Check for updates

Special Issue: Proceedings of the 68th HFES International Annual Meeting

Proceedings of the Human Factors and Ergonomics Society Annual Meeting
1–5
Copyright © 2024 Human Factors and Ergonomics Society
DOI: 10.1177/10711813241264204
journals.sagepub.com/home/pro
Sage

Where Do Users Look When Deciding If a Text Message is Safe or Malicious?

Eleni Alexandra Katsarakes[1], Morgan Edwards[1], and Jeremiah D. Still[1]

Abstract

Phishing via SMS, or SMiShing, is a rapidly growing cyber threat that causes significant financial losses. While research on email phishing has explored user behavior, the understanding of human factors in SMiShing detection remains limited. This study bridges the gap by investigating how users visually evaluate real-world SMS message legitimacy using eye-tracking technology. We aim to identify which message components capture user attention (e.g., sender information, typos/grammatical errors, links) and assess if users focus sufficiently on established red flags associated with phishing attempts. This research contributes to more effective user-centric countermeasures against SMiShing attacks by informing the design of security interventions that consider user behavior and mobile device information limitations.

Keywords

SMiShing, cybersecurity, eye-tracking, phishing, social engineering, user behavior, digital threats

Statement of Purpose

Phishing, a social engineering attack where users are tricked into revealing sensitive information, is a prevalent threat in modern society (Dong, 2009; Mitnick & Simon, 2001; Yeboah-Boateng & Amanor, 2014). While email is the most common platform for phishing attacks, SMS phishing, that is, "SMiShing," is rapidly gaining traction (Banu & Banu, 2013; Desolda et al., 2021; Edwards, et al., 2023). SMiShing exploits text messaging systems to deliver fraudulent messages that lure users into clicking malicious links or divulging personal details. The rise of SMiShing coincides with increasing reliance on mobile devices for communication and completion of sensitive tasks such as legal and financial transactions.

Despite the growing prevalence of SMS-based attacks, research in this area remains limited compared to the email vector (Rahman et al., 2023). Existing studies on SMiShing primarily focus on developing automated anti-SMiShing solutions using machine learning and natural language processing techniques (Akande et al., 2023; Goel & Jain, 2018; Joo et al., 2017; Mishra & Soni, 2019; Sonowal & Kuppusamy, 2018). While these efforts are crucial for mitigating SMiShing attacks, they often overlook the human element—the user's ability to detect and resist phishing attacks.

Existing research on email phishing has explored user behavior and decision-making processes when evaluating email legitimacy (Zhuo et al., 2023). McAlaney and Hills (2020) employed eye-tracking to investigate how users scrutinize emails for phishing indicators; their findings revealed that users fixate more on phishing indicators like suspicious sender addresses or misspelled words for shorter durations than legitimate content. This suggests "skim-reading" behavior where users might recognize red flags but fail to devote sufficient attention for gaining deeper insight. Understanding user attention in the context of SMiShing detection is critical for developing effective countermeasures.

Phishing and Smishing Landscape

Phishing attacks exploit social engineering techniques to manipulate users into revealing sensitive information such as usernames, passwords, and credit card details (Yeboah-Boateng & Amanor, 2014). Emails of this nature typically masquerade as legitimate sources such as banks, credit card companies, or social media platforms (Mitnick & Simon, 2001). Often, the emails contain notes of urgency or fear appeals to pressure users into risky behavior like clicking malicious links or downloading attachments containing malware (Desolda et al., 2021).

[1]Old Dominion University, Norfolk, VA, USA

Corresponding Author:
Eleni Alexandra Katsarakes, Old Dominion University, 331B MGB, Norfolk, VA 23529-5000, USA.
Email: ekats002@odu.edu

The rise of mobile phone usage has opened new avenues for phishing attacks. SMiShing tactics leverage SMS to deliver fraudulent messages that mimic legitimate communication from banks, delivery companies, or other trusted entities (Banu & Banu, 2013). These messages often employ social engineering tactics similar to email phishing, like generating a sense of urgency by claiming a user's account is compromised, or a package delivery requires immediate action (Chiew et al., 2018; Mohammad et al., 2015).

The success of SMiShing attacks hinges on user vulnerability, which is enhanced by several factors unique to mobile messaging. First, mobile phone users are accustomed to receiving a high volume of SMS messages, potentially leading to decreased vigilance when evaluating message legitimacy (Edwards et al., 2023). Second, mobile devices' limited screen real estate can restrict users' ability to fully view and scrutinize message details (Mishra & Soni, 2019). Third, SMS messages often lack the visual cues present in emails, such as sender logos or rich formatting, that can aid in legitimacy assessment. As a result of these factors, we are seeing a dramatic rise in financial losses from $86 million in 2020 to $330 million in 2023 (Fletcher, 2023).

Eye-Tracking in Phishing Research

Eye-tracking technology can be a valuable tool for understanding user behavior in phishing detection tasks. Eye-tracking systems record fixations and dwell time across message stimuli (McAlaney & Hills, 2020). The resulting data offers insights into which message components users attend to and for how long, revealing the deployment of their attention before legitimacy decision-making (Proctor & Chen, 2015).

Many previous studies have utilized eye-tracking technology to assess user behavior in phishing scenarios. Researchers such Alsharnouby et al. (2015) have found that eye tracking metrics such as gaze time are associated with a significantly increased ability to detect phishing. In fact, Miyamoto et al. (2015) found that by analyzing users' eye movement patterns, they were able to predict susceptibility to phishing attacks with 79.3% accuracy.

Understanding User Behavior in SMiShing Detection

SMS messages differ significantly from emails in terms of format, length, and information density. Building on the work of Mishra & Soni (2019), who suggest that users are vulnerable to SMiShing due to interface limitations, our study investigates user attentional distribution during SMiShing detection. Specifically, we aim to address the following Research Questions (RQ):

Table 1. Demographic Information.

Demographic question	*n*	%
Biological sex		
Male	8	32
Female	17	68
Level of education		
High school diploma/GED	9	36
Some college (no degree)	13	52
Associate degree	3	12
Major in a technical field		
Yes	3	12
No	18	72
N/A	4	16
Trained in cyber security		
Yes	4	16
No	21	84
Expert in cyber security		
Yes	0	0
No	25	100
Trained in SMiShing		
Yes	6	24
No	19	76

1. Which components of SMS messages do users fixate on when evaluating legitimacy?
2. Do users attend to established indicators of phishing attempts?

By examining these RQs, we aim to gain insights into user vulnerabilities during SMiShing detection.

Method

Participants

The University Institutional Review Board approved all study procedures. Twenty-five participants were recruited from a large southeastern university in the United States in Spring 2023. Participants signed up for the study via the SONA system. Research credit was provided for agreeing to participate. Participant age ranged from 18 to 23 (M=20.04, SD=1.54). The sample comprised 17 females and 8 males (see Table 1). Training and technical experience were measured. 16% of participants (n=4) reported receiving cybersecurity training in the past, 24% of participants (n=6) received SMiShing training, and no participants were technical field majors.

Apparatus and Stimuli

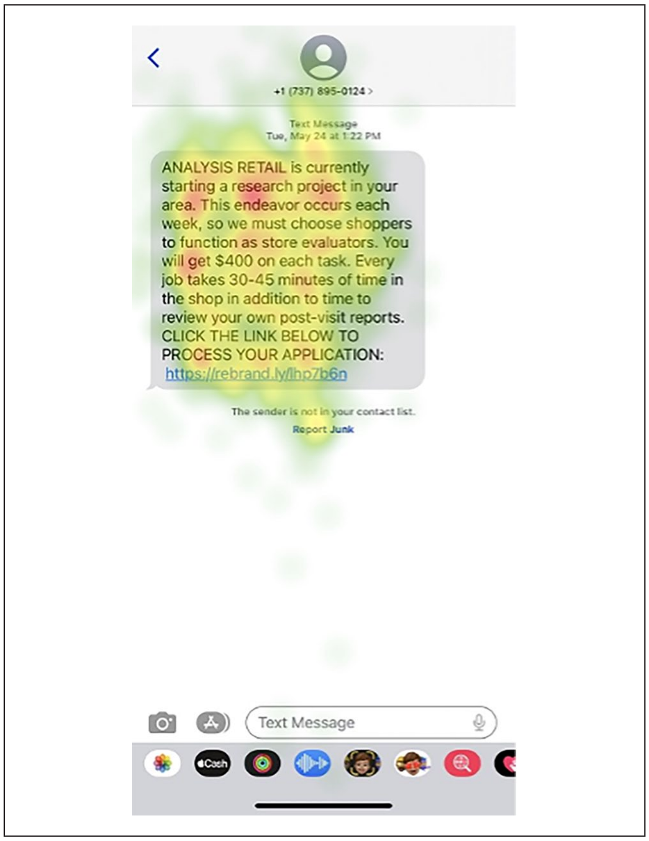
Stimuli were presented on a 43 × 24 cm monitor set to a resolution of 1,024 × 768 pixels at a viewing distance of approximately 60 cm. The system did not restrict participants' head movements. A Tobii X3-120 eye tracker running the Tobii Studio (3.4.6) software package was employed to capture participants' eye movements. The system tracking accuracy was approximately .7 degrees of visual angle.

Participants viewed 32 stimuli. The stimuli were screenshots of real-world text messages received by an author. They were original and not manipulated. Five of the stimuli were safe text messages, and 27 of the stimuli were SMiShing messages. Message presentation order was randomized.

Qualtrics was used to implement and collect survey data from participants. Additional survey data were collected that were beyond the scope of this proceeding (e.g., cyber hygiene inventory, questions about knowledge, behavior, experience, and attitudes).

Procedure

Before starting the study, participants reviewed an informed consent document and verbally consented. The study asked them to follow along during the 9-point calibration sequence. Then, participants were instructed to view the text messages as they naturally would and determine if the message was legitimate or SMiShing. They were told their task was to classify each message as safe or malicious. This task was not the goal of the current study but instead was used to encourage participants to view the messages naturistically. For each trial, participants viewed the stimuli for as long as they needed. To make their decision, they used the mouse to click on "safe" or "malicious." After completing 37 trials, they were handed an iPad to answer the survey questions. The entire study took no longer than 45 min to complete.



+1 (737) 895-0124 >

Text Message
Tue, May 24 at 1:22 PM

ANALYSIS RETAIL is currently starting a research project in your area. This endeavor occurs each week, so we must choose shoppers to function as store evaluators. You will get $400 on each task. Every job takes 30-45 minutes of time in the shop in addition to time to review your own post-visit reports. CLICK THE LINK BELOW TO PROCESS YOUR APPLICATION: https://rebrand.ly/lhp7b6n

The sender is not in your contact list.
Report Junk

Figure 1. Overt attention distribution on a malicious text message.

Findings

RQ1—Message Component Fixations

Our descriptive statistics clearly reveal that participants predominantly focused on the body of the SMS message, with an average fixation duration of 63.38% of the total time spent viewing each message. In contrast, other critical components received less than 10% of the remaining fixation duration:

- Link (if present): 8.07% fixation duration
- Typos/Grammatical Errors: 2.15% fixation duration
- Sender Information (Phone Number/Name): 1.68% fixation duration
- Receiver Information: Negligible fixation duration

These findings suggest that participants prioritize the message content while neglecting crucial indicators of phishing attempts.

RQ2—Attention to Phishing Indicators

The minimal overt attention to sender information, typos/grammatical errors, and links raises concerns about user information gathering needs for SMiShing detection. These components ought to be attended to as they are often associated with the detection of malicious messages, as follows:

- Sender Information: The lack of attention to sender information details suggests users may not be adequately scrutinizing the sender's legitimacy before engaging with the message content.
- Typos/Grammatical Errors: Typos and grammatical errors are established red flags in phishing attempts. However, our findings indicate that participants rarely fixated on these errors, potentially overlooking a vital clue for identifying malicious messages.
- Links: Embedded links within SMS messages often lead to phishing websites that steal user credentials or infect devices with malware. Despite the potential risk, participants only dedicated a small portion of their viewing time to links.

These results highlight a critical gap in user awareness and scrutiny regarding established phishing indicators in the context of SMS text messages.

Subjective Heatmap

Figure 1 contains heat maps for the eye-tracking data. The heatmaps represent the frequency of fixations by spatial location and show that participants are fixating heavily on the body of the text.

Discussion

This study captured the distribution of fixations across SMS messages while participants determined their legitimacy, revealing where users are overtly attending while deciding whether an SMS message is legitimate. Attention was mainly focused on body content, which suggests that users are vulnerable to SMiShing attacks. The message body consumes a significant portion of screen space, which might imply that it provides a rich source of contextual information. Unfortunately, this is not the case for SMiShing texts. The lack of attention to sender information and links might reflect a lack of knowledge regarding indicators of malicious messaging. In a prior eye-tracking study by McAlaney and Hills (2020), participants briefly glanced at phishing indicators, with emails featuring misspellings or threats receiving low trust ratings. In contrast, our findings reveal that crucial elements for identifying SMiShing attacks were infrequently observed by participants. Successfully detecting a malicious message requires systematic scrutiny of all available data (i.e., a greater distribution of attention across the display). The observed attentional narrowing may suggest novice processing, highlighting the need for future research to compare cybersecurity experts and novices.

Comparing these results with findings from similar email phishing studies, it is evident that informational availability differences between platforms are influencing users' information-seeking behaviors. Research on email phishing highlights greater attention to sender details, possibly due to the interface layout and the meaningfulness of the information (e.g., providing an associated domain; Buckley et al., 2023; Gallo et al., 2024). In addition, most users have greater familiarity with scrutinizing email headers (Pfeffel et al., 2019). The minimized attention to sender information in SMS formats might be influenced by interface design characteristics and the limited contextual information (e.g., only a generic phone number), causing distinct vulnerability differences in email and SMS (Mishra & Soni, 2019).

Despite these insights, the study does have its weaknesses; we only sampled undergraduate college students and focused their attention on determining whether a message is safe or malicious. Compared to the general population and naturalistic message sorting, our sample should be a best-case scenario for detecting SMiShing. Unfortunately, our findings suggest that those utilizing SMiShing attacks will find their efforts fruitful. Users fail to appropriately distribute their overt attention, and generally lack the information to resist attacks effectively.

In future research, an area of great promise emerges in efforts to revamp user training protocols while simultaneously refining interface designs. Developing and evaluating training programs designed to raise awareness of SMiShing tactics and equip users with the skills to identify phishing indicators in SMS messages is crucial (Boquetti, 2024; Nijman, 2023). The data from this study underscores the need for tailored educational programs that address specific vulnerabilities associated with different platforms (Boquetti, 2024). Clearly, current user education on phishing might not be fully effective for SMS-based communication, which has distinctly different visual and functional elements compared to email (Aleroud & Zhou, 2017; Niu et al., 2008). Security awareness training programs should incorporate findings from studies like this to recalibrate the focus of training modules to mitigate the risk posed by SMiShing (Nijman, 2023).

Finally, researchers should explore the influence of interface design features on mobile messaging applications. Based on previous research regarding phishing via email, this could involve investigating methods to highlight sender information (e.g., larger font size, salient color) and implement visual nudges to warn users about potential phishing attempts (e.g., red flags next to suspicious links) (Nicholson et al., 2017; Yang et al., 2015). Visual features could be leveraged to help users validate sender information and caution them about untrustworthy links (Felt & Wagner, 2012).

We revealed that participants infrequently observed the crucial elements needed to identify SMiShing attacks. Future developers can more deeply explore how to make these cues apparent. Increasing user informational awareness will help them make safer decisions and better protect themselves from phishing scams.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Akande, O. N., Gbenle, O., Abikoye, O. C., Jimoh, R. G., Akande, H. B., Balogun, A. O., & Fatokun, A. (2023). SMSPROTECT: An automatic smishing detection mobile application. *ICT Express*, *9*(2), 168–176.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies*, *4*, 783–786.

Boquetti, K. (2024). *The evolution of phishing: SMS and voice-based attacks*. CyberHoot. https://cyberhoot.com/blog/the-evolution-of-phishing-sms-and-voice-based-attacks/

Buckley, J., Lottridge, D., Murphy, J., & Corballis, P. (2023). Indicators of employee phishing email behaviors: Intuition, elaboration, attention, and email typology. *International*

Journal of Human-computer Studies, *172*, 102996. https://doi.org/10.1016/j.ijhcs.2023.102996

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems With Applications*, *106*, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, *54*, 1–35.

Dong, X. (2009). *Defending against phishing attacks*. [PhD thesis, University of York].

Edwards, M., Morris, T., Chen, J., & Still, J. (2023). SMiShing attack vector: Surveying end-user behavior, experience, and knowledge. *In Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *67*(1), 1911–1915.

Felt, A., & Wagner, D. (2012). Phishing on mobile devices. *Proceedings of the w2sp'11: Web 2.0 security and privacy*.

Fletcher, E. (2023). *IYKYK: The top text scams of 2022*. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, *139*, 103671. https://doi.org/10.1016/j.cose.2023.103671

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, *73*, 519–544.

Joo, J. W., Moon, S. Y., Singh, S., & Park, J. H. (2017). S-Detector: An enhanced security model for detecting Smishing attack for mobile computing. *Telecommunication Systems*, *66*, 29–38.

McAlaney, J., & Hills, P. J. (2020). Understanding phishing email processing and perceived trustworthiness through eye tracking. *Frontiers in Psychology*, *11*, 537958.

Mishra, S., & Soni, D. (2019). SMS phishing and mitigation approaches. *In 2019 twelfth international conference on contemporary computing (ic3)* (pp. 1–5).

Miyamoto, D., Blanc, G., & Kadobayashi, Y. (2015). Eye can tell: On the correlation between eye movement and phishing identification. In *Lecture notes in computer science* (pp. 223–232). Springer International Publishing. https://doi.org/10.1007/978-3-319-26555-1_26

Mitnick, K. D., & Simon, W. L. (2001). *The art of deception: Controlling the human element of security*. Wiley. http://mario.elinos.org.mx/docencia/seginfo/the_art_of_deception.pdf

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1–24. https://doi.org/10.1016/j.cosrev.2015.04.001

Nijman, R. (2023). *Awareways SMS phishing training*. Awareways. https://awareways.com/en/nieuws/sms-phishing-training.

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 Proceedings of the 13th Symposium on Usable Privacy and Security*, *13*, 285–298. https://www.usenix.org/conference/soups2017/technical-sessions

Niu, Y., Hsu, F., & Chen, H. (2008). iPhish: Phishing vulnerabilities on consumer electronics. *UPSEC*, *8*, 10. https://web.cs.ucdavis.edu/~hchen/paper/upsec2008.pdf

Pfeffel, K., Ulsamer, P., & Müller, N. H. (2019). Where the user does look when reading phishing mails–an eye-tracking study. In Z. Panayiotis & I. Andri (Eds.), *Learning and collaboration technologies. Designing learning experiences* (pp. 277–287). Springer International Publishing.

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security. *Human Factors*, *57*, 721–727.

Rahman, M. L., Timko, D., Wali, H., & Neupane, A. (2023). Users really do respond to smishing. *Proceedings of the thirteenth ACM conference on data and application security and privacy*. https://doi.org/10.1145/3577923.3583640

Sonowal, G., & Kuppusamy, K. S. (2018). SmiDCA: An anti-smishing model with machine learning approach. *The Computer Journal*, *61*(8), 1143–1157.

Yang, W., Chen, J., Xiong, A., Proctor, R. W., & Li, N. (2015). Effectiveness of a phishing warning in field settings. In *Proceedings of the 2015 symposium and bootcamp on the science of security* (pp. 1–2). ACM Press

Yeboah-Boateng, E.O., & Amanor, P.M. (2014). Phishing, SMiShing & vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computer Information Science*, *5*, 297–307.

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., & Russello, G. (2023). SOK: Human-centered phishing susceptibility. *ACM Transactions on Privacy and Security*, *26*(3), 1–27. https://doi.org/10.1145/3575797