FOSTERING SOCIAL ENGINEERING AWARENESS: PROACTIVE MODEL

HAHV Halwatura[1], WGCI Priyadarshana[2], and T Samarasinghe[3]
[1]Junior Information Security Analyst, DPIT,Battaramulla, Sri Lanka
[2]Network Engineer Trainee, People Bank Innovation center, Colombo 01, Sri Lanka
[3]Associate Engineer, Lanka Bell, Sri Lanka
[1]*halwatura.vihanga@gmail.com*

Abstract- Social Engineering aims to trick users into revealing sensitive information by making use of their lack of literacy in Social engineering tricks and the limited or no technical mechanisms on their systems to protect against such attacks. The motive of this research is to check the awareness and perceptions on social media of employees from the Information technology sector as well as the other sectors in an equal proportion. This paper shows a series of results which shows the weak points of defending against Social engineering attacks as an individual and in an organizational point of view. The methodology used to conduct this research was an online survey which was sent through email and social media and was successfully completed by 118 people and rejected by approximately 50 people. The awareness or the need of training to identify Social engineering tricks can be clearly seen by the analysed results. As a solution to this escalating issue, this paper suggests a model which is named as 'Proactive model A' that can be used by individuals as well as organizations to mitigate the risks of Social Engineering attacks by implementing the model in their policies and training programs so that it can help in minimizing the damage to critical assets of the organizations.

Keywords- Social Engineering, proactive defence, Cybersecurity

I. INTRODUCTION

People are the weakest link in technology, they might not be a device or a machine but they are the users and although the technology is evolving faster than we think today there is a human involvement in all its processes. (Streeter, n.d.) This is the main reason why Social engineering is an involving threat to all organizations regardless of how small or big the organization is. Social engineering is a huge threat in the modern world but do you think that it is a modern way of attacking in the Cyberspace? If we think up closely it is similar to the situation where the Greeks gifted a horse to the Trojans as a peace symbol but the wooden horse had warriors hidden to destroy their city. ("Social Engineering," 2018). The social engineering scams today has the similar story but using different techniques. According to an organization the Logical Front, 62% of the business have faced phishing and Social engineering attacks and according to their statistics it was the second in the list of attacks. ("6 Security Threats to Look Out for in 2018," 2017). No matter how hard the professionals in Cybersecurity come up with security mechanisms, if the users are vulnerable it can damage the critical assets of an organization or your personal data. Even if the computer systems or the network is patched, updated and secured in all ways, targeting the people in the relevant area can breach all the security mechanisms of the organizations. (Mouton et al., 2015)

Social engineering attacks are not only about the weaknesses of humans that has led to its increase but also the factors such has it needs low technology involvement, low cost and its simplicity in carrying out attacks. The main types of social engineering techniques that most that most people are aware about is email phishing which involves in sending emails which looks authentic but aims to steal users' sensitive information or digital secrets. (Suganya, 2016) In today's world, that's not all as there are other ways to carry out the same task such as by voice calls, social media as your friends, pretexting and many more. (Banu and Banu, 2013)Another thing to highlight is that Social engineering is not restricted to external attacks, it can also happen as an internal attack. In fact, an article in Digital Guardian says that 63% of these attacks come from internal sources ether from errors, control or frauds. ("Social Engineering Attacks," 2015).

This paper focus on proving the weakness and the lack of awareness and knowledge some people have on Social engineering, all data are collected through a survey and analysed. The final recommendations are depicted through the Proactive model A.

II. RELATED WORK AND FINDINGS

To conduct a social engineering attack, one need not have thorough technical knowledge, it is a process of handling with the human psychology which contains many emotions from shyness to curiosity. Knowing how to deal with these emotions might allow the attacker to get information valuable to them by the users. Sometimes getting this information itself might not be the attack but just an insight to how the major attack must be done. (Cert UK, 2015) Recent social engineering attacks include spear phishing which is involved in directly targeting a specific user whereas the other methods known as the water holing is used to attach a malware to a website where the employees of an organization is expected to get infected. (Krombholz et al., 2015) Four of the common tactics used by the Social engineers to steal information is to attract the users by being confident in what they do, next they try to build your trust by offering something, and then they might make some humor and finally they will request what they want along with a legitimate reason. (Luco, 2013) Despite all these facts, the ways to reduce social engineering impact to our data are limited. In a study it says that although the employees have taken trainings, they still share passwords so humans are very vulnerable. (Cazier and Botelho, 2007) The attack mechanisms are very advanced today, although .exe files cannot be sent through mails due to security reasons, they can still be sent by a zipped folder which can result in a successful attack. (n.d.)

The best way to keep away from social engineering tricks is to be aware and conduct trainings for the employees in the company and make sure that the trained matters are all executed in the practical real world scenarios. (Smith et al., 2009).

III. METHODOLOGY

To check the level of literacy among the people from different fields, this research was initiated. The data collection method used to conduct this survey was a Google survey which was distributed to people from different categories. The survey included quantitative and qualitative questions. The distribution of the survey was done via Email and Social engineering sites such as Facebook, Viber and WhatsApp. The survey was made as simply as possible for the respondents to give answers quickly and easily. The first few questions were related to biography and following were the technical questions. A total of 20 questions were there on the survey. This survey was conducted for five months from December 2017 to May 2018 and it has responses from a 118 people and approximately 50 responses have been rejected due to the fact that the respondents weren't aware about the topic. The questions were made to capture the social engineering behaviour in their personal information and also in their corporate environment.

IV. RESULTS AND DISCUSSION

Figure 1. Field of work/study

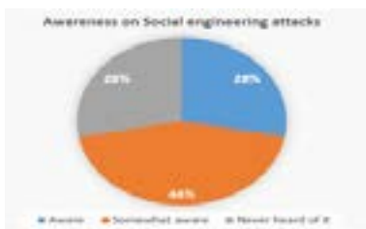

Figure 3. Awareness on Social engineering attacks

All analysed results are presented in this section with a description and a figure containing the statistics.

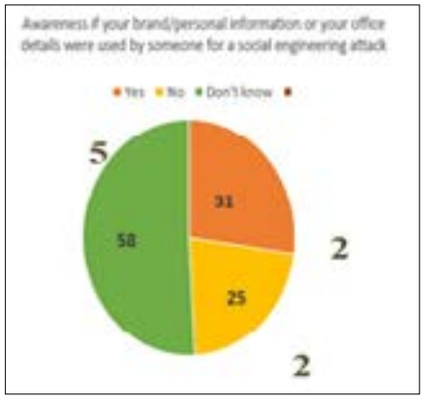

Figure 6. Awareness if your information is used for social

A majority of the respondents were from the age category 18-36 years of age which was 96% from the total statistics where as 2% was from 37 to 48 category and another 2% was from the 49 to 67 category. Their field of career was divided as 6% was from the Cybersecurity field, a majority was from the IT field with a percentage of 49 and the second highest was the Other field or the fields that relates to non IT category which consisted of 45% as depicted in the Figure 1. Majority of the respondents of these fields are represented by undergraduates with a percentage of 44. And in second are the front line professionals and the executives.

Figure 2 shows the percentages of respondents who knows how to identify an email scam and who doesn't. 61% has answered that they know how to identify scams whereas 39% does not know how to.

Figure 2. Positivity on identifying an email scam
Source: Author

According to the respondents the overall awareness of Social Engineering attacks are depicted in Figure 3. 28% are aware about social media attacks, 44% are somewhat aware whereas another 28% has never even heard of it.

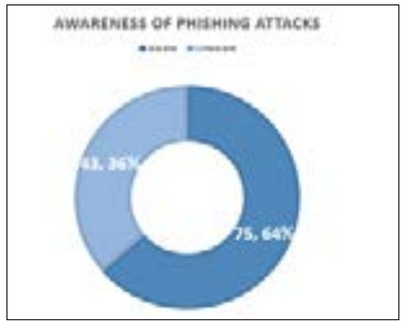

Figure 4. Awareness of phishing

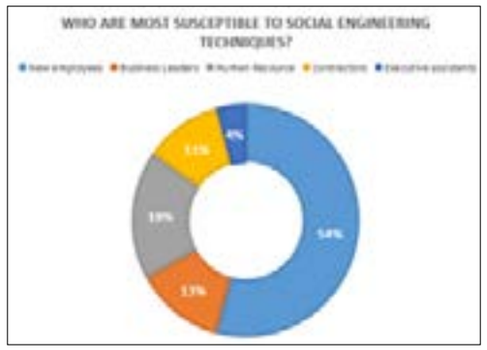

Figure 8. who are most susceptible to social engineering?

The awareness of the most famous social engineering technique phishing attacks can be analysed as the following figure 4. There were 36% who were unaware and only 64% of the respondents were aware about this popular attack.

Figure 5 shows the results for the questions whether the organization they are working for has ever been targeted by a social Engineering attack and a majority answered that they do not know with a percentage of 65%, and 16% answered yes with confidence whereas only 19% answered No.

Another set of answers in Figure 6 showed that only 27% will know if their details are used in a Social engineering attack and 23% said they will not know if their information is used by someone whereas a majority of the people with a percentage of 50% says that they will have no idea if their information is taken for social engineering by a hacker.

Since social engineering is not only about the cyber world so a question regarding social engineering was given on whether they have a method to validate their bank when they get a call from them and as shown in Table 1 a majority replied No with a percentage of 55.9% and No with a percentage of 44.1%.

Table 1. validating your bank/utility supplier

Do you have a method to avalidate your Bank or Utility supplier when they call?	
Yes	48.3%
No	51.7%

A question on how trustful are the employees in their organization in a social engineering attack showed that a majority of the respondents with a 61% think that the some employees might disclose sensitive information where as 16% some employees might definitely disclose information and only 23% thinks that the employees will not give put information as shown in Figure 7.

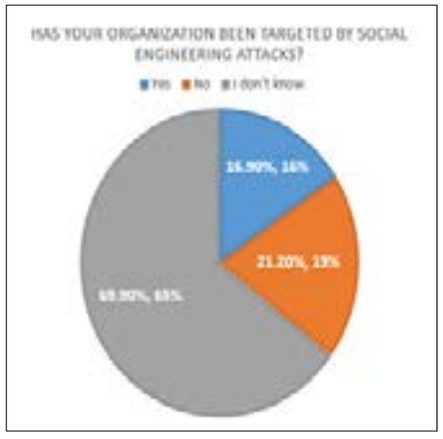

Figure 5. Organizational impact on social engineering

According to the respondents, figure 8 shows the most susceptible people in an organization to Social engineering are the new employees with a percentage of 54% of the respondents, next are the human resource personnel agreed by 18% of the personnel, third highest are the business leaders with a 13% of the responses.

As shown in Table 2. According to the respondents in a case of cyber security incidents, a majority of the people with a percentage of 55.9% doesn't know whom to contact for help, only 44.1% knows the relevant authorities.

Table 2. who do they ask for help?

What is your opinion on the most common source of social engineering threats?	
Email	26.2%
Social Networking Sites	55.1%
Insecure mobile devices	10.2%
Other	8.5%

Source: Author

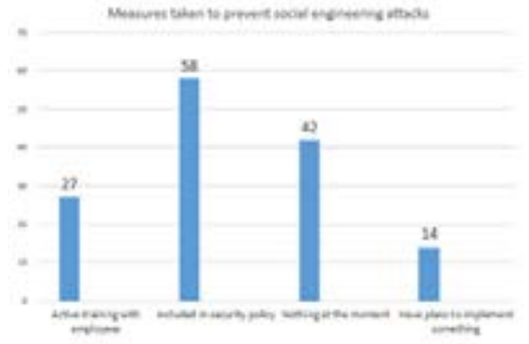

Figure 9. Measures taken to prevent social engineering attacks
Source: Author

Cybersecurity does not depend on the organization since at some point they get involved with the cyberspace whether it's online or offline, the employees must know how to defend themselves against any attack. Therefore, a question on the mechanism they have gone through as an employee to be protected in cyberattacks as such was asked as shown in Figure 9 and 84% respondents replied positively saying they have some security mechanisms whereas the rest of the 56% replied saying either they have plans to implement them or nothing at the moments which is not very positive in this new era of technology.

The survey consisted of a few open ended questions and one was the definition of social engineering in their own terms. Since this was a questions which cannot be answered by all, it was left as a not required questions so only 41 people answered and apart from 3 responses all others were correct but this does not even count 50% of

the responses therefore it shows a weakness in literacy of this term. Following this question was to list three common social engineering attacks and 40 respondents answered to this with the common attack being phishing but 9 responses had to be disregarded due to the fact that they did not have an idea about the question. Having open ended questions in the survey helped to get a better overview on the understanding of the area and scope of knowledge they have.

Table 3. who do they ask for help?

What is your opinion on the most common source of social engineering threats?	
Email	26.2%
Social Networking Sites	55.1%
Insecure mobile devices	10.2%
Other	8.5%

Source: Author

As stated by the respondents in Table 3 the most common source of social engineering attacks are social media websites and emails, insecure mobile devices come third along with other options as the fourth. This might be right because the use of social media is high nowadays but when it comes to a work environment, where social media is not a main source of communication, the main source can be emails and other options such as internal attacks and many more therefore they cannot taken as granted.

The respondents were asked about the way how they can identify a phishing link or email as shown in Figure 10.

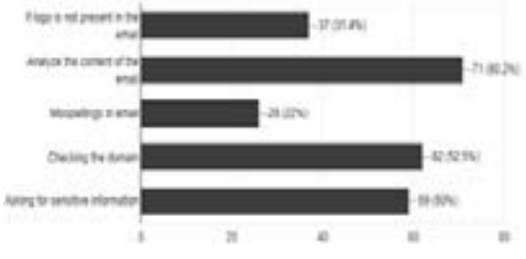

Figure 10. Identifying a phishing email/link
Source: Author

The answers included; If the logo is not present in the email which has percentage of 31.4% and the majority with 60.2% answered Analysing the content of the mail, 22% answered Misspellings in the email, 52.5% answered Checking the domain and 50% answered asking for sensitive information. The answers were different and the percentage of the results varied but this question was a trick to check the literacy rate of how they will react to such kind of email but in reality all the options given in this question but be considered when determining the authenticity of the message or link. The results were taken by both information technology personnel as well as professionals from other fields therefore the results are more reliable.

This study shows an effective message regarding Social engineering and the literacy rate along with their perception of Social engineering and by analysing these results we can come to an obvious fact that the awareness on Social engineering is very low. Approximately 50 responses were rejected and the reason for that was that the technical word Social engineering was not a familiar word and when they opened the link, they couldn't understand the questions because they are less literate about security in technology.

The best way to mitigate the risks in Social engineering is to train or conduct awareness programs to educate the employees and the general public about these tricks that scan happen so that they will be more careful in the future. Majority of the respondents have not been hacked and at the same time majority of the people are unware or somewhat aware about the malware, only 28% are fully aware about it. Therefore, it only means that there's more space for them to get hacked quickly. When it comes to an organizational point of view, 35.6% of the respondents say that no mechanism is used to control it at the moment and 12% said they have plans and the rest have security mechanisms such as policies in place to prevent such attacks along with active training. The new employees in a company is more likely to get targeted in social engineering attacks as shown in the results positively by the respondents, this is because they might not be familiar with the work environment and the appropriate training is not given yet but that doesn't mean the rest of the staff is protected, if they don't adhere to the guidelines of policies and the training programmes they can be equally vulnerable as the new employees. Just by conducting this kind of survey in an organization might even give them a feedback about the state of knowledge of the employees regarding the social engineering attack. Another practical method would be to conduct a drill without the employees knowing so that the weak points can be caught easily and a training to cover the mistakes they did can be conducted separately.

V. DESIGN

An effective solution to address the issues of social engineering is needed to address this problem. Figure 11 shows a model as the proactive solution to the issue and this model can be used by organizations as well as individuals to protect themselves against these attacks. This model as depicted can also be applied to the information security policies in organizations to mitigate the risks of the attack. In the proposed model, the organization or the individuals must research on the new and existing social engineering attacks. With the research findings a good information security policy can be developed to give a clear set of guidelines to the personnel on how to disclose sensitive information with clarity on the source which needs the information. Another sub task is to implement good security measures which can be used to protect the information such as installing anti-virus guards to get protected from attachments which was downloaded by phishing emails, security measures can be divided as preventive, detective, corrective, deterrent, recovery and compensating measures. Last but most importantly training must be given to the individuals to identify and respond to such attacks and these trainings are divided into three options, first option is risk which gives an idea about the risk associated with the threat to the personnel. Next, to give them knowledge on how social engineering attacks occur and how they should react to such instances before disclosing the information. Finally, in organizations the training employees must be tested without them knowing, this is called real time testing so that the weak areas of the employees can be identified and the risks can be mitigated. If these measures in preventing social engineering attacks get failed, the failed outcome must be reviewed and the attack must then be researched as shown in the figure 11. This process will be act as a cycle every time a failed defence occurs or a new social engineering threat is surfaced.

VI. CONCLUSION

Social engineering is on the rise, not because it contains less security measures but because the users are not aware about the social engineering tactics that are used by the attackers to gain access to the sensitive information. Social engineering attacks can be divided as Human based attacks and Computer based attacks.("A Proactive Defence to Social Engineering," 2001) Human errors have caused losses in many industries.(Pollock, 2017) Social engineering

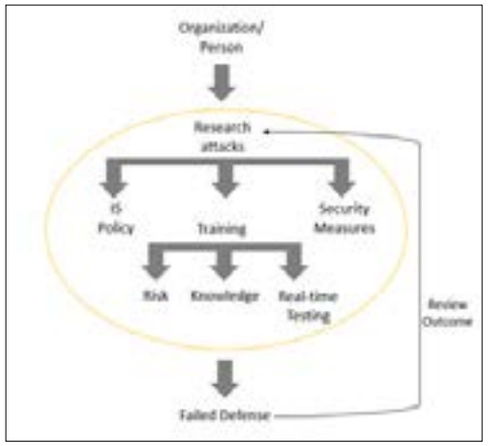

Figure 7. Can the employees be trusted?
Source: Author

attacks such as Phishing attacks which are done by creating different websites are increasing and these sites are from different domains and the average lifetime of those sites are very low.(Cui et al., 2017) If the prevention mechanisms are not enforced to address the social engineering attacks unexpected losses can be surfaced due to the disclosure of sensitive information such as financial loss, loss of public trust and reputation damage. If this situation is critical they might even have to go through legal procedures. To capture the level of awareness of the users from their perspective as well as their organizations, an online survey was distributed and this helped in finding the weak areas of people when dealing with social engineering attacks. The results of the attack give an overall view of the situation and a corresponding solution is proposed to prevent the attack but this does not cover any aspect in detecting the social engineering attacks or responding to the attacks. To mitigate this risk, this research paper has addressed the organizations and individuals with an attack prevention model named as the 'Proactive model A' as a solution which can even be included in the information security policies of the organizations. The aim of this research is to provide a solution to mitigate the risk of the social engineering threats for individuals and organizations. Further advancements include the expansion of the model to Proactive model along with the advancement of threats and risks associated with the issue.

REFERENCES

6 Security Threats to Look Out for in 2018, 2017. . Log. Front LLC.

A Proactive Defence to Social Engineering, 2001. 7.

Banu, D.M.N., Banu, S.M., 2013. A Comprehensive Study of Phishing Attacks 4, 4.

Cazier, J.A., Botelho, C.M., 2007. Social Engineering's Threat to Public Privacy, in: The 6th Security Conference, Las Vegas, Nevada: The Information Institute.

Cert UK, 2015. An introduction to social engineering.

Cui, Q., Jourdan, G.-V., Bochmann, G.V., Couturier, R., Onut, I.-V., 2017. Tracking Phishing Attacks Over Time. ACM Press, pp. 667–676. https://doi.org/10.1145/3038912.3052654

Krombholz, K., Hobel, H., Huber, M., Weippl, E., 2015. Advanced social engineering attacks. J. Inf. Secur. Appl. 22, 113–122.

Luco, D., 2013. The Art of Social Engineering.pdf. ASA Institute for Risk & Innovation.

metasploit, n.d. Best Practices for Social Engineering Attacks.

Mouton, F., Leenen, L., Venter, H.S., 2015. Social Engineering Attack Detection Model: SEADMv2. IEEE, pp. 216–223. https://doi.org/10.1109/CW.2015.52

Pollock, T., 2017. Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). 15.

Smith, A., Papadaki, M., Furnell, S.M., 2009. Improving awareness of social engineering attacks, in: IFIP World Conference on Information Security Education. Springer, pp. 249–256.

Social Engineering: A Scheme as Old as Time, 2018. . Secur. Intell.

Social Engineering Attacks: Common Techniques & How to Prevent an Attack [WWW Document], 2015. . Digit. Guard. URL https : // digitalguardian. com / blog / social - engineering - attacks - common - techniques - how -prevent-attack (accessed 5.7.18).

Streeter, D.C., n.d. The Effect of Human Error on Modern Security Breaches 6.

Suganya, V., 2016. A Review on Phishing Attacks and Various Anti Phishing Techniques. Int. J. Comput. Appl. 139, 20–23. https://doi.org/10.5120/ijca2016909084

PERSONALIZED TRAVEL SPOT RECOMMENDATION AND GUIDANCE SYSTEM FOR SRI LANKAN TOURISTS

C Shiranthika[1], N Premakumara, JP Weerawarnakula, H Lakmal, S Fernando, and S Sumathipala

Faculty of Information Technology, University of Moratuwa, Sri Lanka

[1] *chamanijks2@gmail.com*

Abstract- Tourism in Sri Lanka is an evolving field which is significantly influencing the development of the country. With the rapid advancement of Affective computing and its' diverse paths where applications are being implemented by facilitating user needs and emotions, tourism has become one of the prominent fields to provide a comprehensive analysis of useful inclination in specific travel spots based on the user interests and emotions. Traditional tourism methodologies where a travel guide guides on a tourists' journey has nowadays become an old fashion where the tourist himself has innovative applications which provide a guide in almost all the areas in his journey beginning to end. This study proposes a solution where tourist gets a personalized recommendation on travel spots to visit, a summary of the recommended travel spots with a native language translation facility and a translating system to translate landmarks displayed on travel spots such as notice boards and signboards into their native language. Our system divided into four components focusing on (a) profiling users, (b) identifying user locations and travel spots, (c) extracting user reviews about travel spots, summarize and analyse sentiments levels and (d) identifying landmarks displayed in travel spots and translate them into traveller's native language. This approach makes ease traveller's life providing personalized recommendations based on collaborative and content filtering approaches.

Keywords- Personalized recommendations, Travel spot, Sentiment analysis

I. INTRODUCTION

Tourism can be considered as an evolving field in Sri Lanka which significantly influences on the development of the country. It is the practice of touring, attracting, accommodating and entertaining tourists. With the advancement of Information Technology and mobile computing, several innovative ideas have been implemented to facilitate a better experience in the tourist's journey. While the world is rushing under technological enhancements and English becoming the universal language, development of applications in multiple languages will help tourists to achieve more personalized service. In the tourism industry, it is much necessary to provide personalized services to the tourists. When visiting several locations tourists may be much amused if they get the places they most prefer to visit and watch. When tourists have lots of options to choose from which might make them confused in selecting the best possible and or most suitable place to visit, it is essential to filter the information and personalize the choices for the use of each specific user. As a tourist most of the times, it is really confusing to decide where to go and to select among a large number of possible destinations which may also be unknown and unfamiliar. Hence, information retrieval and decision support systems are widely recognized as a valuable context in the tourism domain (B.Rieder, 2013).

Most of the times tourists do not get the full knowledge from the tourist guides and information displayed on the locations. Moreover, in case of unavailability of a tourist guide, they will find difficulties in understanding essential notices displayed on boards such as "හිස් වැසුම් පාවහන් ගලවා ඇතුළු වන්න" "රථගාන ඉදිරියෙන්" etc. Sometimes they will have to follow a multi way process of access internet, search the location, get the details and translate them using an online translation mechanism or ask from another person about displays on boards. Therefore,

A Proactive Defence to Social Engineering, 2001. 7.

Banu, D.M.N., Banu, S.M., 2013. A Comprehensive Study of Phishing Attacks 4, 4.

Cazier, J.A., Botelho, C.M., 2007. Social Engineering's Threat to Public Privacy, in: The 6th Security Conference, Las Vegas, Nevada: The Information Institute.

Cert UK, 2015. An introduction to social engineering.

Cui, Q., Jourdan, G.-V., Bochmann, G.V., Couturier, R., Onut, I.-V., 2017. Tracking Phishing Attacks Over Time. ACM Press, pp. 667–676. https://doi.org/10.1145/3038912.3052654

Krombholz, K., Hobel, H., Huber, M., Weippl, E., 2015. Advanced social engineering attacks. J. Inf. Secur. Appl. 22, 113–122.

Luco, D., 2013. The Art of Social Engineering.pdf. ASA Institute for Risk & Innovation.

metasploit, n.d. Best Practices for Social Engineering Attacks.

Mouton, F., Leenen, L., Venter, H.S., 2015. Social Engineering Attack Detection Model: SEADMv2. IEEE, pp. 216–223. https://doi.org/10.1109/CW.2015.52

Pollock, T., 2017. Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). 15.

Smith, A., Papadaki, M., Furnell, S.M., 2009. Improving awareness of social engineering attacks, in: IFIP World Conference on Information Security Education. Springer, pp. 249–256.

Social Engineering: A Scheme as Old as Time, 2018. . Secur. Intell.

Social Engineering Attacks: Common Techniques & How to Prevent an Attack [WWW Document], 2015. . Digit. Guard. URL https : // digitalguardian. com / blog / social - engineering - attacks - common - techniques - how -prevent-attack (accessed 5.7.18).

Streeter, D.C., n.d. The Effect of Human Error on Modern Security Breaches 6.

Suganya, V., 2016. A Review on Phishing Attacks and Various Anti Phishing Techniques. Int. J. Comput. Appl. 139, 20–23. https://doi.org/10.5120/ijca2016909084