Proceedings of the Human Factors and
Ergonomics Society Annual Meeting
1–5
Copyright © 2023 Human Factors
and Ergonomics Society
DOI: 10.1177/21695067231192193
journals.sagepub.com/home/pro
Sage

SMiShing Attack Vector: Surveying End-User Behavior, Experience, and Knowledge

Morgan Edwards[1], Thomas Morris[1], Jing Chen[2], and Jeremiah Still[1]

Abstract

Phishing attacks steal sensitive and valuable information from end-users. Human Factors researchers have extensively studied Phishing over decades, revealing numerous psychological vulnerabilities. A greater understanding of the interaction between attackers and end-users has produced more effective: policies, models, training, and defensive mechanisms. The Human Factors literature lacks information about non-technical users' knowledge, experience, and behaviors in response to SMiShing. The current survey collected pilot data from college students with average cyber hygiene scores. Our results suggest that while users do not clearly understand the term SMiShing, they report knowing the danger. While all participants reported that using links within text messages from unknown senders can lead to security vulnerabilities, most reported using the links anyway. Users vet messages based on the sender's phone number and typos, rather than delivery time and other message recipients. These descriptive findings can be used to support future work attempting to defend against SMiShing attacks.

Keywords

Smishing, Phishing, Cyber Security, Cyber Hygiene, Text Message, Human Factors

Introduction

Phishing is accomplished with the use of counterfeit emails posing as legitimate companies and is used to trick users into revealing personal sensitive information, account passwords, credit card or banking accounts, etc. (Yeboah-Boateng & Amanor, 2014). Our interaction with technology is ubiquitous, which easily affords bad actors many platforms for deception. SMiShing attacks are another form of phishing, focusing on reaching their victims through Short Messaging Service (SMS) messages. According to Consumer Reports, US phone users received over 87 billion SMiShing text messages in 2021, up 58% from 2020 (Blanco, 2022). Traditionally, we have seen bad actors employ phishing attacks to successfully steal users' personal or confidential information through email (Banu & Banu, 2013; Proctor & Chen, 2015). Much research has examined the Human Factors behind email phishing, such as susceptibility, trust in anti-phishing automation aid, or behavioral interventions (Sommestad & Karlzén, 2019; Mishler et al., 2019; Nicholson et al., 2017; Yang et al., 2017). However, knowledge about users' interactions with SMiShing is limited, especially from a human-centric perspective. This work surveys end users with average cyber hygiene knowledge and limited technical training. The authors are taking the first step to reveal users' behavior, experience, and knowledge with SMiShing.

Recent popular variations of phishing include spear-phishing (email), Vishing (voice), SMiShing (SMS), and Pharming (malicious code) (Desolda et al., 2021). These attacks are commonly employed because they are effective. These cybercrimes are growing and are predicted to reach over 10 trillion USD within the next few years (Cybersecurity Ventures, 2020). SMiShing occurs similarly to those occurring within the email vector. The end-user would receive a text message that may appear from a legitimate source but contains malicious content. The text message would typically instruct users to click on a link, call a number, send an email, download an attachment, or respond to the text. Yeboah-Boateng & Amanor (2014) highlighted that SMiShing attacks are sophisticated. They can lead to attackers gaining control over the user's cell

[1]Old Dominion University, Norfolk, Virginia, USA
[2]Rice University, Houston, TX, USA

Corresponding Author:
Morgan Edwards, Old Dominion University, 143 Oceanography & Physical Sciences Building, Norfolk, VA 23529, USA.
Email: Mthom122@odu.edu

phone and stealing data directly from the device (e.g., photos, messages, saved passwords, contact information).

Mishra et al. (2019) suggested that users are more susceptible to SMiShing than phishing due to mobile devices' small screen size. While traditional phishing takes place on a full-sized desktop, users have difficulty analyzing the full URL that is seen in the text message. Once a user clicks on a link, the small screen also makes it challenging to investigate the nature of the malicious website.

Behavioral interventions used in the past to combat email phishing have included both technical and human-centered approaches. Most technical approaches include algorithms that detect phishing emails or websites and filter these from being received by the user (Chandrasekaran et al., 2006). There are many differences between the behavioral interventions that might be used for email phishing compared to SMiShing. While the wireless carrier can filter SMiShing messages out. There is no way to retrieve the blocked message, even with administrative credentials (Yeboah-Boateng & Amanor, 2014). An overly conservative algorithm could block legitimate messages from reaching an intended recipient.

Kamau and Kaburu (2022) reviewed mitigation techniques for SMiShing and revealed that only a few studies have investigated this topic. Most mitigation techniques focus on the technical approach to identifying and filtering out text messages, however there is little about user behavior, experience, and understanding. There is a need to study users' awareness of SMiShing and how to communicate with them when they encounter a probable SMiShing message (Kamau & Kaburu, 2022).

Many studies have been dedicated to determining the role of knowledge and experience in relation to traditional phishing attack vectors like email (Bardsley-Marcial, 2022). For instance, it has been revealed that users who understand the definition of phishing were less likely to be tricked by malicious emails. Further, having general knowledge of other cybersecurity concepts was not enough to protect them from malicious emails (Downs et al., 2007).

Specific cybersecurity knowledge appears to be critical to improving user security. Cain et al. (2018) examined cyber hygiene comprehensively and found that most users do not follow best practices regarding phishing. The study found that over 94% of users report using links, downloading attachments, and responding with sensitive information when dealing with emails from unknown senders. There has been little research on how users behave in relation to text messages from unknown senders.

With the prominent use of smartphones and a lack of research on the topic, there is a need to explore users' behaviors and attitudes in relation to SMiShing to better defend against this rapidly growing attack vector. The researchers employed a survey to capture our sample's cyber hygiene and technical knowledge. Critically, the researchers measured users' knowledge, experience, and behaviors to SMiShing messages.

Method

Participants

Twenty-eight undergraduate participants were recruited from a university in the United States in Fall 2022. Participants were recruited using the SONA recruitment system and rewarded with course credit. Participant age ranged from 18-21 (M = 19, SD = 0.82). The sample consisted of 19 females as defined by biological sex. Cybersecurity-related training and technical experience were measured. It was revealed that all the participants except one (> 89% of the sample) were not from a technical field of study or had previously received cybersecurity training. Demographic results can be found in Table 1. The study was approved by the university Institutional Review Board.

Materials

These survey data were part of a larger experiment with eye-tracking measures. The eye-tracking data are beyond the scope of this work. The researchers employed the Qualtrics service to implement and collect data from participants. Participants accessed the survey and answered questions on an iPad within a campus laboratory environment. SPSS statistical software was used to analyze data.

Cyber Hygiene Inventory

Cyber hygiene was measured using the Cyber Hygiene Inventory (CHI) created by Vishwanath et al., (2020). The questionnaire consists of 18 items on a Likert-type scale ranging from one (never) to five (always). Example questions include “Checking to see if email requests have grammatical or typographical errors” and “Checking a sender's email domain name.” Scores closer to one indicate lower cyber hygienic behaviors. Questions are categorized into five domains (storage and device hygiene, transmission and browsing hygiene, Facebook and social media hygiene, authentication and credential hygiene, and email and messaging hygiene), and scores were averaged across these domains for an overall measure of cyber hygiene. Validity for these domains ranged from 0.622-0.679, and alpha reliability ranged from 0.75-0.89.

Knowledge

Examples of knowledge questions are “Clicking on links in text messages can lead to security vulnerabilities” and “After reviewing the message, you believe it is from a trusted sender. This means that it is safe to access the sensitive information in the message.” With answers being true, false, or I don't know. Other questions were answered with a 5-point Likert-type scale ranging from Never to Always. There was a total of eight knowledge questions. After answering the

Table 1. Demographic information.

Demographic Question	*n*	%
Biological sex		
Male	9	32.1
Female	19	67.9
Level of education		
High school diploma/GED	15	53.6
Associate degree	1	3.6
Some college (no degree)	12	42.9
Received training in cyber security		
Yes	1	3.6
No	27	96.4
Majored in a technical field		
Yes	1	3.6
No	25	89.3
N/A	2	7.1
Considered an expert in cyber security		
Yes	0	0
No	28	100

knowledge questions, participants were provided with the definition of SMiShing.

Experience

Three Survey questions were used to measure participants' experience with SMiShing messages. For example, experience questions are "Have you ever received a SMiShing message?" with possible answers being yes or no. Participants were asked how many times in the past year they have received SMiShing messages.

Behavior

These questions were used to measure participants' behavior when interacting with text messages from unknown senders. Examples of behavior questions are "Have you ever clicked on a link in a text message and then used that link to log into an account?" and "Do you preview the link and view the web address in a text message before responding or using the link?" with possible answers being yes or no. Participants were asked to check off, from a list, the qualities of a text message they analyzed to determine the message's legitimacy. There was a total of five behavior questions.

Procedure. Before starting the study, participants were presented with an informed consent document and asked for verbal consent to continue with the study. Participants were then given instructions and allowed to ask any questions before continuing. Participants were given an iPad and told to answer the survey questions honestly based on their opinions and behaviors. They began by answering demographic questions, followed by the CHI, then the knowledge, experience, and behavior questions. The entire study, including the eye-tracking portion, took approximately 45 minutes to complete.

Results

The results reported are descriptive. Other results connected to our eye-tracking manipulations will be discussed in future works. Data were assessed for quality, insufficient effort responding, missing values, and outliers. No data were removed from the set.

Cyber Hygiene Inventory (CHI)

Overall, the participant sample's cyber hygiene scores were measured by averaging across the five domains in the CHI ($M = 2.42$, $SD = 0.89$). In relation to phishing, the sample's Email and Messaging cyber hygiene was averaged ($M = 2.44$, $SD = 0.90$). Therefore, their scores are in the middle of the range, meaning our sample has an average cyber hygiene score.

Results from the phishing portion of the CHI show that most of the participants reported, at least occasionally, checking an incoming email's header ($n = 24$), a sender's email domain name ($n = 21$), and checking for grammatical errors within the email ($n = 19$).

Knowledge

Frequencies were obtained to measure how knowledgeable participants are about the concept of SMiShing and its consequences. Results for participants' knowledge are shown in Table 2. When asked the definition of SMiShing, 3.6% of participants ($n = 1$) answered correctly, while 96.4% of participants ($n = 27$) reported that they did not know. All the participants ($n = 28$) agreed that clicking on links in text messages can lead to security vulnerabilities.

Once a participant believes a text is from a trusted sender, 35.7% of participants ($n = 10$) believed it is safe to access the sensitive information within a text, 42.9% of participants ($n = 12$) believe it is not safe to access, and 21.4% of participants ($n = 6$) did not know.

When asked if having a passcode on their phone protected them from SMiShing scams, 7.1% of participants ($n = 2$) reported this to be true, 82.1% of participants ($n = 23$) reported this to be false, and 10.7% of participants ($n = 3$) did not know.

When asked about the frequency with which it is safe to use links sent over text messages from unknown senders, 82.1% of participants ($n = 23$) reported it is never safe, 10.7% reported it is almost never safe ($n = 3$), 3.6% reported it is occasionally safe ($n = 1$), and 3.6% reported it is safe almost every time ($n = 1$). No participants reported that it is always safe.

Experience

Frequencies were obtained to measure participants' experience with SMiShing messages. When asked if they have ever received SMiShing messages, 25% of participants reported never receiving a SMiShing message ($n = 7$), and 75%

Table 2. Frequency of answers to knowledge questions.

Knowledge Question	*n*	%
SMiShing definition		
Correct	1	3.6
Incorrect	0	0
I don't know	27	96.4
Clicking on links in text messages can lead to security vulnerabilities.		
True	28	100
False	0	0
After reviewing a text message, you believe it is from a trusted sender. This means that it is safe to access the sensitive information in the message.		
True	10	35.7
False	12	42.9
I don't know	6	21.4
Having a passcode on my phone protects me from SMiShing scams.		
True	2	7.1
False	23	82.1
I don't know	3	10.7
It is safe to use links sent over text messages from unknown senders.		
Never	23	82.1
Almost never	3	10.7
Occasionally/Sometimes	1	3.6
Almost every time	1	3.6
Every time	0	0

reported receiving at least one SMiShing message (n = 21). In the last year, the reported amount of SMiShing messages received ranged widely from 0 to 365 (M = 58.39, SD = 105.72).

Behaviors

In relation to behaviors, frequencies were obtained to measure how often participants make cyber hygienic decisions in relation to text messages from unknown senders. Results can be found in Table 3. When asked if they have ever clicked on a link within a text message and used that link to log into an account, 50% of participants reported that they have (n = 14).

A total of 25% of participants reported previewing a link in a text message before clicking it (n = 7), while 75% do not (n = 21).

When participants decide that they trust a message from an unknown sender 21.4% of them reported that they would use the link within the text (n = 6), 42.9% reported that they sometimes use the link (n = 12), and 35.7% reported that they do not use the link (n = 10).

A total of 60.7% of participants reported that they receive legitimate text messages that contain sensitive information (n = 17), 28.6% reported that they do not (n = 8), and 10.7% do not know if they do (n = 3).

Table 3. Frequencies of user behaviors with SMiShing messages.

Behavior Question	*n*	%
Have you ever clicked on a link in a text message and then used that link to log into an account?		
Yes	14	50
No	14	50
Do you preview the link and view the web address in a text message before responding or using the link?		
Yes	7	25
No	21	75
If you receive a text message containing a link, and you decide that you trust the sender, do you use the link provided in the text message?		
Yes	6	21.4
No	10	35.7
Sometimes	12	42.9
Do you receive legitimate text messages that contain sensitive information?		
Yes	17	60.7
No	8	28.6
I don't know	3	10.7

Table 4. Frequencies of message qualities used to determine a message's legitimacy.

Message Quality	*n*	%
Sender's phone number	24	85.7
Time of delivery	5	17.9
Details of the message	26	92.9
Sender's organization	17	60.7
Spelling errors and typos	20	71.4
Qualities of the link	15	53.6
Other recipients	8	28.6
Expectation of the message	16	57.1

Like emails, most participants report checking the sender's phone number (n = 24) and checking for spelling errors (n = 20) when trying to identify malicious text messages. The list of qualities participants used to identify a message's legitimacy is shown in Table 4.

Discussion

Our findings confirm that SMiShing is a common problem among users (Desolda et al., 2021), with some users receiving up to one SMiShing message daily. Our sample has relatively average cyber hygiene which is consistent with other findings, and their technical training is lacking (Vishwanath et al., 2020). Even though most participants did not know the formal definition of SMiShing, the data suggest they were aware of the security vulnerabilities associated with using links within text messages from unknown senders. Most reported that using links sent via text messages from unknown senders is never safe. However, the data also shows that most users are using links sent via text messages and even logging into personal accounts with those links.

There seems to be a disconnect between users' knowledge of SMiShing and their behaviors. The impact of knowledge on email phishing susceptibility has been widely studied, and the results are mixed. Most results suggest that knowledge and experience with phishing should decrease the susceptibility to falling victim (Bardsley-Marcial, 2022). However, this does not seem to be the case when it comes to the behaviors related to SMiShing.

There is some overlap between how one is supposed to diagnose malicious phishing and SMiShing messages. The data suggests that users place the most emphasis on the details of the message, the sender's phone number, and spelling errors. Users report placing the least importance on examining the time of delivery and the other recipients of the message.

Additional research is needed to determine how to defend against SMiShing properly. Can we provide better training? The FBI.gov website suggests that users: 1.) look up a company's phone number or website directly in their browser's search box 2.) never click on links via text message. Do we provide better defense mechanisms? Phone companies could introduce a spam folder option for text messages and allow users to mark messages as such.

Can we design better interface interactions that encourage safer practices? For instance, Sheng et al. (2007) designed anti-phishing phil, a game-based training method, to train users to identify phishing websites. Yang et al. (2017) designed a traffic-ranking based phishing warning system with embedded training and showed its effectiveness in a field experiment. Nicholson et al. (2017) found that employing nudges for email phishing users performed better when their attention was drawn to sender details rather than receiver details. Designers might be able to use training and nudges to help users make more secure decisions within the SMiShing messages.

This survey of non-technical college students shows a growing need to understand the Human Factors of SMiShing. While all participants reported that using links within text messages from unknown senders is risky though the knowledge was not reflected in the behavior. They still reported using them anyway. The information available for users to examine the trustworthiness of a text message is dramatically less than an email. Still, users show an effort to vet messages. Unfortunately, they are still not targeting critical features like who else received the message. Hopefully, these descriptive findings can be cited to support the future development of SMiShing policies, models, training, and defensive mechanisms from a human-centric perspective.

References

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

Bardsley-Marcial, B. (2022). Common factors in susceptibility to phishing. *International Journal of Information, Business and Management*, *14*, 97-104.

Blanco, O. (Sept., 2022). *Smishing: a silly word for a serious fraud risk*. Consumer Reports. https://www.consumerreports.org/money/scams-fraud/smishing-a-silly-word-for-a-serious-fraud-risk-a8541743941/

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*, *42*, 36-45.

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing email detection based on structural properties. In *NYS Cyber Security Conference Proceedings*, *8*, 1-7.

Cybersecurity Ventures (Nov., 2020). Cybercrime to cost the world 10.5 trillion annually by 2025. Retrieved March 2nd, 2023 from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025.

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.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, October). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 37-44).

Kamau, J., & Kaburu, D. (2022). A Review of Smishing Attacks Mitigation Strategies. *International Journal of Computer and Information Technology*, *11*, 2279-0764.

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security. *Human Factors*, *57*, 721–727. https://doi.org/10.1177/0018720815585906

Mishler, S., Jeffcoat, C., & Chen, J. (2019). Effects of anthropomorphic phishing detection aids, transparency information, and feedback on user trust, performance, and aid retention. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*, 183–183. https://doi.org/10.1177/1071181319631351

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

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

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99).

Sommestad, T., & Karlzen, H. (2019). A meta-analysis of field experiments on phishing susceptibility. In *2019 APWG Symposium on Electronic Crime Research*, *13*. https://doi.org/10.1109/ecrime47957.2019.9037502

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160.

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017, April). Use of phishing training to improve security warning compliance: Evidence from a field experiment. In *Proceedings of the hot topics in science of security: symposium and bootcamp* (pp. 52-61).

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.