A Review of Smishing Attaks Mitigation Strategies

David Ng'ang'a Njuguna
Department of Information Technology
Mount Kenya University
Thika, Kenya
Email: dnganga175 [AT] gmail.com

John Kamau
Department of Information Technology
Mount Kenya University
Thika, Kenya
Email: jkamau [AT] mku.ac.ke

Dennis Kaburu
Department of Information Technology
Jomo Kenyatta University of
Agriculture and Technology
Juja, Kenya
Email: dennis.kaburu [AT] gmail.com

Abstract— **Mobile Smishing crime has continued to escalate globally due to technology enhancements and people's growing dependence on smartphones and other technologies. SMS facilitates the distribution of crucial information that is principally important for non-digital savvy users who are typically underprivileged. Smishing, often known as SMS phishing, entails transmitting deceptive text messages to lure someone into revealing individual information or installing malware. The number of incidences of smishing has increased tremendously as the internet and cellphones have spread to even the most remote regions of the globe.**

Keywords-- phishing; Social engineering; vishing; SMS; malware; mobile applications; awareness.

I. INTRODUCTION

Phishing is a type of social engineering assault which involves delivering a message that looks to come from a trusted source to obtain information from a computer user [1]. Social engineering is a crime that involves the use of human shared relations to persuade a person, institution, or other entity to comply with an attacker's wishes. The process of emotionally manipulating somebody in order to obtain information or accomplish a task is known as social engineering. [2]. During the COVID-19 pandemic, the United Nations claims that phishing websites have increased by 350 [3]. Attackers nowadays use a variety of communication methods to interact with their victims, including email, Short Message Service (SMS), phone, and others [4]. SMS are one of the viable ways to effectively engage with one another via mobile phones instead of using the internet. In 2020, the number of mobile subscriptions was expected to reach 5.15 billion. [5]. Mobile phones have become more vulnerable to assaults as a result of their fast proliferation unlike Personal computers [6]. According to CallHub, 98 percent of SMS messages receive a 45 percent response rate, whereas email receives 28-33 percent, meaning that people respond more to text messages than emails [7][8]. Smishing is a form of phishing where attackers transmit messages in form of text that appear to be from a legitimate source and ask recipients to click on a link or divulge their personal information through text messages instead of sending emails [9]. According to a study conducted by Cloudmark, around Thirty million fraudulent text messages are conveyed to mobile phone operators in Europe, North America, and the United Kingdom [10]. COVID-19 quickly shifted our society's reliance on distant communication, according to a survey, and it's clear that hackers are aggressively abusing the mobile platform with an avalanche of text-message phishing attempts [11]. According to [12], smishing increased by 29 percent between March and July 2020. To obscure their identity, smishers may utilize faked phone numbers or "burner phones," which are inexpensive, ephemeral prepaid phones. The Better Business Bureau reported an increase in instances of U.S. government imposters transmitting texts requesting that people take a necessary COVID-19 test via a connected website in April 2020. Smishing messages purporting to offer free iPhone12 and gifts were delivered to mobile phone users containing links to fraudulent websites that would steal private data [13]. SMS phishers could also use these phony text messages to spread spyware or malware. The recipient of these messages is frequently given a sense of urgency to click on the message's link. The victim is then redirected to a potentially dangerous or fake website that can infect the device with malware [14]. Smishers have resulted in using smishing and vishing techniques to increase their chances of success. An example is where the Smisher sends a text message such as" PIUOGFZGDA confirmed. You have received Kshs 7,430.00 from xxxxxxx on 30/9/2021. NEW M-PESA balance is Kshs (*LOCKED*). To reverse dial *334#". The Smisher would then call immediately and inform the recipient that his/her account balance is locked by the service provider and request the recipient to reverse the amount of money wrongly sent so that the account balance is unlocked. The rest of the paper is divided into sections; section 2 examines mobile phone security challenges, section 3 discusses SMS phishing mitigation approaches, and section 4 concludes the paper.

II. MOBILE PHONES SECURITY CHALLENGES

Security challenges in mobile devices include; human weaknesses such as ignorance, theft and accidental loss, hackers, third-party apps, malware, phishing, etc. In 2011, the number of smartphones lost in the United States was 9 million according to statistics [15]. [16] Offer's a list of smartphone assets that may be vulnerable to security threats: confidential data, industry intellectual assets, commercial data and

accessibility and performance of the cellphone, and individual and administrative reputation. As mobile phones are increasingly utilized for commercial purposes, the valuable data held on them offers an extra impetus for fraudsters as well as hackers to seize the device or get remote access to important information. Smishers are also taking advantage of the increasingly popular instant messaging service to steal personal information. Emojis, images, drawings, links, and file attachments may be included in the messages. On social media sites for instance WhatsApp, Telegram, and Facebook, online real-time communications using mobile phones present an avenue for obtaining personal data from unsuspecting users [17]. Third-party application stores are used by cyber-attackers to disseminate software with harmful codes. These programs are free to download and install, and mobile phone users do so at their discretion [18]. Recent statistics show an increase in mobile malware attacks by 57% in the year 2020 [19]. Malware has evolved into a serious menace to modern society that is heavily reliant on smart technologies for routine tasks [20]. As per the G DATA Mobile Malware Report 2019, roughly 4.18 million harmful applications were discovered in 2019, with approximately 11,500 latest Android harmful apps being discovered every day [21]. According to the most recent figures, 5,683,694 harmful mobile installation programs, 156,710 latest mobile banking Trojans, and 20,708 latest smartphone ransomware Trojans were detected in 2020 [22]. Hackers and malware designers have turned to Android malware as a source of income. They are able to make a substantial profit from this source. Criminals use the Dark web as one of the platforms to acquire and sell dangerous software, which is then sold as a component of software bundles. Phishing is another security risk [23]. Phishing lets cybercriminals gain access to and steal personal information from it via fraudulent programs, texts, or emails that look to be authentic. [16]. Smishing and vishing are the two most common mobile phishing attacks. In a smishing attack, the attacker sends phone numbers, self answering links, and ask the victims to call, send money and share the link in the message or send Uniform Resource Locator (URL) by SMS, which when clicked open a browser window, making the device susceptible to cyber-attack. Voice calls, on the other hand, are used in mobile vishing assaults. The attacker can fool the user into contacting a certain number by concealing the genuine voice call id. By impersonating a trustworthy business, such as a bank or insurance provider, the attacker can obtain sensitive information from the user[24]. Another issue is ignorance, which can present itself in a variety of ways, including failure to comprehend how to set up security settings, installing software from untrustworthy sources, and connecting to fraudulent network connections. [25]. Ignorance affects mobile phones users due to a lack of awareness of security challenges.

III. SMS PHISHING MITIGATION APPROACHES

This section focuses on different phishing detection approaches on mobile platforms. The current smishing mitigation approaches include education-based schemes and technology-based schemes

A. Education-based scheme

Because of human fragility and ignorance, phishing attempts are successful. Smishing attacks can be mitigated by increasing user knowledge. Educational-based solutions strive to educate mobile users on the features of phishing messages so that they can correctly recognize phishing attacks through training, workshops, and awareness activities. Software phishing, vishing, multi-media phishing, and Smishing attacks, which are carried out via SMS, multimedia messaging, voice, and the internet, should all be taught to mobile phone users. [26]. As technology is evolving, awareness and best-practice guides become crucial. Most cyberattacks get successful due to human mistakes. Fostering training and awareness of human flaws and emerging dangers is necessary for mitigating cyber-related attacks [27] [28].

B. Technology-based schemes

Various researchers have proposed several technological approaches to mitigate smishing attacks. Wu et al., [29] presented the “MobiFish” anti-phishing technique, which protects users against phishing attacks on mobile apps and online pages. To assess the legitimacy of a webpage, the system scrutinizes the source code for Hypertext mark-up Language (HTML), Internet Protocol (IP) address, and URL. A screenshot of a webpage is also converted into text using an Optical Character Recognition (OCR) tool for additional examination. Sonowal et al. suggested a model based on machine learning methods dubbed "SmiDCA" for discovering smishing messages. The authors identified Thirty-nine essential significant elements from smishing messages using a correlation algorithm in their model. Afterward, they evaluated the model's performance using four machine learning classifiers: Random Forest, Decision Tree, Support Vector Machine, and AdaBoost. [30]. For identifying Smishing attacks, Joo et al., [31] devised the S-Detector model. The S-Detector is made up of an SMS analyzer, SMS determinant, Database, and SMS monitor. The S-Detector examines the text message's URL and contents. The researchers used a Nave Bayesian Classifier to distinguish Smishing messages from valid ones by looking for phrases that were used more frequently in Smishing messages. Depending on the analyzer's examined information, the determinant detects and blocks Smishing SMS messages then warns the user. Yadav et al. [32] created ‘SMS-Assassin,' a mobile spam filtering program that uses Bayesian learning and sender blacklisting mechanism. Messages are classified as ham if they don’t contain smishing content or spam if they contain smishing content. The spam messages are stored in the spam folder. The user can use the blacklisting mechanism to push messages from blacklisted numbers to the spam folder. Support Vector Machine (SVM) and Bayesian classifier are used together to attain improved accuracy. Because spam message patterns and keywords change regularly, crowdsourcing is employed to keep it up to date. Bottazzi et

al. [33] introduced the MP-Shied architecture. MP-Shield is the Mobile application that operates as a proxy service on top of the Transmission Control Protocol (TCP)/IP stack, looking for phishing material in IP packets that emanate from and are routed to a typical mobile phone application. MP-Shield consists of the Blacklist Application Programming Interface (API), the machine learning Classification Engine, and the Watchdog. The Blacklist API queries the Google Safe Browsing, to check if the URL has been blacklisted or not. The machine classification engine uses a variety of machine learning techniques based on the WEKA (Waikato Environment for Knowledge Analysis) architecture to detect Phishing URLs. When unsafe URLs are found, the Watchdog is responsible for executing the other two modules. When a prospective threat is discovered, the Watchdog subsystem shows a cautionary message on the screen and alerts the user. Mishra and Soni [34] developed a Content-Based Approach for discovering Smishing in cell phone, which classifies text messages based on their contents and URL behavior. To perceive the existence of URLs, phone numbers, email addresses, and hazardous phrases in SMS messages, text pre-processing and examination algorithms are used. The message is evaluated using a machine learning algorithm depending on the existence of harmful phrases in the message. They also employed form tag check and APK download check tools to investigate the URL's harmful activity. Based on the results of the detection procedures, text messages will be categorized as malicious or non-malicious. Malicious messages are blocked. Abdallah, et al [35] proposed a hybrid learning model for identifying Spam SMS's written in English and Arabic languages. This detection model is built using Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) deep learning approaches. The proposed model employs a hybrid deep learning architecture that combines CNN and LSTM algorithms. Through the application of convolutional procedures, CNN excels in extracting n-gram features at various places in a message. The model classifies messages as spam if the message contains phishing or theft content or Not-spam. Roy et al. [36] suggested using a deep learning method to identify spam and non-spam text messages. Their method aims to merge two deep learning approaches, namely CNN and LSTM, to achieve its purpose. The purpose is to sort text messages into categories and decide which spam are and which are not. Jain and Gupta recommended a rule-based classification strategy to identify phishing text messages [37].

The research generated 9 rules for identifying authentic SMS from phishing SMS. The authors discovered a true negative rate of 99 percent and a true positive rate of 92 percent in their tests. Goel and Jain [38] proposed a smishing classifier architecture for detecting smishing attacks in mobile platforms. The suggested approach assesses the text message's content and retrieves phrases typically used in Smishing messages. Smishing-Classifier protects users against phishing SMS by blocking them and allowing only normal messages to be sent.

The Naive Bayesian approach is used by Smishing-Classifier to evaluate the message content and categorize it.

Even though smishing attacks on mobile platforms are on the rise, no comprehensive research has been conducted and there are very few articles in the literature that address the topic of detecting smishing assaults globally [39].

IV. CONCLUSION

As the number of people using smartphones grows, so does the threat to these devices. Smishing, or phishing by text message, is a common threat that targets mobile devices. In the literature review, there are few studies that deal with smishing detection and mitigation strategies and no single technique can mitigate smishing attacks efficiently. Most of the proposed technical solutions aim at classifying messages as spam or not-spam or ham. The SMS-assassin approach filters messages containing smishing content and stores them in the spam folder. The content-based approach classifies messages as malicious or non-malicious and blocks malicious messages. The hybrid learning model classifies messages as spam or not spam. The rule-based framework filters smishing messages from genuine ones and blocks suspected smishing messages. The smishing classifier blocks smishing messages and delivers legitimate messages only. Further research is needed to filter malicious smishing content present in a text message and informs the user of such content as a way of enhancing smishing attacks awareness. Further research on the sender authentication mechanism is also required to deal with spam messages that are sent anonymously.

REFERENCES

[1] F. Mouton, L. Leenen and H. S. Venter, "Social Engineering Attack Detection Model: SEADMv2," *2015 International Conference on Cyberworlds (CW)*, 2015, pp. 216-223, doi: 10.1109/CW.2015.52.

[2] R.Thomas, Peltier. Social engineering: concepts and solutions. Information system Security 2006;15(5):13-21, DOI: 10.1201/1086.1065898X/46353.15.4.20060901/9547.3

[3] Newindianexpress.com, "Increasing cybercrime: UN reports 350 percent rise in phishing websites during the pandemic. The New Indian Express," 8 August 2020. [Online]. Available: https://www.newindianexpress.com/business/2020/aug/08/increasing-cybercrime-un-reports-350-per-cent-rise-in-phishing-websites-during-pandemic-2180777.html. [Accessed 8 July 2021].

[4] M. ARAB and M. K. SOHRABI, "Proposing a new clustering method to detect phishing websites," *Turkish Journal of Electrical Engineering & Computer Sciences*, pp. 4757-4767, 2017.

[5] Datareport.com, "Digital 2020: Global Digital Overview-DataReport-Global Digital Insight," 30 January 2020. [Online]. Available: https://datareportal.com/reports/digital-2020-global-digital-overview. [Accessed 11 June 2021].

[6] S. Mishra and D. Soni, "DSmishSMS-A System to Detect Smishing SMS," *Neural Computing and Applications*, 2021

[7] M. Baglia, "Text Marketing Vs. Email Marketing: Which One Packs a Bigger Punch? [Infographic]-Business2Community," 30 June 2015. [Online]. Available: https://www.business2community.com/infographics/text-

marketing-vs-email-marketing-one-packs-bigger-punch-infographic-01249186. [Accessed 15 June 2021].

[8] Callhub.io, ". 6 reasons why SMS is more effective than email marketing||CallHub," 10 August 2016. [Online]. Available: https://callhub.io/6-reasons-sms-effective-email-marketing/. [Accessed 17 June 2021].

[9] MCAfee.com, "Protect yourself from smishing|McAfeeBlog," 22 February 2012. [Online]. Available: https://www.mcafee.com/blogs/consumer/family-safety/protect-yourself-from-smishing/. [Accessed 17 June 2021].

[10] J. Haley, "Protect yourself from smishing (video)," 15 August 2012. [Online]. Available: https://www.cnet.com/tech/services-and-software/protect-yourself-from-smishing-video/. [Accessed 10 May 2021]

[11] M. LAUDON, "Mobile Phishing Increases More Than 300% as 2020 Chaos Continues," 2 November 2020. [Online]. Available: https://www.proofpoint.com/us/blog/threat-protection/mobile-phishing-increases-more-300-2020-chaos-continues. [Accessed 10 May 2021].

[12] L. Irwin, "Catches of the month: Phishing scams for October 2020," 7 OCTOBER 2020. [Online]. Available: https://www.itgovernance.co.uk/blog/catches-of-the-month-phishing-scams-for-october-2020. [Accessed 11 June 2021].

[13] Kaspersky.com, "What is Smishing and How to Defend Against it," 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it. [Accessed 9 10 2021].

[14] B. Muscio, "Smishing Attacks Increased by 328% in 2020!-4iT-Your IT Support Department," 17 march 2021. [Online]. Available: https://4it.com.au/2021/03/17/smishing-attacks-increased-by-328-in-2020/. [Accessed 11 June 2021].

[15] S. Raman, K. Streff and Y. Wang, "Smartphone Security Challenges" in *Computer*, vol. 45, no. 12, pp. 52-58, 2012. doi: 10.1109/MC.2012.288

[16] D. Peraković, S. Husnjak, and V. Remenar, "Research of Security Threats in the Use of Modern Terminal Devices," presented at the 23rd International DAAAM Symposium Intelligent Manufacturing & Automation: Focus on Sustainability, 2012

[17] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches," *Future Internet*, vol. 12, no. 10, p. 168, Sep. 2020.

[18] B. Parnika and B. Kamlesh, "A Survey on Various Threats and Current State of Security in Android Platform," *ACM Computing surveys*, vol. 52, no. 1, pp. 1-35, 2019.

[19] T. Spring, "Mobile Adware Booms, Online Banks Become Prime Target for Attacks|Threatpost," 1 March 2021. [Online]. Available: https://threatpost.com/mobile-adware-booms-attacks/164386/. [Accessed 9 September 2021].

[20] V. KOULIARIDIS, K. BARMPATSALOU, G. KAMBOURAKIS and S. CHEN, "A Survey on Mobile Malware Detection Techniques," *IEICE Transactions on Information and Systems*, vol. E103.D, no. 2, pp. 204-211, 2020.

[21] A. Burris, "G DATA Mobile Malware Report 2019: New high for malicious Android apps," June 2020. [Online]. Available: https://www.gdatasoftware.com/news/g-data-mobile-malware-report-2019-new-high-for-malicious-android-apps. [Accessed 24 June 2021].

[22] V. Chebyshev, "Mobile malware evolution 2020|securelist," 01 March 2021. [Online]. Available: https://securelist.com/mobile-malware-evolution-2020/101029/. [Accessed 09 September 2021].

[23] E. Chickowski, "Cybercrime: A Black Market Price List From The Dark Web," March 2016. [Online]. Available: https://www.darkreading.com/cloud/cybercrime-a-black-market-price-list-from-the-dark-web. [Accessed 10 July 2021].

[24] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," *2011 Proceedings of the 34th International Convention MIPRO*, 2011, pp. 1468-1473.

[25] W. Jeon, J. Kim, Y. Lee, and D. Won, "A Practical Analysis of Smartphone Security," in Human Interface and the Management of Information. Interacting with Information. Human Interface,2011. Lecture Notes in Computer Science, vol 6771. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21793-7_35

[26] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches," *Future Internet*, vol. 12, no. 10, p. 168, Sep. 2020 [Online]. Available: http://dx.doi.org/10.3390/fi12100168

[27] F. Parker, J. Ophoff, J. Van Belle and R. Karia, "Security awareness and adoption of security controls by smartphone users," *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 2015, pp. 99-104, doi: 10.1109/InfoSec.2015.7435513

[28] G. Ali, M. Ally Dida, and A. Elikana Sam, "Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda," *Information*, vol. 11, no. 6, p. 309, Jun. 2020

[29] L. Wu, X. Du and J. Wu, "MobiFish: A lightweight anti-phishing scheme for mobile phones," *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, 2014, pp. 1-8, doi: 10.1109/ICCCN.2014.6911743M

[30] G. Sonowal and K. S. Kuppusamy, "SmiDCA: An Anti-Smishing Model with Machine Learning Approach," *The Computer Journal*, vol. 61, no. 8, pp. 1143-1157, 2018.

[31] J. W. Joo, S. Y. Moon, S. Singh, and J. H. Park, "S-Detector: an enhanced security model for detecting Smishing attack for mobile computing.," *Telecommunication Systems*, vol. 66, pp. 29-38, 2017

[32] K. Yadav, P. Kumaraguru, A. Goyal, A. Gupta, and V. Naik, "Smsassassin: crowdsourcing driven mobile-based system for SMS spam filtering

[33] G. Bottazzi, E. Casalicchio, D. Cingolani, F. Marturana, and M. Piu, "MP-Shield: A Framework for Phishing Detection in Mobile Devices," *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 1977-1983, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.293.

[34] S. Mishra and D. Soni, "A Content-Based Approach for detecting Smishing in Mobile Environment.," in *International Conference on Sustainable Computing in Science, technology, and management(SUSCOM). Jaipur: Amity University Rajasthan*, Jaipur, 2019.

[35] A. Ghourabi, M. A. Mahmood, and Q. M. Alzubi, "A Hybrid CNN-LSTM Model for SMS Spam Detection in Arabic and English Messages," *Future Internet*, vol. 12, no. 9, p. 156, Sep. 2020

[36] P. K. Roy, J. P. Singh, and S. Banerjee, "Deep learning to filter SMS Spam, ISSN 0167-739X," *Future Generation Computer Systems*, vol. 102, pp. 524-533, 2020.

[37] K. Jain and B. B. Gupta, "Rule-Based Framework for Detection of Smishing Messages in Mobile Environment," in *6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8*, Kurukshetra, India, 2018.

[38] D. Goel and A. K. Jain, "Smishing-Classifier: A Novel Framework for Detection of Smishing Attack in Mobile Environment," in *International Conference on Next Generation Computing Technology*, Singapore, 2018.

[39] G. Sonowal, "Detecting Phishing SMS Based on Multiple Correlation Algorithms". *SN COMPUT. SCI.* **1,** 361 (2020). https://doi.org/10.1007/s42979-020-00377-8