Understanding phishing in mobile instant messaging: A study into user behaviour toward shared links

Rufai Ahmad[0000-0002-5580-9988] and Sotirios Terzis[0000-0002-5061-9923]

Department of Computer and Information Sciences
University of Strathclyde, Glasgow, United Kingdom
rufai.ahmad@strath.ac.uk; sotirios.terzis@strath.ac.uk

Abstract. In recent years, users of Mobile Instant Messaging (MIM) apps like WhatsApp and Telegram are being targeted by phishing attacks. While user susceptibility to phishing in other media is well studied, the literature currently lacks studies on phishing susceptibility in MIM apps. This paper presents a study that offers the first insights into the susceptibility of users of MIM apps to phishing by investigating their behaviour towards shared links. Using an online survey, we collected data from 111 users of MIM apps and found that participants frequently click and forward links during instant messaging, while factors such as the user's relationship with the sender and the group context of the communication influence these behaviours. The results show that behaviours of most users towards shared links try to reduce their risk to phishing by trusting their friends, family and colleagues to protect them. This raises some interesting questions for further research on the effectiveness and reliability of their strategy.

Keywords: Mobile Instant Messaging, Phishing, Mobile Phishing.

1 Introduction

Phishing is an attempt to obtain sensitive information from internet users by tricking them into visiting fraudulent websites or downloading malware [1]. According to the Anti-Phishing Working Group (APWG), phishing attacks have tripled since early 2020, with the number of unique phishing URLs detected in the last quarter of 2021 increasing to 316,747 from 260,642 in the third quarter of 2021 [2]. A recent report by Kaspersky shows that phishing is moving to Mobile Instant Messaging (MIM) apps, with a significant share of phishing links on android smartphones between December 2020 and May 2021 distributed through WhatsApp (89.6%), Telegram (5.6%) and Viber (4.7%) [3]. This is not surprising considering the popularity of these apps, with recent data showing that 3.09B mobile phone users communicated using these apps in 2021 [4]. The lack of countermeasures to protect MIM app users from phishing [5] and functions like sharing and forwarding links, creating and joining private and public groups advertised online actually facilitate phishing. The small screen size of mobile devices and the fact that users are likely to check messages while engaged in other activities may also affect users' ability to assess message validity and spot phishing thus increasing their susceptibility. As a result, phishing in MIM apps is a concern in need of attention.

To date there has been little research on how best to address phishing in MIM apps. A key step in this respect is to understand to what extent users engage in behaviours in MIM apps that put them at risk of phishing. This paper aims to fill this gap by answering the following research questions:

RQ1: How frequently do users click and forward links shared in MIM apps?
RQ2: Do factors such as the communicating parties and group context influence users' behaviours towards links shared in MIM apps?

To address these questions, we conducted an online survey about the behaviours of MIM app users towards shared links. The survey targeted MIM app users aged 18 and above. Our findings show that 1) many participants frequently click and share links; 2) participants click links from friends, family, and work colleagues more frequently than other communicating parties; and 3) although participants are as likely to click links in one-to-one and group communication, they are more likely to share links they receive in private rather than public groups. Although these results are encouraging in that they show users take some care to reduce their risk to phishing, they also show that users tend to put their trust on friends, family and work colleagues to protect them from phishing raising some interesting questions on the reliability and effectiveness of this strategy that deserve further research.

We begin the paper with a review of related literature before we focus on the design of our study, the presentation of its results, and a discussion of the result implications and study limitations. We conclude the paper by identifying directions for future work.

2 Literature Review

Research on phishing tends to fall into four categories: (1) solutions that detect and block phishing links and content with minimum or no user intervention [6], [7]; (2) phishing awareness/training approaches that aim to equip users with the required knowledge to defend themselves [8], [9]; (3) approaches that support users to detect phishing attacks by providing security cues [10]; and (4) studies that aim to determine user susceptibility to phishing by analysing their behaviours [11]. Our work falls within the scope of the latter, so this section will provide an overview of research in this area, focusing on the mobile context. However, it is interesting to note that MIM apps do not provide any automated means for detecting and blocking links [5].

Most studies on user susceptibility to phishing focus on fixed devices such as desktop computers and tend to look into phishing emails [12]–[14], phishing web pages [11] and phishing URLs [15]. The main conclusion from these studies is that users do not use the right cues when deciding the legitimacy of emails or URLs and this makes them susceptible to phishing attacks. Moreover, research shows that trust is a significant predictor of phishing susceptibility [16], [17], with trust being the willingness to be vulnerable to others because we expect them to act according to our expectations [17]. This is because the user tendency to trust others is often exploited in phishing attacks. Finally, the study in [18] found that respondents were more likely to respond to phishing emails when the sender was their friend. These findings are likely to be relevant for MIM apps where communication tends to be between known contacts [19].

Research on the susceptibility of mobile device users to phishing is limited. Motivated by the need to understand the impact of mobile device limitations, like smaller screen size compared to desktop computers, in [20] researchers studied mobile phone users to determine which indicators they used when deciding the legitimacy of a webpage. They found that (>90%) of the participants rely on the website's design, content, and functionality to decide its legitimacy. Participants who used URL and other browser security indicators performed better than those who didn't. There was no correlation between participants' scores and their age, technical proficiency, or time spent on a smartphone. Participants also reported being confused with the HTTPS and green padlock in safari. These findings are similar to those found for desktop computers.

In [21], the cybersecurity knowledge and attitudes of 206 mobile phone users from Japan (n=106) and Tanzania (n=100) were assessed. In addition, to lacking knowledge about phishing, 58% of respondents from Tanzania were likely to open a link in an email from an unknown sender. Participants from Japan had higher awareness of the risk as only 38% were likely to do so.

In [22] the authors assessed the susceptibility of mobile phone users to phishing through Quick Response (QR) codes. Their findings show that 225 users visited obscured URLs attached to QR codes placed in public places, with only 58% reading the URLs before visiting, while 36% visited the URLs without checking them.

Despite evidence of phishing in MIM apps, the literature currently offers no insights into users' susceptibility to phishing in them. The popularity of these apps, combined with many features they provide, such as the ability to receive messages from strangers during group-based communication; privately message members of groups; share and forward links; and use of link previews, can facilitate phishing attacks. These features, combined with the lack of automated solutions to detect and block phishing URLs, make investigating user susceptibility to phishing in this context timely and worthwhile.

3 Methodology

This study used a web-based survey to collect data from MIM apps users above 18 years. The survey focused on user behaviour towards links shared through MIM apps both during one-to-one and group communication. Our departmental ethics committee approved the study.

We limited our respondents to those using Signal, Slack, Telegram, Viber, Line, and WhatsApp because of their popularity and the features that they provide, such as group communication, link previews, link sharing, messages/links forwarding, and the ability to join public groups via links shared by group admins online, which can increase the phishing susceptibility of their users

All questions in the survey were based on either a Likert-scale or multiple choice answers. More specifically, the survey includes four demographic questions relating to age, gender, education and country of residence, one device usage question, one question on what MIM apps respondents use, seventeen Likert-type questions relating to the behaviour of the participants during one-to-one and group communication, and six questions on link forwarding behaviours.

We recruited participants using an approach that combines snowball sampling and social media. Snowball sampling is a non-random sampling method appropriate for recruiting research participants that are hard to reach or unknown [23]. The process for recruiting participants involves three steps: (1) the first author used the contact list of all the mobile messaging apps he currently uses to advertise the survey; (2) we identified and posted the survey on various social media groups, including r/SampleSize on Reddit, samplesize on Facebook and SurveyCycle; and (3) we emailed our colleagues asking them to take part and forward the survey to others. At each stage, we asked participants to invite others to participate in the study by sharing the link to the survey with them. Data collection began on Oct. 12 2021, and ended on Nov. 5 2021.

The data collected from the survey was purely nominal or ordinal. We used frequencies and percentages of each response and present the data visually using frequency graphs. Where a test of significance was required, we used non-parametric tests like Wilcoxon signed-rank and Friedman test, as they are considered appropriate for this type of data [24]. However, we acknowledge that the discussion on the appropriateness of either parametric or non-parametric tests is ongoing [25]. All follow-up pairwise comparisons were conducted using Dunn-Bonferroni posthoc tests. All survey questions were optional. Therefore, missing values may exist, but we excluded them from the analysis, in which case, the actual number of participants used is reported. We used SPSS software for the statistical analysis.

4 Results

A total of 129 participants accessed the online survey. After data cleaning, we excluded 18 participants for failing to meet our screening criteria. The participants were skewed with respect to gender (73, 65.8%) male, (37, 33.3%) female, and one participant preferred not to disclose their gender. The highest age group in the sample was 18-30 (54, 48.6%), followed by 31-45 (51, 45.9%) and 46+ (6, 5.4%). Most of the participants have a postgraduate qualification (60, 54.1%), followed by undergraduate (33, 29.7%), further education (13, 11.7%), and secondary education (5, 4.5%). Many participants resided in the UK (64, 58.7%) when they accessed the survey, followed by Nigeria (18, 16.5%), and (29, 26.1%) other countries, including Germany, Canada, the USA, Malaysia, the Netherlands, France, Singapore, Saudi Arabia, Finland, Russia and Libya.

All participants used mobile phones daily (n=111). The highest used MIM app by the participants was WhatsApp (106, 95.5%), followed by Telegram (40, 36.0%), Signal (19, 17.1%), Slack (13, 11.7%), Viber (6, 5.4%) and Line (4, 3.6%). We are not surprised by this, considering that WhatsApp and Telegram are among the most popular messenger apps globally [26]. Figure 1 shows that many participants use MIM apps to communicate with friends (97, 87.4%), family (92, 82.9%) and work colleagues (80, 72.1%). This confirmed earlier findings that showed instant messaging is mainly between friends or family [27]. Most participants are currently members of MIM app groups (103, 92.7%), but when asked whether they know the types of groups, only (71, 68.9%) said yes. We asked this because groups in MIM apps can be public or private, with public groups exposing users to higher phishing risks as they are open to anyone.

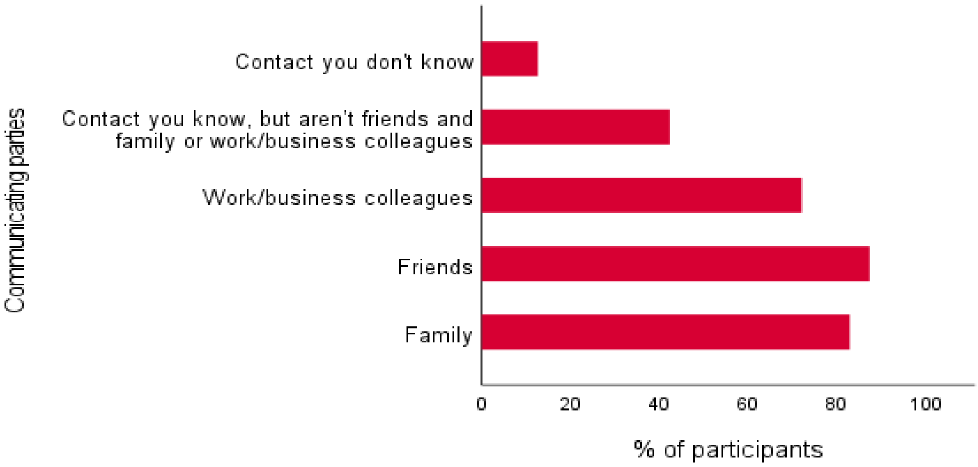

Fig. 1. Participants Communicating Parties (n=111)

To answer RQ1, we first asked the participants to indicate how frequently they click on links during communication in MIM Apps. We followed up with another question regarding their frequency of clicking links shared in groups. We wanted to check if there was any difference in the participants' behaviour across these two conditions. Figure 2 shows that most participants sometimes click on links in both conditions (52, 51%) for general click frequency and (47, 46.1%) for group communication. The figure also shows that a high percentage of the participants tend to engage in these behaviours frequently. We noticed a slight difference in the frequency of clicking shared links in general and during group communication. To test whether this difference is significant, we conducted Wilcoxon signed-rank test. The test results in a Z statistics of -0.394, and a p-value of .680, implying that this difference is not statistically significant. Thus, we cannot reject the null hypothesis of equal medians for the two variables. To measure the participants' link forwarding behaviour, we asked them to indicate the frequency they engage in this behaviour. Out of 105 responses (n=42) indicated that they sometimes forward links to others, as indicated by a median value (Mdn=3). Some participants (n=18) indicated that they often do so, while (n=31) said they rarely do so.

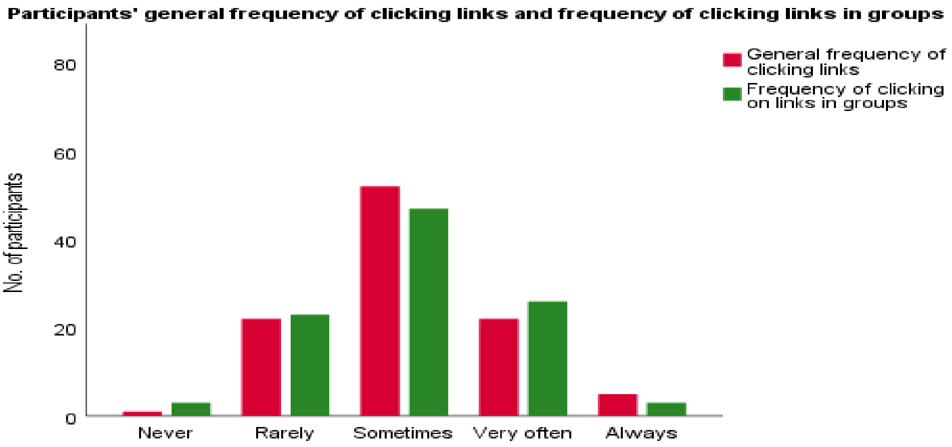

Fig. 2. Frequency of clicking links by the participants (n=102)

To answer RQ2, we first looked into how frequently users click on links from different communicating parties. Due to the design of the questionnaire, questions relating to the frequency of clicking links from communicating parties were only displayed to participants if they had previously indicated to communicate with them. As a result, there were many combinations. Our findings revealed that most participants (n=30) used MIM apps to talk with four different types of people, typically friends, family, work colleagues, and other known contacts, followed by those with three types (n=28) typically friends, family and work colleagues, and those with two (n=13) typically family and friends. Some participants (n=10) indicated they communicate with all five types of people listed in Figure 1, while others (n=17) said they communicate with only one type of people, typically friends (n=7), family (n=4), or work colleagues (n=4). Since we aim to find the difference in user click behaviour based on two or more conditions, our analysis focused only on participants that communicate with more than one type of user. Furthermore, we only report cases where we found a statistically significant difference.

Communicating party	Never	Rarely	Sometimes	Very often	Always	Medians
Friends	0	2	13	8	7	3.5
Family	0	4	10	10	6	4.0
Work colleagues	0	1	12	14	3	4.0
Other known contacts	6	18	4	1	1	2.0

Table 1. Count of participants that selected four types of users with the frequency level

For the participants that selected four communicating parties (n=30), our analysis revealed that many of them rarely (n=18) or never (n=6) clicked on links from contacts they did not know (see Table 1). Clicking links from family and work colleagues received the highest frequency ratings, as indicated by each having a median of (Mdn =4), followed by friends (Mdn=3.50). The frequency of clicking links from contacts who are not family, friends or work colleagues has the lowest rating (Mdn=2). A Friedman test showed a significant difference in the median ratings across the four communicating parties, $\chi2$ (3) =59.416, p<.001. Post hoc tests indicate a significant difference between the first three communicating parties and contacts the participants know but are not friends, family or business colleagues (p<.001).

Some participants (n=10) indicated that they communicate with all the five types of communicating parties. Table 2 shows the number of participants for each frequency level based on communicating parties. Links from friends, family and work colleagues received the highest ratings, with a median (Mdn=3.50) for each. Other communicating parties received lower ratings (Mdn= 2.50) for known contacts but not friends, family or work colleagues, and (Mdn= 2) for unknown contacts. A Friedman test showed a significant difference in the median ratings across the four communicating parties, $\chi2$ (4) =25,638, p<.001. Post hoc tests indicate a significant difference between the participants' frequency of clicking links from work colleagues and contacts not known (p=.007).

Communicating party	Never	Rarely	Sometimes	Very often	Always	Medians
Friends	0	3	2	4	1	3.50
Family	0	2	3	4	1	3.50
Work colleagues	0	1	4	3	2	3.50
Other known contacts	0	5	4	1	0	2.50
Strangers	3	5	2	0	0	2.00

Table 2. Count of participants that selected five types of users with the frequency level

We examined the impact of group type on the participants' link forwarding behaviour by requesting them to indicate how frequently they forward links shared in public or private groups. Figure 3 shows that the frequency of forwarding links received in private groups received the highest ratings, as indicated by the median (Mdn= 3) compared to (Mdn=2) for public groups. A related sample test using the Wilcoxon Signed-Rank test was performed. The outcome revealed a statistically significant difference between the medians of the two behaviours z = 4.884, p<.001.

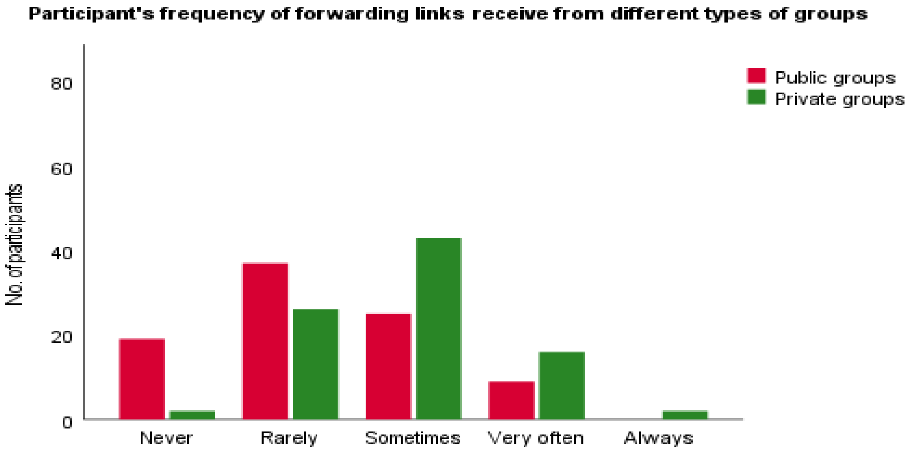

Fig. 3. Participants' frequency of forwarding links received from different types of groups

5 Discussion and limitations

Our study results show that many participants click and forward links shared in MIM apps. A number of them do so not only in one-to-one but also group communication, as we found no statistically significant difference in the frequency of clicking links shared in the both. While it is okay to do so, it becomes a problem when such behaviour becomes habitual since this can affect how users process information [28]. With evidence of phishing in MIM apps, habitual clickers and forwarders are likely to put themselves and others at risk. However, our findings reveal that participants' behaviour is more nuanced, as they are more likely to click on links shared by their friends, family or work colleagues. Moreover, they are more likely to forward links they receive in private rather than in public groups, most likely because private groups comprise known contacts, like friends, family and work colleagues. However, worryingly some users are not aware what types of groups they actually use.

Although the reasons behind these behaviours are not known, trust is likely to be a factor, with participants implicitly or explicitly relying on people in their social circle to protect them from phishing. However, it is unclear whether this reliance is justified. Phishers can abuse people's trust in their social circle. In fact, there is evidence that in the context of phishing emails, trust makes users more susceptible to phishing.

One limitation of this study is that our sample size is relatively small. In addition to this, the use of snowball sampling, despite being powerful, often results in participants with higher interconnectivity than would be seen in the general population, and has introduced some biases in our participant population. Our survey participants are highly educated, as evidenced by the majority having an undergraduate or postgraduate education, which may have an impact on the measured behaviours. Moreover, they are predominantly male, but the effect of gender on user security behaviour has been inconsistent in the literature. They also tend to be younger in age with few of them in the

46+ age groups, but this may reflect the higher popularity of MIM app use in younger ages. Our participants are mostly resident in the UK with some in Nigeria, which may have also an impact on the measured behaviours. Thus, generalising our findings to the whole MIM app large and diverse userbase carries certain risks. Finally, our study relies on self-reported behaviours, as such the data may not be an accurate reflection of how users behave towards links in real-life.

6 Conclusions

MIM apps with billions of people using them to communicate with friends, family, and others have drawn the attention of phishers. The functionalities of these apps, such as the ability to share links or join groups, including public ones, enable easy access to a large pool of users, making these apps an attractive medium for phishing attacks. Despite that, little research to date has focused on phishing in MIM apps.

In this paper, we offer the first insights into the behaviours of users of MIM apps towards shared links. Our online survey study found that participants frequently click and forward shared links, and they do so both in one-to-one and group communication, potentially exposing them to the risk of phishing. However, we also found that participants try to protect themselves from phishing by being less likely to click links that are shared by those that aren't their friends, family and work colleagues. They are also less likely to forward links shared in public rather than private groups. So, most participants appear to trust their friends, family and work colleagues to protect them from phishing.

It is unclear how reliable and effective this strategy is. Research on email phishing indicates that it may be neither reliable nor effective, but further research is required to determine whether this is the case in MIM. In addition to this, future research could also investigate whether technical skills and phishing efficacy influence users' behaviours towards shared links in MIM apps with the aim to establish whether such behaviours differ from those in other media, like email.

References

[1] NCSC, "Phishing attacks: defending your organisation," 2018. https://www.ncsc.gov.uk/guidance/phishing (accessed Jan. 25, 2021).

[2] APWG, “Phishing Activity Trend Report (4th Quarter 2021),” 2022. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf?_ga=2.172997153.361044271.1647946096-1993957391.1647946096&_gl=1*1c9f67o*_ga*MTk5Mzk1NzM5MS4xNjQ3OTQ2MDk2*_ga_55RF0RHXSR*MTY0Nzk0NjA5NS4xLjEuMTY0Nzk0NzU0MC4w.

[3] Kaspersky, "Phishing in messenger apps – what's new?," 2021. https://www.kaspersky.com/about/press-releases/2021_phishing-in-messenger-apps-whats-new (accessed Jan. 04, 2022).

[4] Statista, "Number of mobile phone messaging app users worldwide from 2018 to 2022," 2021. https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-

worldwide/ (accessed Apr. 13, 2021).

[5] G. Stivala and G. Pellegrino, "Deceptive Previews: A Study of the Link Preview Trustworthiness in Social Platforms," 2020.

[6] E. Medvet, E. Kirda, and C. Kruegel, "Visual-similarity-based phishing detection," 2008, doi: 10.1145/1460877.1460905.

[7] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: A content-based approach to detecting phishing web sites," 2007, doi: 10.1145/1242572.1242659.

[8] P. Kumaraguru *et al.*, "School of phish: A real-world evaluation of anti-phishing training," 2009, doi: 10.1145/1572532.1572536.

[9] N. A. G. Arachchilage and M. Cole, "Design a mobile game for home computer users to prevent from 'phishing attacks,'" 2011, doi: 10.1109/i-society18435.2011.5978543.

[10] M. Volkamer, K. Renaud, and B. Reinheimer, “Torpedo: tooltip-powered phishing email detection,” in *IFIP International Conference on ICT Systems Security and Privacy Protection*, 2016, pp. 161–175.

[11] M. Alsharnouby, F. Alaca, and S. Chiasson, “Why phishing still works: User strategies for combating phishing attacks,” *Int. J. Hum. Comput. Stud.*, 2015, doi: 10.1016/j.ijhcs.2015.05.005.

[12] A. Jayatilaka, N. A. G. Arachchilage, and M. A. Babar, “Falling for Phishing: An Empirical Investigation into People’s Email Response Behaviors,” *arXiv Prepr. arXiv2108.04766*, 2021.

[13] K. Parsons, M. Butavicius, M. Pattinson, D. Calic, A. Mccormac, and C. Jerram, “Do users focus on the correct cues to differentiate between phishing and genuine emails?,” *arXiv Prepr. arXiv1605.04717*, 2016.

[14] K. Parsons, M. Butavicius, P. Delfabbro, and M. Lillie, “Predicting susceptibility to social influence in phishing emails,” *Int. J. Hum. Comput. Stud.*, vol. 128, pp. 17–26, 2019.

[15] S. Albakry, K. Vaniea, and M. K. Wolters, “What is this URL’s Destination? Empirical Evaluation of Users’ URL Reading,” 2020, doi: 10.1145/3313831.3376168.

[16] M. Workman, “Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security,” *J. Am. Soc. Inf. Sci. Technol.*, vol. 59, no. 4, pp. 662–674, 2008.

[17] G. D. Moody, D. F. Galletta, and B. K. Dunn, “Which phish get caught? An exploratory study of individuals′ susceptibility to phishing,” *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 564–584, 2017.

[18] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” *Commun. ACM*, vol. 50, no. 10, pp. 94–100, 2007.

[19] K. Church and R. De Oliveira, “What’s up with WhatsApp? Comparing mobile instant messaging behaviors with traditional SMS,” 2013, doi: 10.1145/2493190.2493225.

[20] J. Loxdal, M. Andersson, S. Hacks, and R. Lagerström, “Why Phishing Works on Smartphones: A Preliminary Study.,” in *HICSS*, 2021, pp. 1–10.

[21] J. D. Ndibwile, E. T. Luhanga, D. Fall, D. Miyamoto, and Y. Kadobayashi, “A comparative study of smartphone-user security perception and preference towards redesigned security notifications,” in *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, 2018, pp. 1–6.

[22] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor, and N. Christin, “QRishing: The

susceptibility of smartphone users to QR code phishing attacks," in *International Conference on Financial Cryptography and Data Security*, 2013, pp. 52–69.

[23] Y. Rashidi, K. Vaniea, and L. J. Camp, "Understanding Saudis' privacy concerns when using WhatsApp," in *Proceedings of the Workshop on Usable Security (USEC'16)*, 2016, pp. 1–8.

[24] S. Jamieson, "Likert scales: How to (ab) use them?," *Med. Educ.*, vol. 38, no. 12, pp. 1217–1218, 2004.

[25] G. Norman, "Likert scales, levels of measurement and the 'laws' of statistics," *Adv. Heal. Sci. Educ.*, vol. 15, no. 5, pp. 625–632, 2010.

[26] H. Tankovska, "Most popular global mobile messenger apps as of January 2021, based on number of monthly active users," 2021. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (accessed Apr. 11, 2021).

[27] A. J. Sultan, "Addiction to mobile text messaging applications is nothing to 'lol' about," *Soc. Sci. J.*, 2014, doi: 10.1016/j.soscij.2013.09.003.

[28] E. D. Frauenstein and S. V Flowerday, "Social network phishing: Becoming habituated to clicks and ignorant to threats?," in *2016 Information Security for South Africa (ISSA)*, 2016, pp. 98–105.