Social Engineering Attacks in E-Government System: Detection and Prevention

Musa Midila Ahmed
Faculty of Education, Department of Physical Science Education,
Modibbo Adama University, Yola, Nigeria
OrcidID: 0000-0002-7769-6400; E-mail: ahmedmm4me@yahoo.com

Subject Area: Education Management.
Type of the Paper: Conceptual Research Analysis.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.6085386
Google Scholar Citation: IJAEML

How to Cite this Paper:
Musa Midila Ahmed, (2022). Social Engineering Attacks in E-Government System: Detection and Prevention. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *6*(1), 100-116.
DOI: https://doi.org/10.5281/zenodo.6085386

International Journal of Applied Engineering and Management Letters (IJAEML)
A Refereed International Journal of Srinivas University, India.

Crossref DOI : https://doi.org/10.47992/IJAEML.2581.7000.0123

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

Social Engineering Attacks in E-Government System: Detection and Prevention

Musa Midila Ahmed
Faculty of Education, Department of Physical Science Education,
Modibbo Adama University, Yola, Nigeria
OrcidID: 0000-0002-7769-6400; E-mail: ahmedmm4me@yahoo.com

ABSTRACT

Purpose: *E-Government system emerged as a novel public service provision platform that enables governance in an efficient and transparent manner globally. However, despite the success recorded so far by the increase in the use of information and communication technology (ICT) and E-government for public service provision. Social engineering attack (SEA) is one of the challenging information security attacks that prove to be difficult to tackle. This is because the attackers leverage on peoples' weakness to exploit the system instead of technical vulnerabilities.*

Design/Methodology/Approach: *This paper uses PESTLE (political, economic, social, technology, legal and environment) analysis to critically evaluate the external factors affecting SEAs in E-government system.*

Findings/Result: *The study identified phishing, Baiting, Pretexting, Quid Pro Quo, Honey Trap, Tail Gating, and Pharming as the major SEA techniques used to exploit E-government systems. Furthermore, the author suggest training and awareness programme as the most effective way to detect as well as prevent SEA in E-government system. Users should be aware of the languages with terms requesting urgent response as well as unusual or unexpected situation in a suspicious messages or attachment as factors to detect SEA. Technical controls using natural language processes (NLP), security policies, multifactor authentication (MFA) as well as secured preservation of confidential information from suspicious users are some of the SEA preventive measures.*

Originality/Value: *A flexible and efficient interaction among citizens, businesses and government organizations is a critical factor for successful E-Government system. SEA is one of major challenges affecting communications in E-government system that requires attention. In conclusion, studies toward technological approach for solution of SEA in E-government is recommended.*

Paper Type: *Conceptual Research.*

Keywords: SEA, SE, Social Engineering Attack, Social Engineering Detection, Social Engineering Prevention, E-Government System, PESTLE analysing framework

1. INTRODUCTION :

Social engineering in the information security perspective refers to a collection of fraudulent activities on the network with the aim of getting confidential information from people. The attacker psychologically manipulate users' intelligence as a trick of getting sensitive data. The kind of data sought by attackers using this trick varies, the common sensitive data targeted are bank details, security credentials, password and secret PIN. Nowadays, attackers realised that social engineering attacker is easier than other technological ways of hacking the security systems. In other word, it is easier to fool people to give their security credentials than technically hacking for them. In a nutshell, the weakest security breach channel in the security systems is human error. Consequently, social engineering attack is a serious problem to the information security professionals because no matter how secured a system is, this renders its vulnerable to attacks. Social engineering attack undermines the technical expertise of professionals in protecting software systems by getting unauthorized access to protected data. The success achieved by information security researchers in defending applications and software systems is defeated by social engineering attacks.

A survey conducted by [1] discovered that social engineering attacks rendered e-government systems vulnerable to numerous security violations. E-government is the use of information and communication technology (ICT) for delivery of public services to citizens, businesses and collaboration with other government organs. E-government facilitates transparent involvement of citizens in governance. However, despite the numerous benefits of e-government adoption, security challenges such as security threats to the e-government network, issues of identification violations, the trade-off between security and usability, and access control to sensitive information are some of the barriers to its implementations. A study by [2] identified infrastructure, human and government factors as the key success factors that increases the chances of failure in e-government systems. According to the author, the adoption of e-government is more successful in the developed countries than the developing countries. Consequently, further research toward enhancing the success of e-government projects in developing countries is desired. The study focused on investigating the human factor in the e-government projects.

Advancement of SEA due to the increase in the use of E-government is an information security issue that requires investigation. The study use PESTLE analysis as the method of identification of factors responsible for SEA as well as the characteristics for potential impact of SEA in E-government system. This study is to identify the SEA techniques used to attack E-government system. In addition, this study is to suggest measures of detecting potential SEA and ways of preventing SEA in E-government system. The remaining part of this paper is organize as follow; section 2 discusses on social engineering attack. Section 3 is for social engineering attack in E-government. While section 4 provides detection methods of social engineering attacks and section 5 focuses on protection methods of social engineering attacks. Finally, section 6 summarises and concludes the paper.

2. OBJECTIVES OF THE STUDY :

The objective of this study is to:

(1) Identify the SEA techniques used to attack E-government system.
(2) Analysis for SEA in E-Government System using PESTLE framework.
(3) Suggest measures of detecting potential SEA in E-government system.
(4) Suggest ways of preventing SEA in E-government system.

3. RELATED WORK :

Exploitation of software system by technical attacks has declined due to the success in the security mechanisms developed and used in modern software applications. It is difficult for attackers to identify vulnerable points in the systems. Consequently, hackers these days exploits people’s trust and psychology for their malicious activities instead of the technical vulnerabilities of the systems. The most common attack to information security nowadays is social engineering attacks ([3, 4]). According to [3], social engineering attacks deserves the same attention with its technological counterparts. [4] identified E-mails, social media networks, advertisements and mobile phones as the most common medium of social engineering attacks. The use of deception for malicious activities is not new. However, the popularity of the internet and World Wide Web for public service provision has increase the spread and success of online social engineering attacks. [5] defined online social engineering attacks as the use of internet facilities such as World Wide Web applications as a means of manipulating users’ behaviour to exploit the systems resources.

The evolution of internet based communications simplifies information sharing using many social networks such as Emails, Facebook, Twitter, WhatsApp, and Web Services. This platforms enables decentralized, timely, cheap and easy interaction among people. However, it makes it easy for social engineering attackers get confidential or unauthorized information from unsuspecting people, which renders the system vulnerable to cyberattacks. Therefore, it is high time governments and organizations invest on ways of detecting as well as preventing social engineering attacks. An effort to conceptually analyse empirical studies conducted on SEAs, [6] proposed theoretical framework for SEA research to social engineering research by evaluating features of SEA-based on extant theories in the cognitive science. While [7] investigated phishing detection among participant in autism and discovered that social disorder may not necessarily influence SEAs. Similarly, [8] studied cases of cryptocurrency violations in the community by evaluation of ontological cases of SEA to enhance the security awareness among Blockchain users. Relating human factors to specific aspect of SEAs risks and threats, [9] proposed solution to address SEA in cloud environment. Also, a survey of SEA by

[10] broadly classified into Phishing, Baiting, Pretexting and Tailgating. Conceptual researches to provide an overview and taxonomy to classify SEA on knowledge workers [11], types and channel of attacks [12], and analysed identified methods of threats [13].

Table 1: Review Outline of SEAs on E-Government System

S/No	E-Government Attacks	Focus	References
1.	Common E-Government Attacks	Common attack in E-Government information security nowadays is social engineering attacks.	Chinta, et al. (2016) [3] Chitrey, et al. (2012) [4]
2.	Define SEA	Online SEAs as the use of internet facilities such as WWW applications as a means of manipulating users' behaviour to exploit the systems resources.	Ivaturi & Janczewski (2012) [5]
3.	Theoretical framework for SEA	Theoretical framework for SEA by evaluating features of SEA-based on extant theories in the cognitive science.	Burda, et al. (2021) [6]
4.	Detection of SEA	Investigated phishing detection among participant in autism and discovered that social disorder may not necessarily influence SEAs	Neupane, et al. (2018) [7]
5.	cryptocurrency violations	cases of cryptocurrency violations by evaluation of ontological cases of SEA in E-Government	Weber, et al. (2020) [8]
6.	SEA in E-Government Cloud Environment	Solution to address SEA in cloud environment.	Alavi, et al. (2015) [9]
7.	SEA classification	A survey of SEA broadly classified into Phishing, Baiting, Pretexting and Tailgating.	Salahdine & Kaabouch (2019) [10] Krombholz, et al. (2015) [11]
	Types and methods of SEA	Types and channel of attacks and analysed identified methods of threats.	Koyun & Al Janabi (2017) [12] Aldawood & Skinner (2019) [13]

Many studies focused on natural language processing (NLP) to detect potential SEAs. [14] proposed a chat-based SEA recognition by evaluation of specific purpose written text on social engineering domain. The study enhanced the understanding of in-context features used by attackers. Similarly, [15] provides a practical and efficient SEA detection method by NLP and machine learning. Another approach by [16] used two-stage feature extraction process to detect SEA by NLP and case-base technique. This approach identifies possible SEA with high accuracy results. Also, [17] used NLP for detection of ask and framing risks situations by an experiment to determine the precision of lexical structure for enhanced detection. According to the author, this approach improves ask and framing detection to inform users on potential SEA threats. A review of the popularity of SEA in the corona virus pandemic by [18] suggest ways to reduce success of the attack in the period. According to the author, the use of technology alone is not sufficient to resolve SEA threats. An effort to improve awareness of SEA through persuasive training. [19] used game designed to provide knowledge on social psychology theory of resistant to persuasion. This is to improve SEA awareness in a friendly manner in the general populace.

In information security, semantic attacks refers to manipulation of systems' interface by deception of users to breach the security setting of the systems. In this perspective, [20] proposed an online game to detect social engineering attacks by enhancing peoples' awareness in an entertaining way. To enable users detect and report of semantic SEA, [21] conducted an experiment to evaluate human sensor cogni-sense attacks. The results shows that users involvement help in detecting human-based threats. In the vein, [22] uses signal detection theory to explore ways of enhancing users detection of malicious emails. The author discovered that paying attention on senders' details improves detection of phishing attacks.

Table 2: Review Outline of SEAs Detection on E-Government System

S/No	SEA Detection in E-Government	Focus	References
1.	Natural language processing (NLP)	A chat-based SEA recognition, NLP and machine learning, two-stage feature extraction process, NLP and case-base technique and detection of ask and framing risks to recognize SEA.	Tsinganos & Mavridis (2021) [14] Lansley, et al. (2020) [15] Lansley, et al. (2019) [16] Dorr, et al. (2020) [17]
2.	SEA in Corona Virus pandemic	A review of the popularity of SEA in the corona virus pandemic	Alzahrani, A. (2020) [18]
3.	Awareness and Training	Awareness of SEA through persuasive training to provide knowledge on social psychology theory of resistant to persuasion	Aladawy, et al. (2018) [19]
4.	Online game	Detect SEAs by enhancing peoples' awareness to enable users detect and report semantic SEA.	Goeke, et al. (2019) [20]
5.	Semantic SEA	An experiment to evaluate human sensor cogni-sense attacks to enable users detect and report of semantic SEA.	Heartfield & Loukas (2018) [21]
6.	Signal Detection Theory	Enhancing users detection of malicious emails by paying attention on senders' details.	Nicholson, et al. (2017) [22]
7.	Telephone-based SEA	An experimental evaluation of successful telephone-based SEA threats.	Bullée, et al. (2016) [23]
8.	STRAYSHEEP system	Experiment to evaluate the STRAYSHEEP system by screening and creeping sequences of malicious web pages to detect SEAs.	Koide, et al. (2020). [24] Koide, et al. (2021) [25]
9.	Chat-Based SEA automated recognition system	Detection of SEA by recognition of potential attacks by critical enablers such as stages, forms and attribute.	Tsinganos, et al. (2018) [26]
10.	Identification of attackers' tactics	Success rate of web-based SEA through downloads of unsolicited malicious software.	Nelms, et al. (2016) [27]

An experimental evaluation of successful telephone-based SEA by [23] shows that awareness on threats reduces vulnerability rate. Similarly, an experiment by [24] to evaluate the STRAYSHEEP system that screens web pages to detect SEAs shows that the system can collect diverse SEAs as well as identifies the tricks employed in the attack. An extension of the STRAYSHEEP by [25] conducted an experiment that creeps sequences of malicious web pages that detects and gathered potential SEAs generally as well as identified tricks used by attackers. A holistic approach that recognizes the critical enablers such as stages, forms and attributes of chat-based SEAs in enterprise environment by [26] proposed an automated attack recognition system for SEA. The study focused on detection of SEA by recognition of potential attacks. Working toward measuring and mitigating social engineering software download attacks, [27] investigated on the success rate of web-based SEA through downloads of unsolicited malicious software. The author identified the tactics used by attackers to deceive and persuade users to download malicious software by collecting and labelling SEAs web-downloads using packets inspection and analysis.

Analysis of broad range of vulnerabilities of organization on the internet by [28] evaluated the role of SEA in intrusion detection and identity theft. The author recommends SE vulnerability risks and countermeasure to prevent SEA. Also focusing on preventive measures, [29] proposed a managerial method of preventing SEA by a security lifecycle model. The author discovered that staff in public service in Turkey has insufficient awareness on SEA. Although, the study is toward development of security lifecycle model against SEA. It generally focussed on awareness for security protection portfolio. However, [30] conducted an experiment to test users' error judgement based on different kinds of interactions. The results enhances chances of being scammed by SEA in distractive environment. According to [31], it is essential to invest on both human-based and technology-based information security attacks for adequate protection of information systems. An attempt to obtain solution to the social engineering attacks by [32] provides a taxonomy for an overview of semantic attacks by a survey of adequate protection methods against the attacks. An experimental trials of anti-phishing working group site on sample drawn from students and academic staff by [33] discovered that web-based approach could promote awareness and reduces success of SEAs. A similar human factor vulnerability analysis by [34] proposed linguistic approach for managing SEAs. The author identified human as a leading factor of SEA.

A survey by use of open-ended questionnaires by [35] evaluated the impact of information security awareness on data breaches originating from SEAs identified actionable information on security awareness. [36] investigated various categories of SEAs in COVID19 and proposed preventive guidelines to these attacks. The author presents strong authentication, avoid reciprocation of unexpected contacts, verify and validate data received to get out of SEAs. A multivariate experiment design with priming and warning conditions with a sample of 290 respondents by [37] discovered that neither priming nor warning influenced the rate of disclosure of sensitive information. The author, conclude that priming and warning are not effective to prevent SEAs because users lack awareness on what is sensitive data. Similarly, [38] investigated the key components and basic concepts of SEA by user-reflective model to prevent the attack on New Zealand banking sector. The proposed model helps in decreasing the effect of SEA on New Zealand banking sector. Also [39] proposed an access control model and evaluates success rate of the model on SEAs by a hybrid linguistic fuzzy variable with decision support design model. An experiment that uses a game theoretic model to provide an automatic protection for organization by [40] explored water-hole attacks to implement download attacks by diverting users to malicious sites. The author proposed a deception game model for SEA to optimize protection policy towards protecting SEAs.

Table 3: Review Outline of SEAs Prevention on E-Government System

S/No	SEA Prevention in E-Government	Focus	References
1.	vulnerability risks and countermeasure	Analysis of broad range of vulnerabilities on the internet to prevent SEA.	Conteh & Schmick (2016) [28]
2.	Security lifecycle model	Awareness for security protection portfolio by a managerial method of preventing SEA.	Mataracioglu, et al. (2015) [29]
3.	SEA in distractive environment	Experiment to test users' error judgement based on different kinds of interactions in distractive environment.	Pollock, et al. (2020) [30]
4.	Investment for security protection	It is essential to invest on both human-based and technology-based information security attacks for	Aldawood & Skinner (2020) [31]

		adequate protection of information systems.	
5.	SEA protection methods.	A taxonomy for semantic attacks by a survey of adequate SEA protection methods.	Heartfield & Loukas (2015) [32]
6.	Awareness to reduces success of SEAs	An experimental trials of anti-phishing working group site on sample drawn from students and academic.	Smith, et al. (2013) [33] Junger, et al. (2017) [37]
7.	Human factor vulnerability	A similar human factor vulnerability analysis by linguistic approach for managing SEAs.	Alavi, et al. (2015) [34]
8.	A survey by Questionnaire	A survey by use of open-ended questionnaires to evaluated the impact of information security awareness on data breaches originating from SEAs.	Kostic (2020) [35]
9.	Categorize SEAs in COVID19	Preventive guidelines to get out of SEAs.	Venkatesha, et al. (2021) [36]
10.	User-reflective model	To prevent SEA attack on New Zealand banking sector.	Airehrour, et al. (2018) [38]
11.	Access control model	Evaluates success rate of SEAs by a hybrid linguistic fuzzy variable with decision support design model.	Khlobystovaa & Abramova (2020) [39]
12.	Game theoretic model	To provide an automatic protection for organization by a deception game model to optimize SEA protection policy.	Shi, et al. (2019) [40]

3.1 Research Gap

In a nutshell, the rapid advancement of ICT for interactions in governance made sensitive information easily obtainable on the network. Full protection of sensitive data on the network is challenging particularly with the technique of deceiving people to reveal sensitive information. SEA is one of the dangerous information security attacks, since it cannot be fully protected by technical means. Consequently, it is difficult to prevent this attacks, since attackers leverage on human weaknesses. Therefore, prevention of social engineering attacks is challenging due to the numerous tricks use by attackers. So also, detection of social engineering attacks is challenging since attackers exploits human instead of technical vulnerabilities. Overall, the best way to prevent social engineering attacks is by detection mechanism. This study focus on the detection and prevention of SEA in E-government systems.

Nowadays, governance has shifted from the traditional paper and pen to a more reliable, transparent and efficient E-government environment. This has amplified information security vulnerabilities generally and SEA in particular in which attackers exploits human weaknesses instead of technical vulnerabilities. Consequently, empirical evidence on identification of SEA techniques and formulation of strategies for detection as well as prevention of SEAs in E-government system is timely. In view of the dynamic nature of techniques used by SEAs, studies to identify the current techniques used for exploitation of E-government system is required. Furthermore, it is important to address the increase in SEAs in E-government by detection and prevention of these attacks. Particularly, there is no sufficient studies on measures for detection and countermeasures of SEAs in E-government system. Therefore, information concerning both detection and prevention of potential SEA in E-government is needed.

3.2 Research Agenda

Social engineering is regarded as one of the leading information security threats in E-government system that leverages on the weakness of human being. Therefore, further study toward the effect of education and training on SEA success is recommended. Since this kind of attach exploits human qualities especially greed, fear or eagerness to gain, empirical studies that focus on knowledge and experience of the kind as well as characteristics of the languages and tricks use by attackers is crucial. Sequel to identification of the common SEA techniques for E-government attacks, future research shall be on experimental evaluation of the detection and prevention of these common attacks. However, SEAs is increasing in both volume and sophistications that makes it extremely difficult to detect and mitigate at the both national and global scale. Therefore, automated authentication methods by security technologies to counter potential threats in addition to awareness programme for citizens' understanding of the need to abide by all policies, rules and regulations.

4. PESTLE ANALYSIS :

PESTLE (Political, Economical, Sociological, Technological, Legal and Environmental factors) analysis evaluates the key external factors that affects an organization. PESTLE analysis is a great tool for gathering information on potential impacts of the six external factors of SEA in E-government system. This tool is used to improve the quality of decision making which can change the whole operation of the system. The advancement of ICT has turn the world into a global village, where every internal activities is optimized or automated technologically. This results in having control of most of the internal factors affecting smooth running of an information systems. However, SEA is an external factors affects the success of a system which cannot be controlled by stakeholders and managers. Therefore, PESTLE analysis is leveraged in this study to identify the factors that affects the operations of SEA in E-government system. PESTLE enable an organization to anticipate potential business threats and plan ways of avoiding or minimizing its impact. Therefore, it is imperative that any new strategy developed for a system have PESTLE analysis to form a comprehensive list of potential risks associated with it.

POLITICAL

- Bureaucracy
- Legislation
- Regulation
- Policy Making
- Restrictions
- Security
- Tariff
- Stability
- Trade agreements

ECONOMICAL

- Unemployment
- Cost of living
- Interest Rate
- Inflation
- Wage Rate
- Working hours
- Exchange Rate

SOCIOLOGICAL

- Religion Trends
- Cultural norms
- Societal Expectations
- Consumer Attitudes
- Age Distribution
- Population
- Family Size
- Life Style
- Consumer Test

TECHNOLOGICAL

- Innovations
- Research Development
- Technological Advancement
- E-commerce
- Social Media
- Information Security Level
- Automation
- Robotic/Artificial intelligence
- Smart Devices

LEGAL

- Law Enforcement
- Legal Protection
- Labour Laws
- Safety Regulation
- Licence and Permit
- Intellectual Properties
- Equal Opportunity

ENVIRONMENTAL

- Professional Ethics
- Cooperate Social Responsibility
- Awareness
- Sanctions
- Procurement Procedures
- Business Supply management
- Scarcity

(Source: Compiled by Researcher)

Fig. 1: PESTLE Analysis for SEA in E-Government System

4.1 Political Factors

Political factors refers to the relationship between legitimate business operations and government restrictions through policies, rules and regulations. Legislation on business operations and trade agreements between service provider and service consumer are political factors in PESTLE analysis to determine the extent to which government may influence the impact of SEA in E-government system. Another major factor that fuel SEA is inadequate bureaucracy in government operations. Bad bureaucracy in E-government operations centralises power structures and decision making, which forces citizens to comply with the stringent rules and procedures. This generally discourage people from participating transparently in the E-government system instead look for short and cheaper ways entice by SEAs. Politically stable nations will have less risks of SEAs as a results of its predictability, transparency and accountability. This encourages citizens transparently participate in the E-governance confidently and honestly. Tariff serves as a means of generating revenue to government as well as protect domestic industries from collapse. However, excess imposition of tax and tariff will adversely affect the purchasing power as well as loyalty of citizens in governance. Consequently, disloyal citizens may engage in SEAs or there victims of SEAs. Generally, one of the main responsibility of government is to provide security of life and properties of its citizens. Therefore, government should find means of tackling the threats of SEAs.

4.2 Economic Factors

Economic factors of PESTLE for SEAs in E-government are factors that affects the financial status of people in the country. They include interest rate, unemployment, cost of living and inflation. Others are wage rate, working hours, exchange rate, education and training as well as economic growth or decline. Interest rate affects the liquidity of cash flow in the country. Unemployment affects the purchasing power of citizens particularly getting necessary needs such as food, cloths, shelter, etc., which forces people find ways of survival by either legitimate or illegitimate means. Inflation, cost of living and wage rate influences the economic status and standard of living of people in the country. Citizens might partake in SEAs in order to attain an average or higher standards of living. Working hour rate affects the growth of SEAs in a country, low working hours might increases involvement in SEAs. Similarly, exchange rate influences the price of goods and services in a country, which in turn affects the living condition of people. Education and training is an important factor for rapid growth and development of a country. Ultimately, education and training enables citizens develops intellectual skills, which results in high income and development of the economy.

4.3 Social Factors

Social factors are forces that are capable of influencing peoples’ behaviours and spending, which are closely related to the cultural norms and religious trends in the society. Also, societal expectation and consumer attitudes are key to determining peoples’ behaviour on SEA. Other factors that can influence SEA are age distribution, population growth rate and family size, which affects the economic status of citizen. A study by [41] shows that a gradual growth of corruption occurs before the age of 40 years and declined at 55 years. Population and family size is a critical factor in keeping the public sector honest, transparent and accountable to ensure that the public sector act in the public interest. Therefore, government need to find ways to stop dishonest practices and corrupt activities as well as hidden risks. Generally, lifestyle and consumer tests are social factors affecting the prevalence of SEAs in E-government system. Customer test and lifestyle of individuals are key factors in revealing unjust self-enrichment and a clue for potential fraud or corrupt activities. This can be audited by comparing the living standards of suspects with their legitimate source of income.

4.4 Technological Factors

Advancement in technological has been used to facilitate SRA in E-government by easily getting access to official information. Although, digitalization by E-commerce and service automation enables online delivery of services to citizens, which increases the prevalence of SEAs in E-government system. Popularity of smartphones and social media in the society does not only spread hate and stupidity in the society but exposes unsuspecting citizens to SEAs. Social media serves as catalyst for success of SEAs and other cybercrimes. However, it can as well serve an important role in the fight against SEA and other related corrupt practices. As the cybersecurity experts conduct research for innovative ways of protecting service systems, so also cybercriminals do to exploit the system.

Nowadays, cybercriminals use a combination of social engineering method and malware to increase the chances of exploiting the systems. In view of the mutual relationship between advancement in technology and anti-corruption in the effectiveness of digital government. Technology enables rapid, transparent and accountable interactions in E-government system. Therefore, government should invest toward enhancing information security in governance by robotics and artificial intelligence innovations.

4.5 Legal Factors

Legal factors refers to any legal forces pertains to what a legitimate business can do and what it cannot do. It highlights ways citizens can be restricted by law enforcement in government. Government can decide to enact safety regulations for both producers and consumers as a legal protection of citizens. This regulations must be abided by interacting parties to check-mate any violation or irregularities in businesses and governance. Consumer protection, labour and safety laws be designed to protect the citizens from fraudulent practices generally. Furthermore, government should play the big part of ensuring that equal opportunity is provided to all citizens and intellectual property is adequately protected. Similarly, government should make sure all businesses has requisite license and permit to legally operate the business and also ensure that only legitimate business obtain operational license and permit. Finally, citizens be educated on the fact that any business operating without proper license and permit is a criminal violation.

4.6 Environmental Factors

Environment factors of PESTLE analysis helps with strategies of keeping decision-makers informed on the external factors affecting the success of the organization. It helps in improving awareness of the potential threats are risks associated with SEAs in E-government system. Education and awareness of citizen on cooperate social responsibility (CSR), procurement procedures and business supply management will greatly enhance detection of SEAs in E-government system. Professional ethics is a set of principles designed to ensure that employees behaves in an acceptable respectable manner. It is a rule of behaviour that requires universal compliance by all members. Professional ethics serves as not only as a guide internally but as a guide statement for external individuals' commitment in agreements and contracts. Violation of professional ethics may lead to sanction depending on the seriousness and circumstances surrounding the professional misconduct. Finally, scarcity of essential resources leads to increase in its demand. Consequently, scarcity is the root cause of the essential problems in E-government system. Particularly, it is one of the key factor that influences citizens' decision on commitment.

5. FINDINGS AND SUGGESTIONS :

This section presents the results of the conceptual investigation. First, the section identified to Phishing, Baiting, Pretexting, Quid Pro quo, Honey Trap, Tailgating, Pharming attack as techniques of social engineering in E-government system. Furthermore, the section present some measures for detection and prevention of SEAs in E-government system.

5.1 Social Engineering Attacks in E-Government System

Despite the huge investment made in E-government system worldwide, the expected success of this novel innovation is not yet fully realised due to security challenges. According to [42], there is a growing shift to E-government initiative worldwide. The author identified enhanced information sharing, interaction, transaction and transformation as E-services fundamentals. E-government services reduces governance cost and simplifies service provision to citizens, which ultimately enhances productivity and quality of services. Furthermore, it improves transparency and communication for productive decision making in governance [43]. E-government emerged as an innovative way of service delivery to citizens and transparent information sharing with citizens globally. Furthermore, it provides opportunity to curb frauds and corruption in governance. However, despite the success of security technologies designed to support secured communication as well as detect breaches in E-government systems, SEA exploits the "weakest link" vulnerability of people leading to improper protection of personal and confidential information in the systems. Nowadays, attackers recognized social engineering as one of the most effective ways of getting confidential information to break firewalls and overall software security easily irrespective of the technical security protection provided.

Advancement of E-government means more people are connected public services on the internet, which leads to increase in risk of falling victims of SEAs. SEA is one of the major challenges of implementing E-government services because attackers exploit the weakest link of human resources in the system. SE is a broad range of malicious activities by psychological manipulation of human interactions to trick E-government service consumers into releasing sensitive information mistakenly. As the technological protection for E-government system advance and become more robust, so also SE techniques increases exploitations of people by using both online and offline means of compromising unsuspecting citizens to give out secret information or transfer money. It is not possible to eliminate these threats, instead let's focus on detection and prevention strategies for the safety of E-government system. In order to achieve this, adequate knowledge and understanding on SE techniques play a crucial role in supporting citizens becoming victims of numerous categories of this attacks. The major SE attack techniques used to exploit E-government system include but not limited to Phishing, Baiting, Pretexting, Quid Pro quo, Honey Trap, Tailgating, Pharming, etc.

a) Phishing

Phishing is a SEA where users' username and password as well as sensitive information such as login credentials and credit card number are revealed to the attackers. Attackers interact with victims of phishing attacks by email, telephone or SMS message pretending as trusted entity to tactfully request for sensitive information. This kind of attackers usually contact many people with the hope that at least few target will fall victims to release their sensitive information. Advanced Phishing attacks leads victims to click or download an attachment containing malware, ransomware or malicious web sites. Phishing attack is the most common type of SEA and the common techniques of Phishing attack include Spear phishing, Smishing, Vishing, Whaling, etc. Spear Phishing targets a specific categories of people or groups within an organization. While, Vishing attackers uses phone calls or voice message, Smishing attackers uses text messages. Whereas, Whaling is a high-profile category of Spear Phishing that target senior executives and higher authorities. Although, the approaches of these categories of Phishing attackers differs, their aim largely remains the same.

b) Baiting

Baiting is an online or physical SEA that leverages on victims curiosity or greed. The attacker usually entice victims with promise of free gift, downloads or highly subsidized items. These attack aims at exploiting peoples' curiosity or greed, either physically but using online media or online by spreading malicious codes.

c) Pretexting

Pretexting is a category of SEA whereby attackers tries to convince the user by using a fake story to fool and persuade victims give out critical information or unauthorized access to system. The attacker usually impersonate someone in authority or has access right to the information pretending as someone to help the victim. Pretexting attackers often target cooperation that host users' data such as bank and credit card companies. Sometimes, the attacker seek for critical information by impersonating the client mostly using phone calls.

d) Quid Pro quo

Quid pro quo attack is a low-level attack that persuade victims to release sensitive information for technical service provision. The information sought enables hackers spread malware to victims' computers or gain unauthorized access to systems' resources. This is a simple SEA, since hackers only need to pretend as technical expert and make random spam calls to unsuspecting audience. Among the random calls, there are chances that some targets will accept the service offered by the hacker. Consequently, the attacker exploits the victims by obtaining money or crucial information such as bank details or login credentials.

e) Honey Trap

Honey trap is a category of SEA in which the attacker impersonate as an attractive person to establish a fake romantic relationship with unsuspecting users with the aim getting secret information. It is similar to Baiting attack, only that the hacker entice victims with romantic or sexual advances instead of curiosity or greed. Conversely, honey trap serves as an investigation techniques that leverages on the fidelity of a person by romantic or sexual liaison to discover secret information from criminals.

f) Tail Gating

Tail gating SEA is the passage of unauthorized user, either forcefully or unintentionally behind an authorized user enabling the hacker gain access to confidential information. In a nutshell, tail gating refers to getting access of restricted area unauthenticated by closely following an authorized person. It is a SE, principle that exploits human behaviours to use an authorized personnel credential to gain access to protect environment unauthenticated. Therefore, Tail gating attack is a physical SE attack that exploits human behaviours to use an authorized personnel's credential to gain access to protected environment unauthenticated. Therefore, Tail gating attack is a physical SE attack that can results in a huge lost to the organization through data breaches, theft, data manipulation and malware attacks, etc.

g) Pharming

Pharming attack is a category of SEA that redirects users to a fake website that looks like the real site. The danger of this SEA is that users are automatically redirected to fake web site that resembles real web site despite providing correct address of the legitimate web site.

Despite the difficulty of identifying SEAs, security awareness training is the most efficient tool of detecting and preventing all categories of SEA. An effective way of detection of SEA in E-government is nation-wide awareness training for recognizing common attacks. It is especially dangerous cybercrime that relies on human error instead of software vulnerability. The following are some measures of detection and prevention of SEAs in E-government system.

5.2 Detection of Social Engineering Attacks in E-Government System

Social engineers exploits peoples' trust by psychological manipulation of system users with aim of stealing money or getting confidential information. The following are ways to recognize social engineering attacks.

a) Education and Training

SE training help citizens recognize these and other categories of cyberattack as part of government security awareness programme. This is to groom responsible employees and patriotism as well as to better equip the populace with knowledge and skill for detection and protection from SEA. Due to lack of awareness of SEA, many employees share their confidential information with third parties, which leads to the attack. Consequently, government and organizations should educate people on the importance of keeping confidential data secured.

b) Technological Detection

Although, SE attacker do not require any technical skills in most of the SE techniques to operate a sophisticated attack. Implementation of technical solution by using game by [20] and NLP by machine learning and case-based reasoning system by [16] Therefore, research has shown that SEA can be detected by using technological means. Further studies toward technological approach for solution of SEA in E-government is recommended.

c) Natural Language Processing (NLP) Detection

NLP techniques can be applied for detection SEAs by evaluation of some key factor such as voice modulation, suspicious phrases, motives and targets of offline and online communication text by artificial intelligence method. This method can detect and flag conversation as SEA or not. This method leverage on the known characteristics of SEAs to technologically identify them in language of conversations.

d) Unusual or Unexpected Situation

SEAs mostly uses extraordinary messages in a way that is interesting, attractive, or impressive to unsuspecting system users. Attackers usually send many such unusual messages that should be of interest or appeal to at least small number of victims. Unusual or unexpected messages, attachment and links might be from potential malicious source. This kind of malicious messages looks irrelevant and do not match any message previously sent or requested. Therefore, scrutinize any unusual or unexpected massage or attachment very well before commitment and response. If you think the message is real, contact the sender using the real phone number, Email address or website to verify.

e) Force to make decision or take action on the spot

SE Attackers use language that requires victims act urgently to rush into action without thinking about it. Attackers exploits difficulty for many people to think quick and come up with a good response. Therefore, any interaction that requires urgent transfer of money is a sign of SEA. So, take time to ensure that the transaction you are about to conduct is legitimate.

f) Security Decision under Stress and Pressure

SE attackers normally put pressure on victims to make demands and persuade compliance urgently. Attackers exerts pressure on victims to act fast to avoid certain negative consequences. Due to the pressure, stress will be developed. Therefore, avoid decision under stress and pressure induced externally during interaction with unknown persons either synchronously or asynchronously.

g) Suspicious Messages and/or Attachments

Scammers usually send fake messages as a way of tricking unsuspecting users release their money or credentials information to gain access to victims email, bank or other accounts. Attackers use variety of ever-changing tricks such as fake stories, gift, cheap items or s services. They may send fake message claiming to solve some suspicious activity that happened to victim's account, which the scammer ask for some personal information from the victim or ask the victim to download malicious attachment. Therefore, Messages from unknown sender could be a scammer trying to steal confidential information. Consequently, any suspicious message or attachment should be treated with caution.

5.3 Prevention of Social Engineering Attacks in E-government System

a) Training and Awareness Programmes

Education and training for awareness on attackers' techniques is one of the most effective method of detecting as well as preventing SEAs generally.

b) Security policies

Security policy is generally regarded as one of the most critical aspect of protecting any information system. A good and realistic security policy and procedures should be in place for protection of SEA in E-government system.

c) MFA and Other Technical control

Implementation of multistage authentication and other technical security controls has proved to be a successful way of preventing SEA. This is because even if scammers succeed in compromising one verification stage, it still requires other authentications to gain access to organizations' network resources.

d) Preserve Confidential Information Secured

Basically, ability of safe keeping confidential information is the key requirement for prevention of SEA. Therefore, ensure all confidential information is kept secured both online and offline.

e) Suspicious Mails, Calls and Attachments detection

Learn ways to detect fake emails, call, links and attachment. Verify suspicious messages and calls by contacting the real organization or individual directly but not through the suspicious channel.

f) Cooperation and Team Work

Working together in cooperative manner enable people share knowledge and experience and further support each other to improve productivity as well as prevent SEA and other threats.

g) Scan for Malware

Modern SEAs spread malicious software (malware) infection or redirects users to malicious websites. Therefore, frequent malware scanning that find and removes malware in the systems is a critical preventive measure.

5. CONCLUSION :

The most effective way of detection as well as prevention of SEA in E-government system is nation-wide education and training for awareness on the techniques used in these attacks. Furthermore, research toward technological approach leveraging on NLP key factors such as unusual, unexpected and urgency terms to identify suspicious messages for solution of SEA in E-government system is recommended.

REFERENCES :

[1] Marczak, William R., and Vern Paxson. (2017). Social Engineering Attacks on Government Opponents: Target Perspectives. *Proc. Priv. Enhancing Technol.*, *1*(2), 172-185.
Google Scholar↗

[2] Abu-Shanab, E., & Bataineh, L. Q. (2014). Challenges facing e-government projects: how to avoid failure?. *International Journal of Emerging Sciences*, *4*(4), 207-217.
Google Scholar↗

[3] Chinta, M., Alaparthi, J., & Kodali, E. (2016). A Study on Social Engineering Attacks and Defence Mechanisms. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(1), 225-231.
Google Scholar↗

[4] Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering-based attacks in india to develop a conceptual model. *International Journal of Information and Network Security*, *1*(2), 45-53.
Google Scholar↗

[5] Ivaturi, K., & Janczewski, L. J. (2012). A Typology of Social Engineering Attacks-An Information Science Perspective. In *PACIS*. *1*(1), 145-160.
Google Scholar↗

[6] Burda, P., Allodi, L., & Zannone, N. (2021, September). Dissecting Social Engineering Attacks Through the Lenses of Cognition. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW)*. IEEE. *1*(1), 149-160.
Google Scholar↗

[7] Neupane, A., Satvat, K., Saxena, N., Stavrinos, D., & Bishop, H. J. (2018, December). Do social disorders facilitate social engineering? A case study of autism and phishing attacks. In *Proceedings of the 34th Annual Computer Security Applications Conference*. *1*(1), 467-477.
Google Scholar↗

[8] Weber, K., Schütz, A. E., Fertig, T., & Müller, N. H. (2020, July). Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users. In *International Conference on Human-Computer Interaction* Springer, Cham. *1*(1), 650-668.
Google Scholar↗

[9] Alavi, R., Islam, S., & Mouratidis, H. (2015, September). Human factors of social engineering attacks (SEAs) in hybrid cloud environment: Threats and risks. In *International Conference on Global Security, Safety, and Sustainability* Springer, Cham. *1*(1), 50-56).
Google Scholar↗

[10] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89-106.
Google Scholar↗

[11] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*(1), 113-122.
Google Scholar↗

[12] Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, *4*(6), 7533-7538.
Google Scholar↗

[13] Aldawood, H., & Skinner, G. (2019). A taxonomy for social engineering attacks via personal devices. *International Journal of Computer Applications*, *176*(50), 19-26.
Google Scholar↗

[14] Tsinganos, N., & Mavridis, I. (2021). Building and Evaluating an Annotated Corpus for Automated Recognition of Chat-Based Social Engineering Attacks. *Applied Sciences*, *11*(22), 1-23.
Google Scholar↗

[15] Lansley, M., Kapetanakis, S., & Polatidis, N. (2020, August). SEADer++ v2: Detecting Social Engineering Attacks using Natural Language Processing and Machine Learning. In *2020 International Conference on Innovations in Intelligent SysTems and Applications (INISTA)*, IEEE. *1*(1), 1-6.
Google Scholar↗

[16] Lansley, M., Polatidis, N., Kapetanakis, S., Amin, K., Samakovitis, G., & Petridis, M. (2019). Seen the villains: Detecting Social Engineering Attacks using Case-based Reasoning and Deep Learning. In *ICCBR Workshops*. *1*(1), 39-48.
Google Scholar↗

[17] Dorr, B., Bhatia, A., Dalton, A., Mather, B., Hebenstreit, B., Santhanam, S., ... & Strzalkowski, T. (2020, April). Detecting asks in social engineering attacks: Impact of linguistic and structural knowledge. In *Proceedings of the AAAI Conference on Artificial Intelligence*, *34*(5), 7675-7682.
Google Scholar↗

[18] Alzahrani, A. (2020). Coronavirus social engineering attacks: Issues and recommendations. *IJACSA*, *11*(5), 154-161.
Google Scholar↗

[19] Aladawy, D., Beckers, K., & Pape, S. (2018, September). PERSUADED: fighting social engineering attacks with a serious game. In *International Conference on Trust and Privacy in Digital Business.* Springer, Cham. *11033*(1), 103-118.
Google Scholar↗

[20] Goeke, L., Quintanar, A., Beckers, K., & Pape, S. (2019). PROTECT–an easy configurable serious game to train employees against social engineering attacks. In *Computer Security*. Springer, Cham. *1*(1), 156-171.
Google Scholar↗

[21] Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, *76(1)*, 101-127.
Google Scholar↗

[22] Nicholson, J., Coventry, L., & Briggs, P. (2017). Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, *1*(1), 285-298.
Google Scholar↗

[23] Bullée, J. W., Montoya, L., Junger, M., & Hartel, P. H. (2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. In *Proceedings of the Singapore Cyber-Security Conference (SG-CRC)* IOS Press, *1*(1), 107-114.
Google Scholar↗

[24] Koide, T., Chiba, D., & Akiyama, M. (2020, October). To get lost is to learn the way: Automatically collecting multi-step social engineering attacks on the web. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. *1*(1), 394-408.
Google Scholar↗

[25] Koide, T., Chiba, D., Akiyama, M., Yoshioka, K., & Matsumoto, T. (2021). To Get Lost is to Learn the Way: An Analysis of Multi-Step Social Engineering Attacks on the Web. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*. *104*(1), 162-181.
Google Scholar↗

[26] Tsinganos, N., Sakellariou, G., Fouliras, P., & Mavridis, I. (2018, August). Towards an automated recognition system for chat-based social engineering attacks in enterprise environments. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, *1*(1), 1-10.
Google Scholar↗

[27] Nelms, T., Perdisci, R., Antonakakis, M., & Ahamad, M. (2016). Towards measuring and mitigating social engineering software download attacks. In *25th {USENIX} Security Symposium ({USENIX} Security 16*(1), 773-789.
Google Scholar↗

[28] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31-38.
Google Scholar↗

[29] Mataracioglu, T., Ozkan, S., & Hackney, R. (2015). Towards a security lifecycle model against social engineering attacks: SLM-SEA. *arXiv preprint arXiv:1507.02458*. *1*(1), 1-10.
Google Scholar↗

[30] Pollock, T., Levy, Y., Li, W., & Kumar, A. (2020). Towards an Assessment of Judgment Errors in Social Engineering Attacks Due to Environment and Device Type. 2020 KSU Conference on Cybersecurity Education, Research and Practice, *3*(1), 1-22.
Google Scholar↗

[31] Aldawood, H., & Skinner, G. (2020). An Advanced Taxonomy for Social Engineering Attacks. *International Journal of Computer Applications*, *177*(30), 1-11.
Google Scholar↗

[32] Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, *48*(3), 1-39.
Google Scholar↗

[33] Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving awareness of social engineering attacks. In *Information Assurance and Security Education and Training*, *1*(1), 249-256.
Google Scholar↗

[34] Alavi, R., Islam, S., Mouratidis, H., & Lee, S. (2015, June). Managing Social Engineering Attacks-Considering Human Factors and Security Investment. In *HAISA*, *1*(1), 161-171.
Google Scholar↗

[35] Kostic, L. C. (2020). *Information security awareness techniques that reduce data breaches caused by social engineering attacks* (Doctoral dissertation, Capella University). *1*(1), 1-24.
Google Scholar↗

[36] Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic.*SN computer science*, *2*(2), 1-9.
Google Scholar↗

[37] Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in human behaviour*, *66*(1) 75-87.
Google Scholar↗

[38] Airehrour, D., Vasudevan Nair, N., & Madanian, S. (2018). Social Engineering Attacks and Countermeasures in The New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information*, *110*(9), 1-18.
Google Scholar↗

[39] Khlobystovaa, A., & Abramova, M. (2020, June). The models separation of access rights of users to critical documents of information system as factor of reduce impact of successful social engineering attacks. In *Russian Advances in Fuzzy Systems and Soft Computing: Selected Contributions to the 8th International Conference on "Fuzzy Systems, Soft Computing and Intelligent Technologies (FSSCIT 2020)". Smolensk, Russia*. *1*(1), 264-268.
Google Scholar↗

[40] Shi, Z. R., Schlenker, A., Hay, B., & Fang, F. (2019). Towards thwarting social engineering attacks. *CoRR, abs/1901.00586*. *19*(1), 1-8.
Google Scholar↗

[41] Zhao, Y. P., Chen, X., Miao, X. H., Tan, Y. R., & Song, X. Y. (2021). Never forget where you started: to prevent pre-retirement corruption at China's state-owned enterprises. *Emerging Markets Finance and Trade*, *57*(5), 1380-1398.
Google Scholar↗

[42] Al-Khouri, A. M. (2011). An innovative approach for e-government transformation. *arXiv preprint arXiv:1105.6358*. *1*(1), 22-43.
Google Scholar↗

[43] Al-Shboul, M., Rababah, O., Ghnemat, R., & Al-Saqqa, S. (2014). Challenges and factors affecting the implementation of e-government in Jordan. *Journal of Software Engineering and Applications*, *7*(13), 1111-1127.
Google Scholar↗

******