How Do Children Interact with Phishing Attacks?

Mohammed I Alwanain
malwanain@mu.edu.sa
Majmaah University
Department of Computer Science,
College of Science and Humanities in Alghat, Saudi Arabia

Summary
Today, phishing attacks represent one of the biggest security threats targeting users of the digital world. They consist of an attempt to steal sensitive information, such as a user's identity or credit and debit card details, using various methods that include fake emails, fake websites, and fake social media messages. Protecting the user's security and privacy therefore becomes complex, especially when those users are children. Currently, children are participating in Internet activity more frequently than ever before. This activity includes, for example, online gaming, communication, and schoolwork. However, children tend to have a less well-developed knowledge of privacy and security concepts, compared to adults. Consequently, they often become victims of cybercrime. In this paper, the effects of security awareness on users who are children are investigated, looking at their ability to detect phishing attacks in social media. In this approach, two Experiments were conducted to evaluate the effects of security awareness on WhatsApp application users in their daily communication. The results of the Experiments revealed that phishing awareness training has a significant positive effect on the ability of children using WhatsApp to identify phishing messages and thereby avoid attacks.

Keywords: *Anti-phishing countermeasures, online fraud, E-commerce security, evaluation experiments*

1. Introduction

Internet services such as online banking, e-government services, and online shopping have become a significant part of modern life. However, although these services make our lives more convenient and manageable, criminals have found ways of accessing users via the Internet, in order to steal their sensitive information. This can cost Internet users dearly. Phishing is one of the main crimes perpetrated against Internet users, because the sophistication of phishing attacks continues to develop alongside the expansion of Internet technology and online services. Consequently, phishing has become one of the most serious challenges to businesses and the general public in recent years [1]. The FBI's Internet Crime Report states that in 2019, the Internet Crime Complaint Center (IC3) received 467,361 complaints, associated with estimated losses of over $3.5 billion [2]. These complaints concerned business email compromise (BEC), ransomware, children and elder fraud, and tech support fraud.[3]

Manuscript received March 5, 2021
Manuscript revised March 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.3.17

The number of child Internet users has increased sharply in recent times, causing researchers to pay attention to the digital risks posed to children, and alerting them to the need to educate young Internet users about cybersecurity [3], [4]. In the United States, for instance, it was found in 2020 that more than 46% of children aged 2-4 years and 67% aged 5-8 years had already used their own tablets or smartphones for online viewing, and these figures increased with age [5]. This increase in children's Internet use highlights the pressing need for instruction in how to avoid Internet risks, directed at younger age groups. For example, in 2017, over one million children aged 17 and below were recorded as victims of identity theft in the United States alone, incurring losses of approximately $2.6 billion [6]. This is due to children showing less concern about online risk, due to their lack of knowledge of the need for online privacy.

Hasebrink et al.[7] define three sources of risk facing children online: content, contact, and conduct. Content risk refers to inappropriate online content that could be transmitted, shared, or displayed to children, while contact risk involves children actually being contacted by phishers or users with malicious intent. Finally, conduct risk means the children themselves using the Internet and behaving inappropriately via this medium. Therefore, children urgently need regular formal training to improve their security awareness and therefore avoid the aforementioned risks.

Currently, there are several training tools designed to protect and enhance the awareness of Internet users such as Security Skin [8], SpoofStick [9] , Netcraft [10],and Web Wallet[11]. However, these tools have mainly focused on adults and senior students, leaving the younger age groups understudied as a population. Therefore, in order to investigate the gap of children's Internet security training in more depth, three main research questions were formulated for this study:

Q1: Can children aged 7-13 years detect phishing attacks in social media?

Q2: Does the security awareness training conducted reflect a significant improvement in children's ability to detect phishing?

Q3: Is there any difference in the impact of security awareness between children of different age groups?

In order to answer these questions, two fully automated, real-world experiments were carried out to evaluate the reactions of child users to attacks via WhatsApp. Although a number of studies in the relevant literature have investigated fraud against children [3], [12]–[14], none have examined this type of fraud in the social media context, especially WhatsApp. The results of the experiments outlined in this paper strongly support the assumption presented above, namely that technical solutions cannot prevent phishing attacks without being accompanied by user awareness.

The remainder of this paper is organised as follows: Section two presents the background literature on anti-phishing approaches, while Section 3 explains the research methodology, and Section 4 defines the evaluation methods implemented. In Section 5, the results of the experiment are set out. Section 7 then concludes the paper with a discussion of the findings and recommendations for future work.

2. Related Work

In recent years, phishing attacks that target children have increased dramatically with the rise in very young Internet users. Therefore, several research has been published on how children experience and manage online risk [3], [12]–[14]. These studies show that children are vulnerable to many threats, including phishing attacks where sensitive information is stolen, or where there is online harassment or sexual content.

For instance, Lastdrager et al. [12] examined the effectiveness of anti-phishing training for children aged 9-12 years. The training was conducted manually in the form of storytelling during lecture time. The sampled children were evaluated with a paper-based test, where they had to distinguish between phishing and genuine emails and websites. However, the above author illustrated that the children's awareness was diminished after a period of 2-4 weeks. This work emphasises the need for a regular training program for children to improve their anti-phishing awareness at different educational levels. In Lastdrager et al.'s study, training was performed manually in the storytelling, but evaluation was paper-based in a test.

Likewise, Maqsood et al.[15] implemented a Web-based game to enhance the awareness of children aged 11-13 years, in terms of digital literacy. Several aspects of security were addressed, such as privacy, sharing, racking, cyberbullying, and the authentication of information. The approach proved effective in improving the participants' awareness. In addition, Zaikina-Montgomery and Silver [16] investigated the interaction between common features of the warning messages that are used to attract children, such as icons, colors, and words. These studies have implications for the design of warnings for children. However, they do not offer any insights into why children display certain responses or perceptions.

Al Shamsi [14] studied the effectiveness of the cybersecurity awareness program offered by the Ministry of Education in UAE for students aged 8-10 years. The dataset was collected manually through interviews with both trainers and students on the program. The author found that the various online threats to children, together with other incidents included in the cybersecurity awareness program, corresponded to actual threats that children could be exposed to in the real world. In the above study, the author stated that both the trainers and the students strongly agreed on the efficacy of the awareness program and confirmed that it had influenced their online behavior.

In fact, the idea of automated the prevention of phishing attacks is still under development and research. Therefore, several solutions as aforementioned have been approached to mitigate the risk of phishing attacks by identifying suspicious websites. However, these tools cannot prevent all phishing attacks, since some attacks of this nature are missed, and some genuine emails or websites are flagged as phishing, i.e., there are problems with false positives and negatives [17]. In order to mitigate this issue, Nguyen et al. [18] proposed a technical approach to evaluating webpages, applying six heuristic features extracted from URLs (primary domain, subdomain, path domain) and website ranks (page rank, Alexa rank, Alexa reputation). An evaluation of this approach was conducted in a training dataset of 11,660 phishing webpages and 10 testing datasets, each holding 1,000 phishing webpages or 1,000 legitimate webpages. The above approach achieved high accuracy, detecting 97.16% of phishing websites.

However, despite clear advantages to filtering phishing attacks at the level of emails and websites, these approaches cannot mitigate or prevent phishing attacks on social media that are accessed in daily life. In this regards, Alwanain [19] investigated the effects of security awareness on elderly users and their ability to detect phishing attacks in social media. The author conducted an experiment to evaluate the effects of security awareness on WhatsApp application users in their daily communications. The results of the experiment revealed that phishing awareness has a significant positive effect on the ability of elderly users to identify phishing messages, thereby avoiding attacks. However, the approach was only

focused on elderly users and the phishing experiment conducted manually.

This current paper reports on an evaluation of child users' knowledge in a real environment to discover how they interact with phishing attacks perpetrated via social media. Two fully automated experiments were conducted, targeting primary school children who used the WhatsApp application on a regular basis. In these experiments, the results were analysed with respect to user confidentiality and privacy. The following sections describe these experiments in detail.

3. Methodology

Nowadays, social media platforms have become a primary channel of communication between people around the globe, because they are usually less expensive to use than traditional forms of communication such as phone calls, especially for those who regularly need to communicate internationally for business or personal reasons. Currently, there are various types of social media that can be used for communication, but the most commonly applied is WhatsApp [20], an application developed by Facebook.

WhatsApp has received considerable attention in recent years and is listed among one of the most heavily used applications in daily life worldwide. The latest statistics for the WhatsApp website indicate that in 2020, over two billion people in over 180 countries used WhatsApp in 60 different languages. To illustrate this usage, 65 billion text and voice messages were reported as sent daily via WhatsApp [21]. Due to the application's usability, it is estimated that the average user opens the application 23-25 times a day[20]. These extraordinary statistics make the application an interesting target for attackers. Correspondingly, Vade Secure [22] report that phishing attacks via WhatsApp increased from 13.1% in the third quarter to 24.1% in the fourth quarter of 2019. Such attacks can take place via text messages containing a hyperlink that directs the victim to a fake website, which is identical to a legitimate website, so that the victim's personal information can be stolen. However, not all users are interesting to attackers. As mentioned earlier, child users are becoming an especially attractive target for phishers. Thus, the recent statistics state that the number of crimes against children in 2017 reached over one million attacks in the United States alone, costing $2.6 billion [6]. The above statistic shows that the number of victims may be on the increase, especially with higher numbers of children using the Internet daily during the COVID-19 pandemic. Therefore, due to the lack of awareness training aimed at children and the rise in phishing attacks against them, it was decided to focus the current investigation on age group, 7-13 years, which is the age of the student at Saudi primary school.

In this paper, two experiments were consequently executed using 30 participants. The participants were divided into two groups: a Control and a Treatment group, each consisting of 15 participants. In the first experiment (Experiment 1), a phishing message (written in Arabic) was sent to the Treatment group. The message offered a discount for a popular game that would be known to most of the children, whether male or female. The message contained a hyperlink that directed the users to a website, which informed them that they had been the target of a phishing attack. The website consisted of information about phishing and the most common phishing scenarios, with the aim of training users, improving their knowledge, and thereby avoiding any future phishing attacks (see Figure 1).

Fig 1: A phishing website written in Arabic

In the present study, no information was requested from the participants. However, it was assumed that a participant clicking on the hyperlink would be a phishing victim. Conversely, the Control group participants received the same text message, but the hyperlink related to a real promotional offer for the game. The reason for including a Control group was to measure improvement in the second experiment (Experiment 2).

In Experiment 2, a different text message was sent, containing information about the timetable for the new semester, sent two days before the start of the semester. The message was sent to both the Control and Treatment groups, without any changes, so that the impact of Experiment 1 could be evaluated and the results of the two groups compared.

3.1 Participants

The Experiments in this current study were conducted on primary school children (aged 7-13 years), due to this being the age group in which children generally start using the Internet for their schoolwork, gaming, and social media interaction, for example, communicating via WhatsApp. In addition, this is the age group in which children begin forming a network beyond the family and their parents' friends. Therefore, the expansion of Internet use at this time can increase the risk of fraud, pointing to an urgent need to address the security awareness of the aforementioned age group in this study. Consequently, 30 participants were recruited from school years 1-6 (primary education lasts six years in Saudi Arabia) for a sample consisting of 15 boys and 15 girls to conduct the Experiments.

3.2 Ethics

Ethics are essential in human experiments. In this study, the design of the implementation and Experiments was reviewed and approved by the Deanship of Research at Majmaah University. However, the current study design was not considered likely to hurt or distress any of the participants. Furthermore, in these Experiments, the results were examined with respect to the users' confidentiality and privacy. No sensitive or personal information such as bank details, dates of birth, or passwords were requested from the participants during the Experiments. Additionally, the parents of the nominated participants were asked for written permission to conduct the training and test their children. The parents subsequently signed and returned informed consent forms to the researcher. The consent form contained the researcher's contact information, in case the parents had any questions. After completing the Experiments, each parent was contacted and informed of their child/children's result, which most found helpful.

4. Implementation

4.1 Objective

Nowadays, the Internet is becoming an essential part of daily family life. Up to around a decade ago, Internet services such as online banking, social media, email, and gaming were usually only accessed by adults. However, the American Community Survey (ACS) stated that 94% of children aged 3-18 years had home Internet access in 2018, which illustrates that the number of children who use these services is increasing sharply[23]. However, in connecting to the Internet, children can be exposed to various kinds of security threat such as phishing attacks and cyberbullying. Therefore, improving children's awareness of phishing attacks is an essential step toward preventing such attacks.

4.2 Design

The design of the training awareness tool used in this approach has three main components: a Web server, database server, and WhatsApp API (an application programming interface). The Web server was used for a website implemented in PHP Laravel, operated and stored on a local machine and run by an Apache server. The domain name system (DNS) host files in the Windows operating system were modified, so that the Web browsers displayed the URL of the actual phishing websites. When a user clicked on the corresponding link, the website would store information of importance to the Experiments, such as the user's IP address, telephone number, and the date and time of the action. All this information was saved in the local database server, so that a statistical analysis could be carried out.

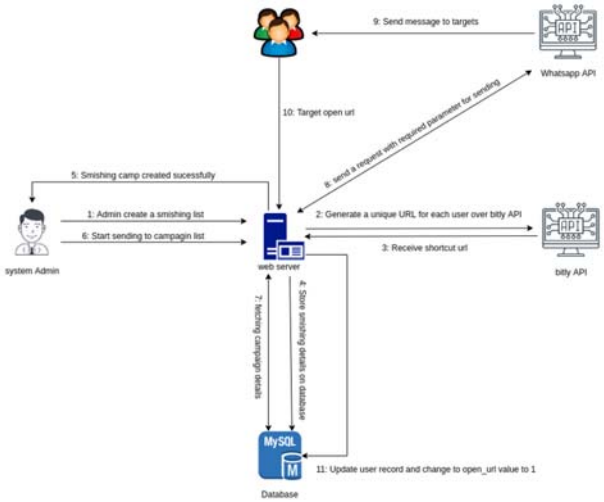

Fig 2: A phishing scenario

As Figure 2 shows, a system administrator can create a new phishing campaign, required to define several values, such as 'Target group numbers', 'Message to be sent', 'Landing page', and 'Fake landing page'. Once these values have been filled, the system will automatically create a new campaign, consisting of a campaign ID (incremental value), the target number of participants, and the unique URL for each participant. However, the URL generated will be long, potentially making it look suspicious and illegitimate. Thus, to make the URL seem more authentic in this current study, the system was connected at the backend to a shortcut URL service called Bitly API [24]. After sending a valid request to this API, a shortened link was automatically generated by Bitly for each participant. The system then appended the unique URL to the message and sent it to specific

participants, using the WhatsApp API. If the targets opened the URL, they would be redirected to a real landing page (an awareness page) and their records would be updated in the database.

5. Results

Once the Experiments were completed, a statistical analysis was carried out, using the IBM SPSS statistical software package.

5.1 Experiment 1

In Experiment 1, 15 WhatsApp messages containing a hyperlink to a legitimate website – where a promotional discount for a game was displayed – were sent to the participants in the Control group. Meanwhile, the Treatment group received 15 WhatsApp messages containing a hyperlink to a fake website. Experiment 1 was initiated on 1st December 2020, with the participants' parents being asked to observe their child/children's reaction to receiving the message. The results for both groups showed that only one participant clicked on the link sent on 1st December, whereas six participants clicked on the link sent on 2nd December: four participants (27%) in the Treatment group clicked on the fake links (1 girl; 3 boys), as shown in Table 2. Conversely, three participants (20%) in the Control group clicked on a legitimate link (1 boy; 2 girls). In total, seven of the 30 participants (23% of both groups combined) responded and clicked on the link (4 boys; 3 girls), as illustrated in Table 1. According to the parents' observations, all the male phishing victims blocked the sender immediately and reported the incident to WhatsApp, whereas the female victims informed their parents immediately after clicking on the suspicious link. However, none of the boy's victims informed their parents after clicking on the link.

Table (1): Distribution of the sample

Group	Control	Treatment	Total
Number of messages	15	15	30
Respond and click on the links (open fake and legitimate links)	3	4	7

Table (2): Victims' gender

Gender	Number of Victims (Open Fake Link)
Male	3
Female	1
Total	4

5.2 Experiment 2

In Experiment 2, the participants from both groups received a WhatsApp message containing a hyperlink related to a fake website. Similar to Experiment 1, a total of 30 messages were sent to both groups, each participant receiving one message (see Table 3).

Table (3): Distribution of the sample

Group	EXPERIMENTS			
	EXPERIMENT 1		EXPERIMENT 2	
	Open Url	Not OpenUrl	OpenUrl	Not OpenUrl
Treatment	4	11	2	13
Control	3	12	1	14
Total	7	23	3	27

The messages appeared legitimate, as they contained information about the school timetable. They were sent two days before the start of the new semester. This Experiment was initiated on 15th January 2021. Only three participants (10%) clicked on the link, all of whom were boys. Two of these boys had already been victims in the Treatment group in Experiment 1. Only one victim clicked on the link on the first day, whereas the other two clicked on the link on the second day.

The results show that the number of victims in the Treatment group was reduced from 27% in Experiment 1 to 13.3% in Experiment 2, while the number of victims in the Control group was reduced from 20% to 6.7% across the two Experiments. Therefore, overall, security awareness seemed to have significantly improved among the 30 participants, differing between Experiments 1 and 2 ($t(29)= -2.112$, $P<0.05$). However, the Treatment group showed a non-significant difference in security awareness in Experiment 1 ($t(13)= -0.978$, $P>0.05$) and Experiment 2 ($t(13)= -1.422$, $P>0.05$). Similarly, the Control group showed a non-significant difference in security awareness in Experiment 1 ($t(13)= -1.486$, $P>0.05$) and Experiment 2 ($t(13)= -1.075$, $P>0.05$).

Furthermore, there was no significant difference in the change in security awareness between the Control and Treatment groups. The Treatment group registered non-significant change in Experiment 2: ($M=1.73$, $SD=0.458$), ($M=1.87$, $SD=0.352$), and $t(14)= -1.468$, $P>0.05$), as did the Control group in Experiment 1: ($M=1.8$, $SD=0.414$), $t(14)= -1.468$, $P>0.05$, and Experiment 2: ($M=1.93$, $SD=0.258$) and $t(14)= -1.468$, $P>0.05$). In addition, the

gender variable had no significant effect on the degree of security awareness in either the Control or Ttreatment group. The reason for the low significant difference shown above was due to the significant impact observed of the security awareness that the children receive before they participate in experiments, from their society.

6. Discussion

The Experiments described above illustrate the effect of raising phishing awareness among child users, with regard to correctly identifying a phishing message in WhatsApp and thereby avoiding a phishing attack. This led to a higher rate of phishing avoidance amongst the phishing-aware users in both Experiments. It was therefore observed from the Experiments and the parents' feedback that most of the children ignored the phishing messages due to the high impact of the security awareness that the children received from their parents or society. For example, Table 3 shows that from the Treatment group, only 4 out of 15 participants in Experiment 1 interacted with the phishing message and clicked on the link. This number was then reduced by 50% in Experiment 2. The participants in the Control group also displayed a reduction in Experiment 2, compared to Experiment 1. Moreover, in Experiment 1, 5 participants in the Treatment group who did not click on the link, took action against the sender; 3 responded to the sender by indicating that they did not trust the messages and blocked the number, and the other 2 participants reported the suspicious messages to WhatsApp. Conversely, only 1 participant from the Treatment group who clicked on the link in Experiment 1 reported the issue to her parents, whereas the other victims did not report the incident to their parents.

In Experiment 2, the number of victims in both groups was reduced by approximately 43%. As mentioned in Experiment 2, the 2 victims from the Treatment group had already clicked on the link in Experiment 1. The investigation revealed that their knowledge of phishing was weak, and they did not have any idea of how to deal with phishing attacks.

From the above Experiments, unexpectedly high awareness results were observed in the sample. Interviews with the participants who ignored the messages in both Experiments illustrated that their awareness had been enhanced through education that they had regularly received from parents and friends, revealing a significant positive effect. The above finding answers Research Question 1, indicating that the children demonstrated a significant ability to detect phishing attacks perpetrated via social media. Consequently, it appears that phishing awareness has a significant positive effect on users' ability to detect and therefore prevent phishing, which answers Research Question 2.

Finally, it is clear from the aforementioned Experiments that children have some existing phishing awareness, as there was no significant impact of the training administered in this study. This compares favorably with the findings in [19], where elderly Internet users appeared to have poor phishing awareness. It indicates a possibly significant positive effect on users' ability to detect and understand the concept of phishing. However, no difference was found in the impact of security awareness between children of different ages, which answers Research Question 3.

7. Conclusion

This paper investigates the effects of user awareness on the ability of children aged 7-13 years to detect phishing attacks. Two Experiments were conducted, using the WhatsApp application with a sample of child users in a real environment, whereupon the results were reported and interpreted. The results showed a significant positive effect, as regards the ability of child users to recognise phishing messages after receiving phishing awareness training. However, there was no significant difference noted between the Control and Treatment groups, with regard to the impact of the phishing awareness training provided in the study, thereby indicating an existing level of awareness among the users, irrespective of the training.

Future work will expand the current automated tool to categorise users by age and conduct specific training based on users' age, with regard to avoiding phishing attacks, thereby improving their security awareness.

References

[1] A. K. Jain and B. B. Gupta, "Phishing detection: analysis of visual similarity based approaches," *Secur. Commun. Networks*, vol. 2017, no. 5421046, 2017.

[2] FBI, "INTERNET CRIME REPORT," 2019. [Online]. Available: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120. [Accessed: 01-Oct-2020].

[3] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. Vitak, "No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online," *Proc. ACM Human-Computer Interact.*, vol. 1, pp. 1–21, 2017.

[4] D. Holloway, L. Green, and S. Livingstone, "Zero to eight: Young children and their internet use," London, 2013.

[5] V. Rideout and M. Robb, "The Common Sense census: Media use by kids age zero to eight," *San Fr. CA*

Common Sense Media, 2020.
[6] K. Grant, "Child identity theft is a growing and expensive problem," *CNBC*, 2018. [Online]. Available: https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html. [Accessed: 29-Dec-2020].
[7] U. Hasebrink, S. Livingstone, L. Haddon, and K. Olafsson, "Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online," *EU Kids Online*, 2008.
[8] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins," in *ACM Symposium on Usable Security and Privacy (SOUPS 2005)*, 2005, pp. 77–88.
[9] "Core Street, Spoofstick, 'Browser freely but carry a Spoofstick,'" 2005. [Online]. Available: http://www.spoofstick.com. [Accessed: 10-Dec-2020].
[10] L. Netcraft, "Netcraft anti-phishing toolbar," 2008. [Online]. Available: https://www.netcraft.com/. [Accessed: 15-Dec-2020].
[11] M. Wu, R. C. Miller, and G. Little, "Web wallet: preventing phishing attacks by revealing user intentions," in *Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 102–113.
[12] E. Lastdrager, I. C. Gallardo, P. Hartel, and M. Junger, "How effective is anti-phishing training for children?," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 229–239.
[13] J. Nicholson, Y. Javed, M. Dixon, L. Coventry, O. D. Ajayi, and P. Anderson, "Investigating Teenagers' Ability to Detect Phishing Messages," in *IEEE European Symposium on Security and Privacy Workshops*, 2020, pp. 140–149.
[14] A. A. Al Shamsi, "Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE," *Int. J. Inf. Technol. Lang. Stud.*, vol. 3, no. 2, pp. 8–29, 2019.
[15] S. Maqsood, R. Biddle, S. Maqsood, and S. Chiasson, "An exploratory study of children's online password behaviours," in *Proceedings of the 17th ACM Conference on Interaction Design and Children*, 2018, pp. 539–544.
[16] H. Zaikina-Montgomery and N. C. Silver, "An examination of icons, signal words, color, and messages in warnings for children on the Internet," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2018, vol. 62, no. 1, pp. 251–255.
[17] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, "Phinding phish: Evaluating anti-phishing tools," in *In Proceedings of The 14th Annual Network and Distributed System Security Symposium (NDSS '07)*, 2007.
[18] L. A. T. Nguyen, B. L. To, H. K. Nguyen, and M. H. Nguyen, "A novel approach for phishing detection using URL-based heuristic," in *International Conference on Computing, Management and Telecommunications (ComManTel)*, 2014, pp. 298–303.
[19] M. Alwanain, "Phishing Awareness and Elderly Users in Social Media," *Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 9, pp. 114–119, 2020.
[20] S. Hashmi, "WhatsApp Facts and Stats that You Must Know in 2020," *Connectiva Systems*, 2020. [Online]. Available:https://www.connectivasystems.com/whatsapp-facts-stats-2020/#WhatsApp_Facts_and_Stats_about_Usage_in_2020.
[21] "WhatsApp website," 2020. [Online]. Available: https://www.whatsapp.com/about/. [Accessed: 10-Nov-2020].
[22] M. Boston, "Q4 Phishers' Favorites report," *Vade Secure*, 2020. [Online]. Available: https://www.vadesecure.com/en/blog/phishers-favorites-q4-2019. [Accessed: 12-Sep-2020].
[23] "American Community Survey (ACS)," 2018. [Online]. Available: https://www.census.gov/programs-surveys/acs/. [Accessed: 11-Jan-2021].
[24] "Bitly." [Online]. Available: https://bitly.com/. [Accessed: 22-Oct-2020].

Dr. Mohammed Alwanain is an information security and academic consultant. He is also a faculty in the Computer Science Department, at Majmaah University, Saudi Arabia. Dr. Alwanain obtained the BSc in Computer Science from King Saud University in 2004. He received the MSc in Software Engineering from Heriot-Watt University-Edinburgh in 2010 and the Ph.D. in Software Engineering from Birmingham University-United Kingdom in 2016. Currently, he is the dean of the Information Technology at Majmaah University. Dr. Alwanain‟s research interests involve network security, Internet security and frauds that encounter web applications especially online banking, e-commerce applications.