to launch on a system. If the employee was made knowledgeable about different social engineering tactics such as text messages urging for a quick response,then it is less likely they would have clicked on the link. This is why increased employee training and awareness is recommended so that employees can spot different methods used by attackers to prevent them from being exploited. Employee training and awareness is an existing solution used by companies which was pointed out in the previous section.

* **Implement An Incident Response Team And Plan**

One of the reasons why the attack was unsuccessful is because Coinbase had an incident response team that responded swiftly from when the attack was first suspected. The employee was inquired about the unusual activity and subsequently ended all communication with the attacker preventing any further malicious attempts. Through incorporating an incident response plan,it will outline the necessary steps an employee should follow if they suspect an attack. It is imperative all employees are aware of the plan and understand the steps that are presented.

* **Conduct Regular Monitoring Of Accounts**

Monitoring accounts regularly will assist in early detection of an attack as any abnormal behaviour or unusual account access to files or sensitive information can be flagged and inquired about by the response team. From the case study, the incident response team was alerted of the unusual activity on the employee's account and followed up with the appropriate procedures. The concept of intrusion detection is an existing solution pointed out in the previous chapter.

* **Set Up A Platform Where Employees Can Report Suspicious Activity**

Having a channel where employees can report cyber attacks or malicious activity can help reduce the time in which a response is made to the attack identified,subsequently reducing the likelihood of an attacker doing damage to the system. Within the case study, the incident response team responded within 10 minutes of the attack being flagged. Because of this quick response the attacker was unable to do any major damage highlighting how a quick response is crucial.

* **Encourage Sharing Details About Attacks Such As Attack Vectors And Mitigation Techniques**

By informing others about your own experiences of attacks whether successful or not and detailing how you dealt with them, other organisations can implement the techniques and strengthen the areas that were vulnerable to prevent an attack happening in their own system.

.

* **Conduct Regular Adaptations Of Security Policies**

Social engineering tactics change constantly and attackers develop new methods. To ensure an organisation is up to date with recent strategies,policies should be regularly assessed and modified so that they account for any new tactics discovered.

* **Conduct Vulnerability Assessment**

Regular risk assessments should be carried out to identify levels of risk different components within an organisation carry. Any weak points identified whether it be security protocols,employees or hardware should then be addressed appropriately to ensure the risks are reduced as much as possible. In context with the case study,employees should undertake a social engineering test to identify who would be more susceptible to fall for an attack so that relevant training can be provided.

Even with all these recommendations, it is important to point out that no system or organisation no matter how many layers of security they implement will be 100% secure. Hence why it is necessary to undertake regular review of policies,systems and procedures and adapt them to evolving threats. Refining strategies for social engineering attacks should be an ongoing process so that an organisation is less vulnerable to the attacks.

# 4.0 Evaluation

The initial aim of the recommendations was to provide strategies to help reduce the difficulties of social engineering forensics and attacks.

* **Implement 2 Factor Authentication**

In regards to implementing 2fa,no studies could be found that show quantitative data highlighting that 2fa is effective in mitigating social engineering attacks. However, within the coinbase case study, the 2fa that was enabled prevented the attacker from gaining access. From this it can be argued that 2fa is effective however this is only one example of its effectiveness being proven. To gain a better understanding, more studies that test its effectiveness will need to be produced.

* **Regularly Update Employee Training And Awareness**

Training and awareness was mentioned as a recommendation within the coinbase study. Whilst it can be inferred that more training could reduce social engineering attacks, more research would need to be conducted that measures the effectiveness of training against the attacks. One article discusses how training should be tailored to specific issues identified(Alruwaili, 2019). With the coinbase example, the employee fell for the sms message. An appropriate training exercise to handle this flaw would be to educate the employee on different social engineering vectors such as phishing emails and messages and then have them do a test where they identify legitimate emails or messages from social engineering ones.

* **Implement An Incident Response Team And Plan**

The incident response team and plan can be argued to be effective. This is because, due to their swift actions of reacting to the social engineering attack within 10 minutes,they were able to prevent the attack from proceeding further and avoided any damages being done.

* **Conduct Regular Monitoring Of Accounts**

Regular monitoring for intrusion detection systems has been demonstrated to be effective from the coinbase study. The unusual activity of the employees account has been flagged and alerted to the response team who responded with the appropriate actions. This demonstrated how the monitoring of accounts played a crucial role in identifying the attack. However the continuous monitoring of different accounts could have a strain on the systems resources depending on how many accounts there are. This factor would have to be brought into consideration when deciding to implement or not

* **Set Up A Platform Where Employees Can Report Suspicious Activity**

Reporting suspicious activity as soon as it is discovered can help reduce the time it takes for action to be taken against the activity. If this is done as soon as possible then potential damage can be minimised. With the reporting system, it is important that employees are aware of its purpose and the benefit of it and understand how to access it. If the employee is confident and transparent about it, then the system would have limited effect in reducing social engineering attacks.

* **Encourage Sharing Details About Attacks Such As Attack Vectors And Mitigation Techniques**

Sharing information about attacks can help other organisations who may or have experienced similar attacks to their own infrastructure. With the information,companies can prepare their defences accordingly, to significantly reduce the damage or prevent the attack from being successful at all. This can be an effective mitigation technique. However, the idea of revealing information about an attack has mixed reactions between companies. Coming forth about an attack can lead to heavy fines,loss of customer trust and reputational damage(Huang et al., 2023). Because of this, some companies are reluctant to announce that they have been attacked.

* **Conduct Regular Adaptations Of Security Policies**

Some policies within organisations will be tailored to reduce certain types of cyber attacks. For example generating a strong password for an account that meets a criteria specified by the organisation would be a policy to help reduce the risk of a brute force attack. Updating policies based on newfound social engineering tactics can help reduce the success of that attack. However these policies would only be effective if the employees are complying with it. This would require someone to check whether employees are complying with the policies. However there is not a study that shows a positive correlation between the policies a company has and the unsuccessful cyber attacks they have experienced. This research of quantitative data would be beneficial to show that updating policies is an effective mitigation technique.

* **Conduct Vulnerability Assessment**

Vulnerability assessments assist in identifying weaknesses within an organisation. Through identifying the major risks,appropriate action can be taken to resolve the risks. If a social engineering test was done on the employee who fell for the sms message, the company would have identified that they are especially susceptible to social engineering and could have provided the correct training to reduce that susceptibility thereby reducing the chance of a social engineering attack.

As a whole, the recommendations listed can be suggested to be effective against social engineering attacks. However without the appropriate statistical data, the effectiveness for the solutions is still debatable. Furthermore the recommendations were only based on one study. This has issues of generalisation because each company operates differently to another and has different policies and procedures. More case studies should have been used to gain different perspectives of the social engineering attacks that occur so that the recommendations suggested would be more tailored to the practices of any company.

**4.2 Future Considerations**

For future work related to social engineering, the biggest suggestions would be to test any existing or newly discovered solutions and generate quantitative data from the research. From conducting this research it has been made apparent how there is limited quantitative statistics that can strongly argue that the existing solutions are effective in mitigating social engineering attacks. Without this data, organisations would be unintelligible as to whether their current solutions are effective or if they should adopt new solutions which have been proven to reduce social engineering attacks.

# 5.0 Conclusion

This research has been done to answer the research questions of what are the obstacles a forensic analyst faces when conducting social engineering forensics? What strategies can be utilised to mitigate those challenges with desirable results? By trying to answer these questions, the paper has attempted to contribute insights into the field of social engineering and digital forensics. The increase of social engineering attacks along with the damages they can inflict highlights why the research into the challenges faced by forensics should be sought after so that they can be reduced as much as possible. The research gave a background into social engineering, identified challenges and proposed solutions based on a real world case study. Whilst the recommendation can be valid solutions, the lack of quantitative data showing their effectiveness creates issues as to whether they should be implemented or not. Creating recommendations from a wider range of case studies would have made the proposed recommendations more generalisable to the public instead of using a single case. For further research in this space, it is recommended that any solutions developed should be tested thoroughly to ensure they are applicable in reducing social engineering attacks. To add on, by having the quantitative data to back up the solutions, it will create a more justified solution to fortying people's defences against social engineering attacks.In conclusion, this research paper provides more insight into the challenges of social engineering forensics and offers techniques to mitigate those challenges.

# 

# 

# 

# 

# 6.0 References

# 

Alazri, A. S. (2015). The awareness of social engineering in the information revolution: Techniques and challenges. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. https://doi.org/10.1109/icitst.2015.7412088

Aldawood, H., & Skinner, G. (2019, May 1). *Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering*. IEEE Xplore. https://doi.org/10.1109/CCC.2019.00004

aldewood, hussain, & skinner, geoffrey. (2018, December 4). *Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review*. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/abstract/document/8615162?casa\_token=DnjeNN07rIgAAAAA:-ajsC6H\_GO4OaHAAWvqjeH78JOIGOfhyG1WmVmQ-IeSevp1QINrityiheOgEhJwurMYY3AGge10a

Algarni, A., Xu, Y., & Chan, T. (2014, June 27). *Social Engineering in Social Networking Sites: The Art of Impersonation*. IEEE Xplore. https://doi.org/10.1109/SCC.2014.108

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A Survey of Phishing Email Filtering Techniques. *IEEE Communications Surveys & Tutorials*, *15*(4), 2070–2090. https://doi.org/10.1109/surv.2013.030713.00020

Alruwaili, A. (2019). A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS. *International Journal of Advanced Research in Computer Science*, *10*(5), 1–3. https://doi.org/10.26483/ijarcs.v10i5.6476

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2017). On the anatomy of social engineering attacks-A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, *15*(1), 20–45. https://doi.org/10.1002/jip.1482

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017, October 1). *Social engineering as an attack vector for ransomware*. IEEE Xplore. https://doi.org/10.1109/CHILECON.2017.8229528

Garuba, M., Liu, C., & Fraites, D. (2008, April 1). *Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems*. IEEE Xplore. https://doi.org/10.1109/ITNG.2008.231

Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016, August 1). *Social Engineering Attack Strategies and Defence Approaches*. IEEE Xplore. https://doi.org/10.1109/FiCloud.2016.28

Greig, J. (2021, July 28). *Average organization targeted by over 700 social engineering attacks each year: report*. ZDNet. https://www.zdnet.com/article/average-organization-targeted-by-over-700-social-engineering-attacks-each-year-report/

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*. https://doi.org/10.1109/ccaa.2016.7813778

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

Heartfield, R., Loukas, G., & Gan, D. (2016). You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks. *IEEE Access*, *4*, 6910–6928. https://doi.org/10.1109/access.2016.2616285

Henricks, A., & Kettani, H. (2019). On Data Protection Using Multi-Factor Authentication. *Proceedings of the 2019 International Conference on Information System and System Management*. https://doi.org/10.1145/3394788.3394789

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023, May 4). *The Devastating Business Impacts of a Cyber Breach*. Harvard Business Review. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3*, 29–36. https://doi.org/10.1016/j.diin.2006.06.004

Kirda, E., & Kruegel, C. (2005). Protecting Users Against Phishing Attacks with AntiPhish. *29th Annual International Computer Software and Applications Conference (COMPSAC’05)*, *1*. https://doi.org/10.1109/compsac.2005.126

Kostic, N. (2023, July 26). *The 15 Most Famous Social Engineering Attacks*. PhoenixNAP Blog. https://phoenixnap.com/blog/social-engineering-examples

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

kumar trivedi, shrawan, & dey, shubhamoy. (2016, March 23). *A Combining Classifiers Approach for Detecting Email Spams*. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/abstract/document/7471226?casa\_token=qevtwq05uEIAAAAA:pcZIpsFiHO4smeIP\_VLMkcUKcGYUR2\_Ha4iLcan1j\_CIDnCvbSkRxskm9daQO9oo0B1OUvr3VDHmrw

Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

marzuoli, aude, kingravi, hassan, dewey, david, & pienta, robert. (2016, December 18). *Uncovering the Landscape of Fraud and Spam in the Telephony Channel*. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/abstract/document/7838257

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Partida, D. (2020, December 21). *StackPath*. Www.securityinfowatch.com. https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses

Proofpoint. (2023, October 22). *2020 State of the Phish - Cyber Security Insights Report | Proofpoint US*. Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

PurpleSec LLC. (2021). *2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends*. PurpleSec. https://purplesec.us/resources/cyber-security-statistics/

Sanz, E. P., Gómez Hidalgo, J. M., & Cortizo Pérez, J. C. (2008, January 1). *Chapter 3 Email Spam Filtering*. ScienceDirect; Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S0065245808006037

Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security*, *65*, 14–28. https://doi.org/10.1016/j.cose.2016.09.009

Tessian. (2023, February 7). *11 Social Engineering Examples - Real Attacks - Updated 2021*. Tessian. https://www.tessian.com/blog/examples-of-social-engineering-attacks/

Tetnowski, J. A., & Damico, J. S. (2001). A demonstration of the advantages of qualitative methodologies in stuttering research. *Journal of Fluency Disorders*, *26*(1), 17–42. https://doi.org/10.1016/s0094-730x(01)00094-8

Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. *SN Computer Science*, *2*(2). https://doi.org/10.1007/s42979-020-00443-1

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183–194. https://doi.org/10.1080/15614263.2015.1128163

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094–85115. https://doi.org/10.1109/access.2020.2992807