International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362
IJARST

A SYSTEMATIC EVALUATION OF RESEARCH ON SOCIAL ENGINEERING ATTACKS PREVENTION

D.MAHESH
Master of Computer Applications (MCA),
SVKP & Dr.K.S.Raju Arts & Science College(A),
Achanta ,W.G.Dt.,A.P, India.
dongamahesh159@gmail.com

P SRINIVASA REDDY
Associate Professor in Computer Science,
SVKP & Dr.K.S.Raju Arts & Science College(A),
Penugonda,W.G.Dt.,A.P.India.
psreddy1036@gmail.com

ABSTRACT:

Social engineering is a method of information security that allows for system or network access. When victims are unaware of techniques, models, and frameworks to prevent them, social engineering attacks happen. In order to stop social engineering attacks, the current research describes user studies, constructs, assessment, concepts, frameworks, models, and techniques. Sadly, there isn't any specific prior research on mitigating social engineering attacks that thoroughly and efficiently analyzes it. Health campaigns, human security sensor frameworks, user-centric frameworks, and user vulnerability models are examples of current social engineering attack prevention techniques, models, and frameworks. Guidance is required to examine cybersecurity as super-recognizers, possibly acting as police for a secure system, for the human as a security sensor architecture. This research aims to critically and systematically analyze earlier material on social engineering attack prevention strategies, models, and frameworks. Based on Bryman & Bell's methodology for conducting literature reviews, we carried out a systematic review of the available research. Using a protocol, we discovered a novel strategy to stop social engineering assaults in addition to approaches, frameworks, models, and assessments, based on our review. We discovered that the protocol can successfully stop social engineering assaults, including health campaigns, the susceptibility of social engineering victims, and co-utile protocol, which can control information sharing on a social network. This comprehensive evaluation of the research is what we're presenting in order to suggest safeguards against social engineering assaults.

KEYWORDS: Security Sensor Framework ,user-Centric Framework, Social Engineering Victims,Social Engineering Attacks.

.INTRODUCTION

Attacks on the weakest link are how social engineering tricks its victims. A victim must have an unequal knowledge relationship with the attacker for social engineering to work, and the attacker utilizes this asymmetry to impose technocratic control over the victim. People with specialized technical expertise, such as those in dentistry or financial planning, are known as technocrats. When certain individuals or groups are significantly more knowledgeable and satisfied than others in a given field of knowledge, this is known as asymmetric knowledge. For more information on social engineering assaults from 1842 to the present, see Hatfield . Since this work solely discussed the evolution theory of social engineering, it is only somewhat useful.

A social engineering attacker is someone who seeks to get access to confidential data or money. When influencing the victim, the assailant will create suffering to get around, alerting the victim of their vindictive intent. According to The National Institute of Standards and Technology (NIST), social engineering refers to a strategy used to attack systems or networks by persuading someone to give information (such as a password). The ability to persuade or deceive a target into divulging personal information is essential for the success of social engineering assaults .

Attacks by social engineers now take the form of phone calls, emails, and in-person meetings. Impersonation, assaults on social media or online communities, automated social engineering, and semantic attacks are all examples of social engineering attack techniques. Along with the growth of information technology, several forms of social engineering are emerging. Previous study on human manipulation discovered that offenders mentally influenced or misled workers, for instance, through social engineering and phishing assaults, into making security mistakes or disclosing critical information. Phishing and pretexting were cited as the two most common instances in Verizon's data breach investigation report . Social engineering assaults are two of these kinds of attacks, therefore they continue to exist till they succeed in victimizing people. Online frauds cyberbullying, sharing of unfavorable,images or texts, privacy communication , and non-financial disclosure component are further examples of social engineering attacks that can occur online.

Social media ethics of social engineering penetration testing , a human as a security sensor framework , a personality information processing model, a characteristic user framework , game-based analysis , and predicting individuals' vulnerability , computer security policy , and cyber security are some methods used to prevent social engineering attacks.

Security and privacy were discussed in another study . presented a topic for study on behavioral aspects of cyber security. View the most recent analysis of the Sybil assault on social networks in .

This assessment of the literature provided up-to-date defenses against assaults, including health campaigns to fend against social engineering attempts, psychological consequences of various methods, and widespread awareness of such attacks . But the findings of this earlier study were not explained. Penetration testing can defend against social engineering assaults, but it shouldn't merely be seen as a partial examination of the wider ethics of social engineering in cyber operations . One of the most important links in the detection chain for deception-based attacks can be a human; in addition, study may look into whether cyber security can gain from "super-recognizers" in a similar way to how policing works .

Users can avoid methodological errors by using models for cautious behavior and risk perception. The literature included suggestions for behavioral interventions to increase Facebook users' security and privacy. Future studies should take into account this problem as a predictor of perceived risk and preventive behavior .

The issue with this study is that it assumes that social engineering assaults can be prevented by taking certain precautions. For the identification of harmful information, there is no solution that is connected to Sánchez's study. An organized examination of the literature on techniques and frameworks for avoiding social engineering scams and practically locating bad material will address this issue. This review's reference material was released between 2018 and 2021. Fig. 1 displays the research summary. The following is the format for this literature review. In Section II, the comprehensive literature review for preventing social engineering assaults is explained. The approach is explained in Section III. The outcomes of this comprehensive literature review are described in Section IV. The conclusions of this article are presented in Section V.

□.LITERATURE SURVEY

The prevention of social engineering assaults has received very little attention from researchers. However, social engineering tactics are dangerous and may cost the business a great deal of money. Using the Multivocal Literature Review (MLR) method, Hijji and Alam examined social engineering assaults committed during the Covid-19 epidemic. During the Covid-19 epidemic, Hijji and Alam analyzed the methods, strategies, and platforms employed . MLR combines research findings with practitioner viewpoints. The MLR done by Hijji and Alam contains shortcomings in terms of discussion, such as source criteria from a practitioner's perspective and study outcomes that are not described in more depth. According to Hijji and Alam, credible reports, blogs, websites, whitepapers, and periodicals make up a practitioner's viewpoint criterion. Only Google search, Google Scholar, and Scopus are available for study findings. Bulle and Junger analyzed social engineering assaults by looking into ways to lessen their impact. The review was carried out via meta-analysis. To quantitatively synthesize study results, the meta-analysis integrates review findings and statistical approaches. The requirement for publications to be included for review is that they must examine experimental designs created to lessen the susceptibility of social engineering assaults. Bulle and Junger's research has a constraint because it only looks at nations classified as Western, Educated, Industrialized, Rich, and Democratic (WEIRD) . The failure to find the intervention owing to more precise research criteria means that Bulle and Junger's study did not completely achieve its intended goal. An analysis of the defense tactics used to thwart social engineering attempts is done by Schab et al. Social psychology and information technology security experts' perspectives are combined in the literature cited by Schaab et al. Authority, Social Proof, Liking, Similarity, Deception, Commitment, Reciprocation, Consistency, and Distraction are just a few of the social psychology categories Schab et al. categorized the papers under. Schaab et al., on the other hand, didn't carry out a more thorough study since they didn't apply the same technique as Hijji and Alam when doing their literature review. Schaab et al. only employed social psychology as a preventative measure in their defense against the social engineering onslaught. Social engineering is reviewed by Yasin et al. in two categories: the sort of assault and the persuasive method utilized. In order to describe how social engineering assault actions are carried out, Yasin et al. also integrate many ideas. However, Yasin et al. did not specify how users could apply preventative tactics against the many kinds of assaults and persuasive strategies utilized by social engineering attacks. Therefore, when it comes to technical advice for countering social engineering assaults, Schaab et al.'s study is superior to that of Yasin et al. Four categories—attacks, categorization, detection techniques, and preventative methods—were examined in a social engineering review by Salahdine and Kaabouch . Salahdine and Kaabouch employed the same review methodology as Schaab et al., they only divided it into different categories. But the work by Schaab et al. stands out because it compares assaults and social engineering attack avoidance methods from both a technical and psychological standpoint. Briefly outlined here are the benefits and drawbacks of social engineering attack prevention approaches. The sorts of social engineering and their difficulties were evaluated by Wang et al. and Wang et al . the findings of a review carried out by Wang et al.

□.PROBLEM STATEMENT

Using the Multivocal Literature Review (MLR) method, Hijji and Alam examined social engineering attacks that occurred during the

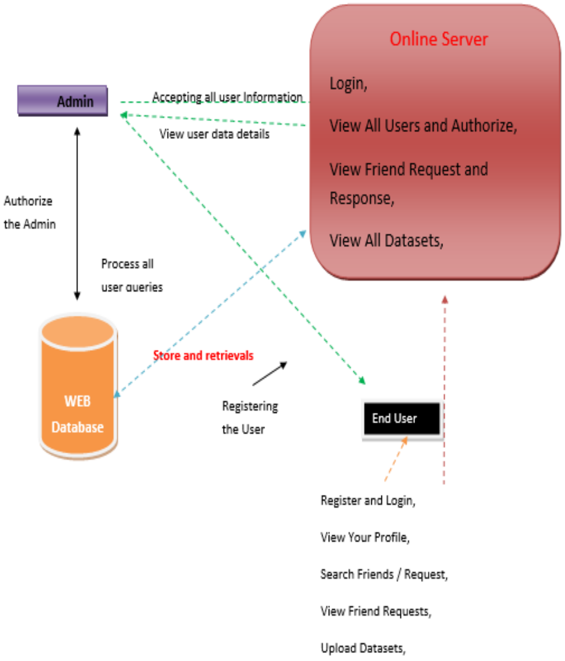
Covid-19 pandemic. Hijji and Alam analyzed the methods,

strategies, and platforms employed during the Covid-19 epidemic . MLR combines research findings with practitioner viewpoints. The MLR conducted by Hijji and Alam contains shortcomings in terms of discussion, such as source criteria from a practitioner's perspective and study outcomes that are not described in more depth. According to Hijji and Alam, credible reports, blogs, websites, whitepapers, and periodicals make up a practitioner's perspective criteria. Only Google search, Google Scholar, and Scopus are available for study findings.

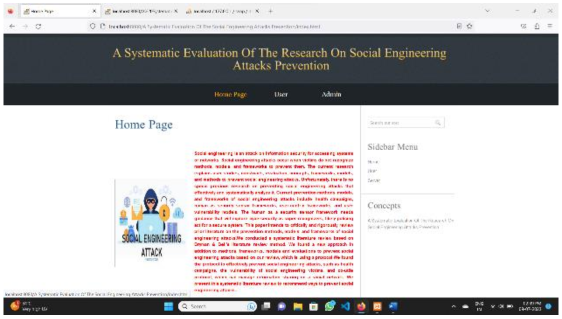
Bulle and Junger examined methods to lessen the effects of social engineering attacks when reviewing social engineering attacks. The evaluation was carried out using meta-analysis. To quantitatively synthesize research results, the meta-analysis integrates review findings and statistical approaches. The requirement for the articles under consideration was that they must examine experimental designs created to lessen the susceptibility to social engineering attacks. Bulle and Junger's research has a constraint because it only looks at nations classified as Western, Educated, Industrialized, Rich, and Democratic (WEIRD). Bulle and Junger's study has another drawback in that the investigation's goal was not fully met because the intervention could not be detected using more precise research criteria.The protection method against social engineering attacks is reviewed by Schab et al. Practitioners of information technology security and social psychology are reflected in the literature cited by Schaab et al. The publications were categorized by Schab et al. into categories related to social psychology, including Authority, Social Proof, Liking, Similarity, Deception, Commitment, Reciprocation, Consistency, and Distraction.

Schaab et al., on the other hand, did not carry out a more thorough assessment since they did not apply the Hijji and Alam-style methodology for conducting literature reviews. Schaab et al. limited their social psychology-based attack defense technique to social psychology prevention.Yasin et al. categorize social engineering into two categories: assault style and persuasion method . To further describe how social engineering assault actions are carried out, Yasin et al. incorporate a number of hypotheses.

□.ARCHITECTURE DESIGN



SCREENS

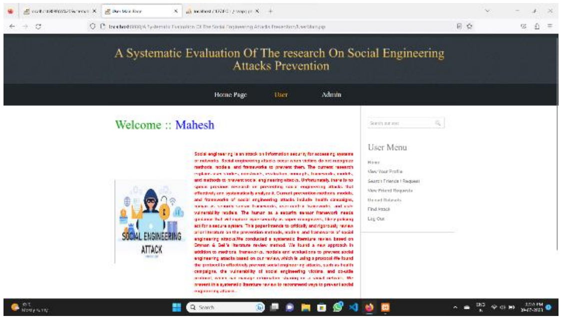


A Systematic Evaluation Of The Research On Social Engineering Attacks Prevention

Home Page

Social engineering is an attack on information security for accessing systems or networks. Social engineering attacks occur when victims do not recognize methods, models, and frameworks to prevent them. The current research explores case studies, constructs, evaluation, concepts, frameworks, models, and methods to prevent social engineering attacks. Unfortunately, there is no special previous research on preventing social engineering attacks that effectively and systematically analyze it. Current prevention methods, models, and frameworks of social engineering attacks include health campaigns, human as security sensor frameworks, user-centric frameworks, and user vulnerability models. The human as a security sensor framework needs guidance that will explore systematically as [illegible], like a policing act for a secure system. This paper intends to critically, and rigorously review prior literature on the prevention methods, models, and frameworks of social engineering attacks.We conducted a systematic literature review based on [illegible]'s literature review method. We found a new approach in addition to methods, frameworks, models and evaluations to prevent social engineering attacks based on our review, which is using a protocol. We found the protocol to effectively prevent social engineering attacks, such as health campaigns, the vulnerability of social engineering victims, and co-utile protocol, which can manage information sharing on a social network. We present this systematic literature review to recommend ways to prevent social engineering attacks.

A Systematic Evaluation Of The Research On Social Engineering Attacks Prevention



A Systematic Evaluation Of The research On Social Engineering Attacks Prevention

Welcome :: Mahesh

Social engineering is an attack on information security for accessing systems or networks. Social engineering attacks occur when victims do not recognize methods, models, and frameworks to prevent them. The current research explores user studies, constructs, evaluation concepts, frameworks, models, and methods to prevent social engineering attacks. Unfortunately, there is no [illegible] research on preventing social engineering attacks that effectively and systematically analyze it. Current prevention methods, models, and frameworks of social engineering attacks include health campaigns, [illegible] frameworks, and user vulnerability models. The human as a security sensor framework needs guidance that will [illegible], like a policing act for a secure system. This paper intends to critically and rigorously review prior literature on the prevention methods, models, and frameworks of social engineering attacks.We conducted a systematic literature review based on Okoli & Dal's literature review method. We found a new approach in addition to methods, frameworks, models and evaluations to prevent social engineering attacks based on our review, which is using a protocol We found the protocol to effectively prevent social engineering attacks, such as health campaigns, the vulnerability of social engineering victims, and co-utile protocol, which can manage information sharing on a social network. We present it in a systematic literature review to recommend ways to prevent social engineering attacks...

□.CONCLUSION

Previous studies have created frameworks and procedures for preventing social engineering attacks, yet these attacks are remain unpredictable for unsuspecting victims. Social engineering attack tactics can be modified to fit different situations and actors, particularly in social media or social network contexts.

Based on this comprehensive review of the literature, research on a protocol to prevent information sharing over social networks, seven user studies, three studies about social engineering attacks prevention concepts, two studies about other concepts, a study on the model for preventing social engineering attacks, six studies about framework construct, one study about framework dimensions, and two studies about social engineering attacks prevention framework.

The three primary areas of research in the approach to preventing social engineering attacks include user vulnerability of social engineering victims, health campaigns to thwart social engineering assaults, and co-use protocol to safeguard information disclosure on social media. The audience reach and campaign content are what determine the best methods for health campaigns. Both the adult and teen campaigns used different strategies.

The campaign's goodness factor also helped to lessen the risk of social engineering assaults. The model of user susceptibility to being a victim of social engineering might utilize some social network knowledge recommendations. This methodology was also used to examine user vulnerability based on user response risk assessment. This model's testing was done in order to breach privacy restrictions or distribute private and confidential information on social networks. Cooperative protocols might facilitate information sharing among social media users and include user reputation to reduce individuals' reluctance to provide their personal information to others.

Our study revealed various works that can aid in the avoidance of social engineering assaults. Practitioners and information security professionals can utilize the reviews we discovered to thwart social engineering attempts. They are able to carry out development based on a cooperation of many techniques, such as protocols, methodologies, frameworks, models, and assessments to stop social engineering assaults.

□.REFERENCES

[1] A. Yasin, R. Fatima, L. Liu, A. Yasin, and J.Wang, ``Contemplating social engineering studies and attack scenarios: A review study,'' *Secur. Privacy*,vol. 2, no. 4, pp. 1_14, Jul. 2019.

[2] S. M. Albladi and G. R. S. Weir, ``Predicting individuals' vulnerability to social engineering in social networks,'' *Cybersecurity*, vol. 3, no. 1, 2020.

[3] Y. M. Yusof and D. Singh, ``Civil servants awareness guideline towards computer security policy: A case study at the manpower department,ministry of human resources,'' *Asia_Paci_c J. Inf. Technol. Multimedia*,vol. 10, no. 8, pp. 86_99, 2021, doi: 10.17576/apjitm-2021-1001-08.

[4] M. A. Pitchan, S. Z. Omar, and A. H. A. Ghazali, ``Amalankeselamatan siberpengguna

internet terhadapbulisiber, pornogra_, E-mel phishingdanpembeliandalamtalian," *JurnalKomunikasi, Malaysian J. Commun.*,vol. 35, no. 3, pp. 212_227, 2019.

[5] P. van Schaik, J. Jansen, J. Onibokun, J. Camp, and P. Kusev, ``Security and privacy in online social networking: Risk perceptions and precautionary behaviour," *Comput. Hum. Behav.*, vol. 78, pp. 283_297, 2018.

[6] B. DasGupta, N. Mobasheri, and I. G. Yero, ``On analyzing and evaluating privacy measures for social networks under active attack," *Inf. Sci.*,vol. 473, pp. 87_100, 2019.

[7] D. Sánchez, J. Domingo-Ferrer, and S. Martínez, ``Co-utile disclosure of private data in social networks," *Inf. Sci.*, vol. 441, pp. 50_65, 2018.

[8] Z. Zhang and B. B. Gupta, ``Social media security and trustworthiness:Overview and new direction," *Future Gener. Comput. Syst.*, vol. 86,pp. 914_925, 2018.

[9] C. Zhang, H. Jiang, X. Cheng, F. Zhao, Z. Cai, and Z. Tian, ``Utility analysis on privacy-preservation algorithms for online social networks: An empirical study," *Pers. Ubiquitous Comput.*, vol. 25, no. 6, pp. 1063-1079,2021.

[10] R. A. M. Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, ``Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3,no. 1, p. 10, Dec. 2020.

[25] S. P. Velayudhan and M. S. B. Somasundaram, ``Compromised account detection in online social networks: A survey," *Concurrency Comput.,Pract. Exper.*, vol. 31, no. 20, pp. 1_15, Oct. 2019.

ABOUT AUTHORS:

D.MAHESH

currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. His research interests include Data Structures, Web Technologies, Data Science and Artificial Intelligence.

P.SRINIVASA REDDY is working as Associate Professor in SVKP & Dr K S Raju Arts & Science College(A), Penugonda , West Godavari District, A.P. He received Master’s Degree in Computer Applications from Andhra University. His research interests include Operational Research, Probability and Statistics, Design and Analysis of Algorithm, Big Data Analyti