South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

AOSIS

Contributing factors to increased susceptibility to social media phishing attacks

Authors:
Heather J. Parker[1]
Stephen V. Flowerday[1]

Affiliations:
[1]Department of Information Systems, Faculty of Commerce, Rhodes University, Grahamstown, South Africa

Corresponding author:
Stephen Flowerday
s.flowerday@ru.ac.za

Dates:
Received: 27 Nov. 2019
Accepted: 31 Mar. 2020
Published: 15 June 2020

How to cite this article:
Parker, H.J. & Flowerday, S.V., 2020, 'Contributing factors to increased susceptibility to social media phishing attacks', *South African Journal of Information Management* 22(1), a1176. https://doi.org/10.4102/sajim.v22i1.1176

Background: The migration of phishing scams to social media platforms poses a serious information security threat to social media users. Users often remain unaware of the various phishing threats on social media and consequently they thoughtlessly engage on these platforms.

Objectives: The objective of this article was to identify the factors that contribute to an increased susceptibility to social media phishing attacks and propose a model to reduce this susceptibility.

Method: A systematic literature review was conducted in Emerald Insight, ScienceDirect and Google Scholar by using a search string. The identified articles underwent two rounds of screening and the articles thus included moved on to a quality assessment round. Finally, these articles were imported into MAXQDA where a content analysis was conducted, which involved extracting, coding and analysing the relevant data.

Results: The final 25 articles included in the study indicated that women with low technical and security knowledge between the age of 18 and 25, who habitually use social media and process content heuristically, are more susceptible to phishing attacks. The insights gained from conducting this review resulted in developing a model that highlights the individuals who are most susceptible to phishing attacks on social media.

Conclusion: This article concludes that certain people are more susceptible to phishing attacks on social media as a result of their online habits, information processing, demographics, Information and Communications Technology (ICT) knowledge and personality traits. As such, these identified people should be more aware that they fall into this susceptibility group and thus should behave more cautiously when engaging on social media platforms.

Keywords: phishing; social media; information processing model; phishing; social media; information processing; awareness; personality traits.

Introduction

Social media websites have gained significant popularity over the years, with 3.484 billion users reported at the start of 2019 (Kemp 2019). The traditional platform for conducting phishing merely via email has evolved. Phishing attacks are now migrating to social media platforms, with a 30% increase in phishing links from the first quarter of 2018 (ProofPoint 2018). Consequently, phishing is still a serious cybersecurity threat, with phishers using social media sites such as Facebook, Instagram and Twitter to target significant numbers of victims. For instance, in the first quarter of 2018, fake Facebook pages were used to launch 60% of phishing attacks on social networks (Kaspersky 2018). Later, in 2019, phishing on Instagram and Facebook among others saw a 74.7% increase (Barker 2019). These statistics highlight that the threat of phishing shows no sign of retreating.

Phishing refers to 'a form of online identity theft that aims to steal sensitive information such as online passwords and credit card information' (Banu & Banu 2013:783). Phishing attacks are effective because they use social engineering techniques to persuade people into performing actions that will advance the phisher's attack (Frauenstein & Flowerday 2016). These social engineering techniques appeal to the victim's emotions and create a sense of trust by using personalised messages. Social media phishing attacks occur in two stages and result in high victimisation and a high success rate. During the first stage, the phisher sends a friend request to the prospective victim (Vishwanath 2015b). At this stage, the phisher can view the victim's friends and personal details. The second stage of the attack takes place when the phisher contacts the victim and requests information via a social media messaging platform such as Facebook messaging (Vishwanath 2015b). Such information requests are personalised using information provided on the user's wall, in posts, photos and news feeds. Messages include links and attachments that could infect the user's device with malware. These attacks lead to more victims, as other users connected to the first victim see the phisher as a mutual friend and believe that they are legitimate (Vishwanath 2015b).

Activities such as posting videos, comments, status updates and photos, as well as sending messages and liking posts, can be rewarding for users and thus encourage further use of social media platforms. This gratification fosters the frequent and repetitive use of social media, which, together with the inability to control these activities, results in people acquiring unconscious habits when engaging on these platforms (Vishwanath 2015b). The habitual use of social media may also make users more susceptible to phishing attacks because they do not process messages and links with enough attention to detail. This, coupled with certain character or personality traits, could lead to some users being more susceptible to phishing attacks than others.

The objective of this article was to identify the factors that contribute to an increased susceptibility to social media phishing attacks and to propose a model to reduce susceptibility. As such, the main research question is as follows:

Why are certain people more susceptible to phishing attacks on social media platforms than others?

Some users spend a considerable amount of time on social media sites and participate in repeated behaviours that form habits. These behaviours include habitually liking pages and posts, as well as not processing messages and comments adequately. To address the inadequate processing of phishing threats on social media, the theoretical foundation for this article is the heuristic–systematic model. This model states that people employ two modes of information processing when making assessments about received messages (Chaiken & Eagly 1989).

This article starts by providing an overview of the method. A review of the literature is then provided, as well as a discussion of the proposed model to reduce phishing susceptibility. The article concludes with a summary that highlights the implications of the findings for both individuals and organisations.

Method

A systematic literature review was conducted by using a post-positivist paradigm to explore why certain people are more susceptible to phishing attacks on social media. This review made use of argumentation theory to develop an argument that was balanced and well reasoned (Metcalfe & Powell 2000). As such, the argument was developed by providing evidence from the literature reviewed to reach conclusions related to the research question and synthesising these findings into a model that identifies people who are most susceptible to phishing attacks on social media.

A 'who', 'what', 'how' and 'where' (WWHW) table was created to ensure all the relevant search terms were present in the search string. Table 1 was developed to ensure that the main research question encapsulated all the aspects that needed to be covered in the review.

To develop the final search string, susceptibility had to be broken down into information processing and habits. Furthermore, demographics and personality traits were used to determine certain people within the search string.

The final search string used in ScienceDirect and Google Scholar was as follows: ('phishing' OR 'phishing attacks') AND ('information processing' OR 'heuristic systematic processing' OR 'cognitive processing') AND ('habits') AND ('personality traits' OR 'Big Five personality traits') AND ('social media' OR 'Facebook').

A shorter version of the search string had to be developed for Emerald Insight, as the database only allows a maximum of seven terms. The search string for Emerald insight was as follows: ('phishing' and 'phishing attacks') AND ('information processing' OR 'heuristic systematic processing') AND ('habits') AND ('personality types' AND 'social media').

Emerald Insight, ScienceDirect and Google Scholar were the bibliographical databases used in this review. ScienceDirect was used owing to the wide variety of academic journals it contains, encompassing current and relevant articles related to the topic. Similarly, Emerald Insight was chosen because it contains various current journals related to the field of information systems that do not delve into aspects that are too technical. Finally, Google Scholar was used for this search because it accesses multiple databases that have relevant peer-reviewed articles.

A total of 285 articles were identified by using the database search, with 177 results being identified in Emerald Insight, 68 results in ScienceDirect and 40 results in Google Scholar. A total of 14 duplicates were removed, leaving 271 articles to undergo a first round of screening. The first round of screening involved using inclusion and exclusion criteria to filter the results based solely on the title and abstract; subsequently, the number of included articles was

TABLE 1: Who, what, how and where.

Research question	Who	What	How	Where
Why are certain people more susceptible to phishing attacks on social media platforms than others?	Certain people	Phishing attacks	Susceptibility	Social media platforms

reduced to 25. These 25 articles then underwent a second round of screening, which resulted in further nine articles being excluded, thus leaving 16 articles for inclusion. During the second round of screening, the articles had to focus on one or more aspects of the inclusion criteria. Thus, the articles had to discuss the personality traits, demographics and social media habits that influence the user's susceptibility to phishing on social media. Articles were excluded if they were irrelevant, too technical, in a foreign language, had a publication date prior to 2010 and/or focussed on the wrong platform such as mobile messages. Backward searching was applied to the 16 articles included by identifying useful works cited in these articles and, accordingly, nine useful articles were identified. These 25 articles moved on to a quality assessment round to ensure that the results presented in each article were trustworthy and met the specifications. This assessment, which is shown in Appendix 1, consisted of 14 questions divided into sections for design, conduct, analysis, conclusion and general. These questions were answered by assigning a ranking and the results were tallied to determine the final score for each article. An illustration of the study selection process is provided in the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram in Appendix 2 (University of Carolina 2018). This diagram illustrates the flow of information through the phases of a systematic literature review.

The qualitative data analysis software tool MAXQDA was used to extract, code and analyse the data from the sample of articles found in Appendix 3. MAXQDA was used for performing the content analysis of the sample of articles generated through the systematic literature review. The data extraction process included collecting all the data pertaining to the main research question and sub-questions. This was performed by grouping sections of text from each article together with a corresponding code. By using codes, the researcher was able to concentrate on specific aspects of the data found in an article (Nowell et al. 2017). Table 2 depicts the number of tags for each code. This refers to the number of times a code appeared in the 25 articles imported into MAXQDA.

Results gathered from this tagging process were analysed and thematic analysis was conducted to combined codes that focussed on similar aspects into themes, which can be seen in Figure 1. Thus, heuristic processing and systematic processing were combined to create the information processing theme; age and gender were combined to create the demographic theme; and phishing education, computer and security knowledge, and Internet and computer usage experience were combined to form Information and Communications Technology (ICT) knowledge. Following this, a data extraction table was created to report the results of this process and to highlight the similarities and differences among the articles. Figure 2 shows a chart depicting the number of articles that discussed each theme. Where an article discussed more than one theme, it was counted in several themes. As may be seen, some themes were studied extensively in comparison with the others. The findings related to the overarching themes are discussed in the next section as factors that influence phishing susceptibility.

TABLE 2: Number of tags for each code.

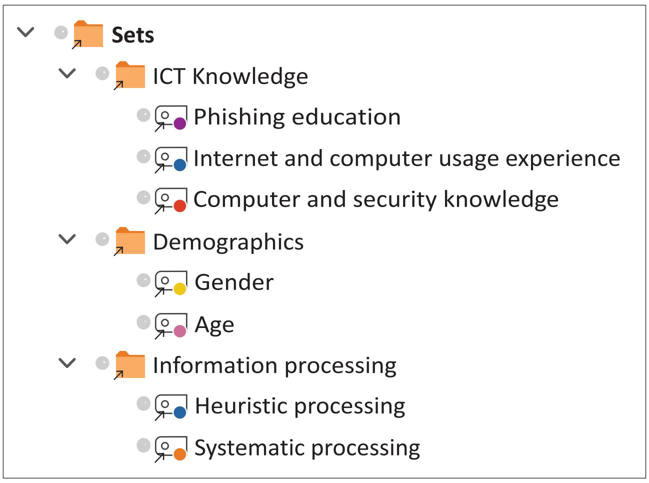
Code	Number of tags
Heuristic processing	134
Gender	106
Online habits	96
Age	92
Personality traits	83
Systematic processing	61
Phishing education	15
Computer and security knowledge	10
Internet and computer usage experience	4

Factors influencing susceptibility to phishing attacks on social media

In this section, a discussion of the themes identified that influence a user's susceptibility to phishing on social media is presented. These themes will inform the creation of the phishing reduction model in the following section.

Information processing

The first factor identified that influences a user's susceptibility to phishing attacks refers to the way in which users process the messages, posts and comments that they encounter on social media. The articles related to information processing



- Sets
  - ICT Knowledge
    - Phishing education
    - Internet and computer usage experience
    - Computer and security knowledge
  - Demographics
    - Gender
    - Age
  - Information processing
    - Heuristic processing
    - Systematic processing

FIGURE 1: Code sets representing themes.

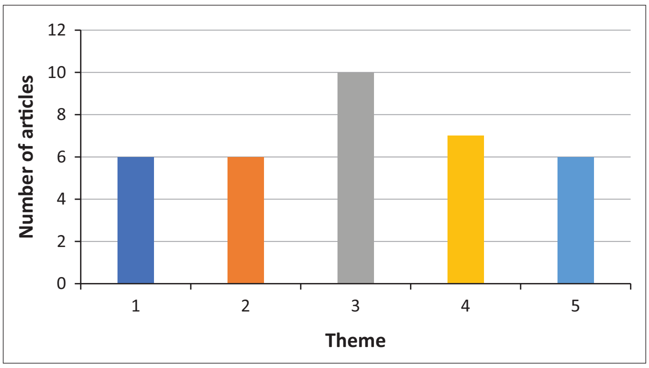


FIGURE 2: Graph depicting number of articles per theme.

on social media discussed the two modes of processing found in the heuristic–systematic model (Chaiken & Eagly 1989). The choice of which processing method to employ is determined by the individual's perception of the sufficiency of the available information (Chaiken & Eagly 1989). In terms of the heuristic–systematic model, individuals utilise both heuristic processing and systematic processing. The former involves using simple heuristic cues that utilise limited cognitive resources to make judgements and decisions (Vishwanath, Harrison & Ng 2016), although the latter involves carefully examining information to reach a decision or make a judgement (Harrison, Vishwanath & Rao 2016). Thus, systematic processing is effortful and requires the use of far more cognitive resources than heuristic processing, which is more efficient and time sparing (Vishwanath et al. 2016). Overall, individuals predominantly use heuristic processing (Harrison et al. 2016; Vishwanath et al. 2016). The risk of information overload on social media and technology affordances encourages individuals to process content heuristically, which leads to quick and effortless judgements (Lin, Spence & Lachlan 2016). Consequently, although processing content heuristically is far more efficient, it significantly increases an individual's susceptibility to phishing attacks (Harrison et al. 2015; Hong 2012; Vishwanath et al. 2011, 2016); the reason for this is that when processing messages heuristically individuals often overlook informational cues that suggest the message is malicious and might pose a threat. Because heuristic processing relies on judging the credibility of information based on superficial cues, users often trust phishing messages (Frauenstein & Flowerday 2016).

Online habits

Online habits have also been found to influence phishing susceptibility, with habitual Facebook use resulting in an increased susceptibility to social media phishing attacks (Vishwanath 2014, 2015b). Users who are highly active on social media platforms are more susceptible to social engineering attacks than those who participate less often (Vishwanath 2015b). Furthermore, an individual's online habits influence the way they process misleading social engineering methods on social media sites (Frauenstein & Flowerday 2016). Thus, poor online habits increase susceptibility because individuals automatically click on links and respond to messages without engaging sufficient cognitive resources or paying enough attention to their online behaviour (Frauenstein & Flowerday 2016; Vishwanath 2015a; Vishwanath et al. 2011). For example, it was determined that individuals who habitually use Facebook are more likely to fall for phoney profiles created to target users and are more prone to reveal sensitive personal information requested by a phisher (Vishwanath 2015b). Thus, online habits influence an individual's susceptibility to fall for phishing on social media by causing them to follow ritualised patterns of social media use that involve little cognitive engagement when using the platform. This increases the probability that these users will thoughtlessly click on malicious links in a message or accept a friend request from a fake profile without thinking about the potential consequences of these actions (Vishwanath 2015b). Behaviours such as clicking on links, sharing and liking posts, and scrolling through posts regularly result in the user not paying attention to suspicious information on social media (Frauenstein & Flowerday 2016). One explanation regarding why Facebook habits lead to an increased vulnerability to social media phishing attacks is that these habits may negatively influence a user's trust and risk perception (Albladi & Weir 2016).

Demographic factors

The next factor that influences susceptibility to phishing attacks is age and gender. Users classified as youth between the ages of 18 and 25 were identified as being the most susceptible to phishing attacks on both email and social media platforms (Algarni, Xu & Chan 2015; Darwish, El Zarka & Aloul 2012; Sheng et al. 2010). This finding is plausible as younger users may be more susceptible to social media phishing because they are constantly engaging on the Internet, and this extensive use often results in Internet addiction (dependence) (Smahel, Brown & Blinka 2012). Excessive Internet and social media use creates ample opportunities for these young people to be targeted by a phisher who gains access to their account to spread malicious links, hijack the accounts of their friends or family and gather information on a specific person for a more targeted attack (Brecht 2017). It should also be noted that age has been linked to risky behaviour, with adolescents in particular being inclined to engage in such behaviour, which could increase their chances of being phished on social media (Sheng et al. 2010). Furthermore, younger users have less education, less distaste for financial risk and less exposure to phishing training (Sheng et al. 2010). Additionally, women have been identified as the most susceptible to phishing and social engineering (Algarni et al. 2015; Darwish et al. 2012; Goel, Williams & Dincelli 2017; Iuga, Nurse & Erola 2016; Sheng et al. 2010). Sheng et al. (2010) attribute this increased susceptibility to a lack of technical skills in comparison with men. In contrast, it has been postulated that women are easier to entice to open phishing emails, but are equally as capable and proficient as men in detecting a deceptive message (Goel et al. 2017).

Furthermore, various factors related to ICT knowledge influence susceptibility to phishing attacks, including computer and security knowledge, phishing education and Internet experience. Although only Algarni et al. (2015) and Albladi and Weir (2018) found that computer and security knowledge decreases a user's susceptibility to phishing attacks, this finding seems credible as greater knowledge increases the user's awareness of possible online social engineering threats and in turn provides them with an increased probability of being able to detect phishing attacks. According to Albladi and Weir (2018), contradictory results relating to whether computer or Internet knowledge reduces susceptibility to phishing exist; this might be because it is a general concept and its influence on risky or cautious online behaviour might be difficult to measure. Phishing education conducted through anti-phishing training received a weak result in this review, but the notion that exposure to phishing education is related to reduced susceptibility to phishing attacks is supported by other studies that fall outside the scope of this review, including Alnajim and Munro (2009), Dodge et al. (2011) and Jensen et al. (2017). Internet experience was also identified as a factor that influences phishing susceptibility, and although only Alseadoon et al. (2012) and Moody et al. (2011) found this factor to be important, the study conducted by Wright et al. (2010) supports this finding. Individuals who use the Internet frequently will have an increased awareness of the risks associated with the Internet and social media than individuals who do not use the Internet frequently. This is because frequent Internet users regard the probability of an online threat happening to them as greater than people who use the Internet less (Halevi, Lewis & Memon 2013). Thus, increased Internet experience increases a user's awareness of online threats.

Personality traits

Finally, personality traits were identified as influencing an individual's susceptibility to phishing attacks. The literature that discussed the influence of personality traits on phishing susceptibility in this study focussed on the Big Five model. This model uses the NEO Personality Inventory (NEO PI-R) to determine an individual's Big Five personality traits that assess their experiential, emotional, attitudinal, motivational and interpersonal facets (Costa & McCrae 1992). The Big Five personality traits linked with susceptibility to email-based phishing are extraversion, openness and agreeableness. As the same social engineering techniques that are employed in phishing emails are also employed on social media platforms (Frauenstein & Flowerday 2016), the personality traits of people who are most susceptible to email-based phishing can be applied to social media-based phishing. Individuals scoring high in extraversion are sociable, talkative, optimistic and driven (Costa & McCrae 1992). Hence, on social media, these individuals are likely to engage in greater amounts of social activity because of their sociable nature (Liu & Campbell 2017). Individuals with high openness to experience are curious and creative (Liu & Campbell 2017); online these individuals are curious, like to explore sites and are more likely to try all social media activities (Liu & Campbell 2017). Moreover, individuals scoring high on agreeableness are often trusting, amenable and giving (Costa & McCrae 1992). In a social media environment, these individuals are more likely to engage in online interaction; they are specifically more likely to engage in social networking activities with real-life friends (Liu & Campbell 2017). Interestingly, some studies found that users scoring high in agreeableness and contentiousness are prone to more secure behaviour online and are not more susceptible to phishing attacks (McCormac et al. 2017; Shropshire, Warkentin & Sharma 2015). However, these studies did not specifically test phishing susceptibility, whereas the studies by Darwish et al. (2012) and Alseadoon, Othman and Chan (2015) tested phishing susceptibility and found that high scores of agreeableness increase phishing susceptibility. Lastly, individuals scoring high in conscientiousness are less susceptible to phishing attacks (Darwish et al. 2012).

Model to reduce phishing

Based on the findings above, a model detailing how susceptible people should engage on social media to reduce the possibility of falling for phishing was developed. In this case, a model is a representation of the theoretical components identified by answering the research question. The model shown in Figure 3 proposes that individuals can reduce their susceptibility to phishing on social media by being aware of the individual factors that make them susceptible, by increasing their ICT knowledge and by processing information systematically. The model should be read from the inside out, starting with processing social media content and moving around the circle in a clockwise direction. The inner circle illustrates the four high-level factors that individuals need to address to reduce phishing on social media, and the outer circle identifies the specific aspects in these factors that the individual should consider and address. The interaction between the corresponding inner and outer circles is discussed at length in the following paragraph.

The most significant aspect proposed by the model to reduce phishing on social media is processing content systematically. This is proposed because it increases the likelihood that a user will correctly identify deceptive messages because they are consciously analysing the message content. By employing systematic processing, individuals are provided with more evidence of the validity of the information or message (Chaiken & Eagly 1989). Thus, systematic information processing is methodical and involves extensive, in-depth processing of the messages and information received (Chaiken & Eagly 1989). Although this method of processing information

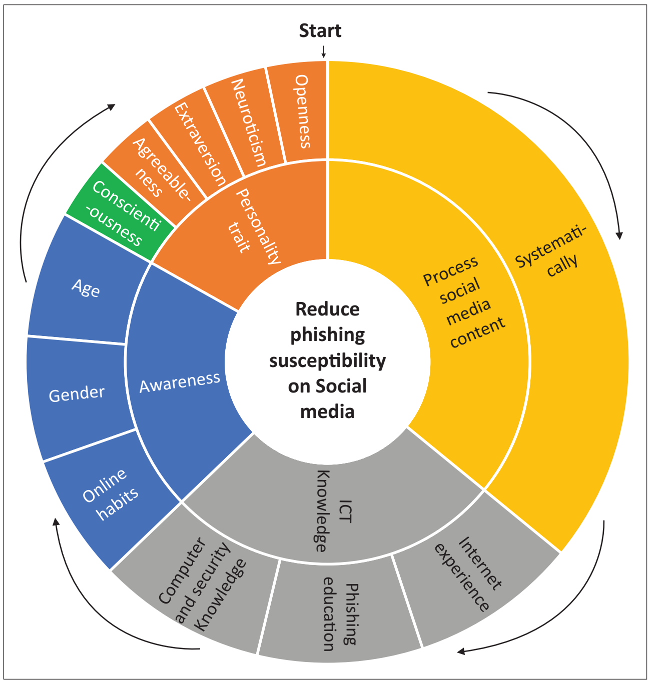


FIGURE 3: Model to reduce phishing susceptibility on social media.

requires more cognitive effort, it significantly decreases susceptibility to phishing attacks on social media (Frauenstein & Flowerday 2016). To further reduce their susceptibility to social media phishing, individuals should have basic computer and security knowledge, as well as use the Internet frequently to increase their awareness of online threats and social engineering attacks. Furthermore, users can take an online anti-phishing training course to learn how to detect phishing attacks. Additionally, individuals should be aware of their habits on social media. Users who use social media habitually are more inclined to be absentminded and automatically provide requested personal information (Vishwanath 2015b). This awareness will allow them to be conscious of the way they use the platform and thus they could try to engage on social media in a conscious and attentive manner.

Moreover, individuals should be aware of potential individual factors that could increase their susceptibility to social media phishing such as their age, gender and personality traits. The age group that is most susceptible to phishing includes individuals between 18 and 25 years, and the gender that is more susceptible is female. Increased awareness of these factors could allow the individual to take preventative measures such as learning how to identify phishing scams and investing in phishing detection software. Finally, individuals should determine their personality traits by completing an online Big Five personality test (e.g. https://www.truity.com/test/big-five-personality-test) to see whether they are more inclined to fall for phishing attacks, which will give them the opportunity to try and behave in a more secure manner on social media. As illustrated by the model, individuals with high consciousness scores have a decreased likelihood of falling for phishing attacks. These individuals tend to be dutiful and industrious and follow the rules (Liu & Campbell 2017). Thus, the model postulates that if individuals process content systematically, increase their ICT knowledge, identify their personality traits and online habits and have an overall awareness of the most susceptible age group and gender, they should be less susceptible to phishing on social media.

Additionally, it is important to note that social media platforms provide controls and measures to educate users and prevent phishing attacks. For instance, Facebook launched phish@fb.com, a dedicated email address where users can report phishing attempts (Facebook 2012). This allows Facebook to investigate, blacklist and hold phishers accountable for their actions (Facebook 2012). They also provide users with information and steps to follow if a user has been phished on Facebook (2020a) or if their device is infected with malware (Facebook 2020b). Together both the user and the social media platform are responsible for preventing, reporting, dissolving and remaining aware of phishing attacks. The social media platform is responsible for educating users and providing controls to reduce phishing attacks. On the other hand, users bear the responsibility of staying informed regarding prevention techniques and using the controls put in place to reduce these incidents.

Limitations and future research

The main limitation of this review is that the effectiveness of the model has not yet been evaluated. As such, additional research could empirically test the proposed model and its ability to assist in reducing phishing susceptibility to social media phishing attacks. Moreover, country of residence could be investigated to determine the impact of culture, Internet access and education level on phishing susceptibility. This could also determine which countries are targeted most by social media phishing attacks. In addition, research should be conducted on how to mitigate the influence of incorrect information processing, online habits, demographics, ICT knowledge and personality traits. This research could include the controls social media platforms implement to reduce phishing attempts and preventative measures an individual could follow to reduce their susceptibility to social media phishing attacks. It would also be useful to test the effectiveness of these controls.

Conclusion

The increasing popularity of social media sites has led to the migration of phishing attacks to these platforms. Hence, phishing poses a serious threat to social media users, as phishers are able to target a significant number of victims across various platforms such as Facebook, Instagram, Twitter and Snapchat. In the face of evolving phishing threats, users often lack the awareness and ability to manage these threats, and thus they thoughtlessly engage on these platforms. As a result of this problem, the objective of this article was to identify the factors that contribute to phishing susceptibility on social media and produce a model that will reduce the likelihood that identified individuals would fall for phishing attacks on social media. To facilitate this, a systematic literature review was conducted to determine the specific factors that contribute to an increased susceptibility to phishing attacks on social media platforms. The method employed in this review started by determining a suitable search string, and after various rounds of screening a total of 25 articles were finally included in the content analysis. From these articles, it was established that women with low technical and security knowledge between the age of 18 and 25, who habitually use social media and process content heuristically, are more susceptible to falling for phishing attacks. These findings served as the basis for the proposed phishing reduction model that facilitates an increased awareness of the factors that influence a user's susceptibility to social media phishing. Based on the heuristic–systematic model, which served as the theoretical foundation of this article, the most significant aspect in the proposed model to reduce phishing on social media is processing content systematically. It is hoped that the individuals belonging to the susceptible groups identified, who follow the model, will reduce their susceptibility to falling for phishing attacks. Additionally, organisations can increase their knowledge of the specific factors that contribute to an increased susceptibility to social media-based phishing attacks. This will enable them to identify the specific groups that are susceptible to phishing attacks on social media to conduct targeted security training.

Acknowledgements

Competing interests

The views expressed in this article are that of the authors and not an official position of Rhodes University.

Authors' contributions

H.J.P. was responsible for the research and write-up of the article. S.V.F. acted in a supervisory capacity and was responsible for model refinement, manuscript review and submission.

Ethical consideration

This article followed all ethical standards for carrying out research.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

Albladi, S.M. & Weir, G.R.S., 2016, 'Vulnerability to social engineering in social networks: A proposed user-centric framework', in *Proceedings of the IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, IEEE, Vancouver, Canada, June 12–14, 2016, pp. 1–6.

Albladi, S.M. & Weir, G.R.S., 2018, 'User characteristics that influence judgment of social engineering attacks in social networks', *Human-Centric Computing and Information Sciences* 8(5), 1–24. https://doi.org/10.1186/s13673-018-0128-7

Algarni, A., Xu, Y. & Chan, T., 2015, 'Susceptibility to social engineering in social networking sites: The case of Facebook', in *Proceedings of the 36th International Conference on Information Systems*, AIS, Fort Worth, TX, December 13–16, 2015, pp. 1–23.

Alnajim, A. & Munro, M., 2009, 'An anti-phishing approach that uses training intervention for phishing websites detection', in *Proceedings of the 6th International Conference on Information Technology: New Generations*, IEEE, Las Vegas, NV, April 27–29, 2009, pp. 405–410.

Alseadoon, I., Chan, T., Foo, E. & Gonzales Nieto, J., 2012, 'Who is more susceptible to phishing emails?: A Saudi Arabian study', in *Proceedings of the 23rd Australasian Conference on Information Systems*, ACIS, Geelong, December 03–05, 2012, pp. 1–11.

Alseadoon, I., Othman, M. & Chan, T., 2015, 'What is the influence of users' characteristics on their ability to detect phishing emails?', in H.A. Sulaiman, M.A. Othman, M.F.I. Othman, Y.A. Rahim & N.C. Pee (eds.), *Advanced computer and communication engineering technology*, pp. 949–962, Springer, Cham.

Banu, M.N. & Banu, S.M., 2013, 'A comprehensive study of phishing attacks', *International Journal of Computer Science and Information Technologies* 4(6), 783–786.

Barker, I., 2019, *Social media phishing attacks up more than 70 percent*, viewed 15 September 2019, from https://betanews.com/2019/05/02/social-media-phishing/

Brecht, D, 2017, *Phishing attacks targeting young adults, in Infosec*, viewed 10 March 2020, from https://resources.infosecinstitute.com/phishing-attacks-targeting-young-adults/#gref

Chaiken, S. & Eagly, A.H., 1989, 'Heuristic and systematic information processing within and beyond the persuasion context', in J.S. Uleman & J.A. Bargh (eds.), *Unintended thought*, pp. 212–252, Guilford Press, New York, NY.

Costa, P.T. & McCrae, R.R., 1992, *NEO Personality Inventory-Revised (NEO PI-R)*, Psychological Assessment Resources, Odessa, FL.

Darwish, A., El Zarka, A. & Aloul, F., 2012, 'Towards understanding phishing victims' profile', in *Proceedings of the International Conference on Computer Systems and Industrial Informatics*, pp. 1–5, IEEE, Sharjah, December 18–20, 2012.

Dodge, R., Rovira, E., Zachary, R. & Joseph, S., 2011, 'Phishing awareness exercises', in *Proceedings of the 15th colloquium for Information Systems Security Education*, pp. 120–125, CISSE, Fairborn, OH, June 13–15, 2011.

Facebook, 2012, *New protections for phishing*, viewed 11 March 2020, from https://www.facebook.com/notes/facebook-security/new-protections-for-phishing/10150960472905766/

Facebook, 2020a, *What can I do if I've been phished on Facebook?* viewed 11 March 2020, from https://www.facebook.com/help/166863010078512?faq=168134929914064#What-is-phishing?

Facebook, 2020b, *What can I do about malicious software on Facebook?* viewed 11 March 2020, from https://www.facebook.com/help/389666567759871

Frauenstein, E.D. & Flowerday, S.V., 2016, 'Social network phishing: Becoming habituated to clicks and ignorant to threats?', in *Proceedings of the 15th International Conference on Information Security South Africa*, IEEE, Johannesburg, August 17–18, 2016, pp. 98–105.

Goel, S., Williams, K. & Dincelli, E., 2017, 'Got phished? Internet security and human vulnerability', *Journal of the Association for Information Systems* 18(1), 22–44. https://doi.org/10.17705/1jais.00447

Halevi, T., Lewis, J. & Memon, N., 2013, 'A pilot study of cyber security and privacy related behavior and personality traits', in *Proceedings of the 22nd International Conference on World Wide Web*, AMC, Rio de Janeiro, May 13–17, 2013, pp. 737–744.

Harrison, B., Vishwanath, A., Ng, Y. & Rao, R., 2015, 'Examining the impact of presence on individual phishing victimization', in *Proceedings of the 48th Hawaii International Conference on System Sciences*, IEEE, Kauai, HI, January 05–08, 2015, pp. 3483–3489.

Harrison, B., Vishwanath, A. & Rao, R., 2016, 'A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing', in *Proceedings of the 49th Hawaii International Conference on System Sciences*, IEEE, Koloa, HI, January 05–08, 2016, pp. 5628–5634.

Hong, J., 2012, 'The state of phishing attacks', *Communications of the ACM* 55(1), 74–81. https://doi.org/10.1145/2063176.2063197

Iuga, C., Nurse, J.R.C. & Erola, A., 2016, 'Baiting the hook: Factors impacting susceptibility to phishing attacks', *Human-centric Computing and Information Sciences* 6(1), 1–20. https://doi.org/10.1186/s13673-016-0065-2

Jensen, M., Dinger, M., Wright, R. & Thatcher, J., 2017, 'Training to mitigate phishing attacks using mindfulness techniques', *Journal of Management Information Systems* 34(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Kaspersky, 2018, *Fake Facebook sites account for 60% of social network phishing in early 2018*, viewed 16 September 2019, from https://www.kaspersky.com/about/press-releases/2018_social-network-phishing-early-2018

Kemp, S., 2019, *Digital trends 2019: Every single stat you need to know about the Internet*, viewed 16 September 2019, from https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet/

Lin, X., Spence, P. & Lachlan, K., 2016, 'Social media and credibility indicators: The effect of influence cues', *Computers in Human Behaviour* 63, 246–271. https://doi.org/10.1016/j.chb.2016.05.002

Liu, D. & Campbell, W., 2017, 'The big five personality traits, big two metatraits and social media: A meta-analysis', *Journal of Research in Personality* 70, 229–240. https://doi.org/10.1016/j.jrp.2017.08.004

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M., 2017, 'Individual differences and information security awareness', *Computers in Human Behavior* 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Metcalfe, M. & Powell, L., 2000, 'Revisiting the argumentative research methodology', *Communications of ACIS Proceedings*, Brisbane, Australia, December 6–8, 2000, pp. 1–13.

Moody, G., Galletta, D., Walker, J. & Dunn, B., 2011, 'Which phish get caught? An exploratory study of individual susceptibility to phishing', *European Journal of Information Systems* 26(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x

Nowell, L.S., Norris, J.M., White, D.E. & Moules, N.J., 2017, 'Thematic analysis: Striving to meet the trustworthiness criteria', *International Journal of Qualitative Methods* 16(1), 1–13. https://doi.org/10.1177/1609406917733847

ProofPoint, 2018, *The latest in phishing trends: October 2018*, viewed 16 September 2019, from https://www.proofpoint.com/us/security-awareness/post/latest-phishing-october-2018.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. & Downs, J., 2010, 'Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Sytems*, AMC, Atlanta, GA, April 10–15, 2010, pp. 373–382.

Shropshire, J., Warkentin, M. & Sharma, S., 2015, 'Personality, attitudes, and intentions: Predicting initial adoption of information security behavior', *Computers & Security* 49, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Smahel, D., Brown, B. & Blinka, L., 2012, 'Associations between online friendship and Internet addiction among adolescents and emerging adults', *Developmental Psychology* 48(2), 381–388. https://doi.org/10.1037/a0027025

University of Carolina, 2018, *Creating a PRISMA flow diagram*, viewed 20 November 2018, from https://guides.lib.unc.edu/prisma

Vishwanath, A., 2014, 'Diffusion of deception in social media: Social contagion effects and its antecedents', *Information Systems Frontiers* 17(6), 1353–1367. https://doi.org/10.1007/s10796-014-9509-2

Vishwanath, A., 2015a, 'Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack', *Journal of Computer-Mediated Communication* 20(5), 570–584. https://doi.org/10.1111/jcc4.12126

Vishwanath, A., 2015b, 'Habitual Facebook use and its impact on getting deceived on social media', *Journal of Computer-Mediated Communication* 20(1), 83–98. https://doi.org/10.1111/jcc4.12100

Vishwanath, A., Harrison, B. & Ng, Y., 2016, 'Suspicion, cognition, and automaticity model of phishing susceptibility', *Communication Research* 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H.R., 2011, 'Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model', *Decision Support Systems* 51(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Wright, R., Chakraborty, S., Basoglu, A. & Marett, K., 2010, 'Where did they go right? Understanding the deception in phishing communications', *Group Decision and Negotiation* 19(4), 391–416. https://doi.org/10.1007/s10726-009-9167-9

Appendices starts on the next page →

Appendix 1

TABLE 1-A1: Quality assessment tool.

Variable	Yes	Partial	No
Design			
Q1. Researcher clearly states the goals of the research?			
Q2. Researcher states why the research is important?			
Q3. Researcher has justified the research design?			
Conduct			
Q4. Researcher makes the method followed explicit?			
Q5. Researcher justifies the chosen method?			
Analysis			
Q6. Researcher provides a detailed description of the analysis process?			
Q7. Researcher takes contradictory evidence into account?			
Q8. Researcher clearly states the findings?			
Q9. Researcher provides adequate discussion of the evidence both for and against the research arguments?			
Q10. Researcher discusses the findings in relation to the original research question?			
Conclusion			
Q11. Researcher discusses the contribution the study makes to existing knowledge or understanding?			
Q12. Researcher identifies new areas where research is still necessary?			
Q13. Research discussed whether or how the findings can be generalised to other situations/populations?			
General			
Q14. Researcher has written the article in a clear and coherent manner?			

Appendix 2

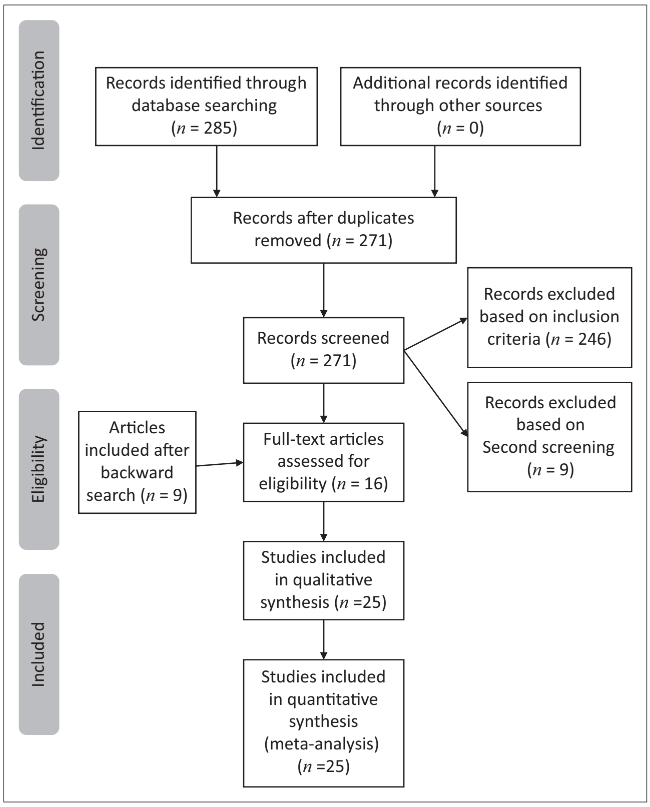

Identification
Screening
Eligibility
Included
Records identified through database searching (*n* = 285)
Additional records identified through other sources (*n* = 0)
Records after duplicates removed (*n* = 271)
Records screened (*n* = 271)
Records excluded based on inclusion criteria (*n* = 246)
Records excluded based on Second screening (*n* = 9)
Articles included after backward search (*n* = 9)
Full-text articles assessed for eligibility (*n* = 16)
Studies included in qualitative synthesis (*n* =25)
Studies included in quantitative synthesis (meta-analysis) (*n* =25)

FIGURE 1-A2: Preferred Reporting Items for Systematic Reviews and Meta-Analyses flow diagram.

Appendix 3

TABLE 1-A3: Sample of articles used for content analysis.

References	Quality assessment result
Frauenstein, E.D. & Flowerday, S.V., 2016, 'Social network phishing: Becoming habituated to clicks and ignorant to threats?', *Proceedings of the 15th international conference on Information Security South Africa*, IEEE, Johannesburg, Gauteng, South Africa, August 17–18, 2016, pp. 98–105.	**11.0**
Goel, S., Williams, K. & Dincelli, E., 2017, 'Got phished? Internet security and human vulnerability', *Journal of the Association for Information Systems* 18(1), 22–44. https://doi.org/10.17705/1jais.00447	**11.0**
Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H.R., 2011, 'Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model', *Decision Support Systems* 51(3), 576–586.	**11.0**
Halevi, T., Lewis, J. & Memon, N., 2013, 'Phishing, personality traits and Facebook', *arXiv preprint arXiv* 1301, 7643.	**10.5**
Harrison, B., Vishwanath, A., Ng, Y. & Rao, R., 2015, 'Examining the impact of presence on individual phishing victimization', *Proceedings of the 48th Hawaii International Conference on System Sciences*, IEEE, Kauai, Hawaii, USA, January 05–08, 2015.	**10.5**
Moody, G., Galletta, D., Walker, J. & Dunn, B., 2011, 'Which phish get caught? An exploratory study of individual susceptibility to phishing', *European Journal of Information Systems* 26(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x	**10.5**
Algarni, A., Xu, Y. & Chan, T., 2015, 'Susceptibility to social engineering in social networking sites: The case of Facebook', *Proceedings of the 36th International Conference on Information Systems*, AIS, Fort Worth, TX, USA, December 13–16, 2015.	**10.0**
Iuga, C., Nurse, J.R.C. & Erola, A., 2016, 'Baiting the hook: Factors impacting susceptibility to phishing attacks', *Human-Centric Computing and Information Sciences* 6(1), 1–20. https://doi.org/10.1186/s13673-016-0065-2	**10.0**
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. & Downs, J., 2010. 'Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions', *Proceedings of the SIGCHI Conference on Human Factors in Computing Sytems*, AMC, Atlanta, GA, USA, April 10–15, 2010, pp. 373–382.	**10.0**
Vishwanath, A., 2015a, 'Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack', *Journal of Computer-Mediated Communication* 20(5), 570–584. https://doi.org/10.1111/jcc4.12126	**10.0**
Alseadoon, I., Chan, T., Foo, E. & Gonzales Nieto, J., 2012, 'Who is more susceptible to phishing emails?: A Saudi Arabian study', *Proceedings of the 23rd Australasian Conference on Information Systems*, ACIS, Geelong, Victoria, Australia, December 03–05, 2012.	**10.0**
Halevi, T., Lewis, J. & Memon, N., 2013, *A pilot study of cyber security and privacy related behavior and personality traits*, pp. 737–744, Association for Computing Machinery (AMC), Rio de Janeiro.	**10.0**
Vishwanath, A., 2015b, 'Habitual Facebook use and its impact on getting deceived on social media', *Journal of Computer-Mediated Communication* 20(1), 83–98. https://doi.org/10.1111/jcc4.12100	**10.0**
Albladi, S.M. & Weir, G.R.S., 2018, 'User characteristics that influence judgment of social engineering attacks in social networks', *Human-Centric Computing and Information Sciences* 8(5), 1–24. https://doi.org/10.1186/s13673-018-0128-7	**9.5**
Darwish, A., El Zarka, A. & Aloul, F., 2012, 'Towards understanding phishing victims' profile', *Proceedings of the International Conference on Computer Systems and Industrial Informatics*, IEEE, Sharjah, United Arab Emirates, December 18–20, 2012.	**9.5**
Halevi, T., Memon, N. & Nov, O., 2015, *Spear-Phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks*, viewed 10 May 2018, from https://doi.org/10.2139/ssrn.2544742**.**	**9.5**
Vishwanath, A., Harrison, B. & Ng, Y., 2016, 'Suspicion, cognition, and automaticity model of phishing susceptibility', *Communication Research* 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483	**9.5**
Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. & Hong, J., 2010, 'Teaching Johnny not to fall for phish', *ACM Transactions on Internet Technology (TOIT)* 10(2), 1–31. https://doi.org/10.1145/1754393.1754396	**9.5**
Vishwanath, A., 2014, 'Diffusion of deception in social media: Social contagion effects and its antecedents', *Information Systems Frontiers* 17(6), 1353–1367. https://doi.org/10.1007/s10796-014-9509-2	**9.5**
Lawson, P., Zielinska, O., Pearson, C. & Mayhorn, C.B., 2017, 'Interaction of personality and persuasion tactics in email phishing attacks', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Sage, California, LA, October 09–13, 2017.	**8.5**
Alseadoon, I., Othman, M. & Chan, T., 2015, 'What is the influence of users' characteristics on their ability to detect phishing emails?', in H.A. Sulaiman, M.A. Othman, M.F.I. Othman, Y.A. Rahim & N.C. Pee (eds.), *Advanced computer and communication engineering technology*, Springer, Cham, pp. 949–962.	**8.5**
Harrison, B., Vishwanath, A. & Rao, R., 2016, 'A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing', *Proceedings of the 49th Hawaii International Conference on System Sciences*, IEEE, Koloa, Hawaii, USA, January 05–08, 2016.	**8.0**
Hong, J., 2012, 'The state of phishing attacks', *Communications of the ACM* 55(1), 74–81. https://doi.org/10.1145/2063176.2063197	**8.0**
Valecha, R., Chen, R., Herath, T., Vishwanath, A., Wang, J. & Rao, R., 2015, 'An exploration of phishing information sharing: A heuristic-systematic approach', *Proceedings of the 10th Pre-ICIS Workshop on Information Security and Privacy*, viewed 13 September 2018, from https://aisel.aisnet.org/wisp2015/2	**6.5**
Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J. & Rovira, E., 2012, 'The influences of social networks on phishing vulnerability', *Proceedings of the 45th Hawaii International Conference on System Sciences*, IEEE, Maui, Hawaii, January 04–07, 2012.	**5.5**