A Preliminary Investigation on User Factors of Phishing E-mail

Ainnur Hafizah Anuar Mokhtar
Fauziah Redzuan
Wan Adilah Wan Adnan
Rosalind J. S. Vincent
Akhmad Sagir
Fazli Abdul-Hamid
Mohd Saleh Abbas

DOI: https://doi.org/10.37178/ca-c.23.1.189

Ainnur Hafizah Anuar Mokhtar, *Faculty of Computer and Mathematical Sciences, Universiti Teknologi Mara (UiTM), Malaysia*
Email: ain_146@ums.edu.my

Fauziah Redzuan, *Faculty of Computer and Mathematical Sciences, Universiti Teknologi Mara (UiTM), Malaysia*
Email: fauziahr@tmsk.uitm.edu.my

Wan Adilah Wan Adnan, *Faculty of Computer and Mathematical Sciences, Universiti Teknologi Mara (UiTM), Malaysia*
Email: adilah@tmsk.uitm.edu.my

Rosalind J. S. Vincent, *Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*
Akhmad Sagir, *UIN Antasari Banjarmasin, Indonesia*

Fazli Abdul-Hamid, *Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia*

Mohd Saleh Abbas, *INTI International University, Malaysia*

ABSTRACT

The increasing rate of Internet users and the adaptation to technology are threatening security. The most prevalent threat is phishing, which uses social engineering attacks to mislead users to reveal confidential and sensitive information such as usernames and passwords. Phishing is a type of e-mail fraud in which an intruder poses a trustworthy or trusted source by clicking on a link or opening an e-mail attachment to deceive the recipient. Phishing e-mails are those that employ both social engineering and technological tricks. It is essential to use e-mails today because almost every person in the world has to use them, whether personal or business. The truth is that anyone who has used e-mails may be a possible target for cybercriminals. User factor is an essential element in a phishing e-mail. In this study, interviews were conducted to get the user factors involved in a phishing e-mail. The findings show that the user factors are demographic, behaviour, weapons of influence and e-mail contents phishing e-mail.

INTRODUCTION

Phishing is the most widely used social engineering technique[1]. According to[2], phishing uses electronic networks to trick users into sharing confidential and sensitive

information, passwords, and account numbers. Phishing has been around for decades, but it has only recently been used to obtain personal information and classified information. Phishing is a well-known security risk in today's digital world, and it is a deceptive attempt to get confidential personal information from an unsuspecting individual. For a variety of attacks and threats, phishing must be the preferred method[3].

Phishing is mainly done through e-mail, where a phisher poses as a trusted or reliable source to persuade the recipient to click on a link or open a file in an electronic message[4]. The user characteristics of a phishing e-mail are user factors and awareness. The user factor focuses on human behaviour where it needs to understand the actions of users to a phishing e-mail[5]. In this study, the user factors are demographic, behavior, e-mail content and weapons of influence. The procedure of phishing e-mails starts with an electronic message aimed at deceiving recipients interested in providing information or logging on to a sender. Usually, the transmitter masks as a legal person and creates communication to persuade the person to act[6].

This act could include disclosing confidential private information such as PINs or unintentionally granting access to their laptop or network[2];[4]. A preliminary investigation on user factors of phishing e-mail is conducted in this study.

LITERATURE REVIEW

Phishing is one of the most significant security threats, as it is the root of most data security incidents[1]. According to the APWG, phishing is an illegal method that combines technical deception and psychological manipulation to obtain private information and account authorisations. In Malaysia, phishing is also a significant concern. Based on the Malaysia Computer Emergency Response Team (MyCERT), phishing is an incident that has the highest priority level over other ventures in Cyber Security in Malaysia; as shown in Figure 1, phishing is among the top four threats, with rising trends. It is also ranked in the same ranking for both years. It demonstrates that phishing trends are growing, while the top risks are increasing year after year.

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, — Stable, ↗ Increasing **Ranking:** ↗ Going up, — Same, ↙ Going down

Figure 1. Summary of Top Threats 2019-2020

2.1 Phishing

In 1996, the term "phishing" was coined after many deceptive clients were recorded on the America Online (AOL) site with forged credit card information[7]. The term "phishing" was first used in phishing on the American Online (AOL) Usenet Newsgroup on January 2, 1996 and has been in use ever since[7]. Most hackers would produce fake AOL reports that automatically generate fraudulent credit card information [8]. Phishing is a sort of community exploitation asset where hackers make people share personal data or install malware on their PCs through spoofed e-mail[9].

Table 1

Various Definition of Phishing

No.	Author	Definition
1.	[8]	A type of social engineer in which an attacker, also known as a phisher, attempts to obtain confidential or sensitive data from legitimate users by automating electronic communications from a trusted or public institution.
2.	[10]	Phishing is a psychological trick aimed at getting deceived individuals to provide personal information on the Internet so that the perpetrator can fraudulently exploit their credentials.
3.	[11]	An online spoofing framework for communication via electronic communication channels of social engineering messages to allow users to perform specific actions for attackers
4.	[2]	A criminal technique that combines social engineering and technological manipulation intending to take individual information from users and financial account credentials.
5.	[10, 12]	A scalable act of deception using impersonation to obtain data from a target.
6.	[13]	A social engineering attack in which hackers use spoofed e-mails to make people use their computers to exchange sensitive data or download malware.
7.	[8]	Phishing is a common form of social engineering in which confidential information is stolen by sending false e-mails from a trusted source.

Phishing in the physical world has the same fundamental concept as “fishing.” According to[8], phishing is a form of social engineering. An intruder, also known as a phisher, tries fraudulently to acquire the confidential or sensitive credentials of legitimate usernames by automatically mimicking electronic messages from a trusted or public institution.

Phishing is defined by the Anti-Phishing Working Group [2] as a criminal tactic that uses both social and technical deception to obtain user identity data and financial account credentials. Besides, [2]reported that it would be a misleading move for users to disclose sensitive and confidential information using technical media, including e-mails, websites, chat, and text messages, such as identity profiles, usernames, etc passwords.

In conclusion, phishing is a common type of social engineering based on the various ways in which phishers use technical media such as e-mails and websites to trick users into sharing personal information and deceive them. Phishing, a well-known security issue in today’s digital world, attempts to deceive an unsuspecting individual into revealing sensible personal data.

2.2. Phishing E-mail

Phishing is an intrusion of social engineering where phishers use technical media like e-mail and websites to dupe and trick users into sharing their personal information[14]. Phishing e-mails are described as e-mails that use both social engineering and technological tricks. It has been used to steal users’ secret

information and manipulate users' behavioural characteristics to enhance users' chances of doing what they desire[2].

Phishing is the practice of sending e-mails to obtain personal information from reputable sources. Phishing e-mails attempt to persuade computer users to share personal information such as credit card numbers, login and username information, and other pertinent data. Phishing e-mails are generally sent to many randomly selected recipients to cater to natural users' emotions of envy, fear, and reverence for authority, as well as sympathy, curiosity, and willingness to interact.

2.3 User Factors

User factors in the context of information security have initiated to expand enhanced attention, especially phishing e-mail. One particularly notable feature of this method is the use of security technologies that have failed to protect companies from cyberattacks[15]. User factors are classified into demographic characteristics: age and gender, user behaviour, e-mail content, and the weapon of influence in an e-mail. [18] analysed gender differences in the adoption and usage of technology in the workplace and found that gender differences became more prevalent with rising age. Gender disparities in perceptions of technology have become far more prominent among older staff and less noticeable among younger employees.

However, recent research by [16] surveyed a Finnish municipal organisation revealed no gender gap in the number of workers. The gender disparities in security behaviour that have been established in the field of information security include women who are more vulnerable to phishing attacks. However, females have been reported to have higher levels of safety issues [14, 17, 18] and

[19-21]studied the correlation between low computer skills and vulnerability to phishing attacks. It was found that computer skills likely play a role in the overall susceptibility to phishing e-mails. However, higher computer literacy can cause users to overestimate their ability to monitor their online environment, contributing to an increased risk of online activity.

A study by [22] showed that participants who use the Internet more frequently are more mindful of the dangers of the online environment. But in terms of enhanced awareness or computer skills, individual guardianship measures do not guarantee complete immunity to phishing attacks[19, 20].

User factors mainly focus on visual cues and indicators to recognise a phishing attack. Kirlappos used techniques such as online games. whereas, phishers tend to exploit human vulnerabilities by tapping into behavioural factors such as temptation[23]. [14]identified the design for phishing e-mail by probing the cues that generally distinguish phishing e-mail from real e-mails. The study revealed that participants frequently use cues that are not good indicators of whether an e-mail is phishing or legitimate. It includes legal disclaimers, the quality of visual presentation, and the positive consequences highlighted in the e-mail.

A study by [24] focused on e-mail content such as weapons of influence which is persuasive techniques that phishers can use to lure individuals into falling for a phishing e-mail attack. Successful phishing e-mails apply psychological principles of influence – authority, commitment, liking, perceptual contrast, reciprocation, scarcity and social proof [25]. These influence concepts in this study exploit general human heuristics and help to simplify decision-making but can often contribute to misrepresentation and deception.

PROBLEM BACKGROUND

The phishing e-mail attacks is a critical cybercrime nowadays, which not only increase as time goes on, but they are also evolving. Statistics disclosed that about 97% of users worldwide are incapable of identifying phishing attacks, which undoubtedly indicates that users lack knowledge regarding this type of attacks[25]. Regarding this situation, user factors are crucial to overcoming phishing attacks.

Phishing e-mails use social and technological tricks to steal users' confidential data [2] and take advantage of human behaviour[26]. The researcher can see the influence of user factors on a phishing e-mail through some demographic elements, user behaviours, e-mail content, and weapons of influence in an e-mail that is persuasive tactics that attackers may use to attract people fall for an attack.

There are some previous studies on the demographic factors which correlated between gender and phishing vulnerability. [19]in their study observed that adult females are substantially more likely to fall for phishing than males. Similarly, [24] discovered that matured females contribute the highest vulnerable unit to phishing susceptibility contrasted to additional demographics, which us same with [27] which stated that adult females are susceptible to phishing e-mails.

On the other hand, they found that gender has a slightly significant difference in phishing attacks where the attacks deceived females and males, as mentioned by[28]. However, the finding was different from[29], where the study found no significant gender association shown in the results of their study.

Some studies have studied phish vulnerability based on age and found that older users are more vulnerable to phishing than other ages between 18 and 25 years of age [30]. Persons up to middle age but not older users (60 years and older) were included. The previous research suggested that the correlation between age and phishing vulnerability is inconsistent. [31] found that people over the age of 59 years are more vulnerable to e-mails from phishing. Same to study by [27] found that older adults are more vulnerable to phishing e-mails than younger users.

User activity is divided into two groups, knowledge and internet use. Research by [22] found that targeted messages would contribute to participants' response who usually use rational decision-making to phishing attacks. And those who use the Internet for diversified reasons are more conscious and less vulnerable to phishing attacks. For instance, a study carried out by [32] showed that university students are alarmingly susceptible to e-mail attacks. Their findings are significant because university students are mostly computer-literate and aware of these types of phishing.

Like the [33] study, 89 per cent of the respondents accepted that they trust that a legitimate e-mail and phishing e-mail can be distinguished based on their previous experience. However, the results have shown that approximately 92 per cent of participants misclassified phishing e-mails. From this contradictory finding, most participants were not only vulnerable to phishing but overconfident to defend themselves from phishing.

E-mail content is also one of the main factors in e-mail phishing. [34]noted that characteristics of e-mail content, such as logo's visual aspects and banners representing the organisation or business or entity, will lead the people to click on the phishing e-mails. In a second study by[35], attention was given to urgent questions and e-mail subject lines, which are considerably susceptible for the consumer to click and respond to phishing e-mails. However, grammar or orthographic awareness levels were significantly less likely to trigger users to click on phishing e-mails. Phishers also use visual cues to reproduce company logos and organisational slogans to boost consumer's trust in the message [42]. [43] found that users had trouble differentiating phishing e-mails because spelling or grammatical errors are more likely to happen than actual e-mails.

It is a success when these e-mails must disclose their data outside of the confidential path as information is not covered outside of the confidence path. They mislead workers into believing that the belief route used to give in this data by impersonating legitimate entities[12]. Two forms of manipulation occur: by clicking or by answering. To steal confidential information from the click action, the user must visit a phishing site. A response behaviour involves a request that the client responds to these e-mails by sending its secret information. The successful attack from phishing e-mail comes from social influence or persuasion strategies. [36]stated that social influence is used as fundamental to get a quick response from the victim. For example,

if the recipient fails to respond or act within a limited period, an e-mail will inform the account termination. So, the recipients will respond as quickly as possible to ensure the bank will not terminate their account.

Studies on the weapon of power of authority, commitment, liking, reciprocity, scarcity and social proof in [27] found that scarcity and authority are the most potent instruments for any group's age. Younger users, however, are more resilient to scarcity, while older adults are most vulnerable. [4]investigated three weapons of influence, namely authority, scarcity, and social proof. That study showed that authority is the most potent means of persuasion in persuading users to click on the e-mail connection and protect the e-mail[4].

Research by [24] showed that all weapons of control that were empirically tested in a single phishing experiment are most vulnerable to the concepts of continuity and reciprocity, contrary to the findings of[37]. [20]The most common methods of persuasion used in a study of social engineering for online fraud are authority, urgency, fear or danger, politeness, and formality. In 100% of these cases, the cybercrime authority was used, and 71% of phishing mails added a sense of urgency[38]. Apart from the factors mentioned above, emotion is one of the essential elements in e-mail phishing activity.

4. RESULTS AND DISCUSSIONS

A preliminary investigation was done through e-mail interview with six real victims who were involved in phishing. Table 2 summarises the respondent's details and the findings from the interview.

Table 2

Findings from the E-mail Interview

No.	Respondent	Findings
1.	Woman, 34, Full-time postgraduate student.	She received an e-mail from the bank asking her to update her username and password. She clicked the link and automatically brought her to a fake website that looked like her online banking website. In the site, she was asked to give OTP numbers, where she filled it up and logged out from the site. After that, she got a message from the bank stated that she already made a transaction by transferring an amount of money to another party account. She clicked the link because she felt scared and fearful because the e-mail stated that if she did not update her username and password, the account will be blocked. At the same time, she did not have any knowledge of phishing and was not familiar about it.
2.	Woman, 38, Engineer	She received an e-mail from a familiar organisation asking her to update her profile. She clicked the link and updated her profile not knowing that the phishers cheated and led her to a fake website. After she updated the profile, she logged out as usual. And an hour after that, she got a message from the bank stated that she made a transaction to overseas with an amount of money by using her credit card. She updated her profile because the e-mail said that if she does not update it, her purchase online after this will have problems. She felt worried and scared that if she did not update her profile, then difficulties will happen after that. She trusted the site because of the logos and banners used are same with the legitimate website.
3.	Man, 45, School Teacher	He was offered a job through an online platform. He felt excited because the salary offered for the job was high, and at the same time, he needed the job. He was asked to fill up the form via online by giving all the personal information in the site. And after that, he got an e-mail stated that an interview will be conducted for him in another two days. All the details for the interview session were provided through the e-mail. But unfortunately, when he came to the place, there was no interview session and there was no job application at all. The building he went to was empty. He explained why he accepted the job because he was excited being offered and at the same time, he was desperate to get a job.
4.	Woman, 27, Actuary	She has experienced several times in phishing e-mails. The trickiest experience that she ever came across was when she was called for an interview by an e-mail pretending to be the Central Bank of Kenya. She replied the e-mail and gave the information they wanted. After that, they asked her to send $800 to activate the application because her name was shortlisted in the final

		list. She paid them the amount of money, and sadly after that, they did not reply to her again. She spent the amount of money because she was excited about being offered a job from a known bank in Kenya. At the same time, she felt happy to get a job, but sadly it was only a con.
5.	Man, 24, Entrepreneur and Marketer	He has experienced e-mail fraud where someone pretended to be bank support and tried to lure him by claiming that his bank account had a problem. That person asked him to provide his account number, PIN and other personal details that he used while registering the account. He later researched on the Internet and noted that the bank uses a different e-mail from that. Luckily, he did not yet perform any actions. However, during the first impression, he felt scared and anxious because the bank asked about personal information. But he took a wise action by searching for the information before taking any action.
6.	Man, 50, Clerk	He got an e-mail from an organisation which told him that he got RM50,000 as a lucky draw. He was so excited and felt fortunate to get the random draw with a lot of money. But he was needed to fill a complete form by providing all the personal information including a photocopy of identity card and needed to pay an amount of money for transaction fees. He did all the requirements of the organisation. But unfortunately, after he sent the documents, there was no reply from the organisation. Then, he tried to contact the organisation by trying to send an e-mail. Unfortunately, the e-mails were bounced back with statements saying that the e-mail does not exist anymore. After he experienced this, he became more cautious when getting any e-mail. He shared that he is a victim because he does not have any knowledge on phishing, lack of education on phishing or scam and at the same time felt greedy to see the amount of money that he will get.

This preliminary investigation summarises that people would become susceptible to phishing e-mail because of their emotion, such as feeling scared or fearful. Simultaneously, the users also feel worried and trust the site based on the logos and banners. Other than that, people are lured into phishing because of their excitement, happiness, and desperation on what is offered in the e-mails. Victims also feel anxious, lack knowledge, lack education, and feel greedy to see a lot of money. Another problem that victim or users always face is the design of phishing e-mail or websites.

In [36] study, 90% of participants in their research were fooled by well-designed phishing websites. They clicked on the websites and followed all the directions. [48] argued that the effect of emotions on responding to phishing should be a crucial area of future research. They proposed that the current emotional condition of a person shapes their decision by moderating the focus, sensitivity and depth of information processing that contributes to user's consciousness.[39]'s study focused on perceived severity and self-efficacy.

Phishers take advantage of standard and current events such as a pandemic, convictions, prizes, faith and politics to draw responses from their victims. These methods may affect data processing by the victim who cannot take appropriate care to verify the message's validity. The material and claims in the body of the message can trigger human emotions such as fear or excitement efficiently and affect cognitive capabilities, a ploy compounded by the use of concepts of persuasion[28, 40].

6. CONCLUSIONS

Phishing is a severe cybercrime that happens every day and it is usually done through e-mail. The findings of this study highlight the user factors of phishing e-mail which is demographic factors that include gender and age. Besides, the user factors also consist of user behaviours that contain user knowledge and experience. Adding the weapon influence following the social influence principles (authority, commitment, liking, reciprocity, scarcity, and social proof) in a phishing e-mail leads the users to intrude into phishing e-mail. This is also the same with the e-mail contents that involve all the visual cues and indicators in a phishing e-mail. Both elements are the user factors of a phishing e-mail. Insights from this study can help individuals understand their own vulnerability level to phishing attacks through e-mail and guide training approaches to reduce vulnerability to phishing e-mails.

ACKNOWLEDGEMENTS

The authors would like to thank and acknowledge Dr Fauziah Redzuan and Associate Professor Dr Wan Adilah Wan Adnan as co-supervisor for all the guidance and support in this study.

REFERENCES

1. Goel, D. and A.K. Jain, *Mobile phishing attacks and defence mechanisms: State of art and open research challenges.* Computers & Security, 2018. **73**: p. 519-544.DOI: https://doi.org/10.1016/j.cose.2017.12.006.
2. APWG:, *Phishing Activity Trends Report Q4 2018," Comput. Fraud Secur., vol 2019, no. 3, p. 4,.* 2019.DOI: https://doi.org/10.1016/S1361-3723(19)30025-9.
3. Hadlington, L., *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.* Heliyon, 2017. **3**(7): p. e00346.DOI: https://doi.org/10.1016/j.heliyon.2017.e00346.
4. Butavicius, M., et al., *Breaching the human firewall: Social engineering in phishing and spear-phishing emails.* arXiv preprint arXiv:1606.00887, 2016.
5. Henshel, D., et al., *Trust as a human factor in holistic cyber security risk assessment.* Procedia Manufacturing, 2015. **3**: p. 1117-1124.DOI: https://doi.org/10.1016/j.promfg.2015.07.186.
6. Harrison, B., E. Svetieva, and A. Vishwanath, *Individual processing of phishing emails: How attention and elaboration protect against phishing.* Online Information Review, vol. 40, no. 2, pp. 265–281, 2016.DOI: https://doi.org/10.1108/OIR-04-2015-0106.
7. K. Rekouche, *"Early Phishing," pp. 1–9.* 2011.
8. Jakobsson, M. and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft, 3rd edition.* 2006: John Wiley & Sons.
9. Lastdrager, E.E.H., *Achieving a consensual definition of phishing based on a systematic review of the literature.* Crime Science, 2014. **3**(1): p. 1-10.DOI: https://doi.org/10.1186/s40163-014-0009-y.
10. Jagatic, T.N., et al., *Social phishing.* Communications of the ACM, 2007. **50**(10): p. 94-100.DOI: https://doi.org/10.1145/1290958.1290968.
11. Khonji, M., Y. Iraqi, and A. Jones, *Phishing detection: a literature survey.* IEEE Communications Surveys & Tutorials, 2013. **15**(4): p. 2091-2121.DOI: https://doi.org/10.1109/SURV.2013.032213.00009.
12. Junger, M., L. Montoya, and F.J. Overink, *Priming and warnings are not effective to prevent social engineering attacks.* Computers in human behavior, 2017. **66**: p. 75-87.DOI: https://doi.org/10.1016/j.chb.2016.09.012.
13. Ferreira, A. and S. Teles, *Persuasion: How phishing emails can influence users and bypass security measures.* International Journal of Human-Computer Studies, 2019. **125**: p. 19-31.DOI: https://doi.org/10.1016/j.ijhcs.2018.12.004.
14. Parsons, K., et al., *Predicting susceptibility to social influence in phishing emails.* International Journal of Human-Computer Studies, 2019. **128**: p. 17-26.DOI: https://doi.org/10.1016/j.ijhcs.2019.02.007.
15. Anwar, M., et al., *Gender difference and employees' cybersecurity behaviors.* Computers in Human Behavior, 2017. **69**: p. 437-443.DOI: https://doi.org/10.1016/j.chb.2016.12.040.
16. Vance, A., M. Siponen, and S. Pahnila, *Motivating IS security compliance: insights from habit and protection motivation theory.* Information & Management, 2012. **49**(3-4): p. 190-198.DOI: https://doi.org/10.1016/j.im.2012.04.002.
17. Hoy, M.G. and G. Milne, *Gender differences in privacy-related measures for young adult Facebook users.* Journal of interactive advertising, 2010. **10**(2): p. 28-45.DOI: https://doi.org/10.1080/15252019.2010.10722168.
18. McGill, T. and N. Thompson, *Gender differences in information security perceptions and behaviour, pp. 1–11,.* 2018.DOI: https://doi.org/10.5130/acis2018.co.
19. Halevi, T., J. Lewis, and N. Memon, *Phishing, personality traits and Facebook.* arXiv preprint arXiv:1301.7643, 2013.
20. Sheng, S., et al. *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*.DOI: https://doi.org/10.1145/1753326.1753383.
21. Wright, R.T. and K. Marett, *The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived.* Journal of Management Information Systems, 2010. **27**(1): p. 273-303.DOI: https://doi.org/10.2753/MIS0742-1222270111.
22. Halevi, T., N. Memon, and O. Nov, *Spear-phishing in the wild: a real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. SSRN Electron. J.(2015)*. 2015.

23. Kirlappos, I., M.A. Sasse, and N. Harvey. *Why trust seals don't work: A study of user perceptions and behavior*. Springer.DOI: https://doi.org/10.1007/978-3-642-30921-2_18.
24. Lin, T., et al., *Susceptibility to spear-phishing emails: Effects of internet user demographics and email content.* ACM Transactions on Computer-Human Interaction (TOCHI), 2019. **26**(5): p. 1-28.DOI: https://doi.org/10.1145/3336141.
25. Verkijika, S.F., *"If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender.* Computers in Human Behavior, 2019. **101**: p. 286-296.DOI: https://doi.org/10.1016/j.chb.2019.07.034.
26. Karakasiliotis, A., S.M. Furnell, and M. Papadaki, *Assessing end-user awareness of social engineering and phishing, pp. 60–72.* 2006.
27. Oliveira, D., et al. *Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing*.DOI: https://doi.org/10.1145/3025453.3025831.
28. Mohebzada, J.G., et al. *Phishing in a university community: Two large scale phishing experiments*. IEEE.DOI: https://doi.org/10.1109/INNOVATIONS.2012.6207742.
29. Diaz, A., A.T. Sherman, and A. Joshi, *Phishing in an academic community: A study of user susceptibility and behavior.* Cryptologia, 2020. **44**(1): p. 53-67.DOI: https://doi.org/10.1080/01611194.2019.1623343.
30. Kumaraguru, P., et al. *Protecting people from phishing: the design and evaluation of an embedded training email system.*DOI: https://doi.org/10.1145/1240624.1240760.
31. Li, W., et al. *Experimental investigation of demographic factors related to phishing susceptibility, pp. 2240–2249,* .DOI: https://doi.org/10.24251/HICSS.2020.274.
32. Parrish Jr, J.L., J.L. Bailey, and J.F. Courtney, *A personality based model for determining susceptibility to phishing attacks.* Little Rock: University of Arkansas, 2009: p. 285-296.
33. Hong, K.W., et al. *Keeping up with the Joneses: Assessing phishing susceptibility in an email task*. SAGE Publications Sage CA: Los Angeles, CA.DOI: https://doi.org/10.1177/1541931213571226.
34. Furnell, S., K. Millet, and M. Papadaki, *Fifteen years of phishing: can technology save us?* Computer Fraud & Security, 2019. **2019**(7): p. 11-16.DOI: https://doi.org/10.1016/S1361-3723(19)30074-0.
35. Vishwanath, A., B. Harrison, and Y.J. Ng, *Suspicion, cognition, and automaticity model of phishing susceptibility.* Communication Research, 2018. **45**(8): p. 1146-1166.DOI: https://doi.org/10.1177/0093650215627483.
36. Musuva, P.M.W., K.W. Getao, and C.K. Chepken, *A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility*. Computers in Human Behavior, 2019. **94**: p. 154-175.DOI: https://doi.org/10.1016/j.chb.2018.12.036.
37. Lastdrager, E., et al. *How Effective is {Anti-Phishing} Training for Children?*DOI: https://doi.org/10.1186/s40163-014-0009-y.
38. Abiodun, O., A.S. Sodiya, and S.O. Kareem, *Linkcalculator–an efficient link-based phishing detection tool.* Acta Informatica Malaysia, 2020. **4**(2): p. 37-44.DOI: https://doi.org/10.26480/aim.02.2020.37.44.
39. Gordon, W.J., et al., *Assessment of employee susceptibility to phishing attacks at US health care institutions.* JAMA network open, 2019. **2**(3): p. e190393-e190393.DOI: https://doi.org/10.1001/jamanetworkopen.2019.0393.
40. Frauenstein, E.D. and S. Flowerday, *Susceptibility to phishing on social network sites: A personality information processing model.* Computers & security, 2020. **94**: p. 101862.DOI: https://doi.org/10.1016/j.cose.2020.101862.