Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.11, No.2, 2021

Simulation Model of Social Engineering Attacks in Business Enterprises

Francis Lowu[1*] Hudson Nandere[2]

1. School of Computing and Informatics, Bugema University, PO box 6529, Kampala, Uganda
2. School of Computing and Informatics, Bugema University, PO box 6529, Kampala, Uganda

* E-mail of the corresponding author: hodct@bugemauniv.com

Abstract

The pervasive use of social media in small and medium enterprises has increased social engineering cyber-attacks. Enterprises that have adopted the use of social media and emails to supplement on their marketing to complete business deals have been attacked or have detected attempted attacks on their infrastructure. Others are still trapped in the social engineering racket. In this paper we identify the dynamic pattern and behavior of social engineering both from within and without the business enterprises. We used analytical method to identify the key factors and parameters that cause social engineering attacks in businesses .Causal loops are used to model the relationships of key parameters that contribute to cyber-attacks through social engineering through the patterns and behavior of social media users. Using stock and flow diagrams, we build a simulation model on Stella platform, analyze it and suggest possible solutions that business enterprises can take to implement measures through policy change.

Keywords: Social Media, Attack, Engineering, Stella, Enterprise, Simulation, Model

DOI: 10.7176/JIEA/11-2-10
Publication date: December 30th 2021

1. Introduction

Among the challenges in today's communication is the issue of social engineering and cyber security. The communication paradigm that happens through the free space over which different nodes or gadgets interconnect for purposes ranging from fun, politics to business has become a security threat. The ability of nodes to interconnect and talk to each other on personal, organizational, national, and business topics has led to an increase in insecurity and mistrust due to the content being transmitted over these networks.

The interconnection has also increased innovation in technology, thus making social media networks a necessity in communication for business enterprises and for fun that can politically, socially and economically change communities. In the traditional communication paradigm of single hop heterogeneous network, communication could occur between the sender and the base station then with the receiver, which implies a limited connectivity between the nodes. However, multi-hop connectivity, which the social media network embraces as a communication paradigm, is an improved reliable connection with high level of efficiency over the space. This reliable connectivity is good, but also a threat in that it provides faster interconnectivity for the cyber-attacks, making it almost impossible to detect the attacks.

There are many social media platforms used world over, with Facebook taking the majority share of users followed by many others such as Twitter, WhatsApp, Instagram, Tick Tok, and Telegram. These social media platforms have made it easy for social engineering attacks to occur within business enterprises, due to the unsuspecting stuff being all over the space internetworking. Social engineering is the art of manipulating unsuspecting mobile or internet users to give out confidential information about their work, themselves, organizations and about their colleague. This implies that there are dynamics that need to be looked at to manage these attacks through simulating behaviour and pattern of attacks. Katharina et.al (2014) say that technical protection measures are usually ineffective against this technical attack. Some people believe that they can detect lies. However, it is not easy to detect lies and deception.

The tantalizing part of social engineering is that the type of information that the attacker seek is always changing. Banks, super markets and service business enterprises including individual working in the same organizations have all been targeted. Business enterprises have not put out stringent measures to invest in information technology's infrastructure security, which has caused many losses than expected. Investment in information security is necessary for businesses if they are to go with the pace of innovation in technology, for example being part of the

cloud.

Password hacking has proved to be very difficult today, so social engineering tactics of fooling workers into giving in their password starts just with the next employee in the organization. Who to trust, what to trust and when to trust are key measures that businesses should put into their policy to make employees understand the concept of trust. Social engineers have many tactics to use in order to get their targets right and therefore fulfil their intentions. Some of the tactics to attack are:

Email Phishing: Here we can first ask ourselves a question: How did they get my contacts? Normally one person is targeted, who is very social in this case, and if the social engineers access email of such a person, then they will get to his or her contacts. While they have email accounts for all employees then it is a deal for them. Many of the messages that you may receive cause curiosity and trust among employees, for example links and downloads which you click and eventually get malware on your computer.

Other messages may urgently ask for help, and because you work in the same enterprise, you bow in to help, to do some kind of charity and so on. Email Phishers will need to know who makes supplies to your organization, whom do you contact daily for a service, which bank usually sends information to you and many other things to try to contact you as if it's that company/friend is communicating.

Because employees in many organizations make innovations within the scope given to them by their managers, they tend to have a lot of time not thinking after completing a given and scheduled task, but socialising as they wait for the next instruction or task. This creates a gap for social engineers to get such idol minds seated in offices. The Baiting attacks may occur in such scenarios, because employees will resort to downloading music, go social media. In addition, baiters always organize workshops and distribute devices with hope that you may insert them inside your company computers. These kinds of attacks are commonly targeting greedy and selfish employees, who want to own and have everything around them different from other.

The rest of the paper is arranged as follows; section two presents the problem that motivated the study, section three presents the objectives that guide the findings of the study, section four shows related work to this research area, section five presents the methodology and shows how parameters were identified and how they are used to build the model, section six show the results of the simulation, and section seven presents the recommendation, future work and lastly conclusion in section eight.

2. Problem

The trend in the use of social network within small and medium size enterprises is a cyber-security threat that calls for a serious attention by the systems administrators and key strategic policy makers in business enterprises. Today few organizations put their ICT Policy into use, to enforce the rules under which communication from within and without the enterprise systems or network is handled. As a result, many businesses today fall victims to the attacks. This craters the IT team's productivity, general employee productivity, and ultimately, the business's productivity. As put by Bregg (2011), the root cause often has to do with failure to link security to business strategy. Employees need to be limited on the kind of information to share with community or strategic business competitors; through ensuring that they adopt a security-aware culture in the way they go about their work and to understand the potential threats of using social media networks for strategic business decisions. This can be achieved if they understand and appreciate the dynamics of cyber security models and how attacks can occur that may kill their business reputation.

3. Objectives

The objectives of the research is to identify the patterns and behaviour of social engineering attacks and design model using causal loops so as to find the relationships of different parameters that relate to cyber security within the social media network platforms. Last to simulate the relationship between the different social engineering attacks using Stella parameters for social media networks using stock and flow.

4. Literature Review

Aldawood et al. (2020) shows that many cyber-attacks target the technical part of a system, but there are other types of attacks designed to target the human element and rely on personnel vulnerabilities. Such attacks are considered to be socially engineered incidents. Human beings can be psychologically manipulated to perform explicit actions that can potentially lead to leakage of confidential information (Sheng et al., 2010). Breda et al.

(2017) adds that socially engineered attacks are designed for employees to leak classified information that can be used to damage an organization's resources or harm its reputation.

According to Fiermonte (2019), the nature of most social engineering attacks is spontaneous. Attackers select their targeted organizations on the basis of ease of access to sensitive data in the due process. Organizations with information systems that have few security measures to secure their data appeal to and become great targets for social engineers (Farooq et al., 2015).

In their paper, Frumento et al. (2016) listed statistics on social engineering attacks, estimating the number of cyber-attacks on private or government organizations. They highlighted that hackers are more inclined to use human vulnerabilities in an attempt to gain access to organizational systems than to focus on the lapses in a system's hardware or software. They also claimed that only 3% of the attacks target the technical infrastructures of organizations. On the other hand, 97% of malware attacks targeted users through social engineering hacking attempts.

Gudaitis (2013) says that an individual's work persona and private persona are permanently blurred. Forums, blogs, and popular social networks like Facebook, LinkedIn, and Twitter are just the tip of the social media iceberg. They continue that, the ubiquitous nature of smartphones and other mobile devices has made the Internet an 'anywhere, anytime' environment in which sensitive company information is often not confined to just behind the corporate perimeter. While social communities are thriving, so are the scams. Risks such as data leakage pose the biggest threat to most organizations. Social media "squatting" and increasingly sophisticated social engineering schemes are changing the landscape, with consequences ranging from brand reputation damage and lost productivity to potential physical harm to employees. The researcher agrees with finding that social engineering is so sophisticated that it has changed the way threats can be mitigated in social media cyber security.

According to the U.S. Department of Justice, social engineering attacks are one of the most dangerous threats over the world. Companies that handle significant valuable data are hacked more and when these companies are hacked, it highly impacts the worldwide economy and privacy (Salahdine & Kaabouch, 2019).

Natalia et.al (2019) studied social engineering techniques with emphasis on human-machine interaction that are used to implement and manipulate illegal human behaviour. They build a matrix of considering criteria qualifying the social engineers and a map of information security risks caused by the actions of social engineers

In his article, Zerfass (2012) examines current uses of social media for communication by enterprises, political organisations, and non-profit organisations (NPOs) and identifies likely future trends. Based on a quantitative online survey among 860 communication professionals in Germany and a follow-up qualitative Delphi study with 32 identified experts from the organisational communication profession and academia, it explores the status quo and aims to identify future directions. While organisations show more advanced structures for social media communication compared to earlier research findings, the empirical data also identifies many shortcomings. The potentials of social media communication are not fully exploited due to missing prerequisites including governance structures, rules, and resources. Looking into the future, the Delphi panel suggests that dedicated budgets, social media guidelines and other structural aspects will increase in the near future. However, many organisations will find specific ways to deal with the issue and common strategies are rare.

Based on the study by Fagade et al (2017), enforcing cyber security controls against malicious insiders touches upon complex issues of people, process, and technology. They continued that, in large and complex systems, addressing the problem of insider cyber threat involves diverse solutions like compliance, technical and procedural controls. Their work applied system dynamics modelling to understand the interrelationships between three distinct indicators of a malicious insider, in order to determine the possibility of a security breach through developing trends and patterns. It combined observable behaviour of actors based on the well-established theory of planned behaviour; technical footprints from incident log information and social network profiling of personality traits, based on the 'big five' personality model.

They also demonstrated how system dynamics as a risk modelling approach can flag early signs of malicious insider threats by aggregating associative properties of different risk elements. They suggested that, key challenges to combating insider threats are uncertainty, irregular intervals between malicious activities and exclusion of different personality factors in the design of cyber-security protocols

According to Katharina et.al (2014), they argue that if any attacker can gain access to the office of the targeted enterprise, it can be easy for them to find information such as passwords written on post-it notes. Most of the time physical attacks are not very sophisticated they involve password theft and some extortion to obtain information.

Presently, social engineering attacks are the biggest threats facing cyber security (Arana, 2017; Chargo, 2018).

According to Pavković & Perkov (2011), they can be detected but not stopped. Social engineers take advantage of victims to get sensitive information, which can be used for specific purposes or sold on the black market and dark web. With the Big Data advent, attackers use big data for capitalizing on valuable data for businesses purposes (Atwell et al., 2016). They package up huge amounts of data to sell in bulk as goods of today's markets.

In addition, Conteh & Schmick (2016) stress that cyber security incidents are growing exponentially in terms of frequency and damage to an organization's reputation in their respective marketplace and users, yet many organizations have not adequately deployed defences to discourage would-be attacker's intent to strike. Hackers are getting increasingly sophisticated and proficient at their social engineering attacks. They are able to piece together disparate data from various sources such as social media, corporate blogs, and data and to pull crucial and key data from well-meaning employees. Conteh & Schmick (2016) add that these cyber-criminals attack networks, steal invaluable data, and even hold corporations hostage and in some cases damage the object of their targets.

To overcome crime in the cyber domain, Conteh & Schmick (2021) state that, lack of resources is perhaps the leading contributor to its exponential growth. Few organizations have dedicated resources to pursue internet crimes and criminals. The challenge of pursuing cyber theft is costly and without return-on-investment (ROI) dedicated resources are difficult to justify.

5. Methodology

5.1 Parameter Identification

The types of social engineering and the different methods used by attackers were identified to help in the building of a causal loop relationship. The parameters that were identified are those that can be used by social engineering through different means to attack the unsuspecting employees in organizations who use social media occasionally to complete business work processes.

5.2 Types of Social Engineering

There many types of social engineering used both from technical and non-technical ones. The study categorised them as insider (with the enterprise) attacks and outsider (without the enterprise) attacks. Since social engineering does not require technical knowledge to be prevented.

5.2.1 Insider Attack

The 'insider attacks' can occur physically where the target trusts the people who in this case are fellow employees. They gather weaknesses of the victim and then use them against the will of the owner. Further office cleaners and tea girls can be used to attack. This is common in Banks, telecommunication, and major industrial ventures. Email phishing and social media are other sources of attacker. Likes received on social media platforms can be a good source of attack

5.2.2 Outsider Attack

The outsider attacker can also use physical attacks. The use of friendship like with managers, employees can support them to come in at any time and get any information they find useful for them. Because of trust they can get information about the person, like your Bank accounts, mobile money or ATM pins. They may go further to attack the physical infrastructure of the system used in the enterprise. Software installation such as those used for movies, videos and games on employee's computers can also be an outsiders target or mission.

The following areas were considered for parameter identification and each of the matched to the other for purpose of getting a relationship.

- The number of Facebook users in business enterprises
- Employer ICT and Social media, email usage policy
- The number of service organizations
- External and internal email usage
- Infrastructure weaknesses
- Insider behaviour to facilitate hacker
- Management decisions
- Technology decision
- Lack of firewalls and Antivirus on computers

- Lack of intrusion detection systems
- Changes in technology
- Business growth
- Increased returns

These parameters were used to design causal loop as shown in the next section.

5.3 Causal Loop Relationship Diagram

This causal loop shows that an increase in mobile device users will increase social engineering attacks. Further that if the attacks increase, it will increase on the social engineering, because they will find a good return in investment.

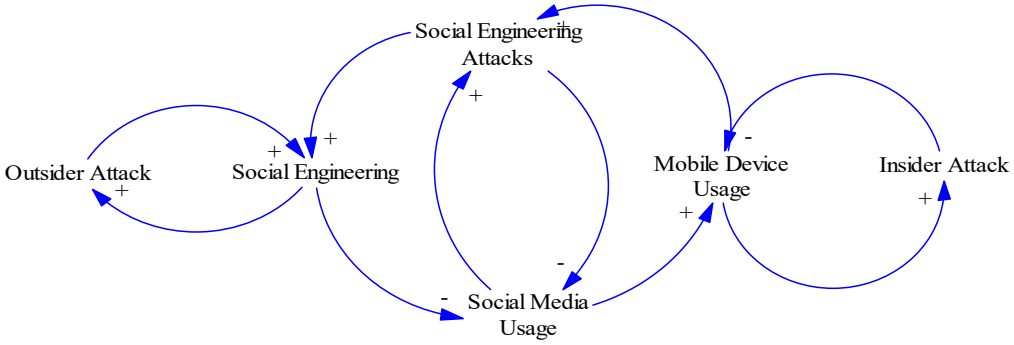

Figure 1: Causal Loop Relationships Diagram

However an increase in social engineering will discourage social media users, this will further decrease due to increased attacks. However, if the social media users increase more attack occur due to increased use of mobile devices. All the loops are negative meaning that they are goal-seeking loops.

5.4 Stock and Flow Diagram

The stock and flow diagram was constructed using the expanded causal loop diagram as shown in Figure 2 below.

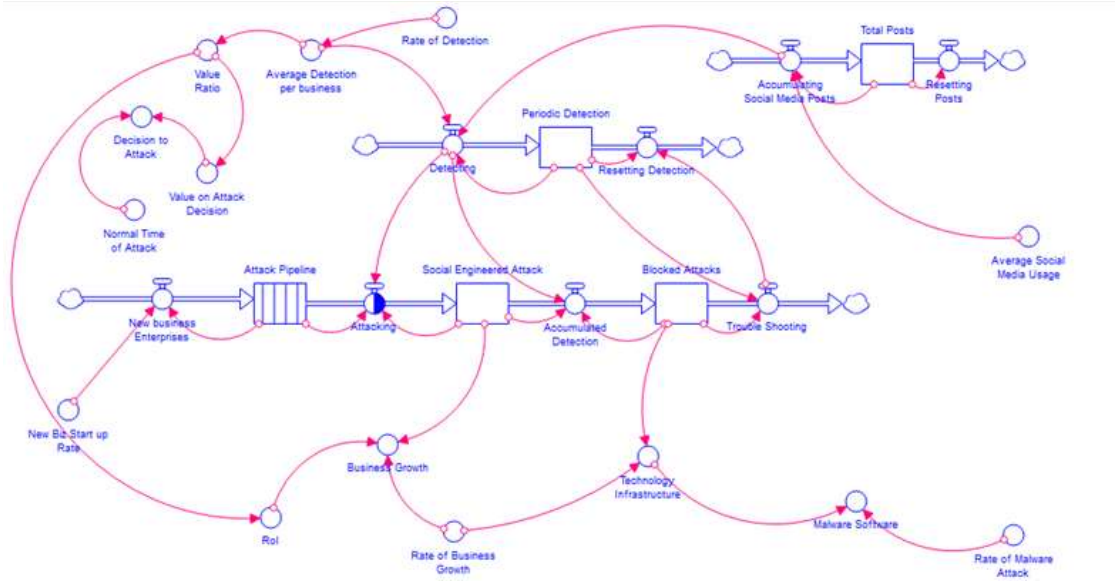

Figure 2: Stock and Flow Diagram for Model

6. Results

After simulating the above model you get;

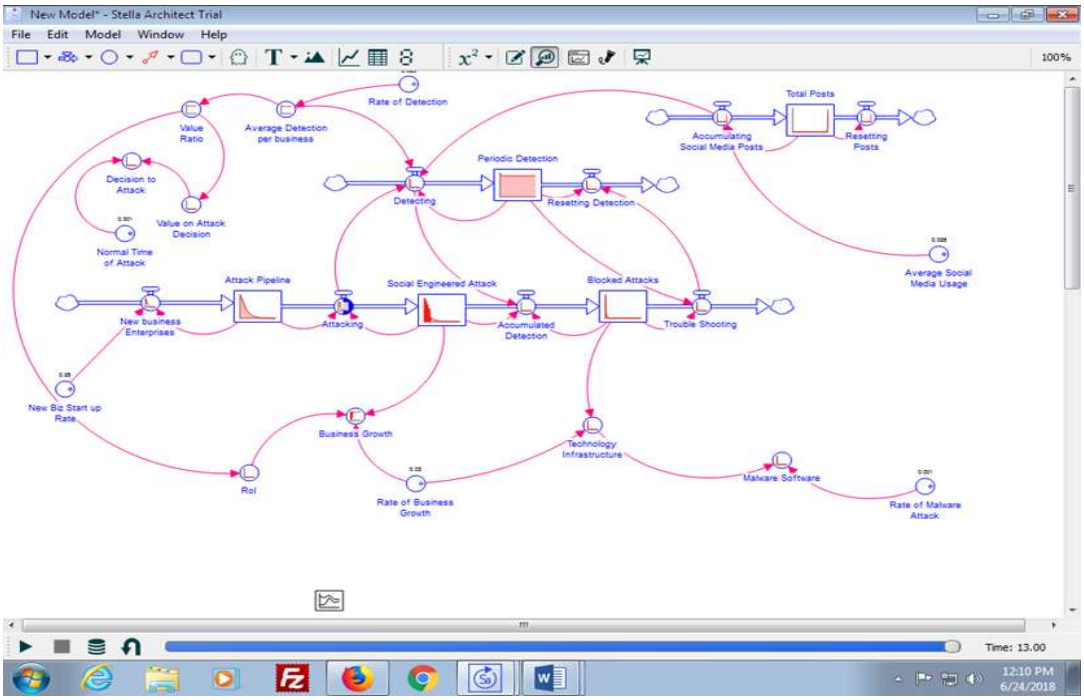

Figure 3: Showing a Simulated Model

Simulation model shows the relationship between the parameters. Many parameters come into play during social engineering. For example, we looked at business growth as a factor that makes social engineers get interest in attaching any business. They do not attack businesses that have low return on investment. New businesses also are targeted for attack because most of the time, they want to succeed in business and the social engineers use that gap

as an advantage.

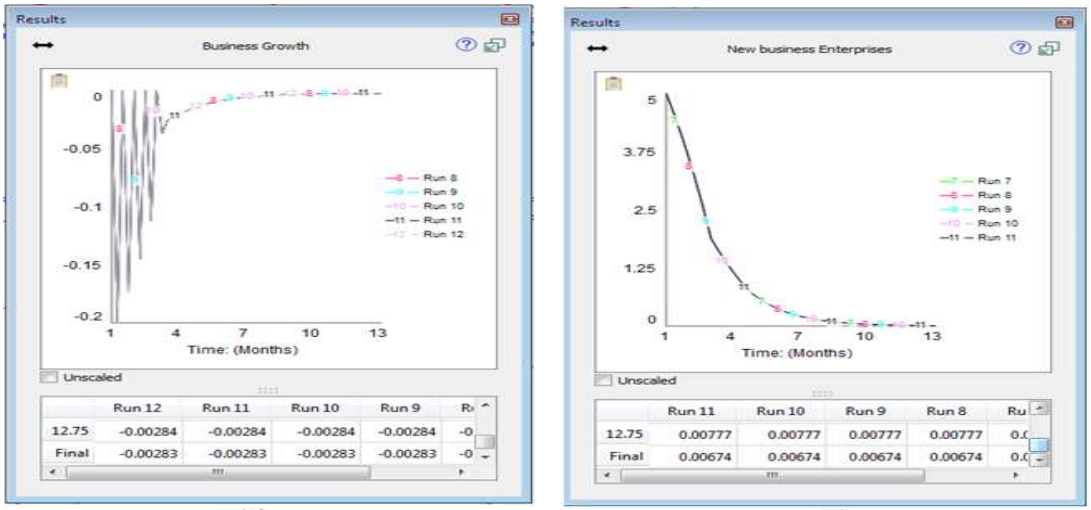

Figure 4: Showing Graphs from Simulated Model

Graph (a) shows that businesses grow from deficit. Therefore, if a business is attacked early, it may stagnate without making loss or profit. That is why there is a kind of sinusoidal growth. In graph (b) if businesses are attacked there will be sharp decline in their operations over time.

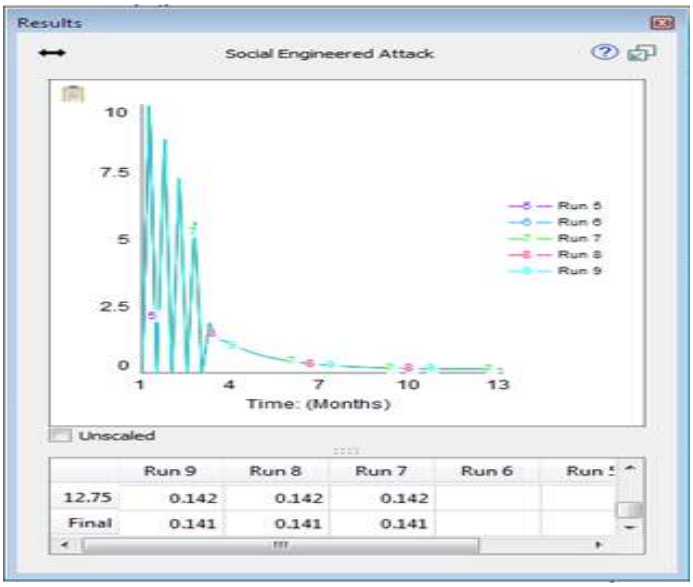

Figure 5: Graph for Social Engineering Attack

Social Engineering attacks work in shortest time possible to be successful to avoid detection. The more time they take the less attacks that occur, because the attackers' interest in the target diminishes due to the method used for that specific attack or when they are detected. From the graph above, in less than four months, they have attached all 10 enterprises. The nature of the graph shows that there are peak hours when the attacks may occur very fast to avoid detection being blocked.

7. Recommendation and Future Work

There are many requirements to take cares of in securing business enterprises today, due to the increase in cyber-attacks. Social engineering has taken the lead due to the increase in the use of mobile device and social media. Internet presence is high among employees, which has become a catalyst of social engineering attacks. We

recommend the following for business enterprises and employees in order to reduce or prevent social media attacks.

7.1 Recommendation - Business Enterprises

Businesses need to review their existing IT usage policies in order to be within the modern technological innovations. This will make it possible for adopting social media usage in their policies, to make employees. Businesses also need to put social media sections within their IT departments to make it easy to regulate their usage and to know which employees are supposed to deal with customers on the social media network. This makes it easy to trace the investment in IT infrastructure security that makes business enterprise to be safe at some percentage. Detection systems and other methods can help realise attacks soon.

7.2 Recommendation - Employees

Employees need not trust everyone, from customers to fellow employees. Social media network usage for business deals should be restricted for only the social media personnel. This is will help in reducing inside attacks through fellow employees. In addition, the use of emails, websites, and opening links that come from unknown source should be restricted and blocked at server level by systems administrators.

8. Conclusion

The objectives of this paper are to identifying patterns and behaviour of social engineering attacks using causal loops. Simulation using Stella is run to analyse and propose a policy shift on the implementation of cyber security measures and social media usage in business enterprises. We identified different methods used by social engineers such as phishing using email, websites, social media networks, instant messaging using analytical research method. Where social engineers use social media and emails, baiting, among other tricks; which occur in physical presence of the attacker due to human error and or greed to again very fast. For example, in Fig: 1, we see in the relationship causal loop, that there will be an increase in social engineering attacks with the increase in the use of mobile devise, while increase in social engineering attacks increase social engineering. Other attacks originate from within the organization due to the socio-technical approach of businesses. The study simulated the scenario and found out that business enterprises still have challenges of understanding how to handle social engineering attacks. Social engineering is the most effective way of gaining access to secure enterprise systems today to obtain sensitive data and information from unsuspecting employees. Nonetheless, it is one of the methods that do not need a lot of technical knowledge to prevent attacks.

More so, we have provided an overview of social engineering attacks, some existing detection techniques, and provided some countermeasure methods. Nevertheless, these attacks cannot be stopped by using only technology and the suggested methods. Social engineering attacks have been increasing in intensity and number therefore causing emotional and financial damage to people and companies. Consequently, there is a great need for unusual detection techniques and countermeasure techniques as well as programs to train employees and/or staff members within organizations. Nations are also obliged to invest in cyber security education to build skilled and trained individuals.

9. Acknowledgement

This work was supported by the directorate of research and School of Computing & Informatics, Bugema University.

References

Aldawood, H., Alashoor, T. and Skinner, G., 2020. Does awareness of social engineering make employees more secure?. International Journal of Computer Applications, 177(38), pp.45-49.

Arana, M., 2017. How much does a cyberattack cost companies. Open Data Security, pp.1-4.

Atwell, C., Blasi, T. and Hayajneh, T., 2016, April. Reverse TCP and social engineering attacks in the era of big data. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 90-95). IEEE.

Breda, F., Barbosa, H. and Morais, T., 2017, March. Social engineering and cyber security. In International Technology, Education and Development Conference (Vol. 3, No. 3, pp. 106-108).

Chargo, M.A., 2018. You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data. Transactions: Tenn. J. Bus. L., 20, p.115.

Conteh, N.Y. and Schmick, P.J., 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), p.31.

Conteh, N.Y. and Schmick, P.J., 2021. Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks. In Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 19-31). IGI Global.

Fagade, T., Spyridopoulos, T., Albishry, N. and Tryfonas, T., 2017, July. System dynamics approach to malicious insider cyber-threat modelling and analysis. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 309-321). Springer, Cham.

Farooq, A., Isoaho, J., Virtanen, S. and Isoaho, J., 2015, August. Information security awareness in educational institution: An analysis of students' individual factors. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 352-359). IEEE.

Fiermonte, M., 2019. The Threat of Social Engineering to Networked Systems (Doctoral dissertation, Utica College).

Frumento, E., Puricelli, R., Freschi, F., Ariu, D., Weiss, N., Dambra, C., Cotoi, I., Roccetti, P., Rodriguez, M., Adrei, L. and Marinelli, G., 2016. The role of Social Engineering in evolution of attacks.

Gudaitis., 2013, The Impact of Social Media on Information Security: What every company needs to know.

Katharina, K., Heidelinde, H., Markus, H., Edgar, W., 2014, Advanced Social Engineering Attacks. SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria

Linke, A. and Zerfass, A., 2012. Future trends in social media use for strategic organisation communication: Results of a Delphi study. Public Communication Review, 2(2).

Mamedova, N., Urintsov, A., Staroverova, O., Ivanov, E. and Galahov, D., 2019. Social engineering in the context of ensuring information security. In SHS Web of Conferences (Vol. 69, p. 00073). EDP Sciences.

Pavković, N. and Perkov, L., 2011, May. Social Engineering Toolkit—A systematic approach to social engineering. In 2011 Proceedings of the 34th International Convention MIPRO (pp. 1485-1489). IEEE.

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. Future Internet, 11(4), p.89.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J., 2010, April. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 373-382).