Phishing Awareness and Elderly Users in Social Media

Mohammed I Alwanain

Majmaah University
Department of Computer Science,
College of Science and Humanities in Alghat, Saudi Arabia

Summary
Nowadays, banking, mobile phone communications, transportation, and other daily services are closely intertwined with the Internet. However, although online services make our lives more convenient and manageable, criminals have found ways of accessing users via the Internet to steal sensitive information such as passwords and bank details. This can cost Internet users dearly. Elderly users are the main target for online criminals, due to their relative lack of knowledge about the Internet and its risks. Therefore, they often become victims of various types of cybercrime. This paper studies the effects of security awareness on elderly users and their ability to detect phishing attacks in social media. With this approach, a real experiment was conducted to evaluate the effects of security awareness on WhatsApp application users in their daily communications. The results of the experiment revealed that phishing awareness training has a significant positive effect on the ability of elderly users to identify phishing messages, thereby avoiding attacks.

Key words:
Anti-phishing countermeasures, online fraud, E-commerce security, evaluation experiments

1. Introduction

Today, phishing is one of the most serious crimes in the digital world. It refers to an attempt to steal a user's sensitive information, such as credit and debit card details, phone numbers, and addresses, using fake emails, fake websites, or both.[1] Such crimes represent a threat to Internet security, 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.[2] The FBI's Internet Crime Report states that in 2019, the Internet Crime Complaint Center (IC3) received 467,361 complaints, with estimated losses of over $3.5 billion. These reported complaints were from Business Email Compromise (BEC), Ransomware, Elder Fraud, and Tech Support Fraud.[3]

Elderly users are a particularly interesting target for attackers, as they are anticipated to have high credit card limits. In addition, they are expected to be less likely to report a phishing attack, due to their lack of knowledge about digital fraud and to whom they should report it. Therefore, fraud perpetrated against the elderly is sharply increasing at this current time, especially in the form of financial scams, these being classed as the crime of the 21st century. For example, in 2019, the IC3 received 68,013 complaints from victims over the age of 60, amounting to personal losses of around $835 million. This placed the elderly at the top of the fraud list in 2019,[3] due to users over the age of 60 not having enough information about the latest technology, especially where computers are concerned. These users also tend to lack knowledge about Internet risks. In fact, when financial crime occurs, the health issues and economic security of millions of elderly people is breached and difficult to recover. Therefore, such issues cost millions of dollars annually in healthcare expenses and investigative and legal costs.[4]

Currently, the top five organisations targeted by phishers are PayPal, Facebook, Microsoft, Netflix, and WhatsApp, indicating that phishing attacks target people's social lives, as well as their financial interests.[5] Consequently, both industry and academia are working hard to develop solutions to the phishing threat. It is therefore of paramount importance that organisations pay attention to end-user awareness when attempting to prevent phishing.

Recently, a number of technical solutions have been proposed to mitigate the problem of phishing, such as SpoofStick, Netcraft, and SpoofGuard. However, these tools are not the only means developed to prevent attacks.[6] For instance, Dhamija et al.[7] conducted a phishing experiment, producing results that revealed how 23% of the study participants never looked at the address bar and did not even understand anti-phishing tool indicators. This led to them making mistakes 40% of the time during the experiment, and these mistakes were the main reasons for phishing attacks. It demonstrated that anti-phishing training for end-users should be mandatory in any technical solution proposed, especially in the case of elderly users. According to Symantec,[8] user awareness is central to helping to change users' behaviour and prevent online scams. A higher level of awareness would reduce

Manuscript received September 5, 2020
Manuscript revised September 20, 2020

DOI: 10.22937/IJCSNS.2020.20.09.14

the number of mistakes made by users when dealing with social media, emails, and websites.

In this paper, a real-world experiment is described, conducted for the purpose of evaluating elderly users' reactions to attacks via WhatsApp. Although a number of studies have investigated fraud against the elderly, none examine this type of fraud in the social media context, especially WhatsApp. The results of the experiment outlined in this paper strongly support the assumption presented above, namely that technical solutions cannot prevent phishing attacks without user awareness.

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

2. Related Work

Older people and their phishing awareness have received considerable attention in recent years, especially with the growth of online services such as Internet banking and shopping. Such services carry a serious risk to online users who lack security awareness. In fact, there are many technical approaches (for example, toolbars) to mitigate phishing risk. However, technical tools are inadequate in themselves to prevent phishing attacks; rather, improving the level of security awareness is effective for reducing phishing risk.[1],[2],[9],[10] However, in recent years, phishing attacks have become increasingly sophisticated, with the ability to target specific types of Internet user.

Lahtiranta et al.[11] state that elderly people are especially vulnerable to social engineering and therefore more likely to be targeted by attackers, compared to their younger counterparts. This is due to their lack of training in the use of state of the art technology, as well as their inexperience in its use through work, etc., rendering them a clear attack vector for attackers. The above-mentioned study lists several important factors focused on and exploited by attackers when they target elderly people. However, no actual experiments were conducted to validate the factors mentioned in this study.

The security risk to elderly people is also investigated in another study,[12] where the vulnerability of the elderly in health systems is discussed. Here, the researchers emphasized that privacy measures should be stated before implementing health systems. The proposed privacy measures were evaluated in a case study. In addition, the research defined several guidelines that could be useful in the process of developing e-health monitoring systems to mitigate the risk of attacks. However, the study focused solely on e-health systems, with no mention of enhancing risk awareness.

Meanwhile, Nino et al.[13] carried out a survey among elderly residents of a nursing home and members of a Swedish national senior citizens' organization. The survey consisted of a questionnaire, in an attempt to reveal the importance of clarifying the technical aspects of phishing to the group under study, so that they could make more accurate assessments of the emails that they received. The results showed that most of the participants had failed to identify links that looked suspicious in an email.

Similarly, Sannd and Cook[4] outlined a grammar and syntax-derived framework to assist older users in becoming more capable of recognizing fraudulent emails. Their study examined responses from older people to assess their ability to recognize phishing and ransomware offers, distributed via email. The sample participating in the investigation consisted of Australians over the age of 65. The research focused on two main aspects: the first being the ability of older adults to differentiate between legitimate and fake emails based on grammar, syntax, and the legitimacy of the associated context. The second aspect was addressed with an analysis of a sample of 21 identified ransomware and phishing attacks through the lens of grammatical and syntax-related diversity. However, this approach was complex for elderly users to follow.

In addition to the aforementioned approaches, there have been numerous attempts to reduce the incidence of phishing, for example, through the introduction of anti-phishing toolbars. These are Web browser plug-ins that warn users when they access a suspected phishing site.[14] Likewise, many financial, commercial, private, and government institutions (for example, eBay and HSBC) offer guidance on how to prevent phishing. The aim of these tips is to train users to look for signs of phishing in emails and websites, thereby enabling them to identify phishing attempts more effectively. In general, however, ordinary users tend not to read online material intended as anti-phishing training, even though this can be effective if applied.[15]

In contrast, Sheng et al.[16] proposed an online game to teach users good habits, helping them to avoid phishing attacks. Kumaraguru et al.[17] also considered training users to identify and deal with phishing emails during their everyday email use. Their aim was to teach users to look for phishing clues in their emails, whereupon they found that this training approach worked better than the current practice of sending anti-phishing tips by email. However, the above approach did not include teaching users how to avoid phishing websites.

There are various ways in which phishing sites can be accessed, such as in online advertisements. Alnajim and

Munro[18] proposed an anti-phishing strategy in the form of a training intervention, designed to help users ascertain whether a website is legitimate. Their strategy provided information for end-users and helped them as soon as they made a mistake. The above authors found a positive effect of using this approach, compared with the earlier strategy of sending anti-phishing tips by email.

Conversely, the approaches presented by Kumaraguru et al.[17] and Sheng et al.[16] were evaluated in studies involving participants who had been recruited on the basis of their technical background. Prospective participants were classified as either 'expert' or 'non-expert' users, based on pre-study screening questions. Their technical background was assessed according to whether they had ever changed their preferences or settings in Web browsers, created a Web page, or helped someone resolve a computer problem. Any participant who answered 'No' to at least two of the screening questions was selected to take part in the experiments. This assessment of technical background was therefore used to recruit non-experts. However, these apparent non-experts in the use of the relevant technology may have already been aware of phishing and how to detect attacks before taking part in the evaluation experiments, leading to biased results. This is because participants with prior knowledge of phishing may have applied their existing knowledge, rather than the anti-phishing approaches taught in the experiment.

From another perspective, Fettel et al.[19] proposed machine-learning methods to detect a phishing attack. This approach involved assessing the properties of URLs contained within an email (for example, the number of dots in the URL, the age of the linked domains, and the number of links in the email) to flag up phishing emails. These techniques are helpful for filtering phishing emails, but still cannot prevent attacks without improving the user's phishing knowledge.

A similar approach was proposed by Alnajim,[20] who presented a model that was mainly a prototype of an automated analyzer of users' anti-phishing behavior within a LAN. This analyzer automatically performed ongoing analysis of users' behavior in response to phishing attacks. Based on the results of this analysis, the analyzer decided whether the users required training in phishing detection and avoidance. However, this approach went further by adding an advanced setting to fully automate the training without human intervention. This approach has been implemented and evaluated in a real-world context.

However, despite clear advantages to filtering phishing attacks at email and website level, these approaches cannot mitigate or prevent phishing attacks in the social media that is accessed in daily life, especially among elderly users. This current paper reports on an evaluation of elderly users' knowledge in a real environment to discover how they interact with phishing attacks in social media. Two different phishing experiments were therefore conducted, targeting elderly users of the WhatsApp application. The sample was randomly selected from different specialties, with varying levels of knowledge. In these experiments, the results were analyzed with respect to the users' confidentiality and privacy. The following sections describe these experiments in detail.

3. Methodology

Currently, social media are becoming the main channel of communication between people around the globe. Various types of social media are commonly used for communication, but the most common application is WhatsApp.[21] WhatsApp is an application developed by Facebook. It has received considerable attention in recent years and may be listed among one of the most heavily used applications in daily life worldwide. The latest statistics for the WhatsApp website indicate that so far in 2020, over two billion people in over 180 countries have used WhatsApp in 60 different languages. To illustrate this usage, 65 billion text and voice messages are sent daily via WhatsApp.[22] Due to the application's usability, it is estimated that the average user opens the application 23-25 times a day.[21] These extraordinary statistics make the application an interesting target for attackers. Correspondingly, Vade Secure[23] report that phishing attacks via WhatsApp increased egregiously in Q4 of 2019, reaching 13,467.6%. Such attacks can take place via text messages containing a hyperlink, which directs the victim to a fake website that is identical to the legitimate website, so that the victim's personal information can be stolen. However, not all users are interesting to attackers. According to the FBI's Internet Crime Report,[3] elderly users are becoming an especially attractive target for phishers. This is because they are usually considered to possess credit cards with a high credit limit, which can easily be exploited if their information is accessed. In addition, elderly people tend to be less eager to report such crime, for fear of being harassed further. Moreover, it often takes a long time for a senior citizen to realise that fraud has been committed. For this reason, it was decided to focus the investigation on the age group, 60-75 years.

Fig 1: A phishing website

In this paper, two experiments were consequently executed on a sample comprised of 20 participants, aged between 60 and 75 years. These participants were divided into two groups, designated as the Control and Treatment groups, each consisting of 10 participants. In the first experiment (Phase 1), a phishing message (written in Arabic) was sent to the Treatment group, informing them of the latest statistics for the COVID-19 pandemic. The message contained a hyperlink, which directed users to a website where they were notified that they had been targeted by a phishing attack. This website contained information about phishing and the most common phishing scenarios, with the aim of improving users' knowledge, so that they could avoid any future phishing attacks (see Figure 1).

In this experiment, no information was requested from the participants. However, it was assumed that a participant clicking on the hyperlink would become a phishing victim. Conversely, the Control group received the same text message, but the hyperlink related to a real statistical website about the pandemic. The reason for including the Control group was to measure improvement in the second experiment.

In the second experiment (Phase 2), a text message was sent, containing information about patients' recovery from COVID-19 – a topic of significance and interest during the pandemic. The message was sent to both the Control and Treatment groups without any changes, in order to evaluate the impact of Phase 1 and compare the results of the two groups.

In this approach, the research hypotheses may be expressed as follows:

Hypothesis 1: A significant improvement can be observed in the phishing awareness of the participating sample, after the first experiment.

Hypothesis 2: Elderly users find it difficult to identify phishing messages and so their phishing reporting is low.

An evaluation and analysis of these hypotheses is presented in section 6

4. Implementation

The websites used in these experiments were operated and stored on a local device 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 experiment, such as the IP address, phone number, date, and time. All this information was stored in the local database, so that a statistical analysis could be carried out (see Figure 2).

5. Results

Once the experiments had been completed, a statistical analysis was carried out, using the IBM SPSS Statistics package. In sum, the focus of this study was on training elderly people, in order to improve their security awareness.

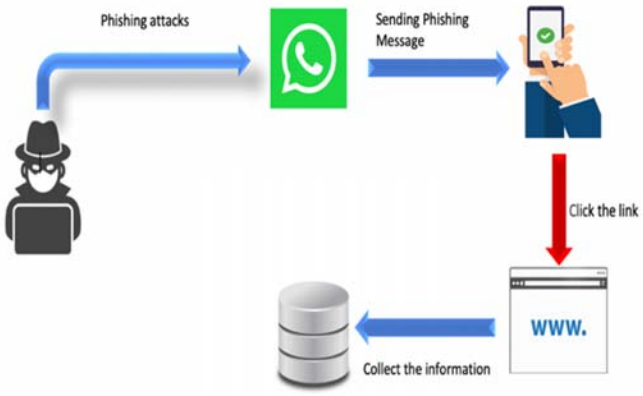

Fig 2: A phishing scenario

5.1 Phase 1

In Phase 1, which called (pre-test), 10 WhatsApp messages, containing a hyperlink related to a legitimate website about the latest COVID-19 statistics, was sent to the participants in the Control group. In contrast, the Treatment group received 10 WhatsApp messages, containing a hyperlink related to a fake website. The results of the experiment showed that 87.5% of those registered in the Control group opened the URL, compared to 72.7% in the Treatment group. Specifically, 12 participants (60%) of the whole sample (both groups) clicked on the link on the first day of the experiment: 3 participants (30%) from the Treatment group and 9 participants (90%) from the Control group. The following day, 5 participants from the Treatment group clicked on the link, compared to 3 participants from the Control group.

Only 4 participants from the Treatment group reported that the link had issues after clicking on it, whereas 3 participants ignored the messages: 2 from the Treatment group and 1 from the Control group. The total number of victims in this Phase was 8 (see Table 1).

Table (1) Number of participants and victims in the sample in Phase 1

Group	Controlled	Treatment
Number of messages	10	10
Clicks on links	9	8

5.2 Phase 2

In Phase 2, which called (post-test), the participants from both groups received a WhatsApp message containing a hyperlink related to a fake website. The total number of messages sent to both groups was 20, each participant receiving 1 message (see Table 2).

Table (2): Distribution of the sample

Group	PHASE			
	PHASE 1		PHASE 2	
	Open Url	Not OpenUrl	OpenUrl	Not OpenUrl
Treatment	8	2	4	6
Control	9	1	7	3
Total	17	3	11	9

This Phase was conducted two months after Phase 1. Ten participants clicked on the link on the first day: 3 from the Treatment group and 7 from the Control group. The following day, only 1 participant from the Control group clicked on the link. Moreover, none of the participants reported that the link had issues and 9 participants ignored the messages: 6 from the Treatment group and 3 from the Control group. The total number of victims was 11.

The result shows that the number of victims in the Treatment group was reduced from 72.7% in Phase 1 to 54.5% in Phase 2, while the number of victims in the Control group was reduced from 87.5% to 62.5%. The improved security awareness of the elderly participants differed significantly between the Control and Treatment groups ($t(17)=0.329$, $P>0.05$). Therefore, Hypothesis 1 is accepted, because a significant improvement was identified in the phishing awareness of those who participated in Phase 1.

In particular, the Treatment group displayed increased security awareness after both Phase 1 ($t(10)=1.9$, $P>0.05$) and Phase 2 ($t(10=2.88$, $P<0.05$). In contrast, the Control group demonstrated increased security awareness after Phase 1 ($t(7)=1$, $P>0.05$), but this increase slowed down after Phase 2 ($t(7)=2.05$, $P>0.05$). A difference in improved security awareness was therefore observed between the Control and Treatment groups, with the Treatment group registering a high degree of improvement after Phase 2 ($pre=1.27\pm0.467$, $post=1.45\pm0.522$, $t(10)= -1.00$, $P>0.05$), while the Control group showed no significant change ($pre=1.13\pm0.345$, $post=1.38\pm0.518$, $t(7)=-1.00$, $P>0.05$).

6. Discussion

In the experiment described above, the results showed a significant effect on users' phishing awareness, demonstrated by elderly users correctly identifying a phishing message in WhatsApp, thereby avoiding a phishing attack. This led to a higher rate of phishing avoidance amongst the phishing-aware users, compared to the less aware elderly users, which is apparent from a comparison between the results of the two experimental Phases. The difference between them indicates a significant positive effect of phishing awareness, as compared to low phishing awareness (see Figure 3). Consequently, it would appear that phishing awareness has a significant positive effect on users' ability to detect and therefore prevent phishing.

In addition, it is clear from the aforementioned experiment that elderly people have a profound lack of security awareness, because most of the sample became victims in the Phase 1, compared with studies involving other age groups [4],[9],[10],[11] This means that Hypothesis 2 is accepted, because most of the sample had not received any training in using the latest technology, nor had they gained any experience of its use through work.

Finally, from the results illustrated in section 5, it is clear that elderly users urgently need training to increase their Internet security awareness and avoid phishing attacks, in order to reduce the level of cybercrime targeting them.

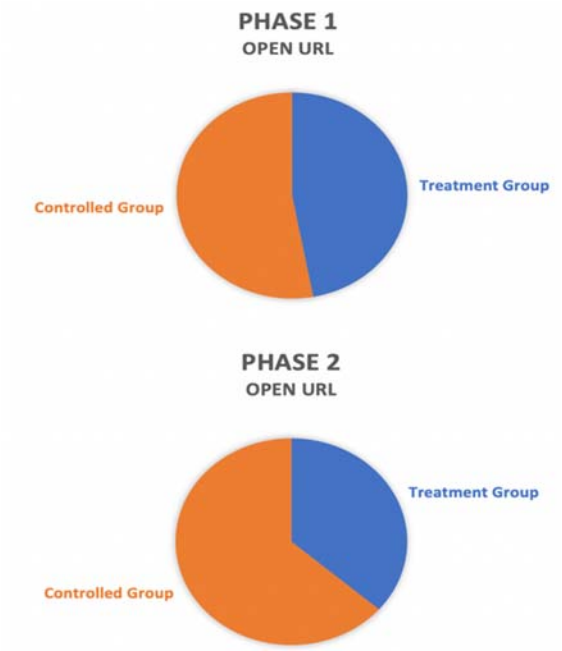

Fig 3: Victims, who clicked on the linkin the two Phases

7. Conclusion

In this paper, the effects of user awareness on the ability of elderly users to detect phishing attacks have been discussed and evaluated. An experiment was conducted, using the WhatsApp application with a sample of elderly users in a real environment, whereupon the results were reported and interpreted. Significant positive effects were found, as regards the ability of elderly users to recognise phishing messages after training in phishing awareness. The results illustrate that there is an urgent need for phishing awareness training, especially among elderly users.

Future work will automate the process of training elderly users to avoid phishing attacks, improving their security awareness.

Acknowledgments

The author would like to thank Deanship of Scientific Research, Majmaah University (Grant no. R-1441-152) for funding this work.

References

[1] B. B. Gupta, N. Arachchilage, and K. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, 2018.

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

[3] FBI, "Internet Crime Report," 2019. [Online]. Available: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[4] P. Sannd and D. Cook, "Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks" in *2018 Fourteenth International Conference on Information Processing (ICINPRO)*, 2018, pp. 1–5.

[5] "Digital Information World," 2020. [Online]. Available: https://www.digitalinformationworld.com/2020/02/report-claims-a-staggering-13467-percent-increase-in-whatsapp-phishing-urls.html.

[6] A. Alnajim, "A country based model towards phishing detection enhancement," *Int. J. Innov. Technol. Explor. Eng.*, vol. 5, no. 1, pp. 52–57, 2015.

[7] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581–590.

[8] "Symantec, Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization.," 2004.[Online].Available:http://www.antiphishing.org/sponsors_technical_papers/symantec_online_fraud.pdf.

[9] M. Alwanain, "Effects of User-Awareness on the Detection of Phishing Emails: A Case Study," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 4, pp. 480–484, 2019.

[10] M. Alwanain, "An Evaluation of User Awareness for the Detection of Phishing Emails," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 10, pp. 323–238, 2019.

[11] J. Lahtiranta and K. Kimppa, "Elderly people and emerging threats of the internet and new media," in *Project E-Society: Building Bricks*, 2006, pp. 13–21.

[12] D. T. Handler, L. Hauge, A. Spognardi, and N. Dragoni, "Security And Privacy Issues in Healthcare Monitoring Systems: A Case Study," in *10th International Joint Conference on Biomedical Engineering Systems and Technologies*, 2017, pp. 383–388.

[13] J.-R. Nino, G. Enstrom, and A. R. Davidson, "Factors in fraudulent emails that deceive elderly people," in *International Conference on Human Aspects of IT for the Aged Population*, 2017, pp. 360–368.

[14] L. F. Cranor, S. Egelman, J. I. Hong, and Y. Zhang, "Phinding Phish: An Evaluation of Anti-Phishing Toolbars," 2006.

[15] A. Alnajim and M. Munro, "An evaluation of users' tips effectiveness for Phishing websites detection," in *The third IEEE International Conference on Digital Information Management ICDIM*, 2008, pp. 63–68.

[16] S. Sheng, B. Magnien, A. Kumaraguru, Ponnurangam Acquisti, L. F. Cranor, and E. Hong, Jason and Nunge, "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish" in *The 3rd symposium on usable privacy and security SOUPS '07*, 2007, pp. 88 – 99.

[17] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system," in *The SIGCHI conference on Human factors in computing systems*, 2007, pp. 905 – 914.

[18] A. Alnajim and M. Munro, "An anti-phishing approach that uses training intervention for phishing websites detection," in *the 6th IEEE International Conference on Information Technology - New Generations (ITNG)*, 2009, pp. 405–410.

[19] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails" in *Proceedings of the 16th international conference on World Wide Web*, 2007, pp. 649–656.

[20] A. Alnajim, "An Automated Analyzer for Users' Anti-Phishing Behaviour within a LAN," *Int. J. Soft Comput. Eng.*, vol. 5, no. 3, pp. 115–119, 2015.

[21] 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

[22] "WhatsApp website," 2020. [Online]. Available: https://www.whatsapp.com/about/.

[23] M. Boston, "Q4 Phishers' Favorites report," *Vade Secure*, 2020. [Online]. Available: https://www.vadesecure.com/en/phishers-favorites-q4-2019/

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.