Online Security Attack Experience and Worries of Young Adults in the Kingdom of Saudi Arabia

Najla Aldaraani (✉) [0000-0002-9126-1630], Helen Petrie [0000-0002-0100-9846], and Siamak F. Shahandashti [0000-0002-5284-6847]

University of York, York YO10 5GH, UK
{nga505,helen.petrie,siamak.shahandashti}@york.ac.uk

Abstract. Online security attacks are a worldwide issue, and increasing rapidly in the Middle East. Much of the research on the human aspects of online security has been conducted in developing countries, and although there have been a number of studies in the Kingdom of Saudi Arabia (KSA), none of which compared experiences of users in different cultures. This study investigated the experiences and worries about online security attacks of 45 young adults in KSA and compared them with a previous study of young adults in the UK. Saudi young adults were most likely to have encountered phishing attacks and least likely to have encountered ransomware attacks. Their worries grouped into Theft Worries and Phishing Worries. These results were very similar to those found in the previous study in the UK, in spite of differences in the educational level, self-reported online security knowledge and ability to identify security attacks between the two samples. This suggests that online security attacks and the resulting worries are more international than might be predicted.

Keywords: Experience of online security attacks, worries about online security attacks, young adults, Kingdom of Saudi Arabia.

1 Introduction

Cyber attacks have become an increasingly prevalent issue worldwide. Statistics for 2018 [23] show that the Middle East[1] saw an 11% year on year increase in malware infections, with an average of 1.5 million attacks per day and 575 million per year. The average total cost of a data breach in the Middle East increased from USD 6.93 million in 2021 to USD 7.46 million in 2022 [21]. The Kingdom of Saudi Arabia (KSA) is one of the countries most commonly targeted by attackers. In 2018, the KSA experienced a significant increase in ransomware attacks, of over 378% [23].

[1] Middle East refers to the geopolitical area that usually is defined as the following countries: Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirate, Yemen [33].

Individual users play an important role in online security as they are the target of many online security attacks. Social engineering techniques are frequently used by cybercriminals to trick people into disclosing sensitive information, downloading malware, or clicking on malicious links. Individual users are also vulnerable to phishing attacks, ransomware, and other forms of online fraud, which can result in monetary loss, identity theft, and reputational harm. The third quarter of 2022 was the worst quarter of phishing that the Anti-Phishing Group has ever documented, with a total of over 1.2 million phishing attacks worldwide [8].

Despite the numerous online security awareness initiatives to raise security awareness and improve online security behaviour, users continue to respond to malicious cyberattacks. A number of studies have investigated how individual differences affect online security behaviours. Psychological and demographic factors have been investigated to improve the methods used to understand users' motivations to engage in risky behaviours. However, little research has investigated online security attitudes and behaviour beyond North American and Europe, or investigated cultural differences in this area. This paper builds on research we recently conducted in the UK investigating the experiences of online security attacks of young adults and their worries about online security [2], but in this paper we present similar research conducted with young adults in KSA, and compare the results with our results from the UK. In both the previous UK study and this study in KSA, we chose to concentrate on young adults for several reasons. Some research has found age differences in attitudes and behaviours in relation to online security issues. This is not surprising, as young adults now aged 18 to 30 were born in the 1990s and early 2000s (they are sometimes known as "digital natives" [28, 29] or Generations Y and Z [11, 30]), so are very likely to have grown up with digital technologies as an integral part of life, unlike older cohorts of adults who would only have come to these technologies as adults. These life experiences will have affected attitudes of and experiences in the online world. By concentrating on a particular age group, we can develop a clearer understanding of attitudes, experiences and needs of this particular age group. Some previous research has found that young adults undertake particularly risky behaviours online, so it is important to understand why this is happening in order to develop appropriate educational and protection mechanisms for this cohort of individuals. If we can support people when they are young, this should equip them with strategies to deal with online security threats more effectively as they go through life.

2 Related Work

A number of studies have investigated the human aspects of online security, and how crucial it is to consider both technical and human approaches when developing security measures. However, despite the numerous awareness initiatives and programs, there is still a lack of understanding of online security issues. For example, Wu et al. [34] found that 61% of the security terms used in security texts were difficult for a large sample of native English speaking young adults to understand. Researchers have been investigating different kinds of users' attitudes, knowledge and behaviour in relation to these issues since for several decades [16,17] but the situation does not seem to improve. For example, two recent studies [10,11] found that young Americans in particular are still often taking risky online behaviours and have rather lax attitudes to online security issues. However, not all research has found that age is a significant factor in relation to online security, for example a study with over 1200 participants in KSA found no effect of age, although the sample was not age balanced (53% of participants were aged between 18 and 29, and only 5% were over 50) [7]. However, this does raise the interesting possibility of cultural differences in this area.

Some researchers have investigated other individual differences which may account for attitudes and behaviour around online security. For example, several studies have investigated the effects of personality traits. Alseadoon et al. [6] found that individuals in the KSA who are high on the *openness* and *extraversion* personality traits are more like to respond to phishing emails than those low on these traits. In contrast, Alohali et al. [4], investigating what appears to have been a multinational sample which included KSA and the UK, found that four of the five "Big Five" personality traits had significant relationships with online security risk behaviours (*conscientiousness*, *agreeableness*, *openness* and *neuroticism*), but *extraversion* was the only trait which was not a predictor of risky behaviour. Whitty et al. [32] investigated a number of other individual characteristics in a UK sample and found that perseverance and self-monitoring were associated with risky online behaviour. Other studies have emphasized the importance of individual factors such as educational level [14] and general internet skills [5] in predicting online security attitudes and behaviour.

Much of the research on human aspects of online security have been conducted in the developed world, particularly in English speaking countries [16, 17, 19, 25, 26], although studies were found in Finland [13] and Greece [15]. However, increasingly there are studies in other parts of the world, including Bangladesh [1], Malaysia [14], and South Africa [24]. Several studies do discuss cultural differences [20,24], but these are in relation to differences within one country, for example differences between users in rural versus urban areas [24] and differences between employees in public versus private organizations [22]. No studies could be found on how differing national or regional cultures and values may affect online security attitudes and behaviour and how this might influence future awareness raising campaigns in different parts of the world.

As noted above, there have been a number of studies on these issues in KSA, which have been focused on online security awareness rather than behaviours [5,7]. The research by Alseadoon et al. [6] on susceptibility to phishing was conducted with Saudi students. Another Saudi study also investigated phishing susceptibility [3].

This paper focuses on investigating the online security experiences of young adult users in KSA, using the method we developed for the UK study [2] which involved presenting participants with a series of short scenarios illustrating the most common online security attacks, asking them whether they had encouraged a scenario like that and if so a series of follow up questions. In addition, participants rated their level of worry about a series of nine common online security issues. This allowed us to assess current levels of experience with online security attacks among young Saudi people, their concerns about such attacks and their level of worry, as well as to compare the results with our recent study in the UK.

3 Method

3.1 Participants

This study sampled young adult users in KSA. The inclusion criteria were to be aged between 18 – 30 years old, to be a Saudi citizen, currently living in KSA. Participants were recruited by sending emails and messages through social media with a link to an online survey. Participants were encouraged to participate by offering them a chance to enter a prize draw for one of 10 gift vouchers worth 50 Saudi Riyals (approximately GBP 10.00) each.

73 completed responses were received, but 28 failed two or more of the four attention check questions (see section 3.2), leaving 45 valid responses for analysis._Table 1 summarizes the demographic details of the participants. Due to an oversight, participants were not asked about their gender[2].

Table 1. Participant demographics

Age	
Range (Mean)	18 – 30 Years (27.4 years)
Highest educational level	
High school	7 (16.0%)
Bachelors degree	28 (62.2%)
Postgraduate degree	10 (22.2%)
Self-reported computer expertise	
Median (Semi Interquartile range)	5.0 (1.5)
Z score (probability)	3.52 ($p < 0 .001$)
Self-report computer security knowledge	
Median (Semi Interquartile range)	4.0 (1.0)
Z score (probability)	0.14 ($p = 0.89$)
Self-reported ability to identify online attacks	
Median (Semi Interquartile range)	5.0 (1.5)
Z score (probability)	1.52 ($p = .129$)

Participants were asked to rate their general computer expertise, online security knowledge, and confidence in their ability to recognize online attacks, on scales of "not at all knowledgeable/confident" (coded as 1) to "very knowledgeable/confident" (coded as 7). Participants rated their computer expertise significantly above the midpoint of the rating scale. But in their security knowledge and their ability to identify

[2] This was also the case in our UK study. However in that case, as participants were recruited through the Prolific research participant website, we were able to recover participants' gender. However gender was not analysed in [2]. As Prolific was not used in this study, this was not possible.

online attacks, they rated themselves not significantly different from the midpoint of the scale, so average (see Table 1).

3.2 Online Questionnaire

The online questionnaire used in our previous study which was developed in English was translated into Arabic for this study by a native speaker with back translation by a second native speaker to ensure accuracy. It was deployed using the survey software Qualtrics. The questionnaire consisted of four parts:

The first part presented the same 12 short scenarios representing a range of online security threats (see Table 2) and asked participants whether they had experienced anything like the situation in the scenario. Scenarios expressed in non-technical language. If participants had experienced a similar scenario, a series of follow-up questions explored a recent experience of this kind of scenario.

The second part asked about participants' worries in relation to online security and consisted of nine statements to be rated on 7-point Likert items (scored as 1 = not worried at all to 7 = very worried) (see Table 3).

The third part comprised two previously developed questionnaires about online security awareness and behaviour [9, 12] (this data is not presented in this paper), through which were interspersed four attention check questions.

The fourth part asked demographic questions and the ratings of general computer expertise, online security knowledge, and confidence in participants' ability to recognize online attacks.

4 Results

Table 2. Results on the 12 online security scenarios

Scenario	Participants N (%)	Median Frequency (SIQR)
S10: Threat type: Spear phishing I receive a message or call from what seems to be a trustworthy source (e.g. via email, social media, SMS or phone call) asking me for personal information (e.g. account details, password) for a legitimate reason (e.g. updating data). At some point I realise this is a fake message or call.	25 (55.6%)	5.0 (1.75)
S8: Threat type: Phishing, Malware I click on a link (e.g. on a website, in social media, in an SMS) and then notice strange things happening on my device (e.g. pop-ups appearing frequently, unrecognized apps being installed). I realise this may have been cause by clicking on the link.	21 (46.7%)	5.0 (2.0)
S7: Threat type: Adware I download some anti-virus/malware software to try to protect my device. But it does not seem to be effective and it keeps showing me advertisements on the device.	21 (46.7%)	4.0 (1.75)

S11: Threat type: Identity theft, Spear phishing I receive a message or call which seems to be from someone I know (e.g. via email, social media, SMS) asking me to give them urgent assistance (e.g. transfer money). At some point I realise this is a fake message.	19 (42.2%)	6.0 (2.0)
S2: Threat type: Phishing, Denial of service I download an attachment (e.g. from an email or website) and then notice my device acting strangely (e.g. device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by downloading the attachment.	17 (37.8%)	5.0 (1.5)
S3: Threat type: Malicious code, Denial of service, Trojan horse I download a free app or game from an unknown or possibly untrustworthy source. Then I notice my device is running slowly or crashing more frequently than normal.	15 (33.3%)	5.0 (2.0)
S1: Threat type: Phishing, Denial of service I click on a link (e.g. on a website, in social media, in a SMS) and then notice my device acting strangely (e.g. the device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by clicking on the link.	14 (31%)	4.0 (2.1)
S5: Threat type: Identity theft I realise that someone has made a purchase using my credit card or bank account details. I remember that I have recently entered these details online and they may have been stolen.	11 (24.4%)	2.0 (1.5)
S12: Threat type: Spoofed website I need to undertake an urgent task on the government website (e.g. renewing my passport or driving licence). I search quickly for the website in Google. The website asks for personal information (e.g. my name, date of birth or credit card details). After entering my personal information and making a payment, I realise it was not the actual government website, but a fraudulent one with a very similar address and information.	9 (20%)	4.0 (2.25)
S6: Threat type: Identity theft I realise that someone has used my personal information or something I have stored online (e.g. your name, a photo). I remember that I have stored that online and they may have been stolen.	7 (15.6%)	5.0 (2.00)
S9: Threat type: Identity theft My friends report receiving strange messages from me (e.g. requesting money because I'm in trouble, including suspicious links). I realise someone must have illegally used one of my accounts.	5 (11.1%)	5.0 (2.00)
S4: Threat type: Phishing, ransomware I install some software or a file on my device from a link or attachment I received in an email, then notice the device acting strangely. I can't access some or all of my files and then I am asked to pay a ransom to be able to retrieve these files. I realise this may have been caused by installing that software/file.	5 (11.1%)	3.0 (1.00)

Table 2 summarizes the analysis of the 12 scenarios that investigated whether participants had experienced any of these online security threats, and if so, how frequently they had experienced them. The results indicate a substantial variation across scenarios in terms of the percentage of the participants reported having encountered them. For instance, over half of the participants (55.6%, 25) reported having encountered a spear phishing attack aiming to convince them to reveal their personal information (S10), while only 5 participants (11.1%) reported encountering ransomware (S4). It is noteworthy that the three scenarios with the highest incidence as reported by participants are spear phishing, phishing, and adware. To obtain an overall measure of experience, the total number of scenarios that participants reported having experience with was calculated. This could theoretically range from 0 to 12 of the scenarios, in fact ranged from 0 to 10, with a median of 4.0 scenarios (semi interquartile range: 1.5).

The analysis of the nine worries statements investigated the extent to which the participants were worried about different security attacks. Table 3 presents the median (and semi-interquartile ranges) for participants' ratings of the nine statements about worries. The participants' level of worry ranged from slightly below the midpoint of the 7-point scale (with a median of 3.0 for two statements 8 and 9) to relatively high (median of 5.0 for statements 6 and 7).

A principal components analysis (PCA) was conducted on the ratings to investigate whether they formed meaningful groups for the participants[3]. The PCA revealed two components that accounted for 73.7% of the variance. The first component was named the Theft Worry component and it accounted for 60.6% of the variance. it included statements 1, 3 - 7 which are related to data and identity theft (with the exception of statement 3 which is about phishing). The second component was named the Phishing Worry component, accounted for 13.3% of the variance and included statements 2, 8 and 9 which are about phishing and spear phishing.

The median scores on the Theft Worry and Phishing Worry components were calculated for each participant to investigate the relationship between the two worry components and participants' total experience with online attacks. However, there was no significant relationship between total number of scenarios experienced and either Theft Worry or Phishing Worry (Theft Worry: rho = 0.18, p = 0.24; Phishing Worry: rho = 0.02, p = 0.88).

In addition, the relationship between these two components and the self-reported computer expertise, online security knowledge and ability to identify security attacks was investigated. There were no significant correlations between Theft Worry and these ratings (Computer Expertise: rho = -0.15, p = 0.34; Online Security Knowledge: rho = -0.17, p = 0.25; Identifying Attacks: rho = -0.19, p = 0.20). However, there were significant relationships with Phishing Worry, which had a significant, if small, negative correlations with Computer Expertise (rho = -0.33, p = 0.025) and with Online Security Knowledge (rho = -0.29, p = 0.05) but no relationship with ability to identify security attacks.

[3] As there were nine statements, 45 participants constituted a sufficient sample for a PCA.

Table 3. Median ratings (with semi-interquartile ranges, SIQRs) on the nine online security worry statements

Statement	Attack type	Median (SIQR)
W1: My device will be accessed by an attacker and my data will be destroyed	Data theft	4.0 (2.50)
W2: I will receive an email with a link leading to a fake website	Phishing	4.0 (2.00)
W3: I will receive an email with an attachment that may include malicious code	Phishing	4.0 (2.00)
W4: Someone will lock me out of my device(s) and demand money to restore access	Ransomware	4.0 (3.00)
W5: Someone will access my device(s) or account(s), look at my information and use it to blackmail me	Ransomware	4.0 (2.75)
W6: Someone will steal my online identity and misuse it	Identity theft	5.0 (3.00)
W7: Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases)	Identity theft	5.0 (2.25)
W8: I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details)	Spear phishing	3.0 (1.75)
W9: I will click on a link in a SMS message or email from a source that I cannot verify its origin, whether it is trustworthy	Phishing	4.0 (2.25)

5 Discussion and Conclusions

This paper studied the frequency of experiencing a range of online attacks by a sample of Saudi young adult users and related the frequency of such experiences to their level of worry about online attacks. This allowed us to assess current levels of experience with online security attacks among young Saudi people and their concerns about such attacks and to compare the results with a similar recent study in the UK.

The results indicated that the participants generally rated themselves as having high levels of computer knowledge but only moderate levels of security expertise and ability to identify online attacks. This suggests that although participants have good general computer skills, they are not as informed about online security issues as they need to be. This result confirms the results of previous studies conducted with Saudi participants [5, 7], although both those studies were conducted with a wide age range of participants (18 to 50 and more years), not only those 30 years and younger, as in this study.

In comparison with the UK sample in our previous study, although we tried to recruit very similar samples in the two countries, there are some differences (see Table 4). The

UK sample was larger, with a younger mean age, whereas the Saudi sample was somewhat better educated (with a higher percentage of participants with a degree or higher degree). This may be partly due to the difference in the age distribution between the two samples. However, we did consider this to be an important difference, as a number of studies have shown educational level to be an important factor in this area. Both samples rated their computer expertise as above average, but the UK sample rated the computer security expertise and their ability to identify online attacks as above average, whereas the Saudi sample rated these as only average. These differences in ratings may also be related to cultural differences in rating one's own skills [20].

Table 4. Participant demographics for the current study and the previous UK study

	Saudi Sample	UK Sample
Number	45	84
Age (both 18 – 30) Mean	27.4	24.0
Highest Educational Level		
High school	16.0%	34.6%
Bachelors degree	62.2	42.0
Postgraduate degree	22.2	18.5
Other		4.9
Self-reported computer expertise		
Median (SIQR)	5.0 (1.5)	5.0 (0.5)
Z score (probability)	3.52 (p < 0.001)	6.25 (p < 0.001)
Self-report computer security knowledge		
Median (Semi Interquartile range)	4.0 (1.0)	5.0 (1.0)
Z score (probability)	0.14 (p = 0.89)	4.90 (p < 0 .001
Self-reported ability to identify online attacks		
Median (Semi Interquartile range)	5.0 (1.5)	5.0 (1.0)
Z score (probability)	1.52 (p = .129)	1.52 (p < 0.001)

Table 5. Results on the 12 online security scenarios for the current study and the previous UK study

Scenario	**Saudi sample % (rank)**	**UK sample % (rank)**
S10: Threat type: Spear phishing	55.6 (1)	55.6% (1)
S8: Threat type: Phishing, Malware	46.7 (2.5)	29.6 (4)
S7: Threat type: Adware	46.7 (2.5)	24.7 (6)
S11: Threat type: Identity theft, Spear phishing	42.2 (4)	38.3 (2)
S2: Threat type: Phishing, Denial of service	37.8 (5)	23.4 (7)
S3: Threat type: Malicious code, Denial of service, Trojan horse	33.3 (6)	21.0 (8)
S1: Threat type: Phishing, Denial of service	31.0 (7)	34.5 (3)
S5: Threat type: Identity theft	24.4 (8)	17.3 (9)
S12: Threat type: Spoofed website	20.0 (9)	2.5 (12)
S6: Threat type: Identity theft	15.6 (10)	13.6 (10)
S9: Threat type: Identity theft	11.1 (11.5)	27.2 (5)
S4: Threat type: Phishing, Ransomware	11.1 (11.5)	3.7 (11)

The results of this study showed that participants are most likely to encounter phishing and spear phishing attacks and least likely to encounter ransomware attacks. The results on frequency of encounters are very similar to those found by in our previous study sample in the UK (see Table 5). Of the four most frequently encountered scenarios for the Saudi sample (S10: Spear phishing; S8: Phishing, Malware; S7: Adware; S11: Identity theft, Spear phishing), three scenarios were also in the top four for the UK study (only S7 did not appear in the top four for the UK sample, being the sixth most frequently encountered scenario). In addition, for the four least frequently encountered scenarios, three were also shared with the UK study, only S9 was not in the bottom four for the UK study where it was the fifth most frequently encountered attack. Perhaps this reflects the international nature of online security attacks.

Participants' ratings of their worries about nine aspects of online security, grouped very clearly into two components, Theft Worry and Phishing Worry. Even though participants reported experiencing phishing and spear phishing attacks more frequently than data or identity theft, they were more worried about their data and identity being theft than being exposed to phishing attacks. This may indicate that participants may not fully understand the consequences of the phishing attacks, or it is possible that they expect the consequences of the data or identity theft to be more severe or longer lasting than those of phishing attacks. Previous studies found that the severity of risk is a strong predictor of risk perception [19,31]. Interestingly, there were not significant relationships between Theft Worry and participants' ratings of their computer expertise, online security knowledge and ability to identify security attacks, but there were significant relationships between Phishing Worry and participants' ratings of their computer expertise and online security knowledge, but not ability to identify security attacks. Participants' who rated their expertise and knowledge higher were less worried about phishing attacks. Further research on these results with a larger sample of Saudi young adults is needed to investigate how robust these relationships are and what they signify.

Overall, these results were strikingly similar to those found with our UK study. The same two components of worries were found, with only one statement grouping in a different way between the two studies: W3 (I am worried I will receive an email with an attachment that may include malicious code) grouped with the Theft Worry for this study but with the Phishing Worry for the UK study. Even the percentage of the variance in the ratings explained by each component were remarkably similar (Theft Worry: 60.6% for this study, 58.6% for the UK study; Phishing Worry: 13.3% for this study, 13.1% for the UK study). Again, this may reflect the international nature of online security attacks, and that individuals' worries are related to their actual experiences and what they learn and read about online security.

In spite of the similarity in the results on both the scenario exercise and the worry ratings in samples of young people in two very different countries, we would still argue that education and awareness raising should build on the culture and values of each country. Although the attacks and worries may be international in nature, the solutions may still involve some specific cultural bases, and this needs to be investigated further.

However, overall the results of this study highlight the importance of educating young adults in KSA about potential online security risks and attacks and ensuring clarifying the associated consequences of different types of attacks to help reduce the likelihood of successful attacks and increase overall awareness.

6 References

1. Ahmed, N., Kulsum, U., Bin Azad, I., Momtaz, A. S. Z., Haque, M. E., Rahman M. S.: Cybersecurity awareness survey: An analysis from Bangladesh perspective. In: IEEE Region 10 Humanitarian Technology Conference (R10-HTC), pp. 788-791, IEEE (2017).
2. Aldaraani, N., Petrie, H. and Shahandashti, S.: Online security attack experience and worries of young adults in the United Kingdom. In: Clarke, N., Furnell, S. (eds) Human Aspects of Information Security and Assurance. HAISA 2022. IFIP Advances in Information and Communication Technology, vol 658. Springer, Cham (2022).
3. Aljeaid, D., Alzhrani, A., Alrougi, M., Almalki, O.: Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. Information, 11(12), 547 (2020)Alohali, M., Clarke, N., Li, F., Furnell, S.: Identifying and predicting the factors affecting end-users' risk-taking behavior. Information and Computer Security, 26(3), 306 – 326, (2018).
4. Alohali, M., Clarke, N., Li, F., Furnell, S.: Identifying and predicting the factors affecting end-users' risk-taking behavior. Information and Computer Security, 26(3), 306 – 326, (2018).
5. Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M.: A survey of cyber-security awareness in Saudi Arabia. In International Conference for Internet Technology and Secured Transactions, pp. 154-158, IEEE, Barcelona (2016)
6. Alseadoon, I., Chan, T., Foo, E., Nieto, J.: Who is more susceptible to phishing emails? a Saudi Arabian study. *Proceedings of the 23rd Australasian Conference on Information Systems 2012*, AIS Electronic Library (AISeL) (2012).
7. Alzubaidi, A.: Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, *7*(1), e06016 (2021).
8. Anti-Phishing Working Group. Phishing Activity Trends Report, 3rd Quarter 2022, last accessed 2023/04/29
9. Bitton, R., Boymgold, K., Puzis, R., Shabtai, A.: Evaluating the Information Security Awareness of Smartphone Users. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-13. ACM, New York (2020).
10. Cain, A. A., Edwards, M. R., Still, J. D.: An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36–45 (2018).
11. Debb, S. M., Schaffer, D. R., Colson, D. G.: A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults. International Journal of Cybersecurity Intelligence and Cybercrime 3(1), 42–55 (2020)
12. Egelman, S., Peer, E.: Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). In Proceedings of the 33rd annual ACM conference on human factors in computing systems pp. 2873-2882. ACM, New York (2015)
13. Farooq, A., Isoaho, J., Virtanen, S., Isoaho, J.: Information security awareness in educational institution: An analysis of students' individual factors. In: 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp 352 – 359, IEEE, Helsinki (2015).

14. Fatokun, F. B., Hamid, S., Norman, A. , Fatokun, J.: The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian Universities. *Journal of Physics*, *1339*(1), 012098 (2019)
15. Filippidis, A.P., Hilas, C. S., Filippidis, G., Politis, A.: Information security awareness of greek higher education students — Preliminary findings. In: 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)2018, pp. 1-4, IEEE, Thessaloniki, (2018).
16. Furnell, S., Bryant, P., Phippen, A.D.: Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410 – 417 (2007).
17. Furnell, S., Jusoh, A., Katsabas, D.: The challenges of understanding and using security: a survey of end-users. Computers & Security, 25(1), 27 – 35 (2006).
18. Garg, V., Camp, J.: End User Perception of Online Risk under Uncertainty. In 45th Hawaii International Conference on System Sciences 2012, pp. 3278-3287, IEEE, Maui (2012).
19. Halevi, T., Lewis, J. D., Memon, N.: A pilot study of cyber security and privacy related behavior and personality traits. In 22nd International Conference *on World Wide Web* 2013, pp.737-744, ACM, Rio de Janeiro (2013)
20. He, J., van de Vijver, F.J.R., Fetvadjiev, V.H. et al.: On enhancing the cross-cultural comparability of Likert-scale personality and value measures: a comparison of common procedures. European Journal of Personality, 31, 642 – 657 (2017).
21. IBM: Cost of a Data Breach 2022 Report, https://www.ibm.com/reports/data-breach, last accessed 2023/04/29
22. Innab, B., AlRasboud, A., AlMahawes, R., AlShebhri, W. Evaluation of the effective anti-phishing awareness and training in governmental and private organizations in Riyadh. In 21st Saudi Computer Society National Computer Conference (NCC)2018, pp 1 – 5, IEEE, Riyadh (2018).
23. Kaspersky: Kaspersky Lab Helps Mitigate Security Risk at the Cyber Defense Summit 2019, https://me-en.kaspersky.com/about/press-releases/2019_cyber-defense-summit, last accessed 2023/04/29
24. Kruger, H.A., Drevin, L., Flowerday, S., Steyn, T.: An assessment of the role of cultural factors in information security awareness. In: 2011 Information Security for South Africa, pp. 1-7, IEEE, Johannesburg (2011).
25. McGill, T., Thompson, N.: Old risks, new challenges: exploring differences in security between home computer and mobile device use. Behaviour & Information Technology, 36(11), 1111–1124 (2017).
26. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165 – 176 (2014).
27. Pew Research Center, *Internet use by age,* https://www.pewresearch.org/internet/chart/internet-use-by-age/, last accessed 2023/05/31
28. Prensky, M.: Digital Natives, Digital Immigrants Part 1. On the Horizon, 9(5), 1–6 (2001a)
29. Prensky, M.: Digital Natives, Digital Immigrants Part 2: Do They Really Think Differently? On the Horizon, 9(6), 1–6 (2001b).
30. Turner, A.: Generation Z: technology and social interest. Journal of Individual Psychology, 71(2), 103 – 113 (2015).
31. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P.: Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75, 547–559 (2017)

32. Whitty, M., Doodson, J., Creese, S., Hodges, D.: Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior, and Social Networks, 18(1), 3 – 7 (2015)
33. Wikipedia. Middle East. https://en.wikipedia.org/wiki/Middle_East, last accessed 2023/04/29
34. Wu, T., Zhang, R., Ma, W., Wen, S., Xia, X., Paris, C., Nepal, S, Xiang, Y.: What risk? I don’t understand. An empirical study on users’ understanding of the terms used in security texts. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS ‘20), pp 248 -262. ACM, New York (2020).