International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-8, July 2023

Spear Watch: A Thorough Examination to Identify Spear Phishing Attacks

Anjali Shrikant Shukla, Sameer Rajendra Chavan, Srivaramangai R

Abstract: ***A form of cybersecurity assault known as phishing involves hostile actors sending messages while posing as a reliable individual or organization. Spear-phishing assaults target a particular victim, and communications that pretend to be from someone they know and contain personal information are updated to address that victim directly. Spear-phishing takes more planning and effort to complete than phishing. Because these attacks are so skillfully customised, conventional security measures often cannot stop them. They are consequently getting harder to find. Spear phishing emails generally require a sophisticated security protocol, including the deployment of threat detection and response tools. Numerous research works apply newer techniques to such systems. Most of them utilise AI and ML algorithms to identify threats and take necessary actions. This paper emphasises the importance of developing more advanced techniques through research and development. To start with, this work focuses on exploring various detection techniques, utilising machine learning and natural language processing algorithms, particularly in behaviour analysis and anomaly detection. This paper lays a foundation for future research in this area.***

Keywords: Spear Phishing, Social Engineering, Email Analysis, Link Analysis, Email Content Analysis, Attack Detection, Malicious Emails, Fraudulent Emails.

I. INTRODUCTION

Phishing is one type of cyber-attack in which an attacker impersonates a reliable firm or individual to deceive people into disclosing confidential information, such as passwords and credit card numbers. Phishing attacks commonly occur through email, but they can also be delivered via text messages, phone calls, or even social media platforms. Phishing is a method used to trick individuals into providing their personal information or clicking on malicious links that lead to fake websites.

Spear phishing is a type of cyber-attack that aims to target individuals or organisations with personalised and highly targeted emails or messages.

Manuscript received on 30 June 2023 | Revised Manuscript received on 08 July 2023 | Manuscript Accepted on 15 July 2023 | Manuscript published on 30 July 2023.
*Correspondence Author(s)
Anjali Shrikant Shukla, Department of Information Technology, University of Mumbai, Mumbai (Maharashtra), India. E-mail: anjalis2414@gmail.com
Sameer Rajendra Chavan, Department of Information Technology, University of Mumbai, Mumbai (Maharashtra), India. E-mail: sameerrchavan16@gmail.com
Srivaramangai R*, Department of Information Technology, University of Mumbai, Mumbai (Maharashtra), India. E-mail: rsrimangai@gmail.com, ORCID ID: 0000-0003-2723-6067

Unlike regular phishing attacks, which are typically sent to a large number of recipients generically, spear phishing attacks are carefully crafted to target specific individuals or groups by exploiting their personal information, interests, or relationships.

The term spear phishing is derived from the concept of using a spear to target a specific victim. Attackers often conduct extensive research on their targets to gather information from various sources, including social media profiles, public databases, and company websites. This information enables them to produce effective and customized messages that seem genuine and trustworthy. Spear phishing attacks can take different forms, including emails, instant messages, or even phone calls.

The messages may appear to be from a trusted source, such as a colleague, a superior, a bank, or a reputable company, making it complicated for the recipient to identify them as malicious. The ultimate purpose of spear phishing attacks is to deceive the individuals targeted into performing specific activities, such as clicking on a malicious link, downloading a malware-infected attachment, or disclosing sensitive information like login credentials or financial details. By gaining access to such information, attackers may penetrate systems, steal data, commit identity theft, launch further attacks, or compromise the security of an entire organization. To protect against spear phishing attacks, individuals and organisations should exercise caution and follow the steps provided by cybersecurity experts. This includes being aware of opening emails or messages from unknown sources, verifying the authenticity of requests for sensitive information, regularly updating and patching software and systems, using strong and unique passwords, and implementing multi-factor authentication. Additionally, cybersecurity awareness training can help educate individuals about the risks of spear phishing, both on an individual and organisational level, by teaching them how to recognise and respond to suspicious messages. It's essential to note that while technology can help mitigate spear phishing attacks, human awareness and diligence play a crucial role in preventing successful attacks.

Email Phishing has become the primary method for gaining data, unauthorised access, and distributing malware. Figure 1, provided below, illustrates a rise in the use of different archive file formats as malicious individuals attempt to conceal harmful payloads.

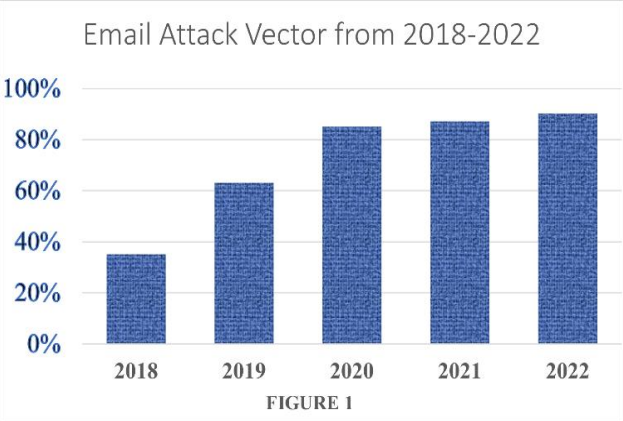

Figure 1: Graph showing the Trend of Email Attacks

II. RELATED WORK

One of the most dangerous fraudulent activities that affects everyday financial transactions is phishing, which involves using social engineering tactics to deceive people and obtain sensitive data such as credit card details, usernames, and passwords. The various ways in which phishing affects online banking and the implementation of effective safety measures. S. Kumudha et.al [1], found that scams in the e-banking sector fall under the category of cyber-deception. Cyber-deception encompasses malicious behaviours like theft, intellectual property infringement, and credit card fraud. The study provides an overview of e-banking and examines various cybercrimes identified explicitly in the banking sector. The financial system is the backbone of the economy, and nowadays, it heavily relies on information technology. The economic system serves as the backbone of the economy, and its reliance on information technology highlights the need to prevent cybercrime through robust authentication, identification, and verification techniques in electronic banking transactions. Although eliminating cybercrime from the internet may seem impossible, it is feasible to closely monitor banking transactions and activities regularly. Individuals need to remain highly vigilant when conducting online banking transactions involving money transfers. Dhruv Rathee et.al [2], present an overview and analysis of several perspectives on the identification of legitimate phishing emails. We found the objective of this research is to explore machine learning (ML) and deep learning (DL) methodologies for effectively identifying phishing emails. Criminals often invest considerable effort in making their emails appear authentic by using believable language, graphical interfaces, and logos. However, phishing emails can be distinguished from genuine ones as they are specifically crafted to achieve their malicious goals. The literature describes various types and variations of phishing emails. Machine learning-based approaches have proven to be more effective in recognising phishing attacks, as they offer lower false-positive rates and higher precision compared to other strategies. The findings suggest that further advancements are needed to leverage modernized DL techniques in studies on detecting phishing emails, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Deep Reinforcement Learning models. Among the various risks associated with online banking, phishing attacks pose a significant threat to both banks and users who fail to implement adequate security precautions. Phishing hackers employ sophisticated methods, ranging from deceptive tactics to DNS attacks, necessitating regular updates to security measures by banks. Numerous research studies have identified security issues like "phishing attacks" as tools employed by hackers to compromise e-banking customers' accounts, Alhuseen O. Alsayed et.al [3]. Defending against phishing attacks involves strategies such as using personalised emails and websites, utilising security software, implementing two-factor authentication, and enhancing customer awareness. The significant impact of phishing compared to other similar methods, emphasizes the potential severe losses it can cause to clients and institutions. N.P. Singh [4] investigates global trends in phishing activities, particularly in the financial sector. The author also examines the reasons behind the increase in phishing attacks, various types of phishing methods, and the process of phishing. Online banking frauds include hoax emails, job scams, computer viruses, spyware, identity theft, phishing, vishing & smishing. Phishing techniques are categorised into four primary methods: the Dragnet Method, Lobsterpot Method, Rod-and-Reel method, and Gillnet phishing. Kara Ilker [5], Focuses on phishing attacks, which aims to swiftly and conveniently extract necessary information from victims through deception, fear, curiosity, or excitement. This study focuses on detecting and analysing phishing attempts in the context of e-banking, proposing a methodology for achieving this goal. The author aims to combat such crimes targeting e-banking through these detection efforts. The analysis findings in the paper indicated that the attacker's information was accessible. Additionally, the analysis of the selected real sample for the study unveiled the availability of the phishing website's content, the attack strategy, and information about the attacker. The approach followed in this paper demonstrates a viable alternative technique that can be applied to e-banking research and the detection of phishing attacks. Deep learning methods, specifically Convolutional Neural Networks (CNN), can contribute to the detection and analysis of large-scale phishing attacks in the field. Providing a clear understanding of phishing as a form of cybercrime that aims to deceive individuals into revealing personal and/or financial information or transferring money directly to the attacker. The analysis of the attack vector considers both social engineering and technical aspects. A typical phishing attack involves three main elements: the lure, the hook, and the catch. To address the issue of phishing, a heuristic approach is recommended, which requires user education, technological advancements, and process engineering. Method of detection is classified into two categories: human detection and machine detection. Junaid Ahsenali Chaudhry et.al [6]. Phishing has emerged as a significant concern in network security, leading to billions of dollars in financial losses for both consumers and e-commerce companies. As a result, trust in e-commerce has diminished among regular consumers. To respond to this issue, Mr. N. Revathy et.al [7] have proposed an anti-phishing algorithm called Link-Guard which was developed on identified characteristics.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The primary objective of the Link-Guard algorithm is to identify phishing emails sent by attackers, thereby safeguarding end-user information. The algorithm was created after carefully analysing the attributes of phishing hyperlinks, as the author states. One of the key advantages of Link-Guard is its characteristic-based approach, which allows it to detect not only known phishing attacks but also unknown ones. Additionally, Link-Guard offers protection against malicious or unsolicited links found in web pages and instant messages, making it a versatile solution. Although the authors have implemented this approach by considering URL and domain identity criteria, there is scope for further refinement and the inclusion of additional criteria in future work. Radha [8] focuses on raising awareness about phishing issues and explores the utilization of various anti-phishing tools such as ANTI-PHISHING Devices, Security Instruments - Netcraft, ESET SECURITY, and others. Phishers employ tactics like sending seemingly legitimate emails from government agencies and financial institutions to obtain personal information or unknowingly install malware on users' computers. Currently, there are several types of phishing attacks, including deceptive phishing, malware-based phishing, and DNS-based phishing (also known as content injection phishing). To address these issues, an anti-phishing browser plug-in is discussed. This plug-in monitors sensitive information and generates a warning when a user attempts to enter such data on a website that has previously been associated with another reputable website. This proves effective in cases where users unintentionally enter their banking login details on a phishing site. However, it should be noted that the anti-phishing tool may also flag legitimate reuse of credentials as suspicious, presenting a potential drawback. Bashir et.al [9] in their work have addressed the following question: “how can an Antiphishing solution be developed that can automatically detect phishing websites based on their visual appearance, patterns, and common characteristics, without relying on frequent updates or maintaining a database of previous phishing sites?”. Relying solely on data mining classification algorithms for this purpose has been found to have a high error rate. Fadare et.al [10] have found a battle against phishing attacks, which will possibly increase the trust between customers and banks relation and even helps to gain new customers. Banks have recognised the crucial role of KM in gaining a competitive edge in the field of risk management, fraud prevention, and ensuring compliance. The purpose of KM is to acquire knowledge more skillfully and proficiently. The integration of KM into internet banking actions facilitates a more accurate understanding of KM as an enabler of information strategy, specifically for the internet banking platform. Hence, KM can be used as a way to help internet banking users defend themselves against attacks. An exploratory assessment of Phishing, Smishing and Vishing attacks against mobile devices is done by Ezer Osei Yeboah-Boateng et.al [11]. The implications of end-user behaviour towards mitigating the risks posed by using mobile devices for online services and facilities. The purpose of this research was to identify the many dangers that affect mobile devices, as well as how end users react to and perceive such threats. Users were also found to be unaware of the frequent phishing attempts made against their mobile devices. Finally, the taxonomy of ‘alluring’ and ‘decoying’ words used in phishing attacks could serve as a benchmark for end-users to guard against becoming cyber-victims. It comprises investigating various types of mobile device attacks. The samples were purposively selected from friends, family, office colleagues, and university students. The operating systems for the chosen sample mobile devices were limited to the most common ones: Microsoft Windows, Android, and iOS. The current issue is preventing cyberattacks in the banking industry, specifically within the realm of e-banking. Fadare et.al [12] propose a scientific demonstration illustrating a method to combat e-banking fraud. The proposed model is based on the classic Lotka-Volterra model with the Holling-Tanner dynamic model. Through simulation experiments using the constructed model, it was observed that the occurrence of a saddle case and a line of stable fixed points is improbable in real-life scenarios. This is due to the implication that, after each successful fraud attempt, at least one new attack must emerge; however, in practice, it is more common for multiple attacks to occur. The most probable scenarios are a stable node and a stable degenerate node. Brad Wardman et.al [13] explains that phishers continuously modify the source code of their phishing web pages to mimic changes in legitimate websites and avoid being detected by anti-phishing measures. This study utilizes file-matching algorithms to determine if a new file or set of files can be classified as a phishing web page. The focus of this research is on achieving efficient runtime performance. Various file matching and string alignment techniques were tested, including Main Index File MD5 matching, Deep MD5 Matching, phishDiff, context-triggered piecewise hashing using ssdeep, and a novel algorithm called Syntactical Fingerprinting. We studied that PhishDiff and ssdeep-based methodologies require additional information to find comparable candidate files, as running them without this information would be time-consuming and impractical. The research experiments in the paper showcased the effectiveness of several string-matching algorithms in quickly and accurately identifying phishing websites based on their content. According to the author, the techniques mentioned in the paper were tested on various sets of phishing websites, yielding a detection outcome of 90%, with manageable false positive rates. Rachna Dhamija et.al [14] explore the topic of authenticating websites in the context of phishing attacks. Phishing presents a significant challenge in terms of usability and security, as both system designers and attackers leverage user interfaces to influence users. To address this issue, a novel approach called Dynamic Security Skins is proposed. This approach allows a remote web server to demonstrate its authenticity in a manner that is easily verifiable by users and difficult for attackers to imitate. The Mozilla platform was selected for its openness and flexibility. The standard Mozilla browser interface, along with our extension, was developed using Mozilla's XML-based User Interface Language (XUL), a markup language for defining user interface components.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In this section, the authors provide an overview of their solution and subsequently delve into detailed explanations of each component. Engin Kirda et.al [15] introduce a new browser extension called AntiPhish, which aims to safeguard users from phishing attacks that occur on spoofed websites. The existence of automated form-filling applications influenced the development of AntiPhish. Popular browsers, such as Mozilla and Internet Explorer, offer built-in features that allow users to store and automatically fill form contents if desired, requiring a master password for access. The prototype of AntiPhish was implemented as a Mozilla browser extension or plug-in, utilising the Mozilla XML User Interface Language (XUL) and JavaScript. The AntiPhish implementation for Mozilla is lightweight, consisting of approximately 900 lines of JavaScript code and 200 lines of XUL user interface code. While the best approach to prevent phishing is to educate users about not clicking on random links and entering sensitive information such as passwords, it is unrealistic to expect that all users will fully grasp the phishing threat and navigate the web accordingly. There will always be users who fall victim to visiting phishing websites. A new method is proposed to address the issue of uncertainty in evaluating e-banking phishing websites, presenting an intelligent, robust, and efficient model for detecting such websites. The model utilizes fuzzy logic in conjunction with data mining algorithms to analyze the characteristics of e-banking phishing websites and classify different types of phishing attacks, Maher Aburrous et.al [16]. It also establishes six attack criteria for e-banking phishing websites through a layered structure. An approach for identifying phishing URLs using the Gated Recurrent Unit (GRU), a fast and accurate method for classifying phishing attempts by Mousa Tayseer Jafar et.al [17]. Phishing websites have become a growing concern in the online world. Phishing involves fraudulent attempts to deceive individuals by impersonating legitimate institutions and tricking them into revealing sensitive information, such as passwords and bank account numbers. The proposed approach involves analysing website URLs by extracting features using a lexical method. The GRU classifier is then trained on a dataset containing both malicious and benign URLs. The experiments conducted in this research utilize the powerful GRU model to detect suspicious websites based on features extracted from the URLs. The focus paper is on leveraging the gate mechanism to enhance the model's speed in identifying phishing URLs. E. Konda Reddy et.al [18] said that phishing is a modern type of scheme in which attackers create a replica of an existing webpage to deceive users into providing personal, financial, or password information, thinking they are interacting with their trusted service provider's website. Link Guard algorithm, which is employed to identify phishing emails sent by phishers and protect end users' information. The system implements the Link Guard algorithm as shown in Figure 2, a host-based algorithm that effectively detects and prevents both known and unknown phishing attacks. Being characteristic-based, Link Guard can identify and prevent not only known phishing attacks but also unknown ones. The project utilizes Java technologies and Oracle for its implementation.

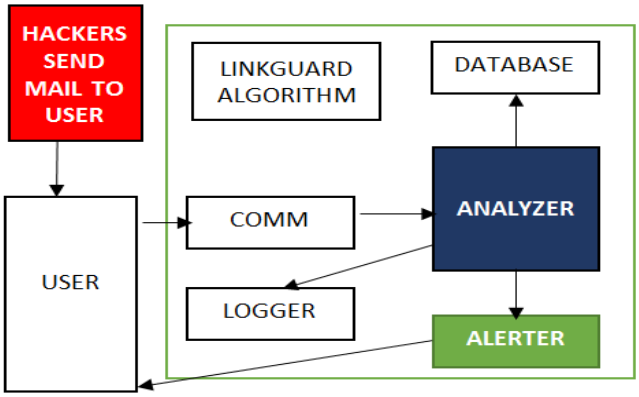

Figure 2: Link guard algorithm Architecture

A forensic case analysis of the e-banking website, prepared for phishing attacks, was conducted by the author. In a real attack example, the attacker's tactics and attack strategy were examined. Since phishing attacks can employ different designs according to the chosen fiction, the detection and analysis approach may vary depending on the case. However, it is similar to other attack examples. By clicking on malicious links within email attachments or fake websites, victims can be targeted, and their computers can be compromised by attackers who execute infected files from emails or malicious links on web pages. The attack strategy and the methods used by the attacker were examined on a real attack example by Ilker Kara [19]. To enhance future research, the author suggests planning investigations using diverse sample datasets to detect and analyse e-banking websites susceptible to phishing attacks. Sayan Karmakar et.al [20] insights into the significant threat of identity theft, which is prevalent in the online realm. Identity theft occurs when an attacker assumes someone's identity to unlawfully acquire their personal information, such as social security numbers, bank details, or credit card numbers, for malicious purposes, including financial theft and various other crimes. Tony UcedaVelez [21] focuses on tackling one of the significant challenges currently faced by the financial industry: Phishing. The author emphasises the need for security professionals and banks to stay current with new developments. In conclusion, the author suggests that the user interface of email services should be carefully designed to provide effective alerts when users encounter suspicious emails.

III. RESULTS AND DISCUSSION

The literature survey helped us understand certain vital factors, such as How Phishers exploit the sense of urgency by utilising terms like "important" to trigger an emotional response from users and entice them to click on "View message." One of the primary challenges of phishing is that attackers continuously seek innovative and emerging methods to deceive users into believing they are interacting with legitimate emails or websites. Phishers have become increasingly adept at creating websites that closely resemble legitimate targets, incorporating graphics and logos in phishing emails to enhance their authenticity.

Phishing is commonly associated with deceptive emails that imitate legitimate companies, such as credit card companies, banks, or popular e-commerce platforms like eBay and Amazon, to deceive victims into disclosing sensitive information. The overall process of the phishing mechanism, as per the existing literature analysis
involves:

1. Planning – Phishers select businesses to target and devise strategies to gather email addresses of their customers.
2. After selecting the spoofed business and victims, phishers distribute messages and employ various methods to collect data, often utilizing web pages and email addresses.
3. Attack – Phishers send spam messages that appear to originate from legitimate sources.
4. Collection – Phishers gather the information provided by victims in pop-up windows or web pages.
5. Once phishers gather the necessary information, they employ it for illegal purchases or other fraudulent activities.

The analysis further helps to focus on the financial sector, as rather than viewing banking security measures as a one-time implementation, they should be seen as an ongoing process of development and adaptation. As phishing attacks become more sophisticated, it is essential to continuously reassess security measures to ensure they can effectively counter these new threats. Some effective defence mechanisms against phishing attacks include:

1. Anti-virus scanning serves the purpose of identifying harmful attachments, embedded HTML, or concealed binary code within a bank's network.
2. Anti-Spam Filtering: Uses rule-based inspection of emails to prevent the successful delivery of spam.
3. Content Filtering: Inspects the content of communication channels, including instant messaging (IM), HTTP, FTP, and others.
4. Proxy Services: Assist in managing different forms of internet communication within a banking network.

By combining technical security measures with effective communication to consumers, the risk associated with social engineering attacks can be significantly minimized.

IV. CONCLUSION

Complete eradication of phishing is unlikely. Phishing refers to the deceptive practice of posing as a trustworthy source in electronic communication to obtain sensitive information, such as usernames, passwords, and credit card details, often with malicious intent. Nowadays, this issue has grown significantly in seriousness, prompting the exploration of various techniques to address it. Through the study of multiple papers, awareness has been raised regarding the problems associated with phishing and the utilization of different algorithms, tools, and other solutions to combat it.
Firstly, education plays a crucial role in preventing successful spear phishing attacks by creating awareness. Secondly, implementing robust email security measures is essential. Advanced email filtering systems can detect and block malicious emails, thus reducing the likelihood of spear phishing attacks reaching the intended targets. Additionally, email authentication protocols such as DMARC (Domain-based Message Authentication, Reporting, and Conformance) can help verify the authenticity of incoming emails, making it harder for attackers to impersonate trusted entities. Furthermore, multi-factor authentication (MFA) should be widely adopted to add an extra layer of security. By requesting users to provide multiple forms of verification, such as a password, biometric data, or a one-time code, the risk of unauthorized access through spear phishing can be significantly reduced. By implementing these solutions, individuals and organisations can better protect themselves against falling victim to this highly targeted form of cyberattack.

DECLARATION

Funding/ Grants/ Financial Support	No, we did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval or consent to participate, as it presents evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. S. Kumudha and Aswathy Rajan, "A Critical Analysis of Cyber Phishing and its Impact on Banking Sector", International Journal of Pure and Applied Mathematics, Vol . 119, No. 17, 2018, ISSN: 1314-3395 (online version), pp. 1-14.
2. Dhruv Rathee and Suman Mann, "Detection of E-Mail Phishing Attacks – using Machine Learning and Deep Learning", International Journal of Computer Applications, Vol . 183, No. 47, 2022, pp. 1-7. [CrossRef]
3. Alhuseen O. Alsayed and Anwar L. Bilgrami, "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities", International Journal of Emerging Technology and Advanced Engineering, Vol . 7, No. 1, 2017, ISSN 2250-2459, ISO 9001:2008, pp. 1-7.
4. N.P. Singh, "Online Frauds in Banks with Phishing", Journal of Internet Banking & Commerce, 2010, ISSN: 1204-5357, pp. 1-18.
5. Kara Ilker, "Don't bite the bait: Phishing Attack for Internet Banking", The Journal of Digital Forensics, Security & Law, Vol . 16, 2021, pp. 1-13.
6. Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry & Robert G. Rittenhouse, " Phishing Attacks and Defences", International Journal of Security and Its Applications, Vol . 10, No. 1, 2016, pp. 1-10. [CrossRef]
7. Dr. N. Revathy, Dr. T. Guhan, Mr. P. Haridharan & Mr. S. Premkumar, " Detection and Prevention of E-Banking Phishing Attack 1 Using Link Guard Algorithm", ANVI BOOKS & PUBLISHERS, Vol . 1, 2020, pp. 1-8.
8. Dr.Radha Damodaram, " STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS", International Research Journal of Engineering and Technology (IRJET), Vol . 3, No. 1, 2016, pp. 1-6
9. Bashir, Tenuche, Agbata, B.C, Emmanuel Ogala, William Obeng-Denteh, " The Fuzzy Experiment Approach for Detection and Prevention of Phishing attacks in online Domain", East African Scholars Journal of Engineering and Computer Sciences, Vol . 3, No. 10, 2020, pp. 1-11. [CrossRef]
10. Fadare Olusolade Aribake and Zahurin Mat Aji, "Fight Against Phishing Attacks Among Internet Banking Users: A Knowledge Management Technique", Knowledge Management

International Conference, 2021, pp. 1-6.
11. Ezer Osei Yeboah-Boateng, Priscilla Mateko Amanor, "Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices", Journal of Emerging Trends in Computing and Information Sciences, Vol . 5, No. 4, 2014, pp. 1-11.
12. Olga Syniavska, Nadiya Dekhtyar, Olga Deyneka & Tetiana Zhukova, "Modelling the Process of Counteracting Fraud in E-banking", Kharkiv National University of Internal Affairs, 2012, pp. 1-11.
13. Brad Wardman, Tommy Stallings, Gary Warner & Anthony Skjellum, " High-Performance Content-Based Phishing Attack Detection", Computer Forensics and Research Laboratory, University of Alabama at Birmingham, 2011, pp. 1-8 [CrossRef]
14. Rachna Dhamija & J.D.Tygar, " The Battle Against Phishing: Dynamic Security Skins", ACM International Conference Proceedings Series, ACM Press, 2005, pp. 1-12 [CrossRef]
15. Engin Kirda & Christopher Kruegel, "Protecting Users Against Phishing Attacks", Oxford University Press, 2005, doi:10.1093/comjnl/bxh000, pp. 1-8
16. Maher Aburrous, M.A. Hossain, Keshav Dahal & Fadi Thabtah, " Intelligent phishing detection system for e-banking using fuzzy data mining", Elsevier Journals, 2010, doi:10.1016/j.eswa.2010.04.044, pp. 1-9. [CrossRef]
17. Mousa Tayseer Jafar, Mohammad Al-Fawareh, Malek Barhoush & Mohammad H. Alshira, "Enhanced Analysis Approach to Detect Phishing Attacks During COVID-19 Crisis", Cybernetics and Information Technologies, Vol . 22, No. 1, 2022, DOI: 10.2478/cait-2022-0004 pp. 1-17. [CrossRef]
18. E.Konda Reddy, Dr. Rajamani and Dr. M. V. Vijaya Saradhi, " Detection of E-Banking Phishing Websites", International Journal of Modern Engineering Research, Vol . 2, No. 1, pp. 1-9.
19. Ilker Kara, "Electronic Banking (e-Banking) Fraud with Phishing Attack Methods", European Journal of Science and Technology, Vol . 31, No. 1, 2021, pp. 1-4.
20. Sayan Karmakar & Dr Munish Bhatia, "Phishing Attacks and Their Working Methodology and How Spear Phishing Is Happening in Modern IT Hubs", International Journal of Mechanical Engineering, Vol . 7, No. 4, 2022, pp. 1-9.
21. Tony UcedaVelez, "Phishing for Banks: A Timely Analysis on Identity Theft & Fraud in the Financial Sector", Global Information Assurance Certification Paper, 2005, pp. 1-8.

AUTHORS PROFILE

Anjali Shukla, Student, M.Sc in Information Technology, Department of IT, University of Mumbai, India. Anjali specialises in cybersecurity and is currently completing an internship at the Maharashtra Cyber Cell in Mumbai. She is also pursuing her training to appear for defence examinations.

Sameer Chavan Student, M.Sc in Information Technology, Department of IT, University of Mumbai, India. Sameer specialises in cybersecurity and cloud computing and has job experience as a developer. He has hands-on experience in using cybersecurity tools and is preparing for EC-Council certifications. He has deployed a small security mechanism as a prototype for the department.

Srivaramangai R, Head, Department of IT, University of Mumbai, India. Having 21 years of experience in teaching and 6 years in industry. The specialisation areas include artificial intelligence, security, and image processing. Has industry experience in web development and report code generators. Has published more than 30 International journal papers, 20 conference papers, and served as a resource person for various workshops, and chaired sessions.