Proceedings Paper:
Aldaraani, Najla, Petrie, Helen orcid.org/0000-0002-0100-9846 and Shahandashti, Siamak F. orcid.org/0000-0002-5284-6847 (2025) A Diary Study to Understand Young Saudi Adult Users' Experiences of Online Security Threats. In: Clarke, Nathan and Furnell, Steven, (eds.) IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2024). 18th IFIP WG 11.12 International Symposium on Human Aspects of Information Security and Assurance, HAISA 2024, 09-11 Jul 2024 IFIP Advances in Information and Communication Technology . Springer Science and Business Media Deutschland GmbH , SWE , pp. 47-60.

https://doi.org/10.1007/978-3-031-72559-3_4

A Diary Study to Understand Young Saudi Adult Users' Experiences of Online Security Threats

Najla Aldaraani[1,2] [0000-0002-9126-1630], Helen Petrie[1] [0000-0002-0100-9846] and Siamak F. Shahandashti[1] [0000-0002-5284-6847]

[1] University of York, York YO10 5GH, UK
[2] King Khalid University, Abha (61421), Saudi Arabia
{nga505|helen.petrie|siamak.shahandashti}@york.ac.uk

Abstract. An online diary study was conducted to investigate the experience of online security threats among Saudi young adults. Over a period of 30 days, 16 participants were asked to record up to three threats they received from online sources on any of their devices. 58 threats were received, and 98 cues were reported in detecting the threats. The Phish Scale proved useful to categorise the detection cues, but needed expansion, largely due to the proliferation of threat types, which can come through many online channels including SMS, WhatsApp and online voice channels. The majority of threats were phishing, with general email phishing and target email phishing (spear phishing) beling the most common types. The cues most commonly used to detect threats were those related to language and content of the threat, technical indicators such as the lack of a sender name or email or a suspicious or hidden link to follow, and tactics such as posing as a business or making an offer "too good to be true".

Keywords: Online Security Threats, Online Security Threat Types, Cues to Detect Online Security Threats, Young Adults, Kingdom of Saudi Arabia.

1 Introduction

Phishing continues to be a major online security problem. In the USA, the FBI [1] has recorded a 260% increase in phishing attacks between 2019 and 2023 and noted that phishing is the most common form of cyberattack. In the UK, the Office for National Statistics has recently found that in phishing attacks on individuals, young adults (25 to 44 years of age) are most likely to be targeted [2]. Attackers can now leverage advances in artificial intelligence in a new era of sophisticated online security attacks. Attackers also use the vast amounts of information available from many sources, including social media and breach databases to personalize their attacks. They can tailor phishing attacks to target individual users with spear phishing and they can also use different online channels like SMS, voice calls, and social media (smishing, vishing, and angler phishing respectively), in attempts to increase their success rate, which also leads to people receiving ever more threats

People are often the first line of defence against online attacks, and their experiences, behaviours, and attitudes significantly impact systems security. Despite increased awareness of online threats, many people are exposed to attacks either due to a lack of

knowledge, or best practices. Thus, knowing people's perceptions, experiences and behaviours are important to improving online security.

A range of research approaches are needed to understand people's experiences of online security attacks. Methods in which participants retrospectively report about their experiences such as surveys, interviews and focus groups provide useful information about their experiences, but are limited due to the fact that people are trying to remember the particulars of experiences and how they reacted to them. In addition, in these situations, participants may be susceptible to socially desirable responses [3]: they may say what they think they should do, rather than what they actually do. Researchers also use experimental methods, for example sending simulated phishing emails or websites to participants and measuring their reactions. Again, this yields useful information, but usually only about a very small number of factors, and not people's overall reactions. Flores et al [4] found there was little correlation between the results of surveys and experimental methods in online security studies, and argued that different methods provide different types of information and thus a range of methods is needed.

To complement these methods, we employed a diary method, asking participants to note any online threats each day and report on up to three of them in a short online diary entry at the end of each day. We believe that this will capture more detailed information about the nature of the threats and because participants are reporting on specific threats on a daily basis, they will become less susceptible to social desirability bias over time. Our study focused on nature of the threats and the cues used by participants to detect and respond to them. We targeted young adults in the Kingdom of Saudi Arabia (KSA), as there is relatively little information about people's experience with online security threats in the Arab world compared to North America and Europe and because of the evidence (albeit from the UK) that young adults are most frequently targeted in individual phishing attacks. We are already planning a future study to compare the results with a sample of young adults in the UK.

2 Background

There is now a considerable body of research on user aspects of phishing, investigating what kinds of users are more susceptible in what kinds of situations, what kinds of phishing attacks is more successful and the characteristics of those successful phishing attacks. It is beyond the scope of this paper to provide a comprehensible review of this research, Sommestad & Karlzén [5] provide a recent review of 48 relevant studies. Here we will concentrate on two aspects of the research, studies conducted with Arab samples, our target group and studies which have investigated age differences in phishing experience and susceptibility, as we have chosen to concentrate on younger participants.

There is now a small but growing body of research on user aspects of online security in the Arab world. Algarni et al. [6] conducted an online survey with 377 employees from three organizations in Saudi Arabia to examine their vulnerability to social engineering attacks through social networks, specifically Facebook. The results indicated that participants with higher levels of security knowledge showed lower susceptibility to social engineering. Gender also played a role, with women being more susceptible

than men. Additionally, the time since joining Facebook was a predictor of susceptibility, with shorter times since joining being associated with higher susceptibility. Innab et al. [7] in another online survey investigated the phishing awareness and training of 116 non-IT employees in governmental and private organizations in Saudi Arabia and found that the awareness and anti-phishing training were at a very low level. Alzubaidi [8] conducted a wider survey of 1230 members of the adult population of Saudi Arabia (although it is not clear how representative it is of the whole population) and found that 53.4% of respondents reported receiving phishing emails at least "sometimes". Respondents also had considerable concerns about phishing and identity theft. We also conducted a small survey with 45 young Saudi participants which found that over half reported having received phishing and particularly spear phishing attacks [9].

Aleroud et al. [10] conducted a laboratory study with university students in Jordan using three simulated phishing websites. They found that these participants were vulnerable to targeted attacks, such as spear phishing, especially when a social context and faked trust signals were integrated in the spoofed website. These results are interesting given in spite the study was conducted in a university laboratory which may affected participants' perception of trust (this may have made them more trusting) and the participants were Information Systems majors (which should mean they are reasonably knowledgeable about online security).

Aljeaid et al. [11] also used simulated phishing websites and emails with staff and students at a Saudi university. A simulated university website was developed and the researchers found that 77% of participants, mostly students, fell victim to the associated phishing attack. In a second simulation, a spear-phishing email was sent to 165 students, 27% of whom clicked on the link included in it. The last simulation was a social network phishing attack, involving a message with a fake URL, in an attempt to obtain sensitive information, allegedly for entry into a prize draw. The message was distributed over WhatsApp, Telegram, and Facebook platforms. Among the 342 recipients, 47% were successfully phished, the majority were students.

In relation to age differences in experience of and susceptibility to phishing, a number of studies have found that younger people are more susceptible, in spite of great experience with online systems. Kumaraguru et al [12] in an early study, evaluating their PhishGuru anti-phishing training program, found this effect, as did Sheng et al [13] in an online roleplaying survey. More recently, Lin et al. [14] conducted a field study in which 100 young participants (mean age 21.7 years) and 58 older participants (mean age 61.7 years) were sent simulated phishing emails over a 21-day period and found that the older participants, particularly older women, were more susceptible to the phishing emails. On the other hand, in the same year, Sarno et al. [15] in a series of small controlled laboratory studies of phishing detections found that younger participants (mean ages 18.5 – 19.6 in three studies) and older participants (mean ages 71.1 – 74.1) do not differ in their ability to accurately classify emails, but older participants were slower in making decisions and when given unlimited time tended to be biased toward classifying an email as phish. These studies show, as Flores et al. [4] discussed, that different methods often produce differing results.

3 Method

3.1 Design

An online diary study was conducted to collect details information about the online security threats received by young Saudi adults. As discussed above, the rationale for using the diary method is that it allows collections of detailed and contextually specific data over a period of time [16, 17] and because the participants are responding repeatedly and specifically, socially desirable answers will decrease.

The study involved asking participants to note the online threats they encountered during the day and complete a short diary entry about up to three threats at the end of each day. If they encountered no threats on a particular day, they would simply report that. For those who reported receiving a threat, they were asked to upload screenshot(s) of it if they could and explain briefly what happened and how they decided whether it was a threat or not. The screenshots provided very useful additional information to the description to understand the nature of the threat, the participant's response and their decision. Participants were asked to report only up to three threats per day, not to put too much burden on them. The diary questions are summarized in Table 1.

Participants were asked to complete the diary for 30 days. Although it was very hard to predict how much data this period would produce, it was chosen in the hope that it would a sufficient amount of data for analysis.

The study received ethical approval from the Physical Sciences Ethics Committee at the University of York.

3.2 Participants

Inclusion criteria were to be a Saudi Arabian citizen and currently living in Saudi Arabia, a regular Internet user, and aged between 18 and 40 years old. Participants were recruited using snowball sampling, which involved inviting people from the first author's social network to participate and encouraging them to share the study invitation with their networks. In addition, announcements about the study were made on social media platforms to reach those who may not have been directly known to the first author's network. Potential respondents were informed about the study's aim, requirements, and duration.

16 participants were recruited. Table 2 summarizes their demographics. An online gift voucher worth 200 Saudi Riyals (approximately GBP 42 or USD 53) was offered for participation in the study.

Participants were asked to rate their general computer knowledge, and their online security knowledge on 7-point Likert items (ranging from 1 = not at all knowledgeable to 7 = very knowledgeable). Participants rated themselves with a median of 6.5 (range: 3 – 7) on their computer knowledge, which is significantly above the midpoint of the scale (One-Sample Wilcoxon Signed Rank Test, $T = -2.55$, $p = 0.011$). Participants rated their online security knowledge lower, with a median score of 5.0 (range 3 – 7), also significantly above the midpoint ($T = -2.96$, $p = 0.003$). They rated their general computer knowledge significantly higher than their online security knowledge (Related-

Samples Wilcoxon Signed Rank Test, T = -2.59, p = 0.01). Thus, participants considered themselves knowledgeable about both computers and online security, but less so about online security.

Participants were also asked if they had attended any online security courses or training, 14 (87.5%) of the participants reported having taken such courses or training. It indicates that the majority of participants were actively looking for information or training on online security.

Table 1. Main diary questions.

Have you received any possible online threats today?	Yes/No
If yes	
For the first/second/third possible threat, please upload the screenshot of the threat if you were able to take one.	
Please briefly explain what happened (open-ended)	
Did you respond to this threat?	Yes/No
How did you decide whether it was a security threat or not? (open-ended)	

Table 2. Demographics of the participants.

Gender	
Men	4 (25.0%)
Women	12 (75.0%)
Age	
Range	18 - 40 years
Mean	23.6
Educational background	
High school	5 (31.3%)
Bachelors degree	10 (62.5%)
Postgraduate degree	1 (6.3%)
Self-rating of computer knowledge	Median: 6.5, SIQR: 1.0
Self-rating of online security knowledge	Median: 5.0, SIQR:1.5

3.3 Online Questionnaire

The study used an online questionnaire implemented using Qualtrics survey software (Qualtrics.com).

The pre-study questionnaire asked for demographic information: age, gender, and educational background, as well as their computer and online security knowledge.

With the pre-study questionnaire, participants were provided with instructions about the procedure for the study. They were asked to monitor for online threats and to note up to three threats a day. They were reassured that they might not receive threats every day, and that was just as interesting as receiving threats. They were asked to report

anything they suspected might be a threat, and not to worry about whether it was or not. If they decided it was not a threat, they could report that, as it was also interesting. They were also asked to report threats on any device: smartphone, tablet, laptop or desktop. They were asked to take screenshots of the threat, if possible, but to remove any personal information such as their username, phone number, etc. But they were also assured that if they forgot to do this, the researchers would do so for them. They also received a file with some example screenshots of the most common current online security threats. They were asked to keep this file during the study and refer to it when needed.

The main diary questions are summarized in Table 1. It first asked if the participant had received any threats that day. If they answered no, that was the only question for that day. If they answered yes, the main section was presented. Then, they were asked if they wanted to report another threat for the day, in which case the main section could be presented up to twice more.

3.4 Procedure

On recruitment to the study, participants received the pre-study questionnaire which included an informed consent page. Over the next 30 days, participants received daily email reminders with a link to the main diary questionnaire prompting them to report any online threats encountered that day. At the end of each week, participants received a follow up email thanking them for their engagement in the study. Participants were informed that they could seek assistance from the researchers at any time if needed. At the end of the study, participants were sent an email of thanks and arrangements were made to send them the gift voucher.

3.5 Data Analysis

Content analysis was conducted to categorise the information about the online threats reported by participants. The texts and screenshots provided by participants about each threat were studied to extract the threat type, source of threat, purpose of threat, and cues the participant used to recognize the threat. Any cues in the screenshot which the participant had not reported (and therefore potentially not noticed) were also coded.

The categories of cues used in this study were those from the Phish Scale [18]. However, we found that to categorise cues for threats coming from a variety of sources such as phone calls, SMS, and social media, we needed to add a new category and add some sub-categories (see Table 3). One sub-category was added to Technical Indicator: “Unknown Phone/SMS Number”. Two sub-categories were added to Language and Content: Wrong Information, and “Not Applicable Information”. We created a new category “Prior Knowledge Source” to cover people's knowledge about online security threats that they may use in detecting a threat. Sources might be “Family or Friends”, “Social Media”, “Official websites and news streams” or a “Common Scam” (when the participant does not specify what the source of their knowledge is).

Coding was conducted by the first author. A sample of the coding was then reviewed by the second author, problem areas in the coding were discussed and adjustments made as needed. Any problematic cases were assessed by the two authors together. Often the information provided by the participant was ambiguous, which made coding difficult.

Given the small sample size, quantitative data were analysed with non-parametric statistics.

Table 3. New cues created in this study (expanding on the Phish Scale ([17]).

Main Cues/ /Sub cues	Definitions
Technical indicator	
Unknown (phone/SMS) number	Is the number for the phone call or message unknown?
Language and Content	
Wrong information	Does a message or call has something wrong, inaccurate or deceptive. For example: false notifications about parcel deliveries when there is no expected shipment, or request from bank using unusual communication methods, such as personal calls requesting sensitive information.
Not Applicable information	Is the information not relevant or applicable to the participant's circumstances, interests, or context at the time of receipt. For example, receiving a job offer based on a CV when no CV has been submitted.
Prior Knowledge Source	
Friends or family	Does the participant already know something about this threat from their family and friends?
Social media	Does the participant already know something about this threat from social media?
Official websites and news streams	Does the participant already know something about this threat type from official websites (e.g. bank or governmental sites) or news streams.
Common scam	Does the participant already know something about this threat because it is commonly known scam method? (no source of knowledge given)

4 Results

58 threats were reported during the study. This is an average of 0.24 threats per participant per month (taking a month as 4 weeks, 28 days), with a range from 1 – 14 threats reported per month in period ranged from 17 – 35 days of monitoring threats (total number of reported days was 431 days of reporting from the 16 participants). As participants were only asked to report up to three threats per day, this does not represent the frequency of threats they were receiving.

The threats included 98 cues detected by the participants, and a further 25 cues detected by the researcher and not mentioned by the participants, a total of 123 cues, or 2.1

cues per threat. The main purpose of the threat was either data theft (22.0%) or financial fraud (27.1%), while the purpose of 50.8% of the threats could not be specified (see Table 4).

Table 4. Categories of purpose of threats.

Category	Definition	Example	Frequency (N/%)
Data theft	Attempts to obtain victims' personal or sensitive data such as name, date of birth, phone number, email, credit card number, or bank details	An international number with no available information is requesting sensitive information (P12-R3)	13 (22.0%)
Financial fraud	Attempts to engage the victims in financial transactions or make payments	Received an email from a shipping company and they asked to complete the payment (P2-R3)	16 (27.1%)
Cannot be specified	The purpose of the attack cannot be specified from the participant's response and screenshot.	A message containing a link from an unknown source has been received (P4-R3)	30 (50.8%)

The frequencies of the different threat types which participants reported are summarized in Table 5. The most frequently reported threat type was phishing, which accounted for nearly 70% of all reported threats. This category broke down into different types of phishing, with email phishing being the most common with 17.25% of threats. Also common was spear phishing (15.52%) and WhatsApp phishing (12.07%) The other phishing types each had less than 10% of the threats. Only 6.90% of threats included a spoofed website and a considerable number of reported threats (24.1%) could not be determined due to insufficient information.

Table 6 lists the cues which participants used to decide whether something was a threat and also the cues which the researchers identified in the screenshots provided by participants. In total, they reported using 98 different instances of the 30 different specific cue sub-categories, 23 from the Phish Scale and seven which we added (see section 3.5). For completeness, we have included all the sub-categories provided in the Phish Scale in Table 6. For six of the Phish Scale sub-categories, no participant reported using them, although for three of the sub-categories in the Common Tactic category, instances were detected by the researchers.

Table 5. Threat types experienced by participants, with examples and frequencies (N = 58)

Threat: main type/Sub-type	**Definition**	**Examples**	**Frequency: N (%)**
PHISHING			**40 (68.97%)**
Email phishing	Email message from unknown source designed to deceive or manipulate recipients into disclosing sensitive information or taking harmful actions	An advertisement arrived via email for jobs, and it contained a link that led to a strange website requesting personal information (P10-R2) I received an email claiming that they have a profitable business project that requires collaboration (P12-12)	10 (17.24)
Spear phishing	Personalised deceptive email to the user with their real name, often from familiar or trusted source such as bank, shipping company, or store	A scam involving a group impersonating "SPL," a shipping company. The scammers use WhatsApp to send messages claiming that you have a shipment and need to pay the shipping (P1-R1)	9 (15.52)
Smishing	Phishing via SMS text message	I received messages on my number claiming that they found my resume and liked it (P15-R1)	2 (3.45)
Spear smishing	Personalised SMS often from familiar or trusted source (as above)	I received a text message claiming to be from Saudi Post (P5-R3)	5 (8.62)
Vishing	Phishing via online voice channel	Deceptive call claiming to suspend the bank account (P13-R5)	4 (6.90)
WhApp phishing	Phishing via WhatsApp message	An international number contacted me through WhatsApp and informed me that they have a remote job I can do in my spare time (P11-R1)	7 (12.07)
Social Media phishing	Phishing via message on social media sites	Message on Twitter attempted to persuade to click on the link (P13-R2)	3 (5.17)
SPOOFED WEBSITE	A fraudulent website that closely resembles a legitimate one	I was searching for the Ministry of Commerce to report an illegal sale. The website that appeared first on my search results was the one I clicked on, it was a fake website did not have the ministry logo or contact information (P1-R3)	**4 (6.90)**
NOT CLEAR	Threat type could not be identified		**14 (24.14)**

Table 6. Cues used by participants (N = 98) and cues found by the researchers (N=25)

Main Cue Category/Sub-category	Participant (N/%)	Researchers (N%)
ERROR	**2 (2.0%)**	**2 (8.0%)**
Spelling and grammarirregularities	1 (1.0)	2 (7.4)
Inconsistency	1 (1.0)	0
TECHNICAL INDICATOR	**27 (27.6)**	**7 (25.9)**
Attachment type	0	0
Sender display name, email address	9 (9.4)	2 (8.0)
Unknown phone/SMS number	6 (6.3)	0
Hidden/shortened URL hyperlink	9 (9.4)	5 (20.0)
Domain spoofing	3 (3.1)	0
VISUAL PRESENTATION INDICATOR	**4 (4.2)**	**0**
No/minimal branding and logos	1 (1.0)	0
Logo imitation or out-of-datebranding/logos	0	0
Unprofessional-looking design or formatting	2 (2.1)	0
Security indicators and icons	1 (1.0)	0
LANGAUGE AND CONTENT	**36 (36.7)**	**5 (18.5)**
Legal language/copyrightinfo/disclaimers	0	0
Distracting detail	1 (1.0)	0
Requests for sensitiveinformation	12 (12.5)	1 (4.0)
Sense of urgency	2 (2.1)	0
Threatening language	1 (1.0)	0
Generic greeting	3 (3.1)	1 (4.0)
Lack of signer details	4 (4.2)	3 (12.0)
Wrong information	9 (9.4%)	0
Not applicable information	4 (4.2%)	0
COMMON TACTIC	**14 (14.6)**	**11 (40.7)**
Humanitarian appeals	2 (2.1)	2 (8.0)
Too good to be true offers	5 (5.2)	5 (20.0)
You're special	0	1 (4.0)
Limited time offer	0	1 (4.0)
Mimics work or business process	7 (7.3)	1 (4.0)
Poses as friend, colleague, supervisor, authority figure	0	1 (4.0)
PRIOR KNOWLEDGE	**15 (15.3%)**	**0**
Family or friends	4 (4.2%)	0
Social media	2 (2.1%)	0
Official websites and news streams	2 (2.1%)	0
Common scam	7 (7.3%)	0

The most frequently mentioned cues reported by participants related to the Language and Content (36.7%), with Requests for sensitive information (12.5%) and Wrong information (9.4%) being the most common sub-categories. The next most frequently mentioned cue category for participants was Technical indicators (27.6%) with Hidden or shortened URL hyperlinks and Lack of/Suspicious sender name or email add both accounting for 9.4% of cues. The categories of Prior knowledge (15.3%) and Common

Tactic (14.6%) were somewhat less frequently reported by participants. Finally, few cues were reported by participants in the Visual presentation indicator category (4.2%) or Errors (2.0%).

In term of cues that were not reported by participants, but which were identified by the researchers from the screenshots (not all threats were accompanied by a screenshot to enable this to happen), Common tactic was the most frequently identified category (40.7%), followed by Technical indicator (25.9%) and Language and content (18.5%). In particular, 5 instances of the Common Tactic sub-category of Too good to be true offers were not reported by the participants, but were identified by the researchers as well as 5 instances of the Technical Indicator sub-category of Hidden/shortened URL hyperlinks. It is not known whether the participants simply forgot to include these cues in their report or whether they actually failed to notice them.

5 Discussion and Conclusion

This study investigated the experiences of online security threats by a sample of young adults in KSA using a diary method. The participants' educational background, most of whom had Bachelor's degrees, may have influenced their perspective and response to these threats. Alzubaidi [8] certainly found differences in cybersecurity awareness and practices due to educational level amongst Saudi participants. The present study found that participants only reported an average of 0.24 threats in a month, which equates to only approximately three threats per year. This figure appears relatively low, considering the frequency of online security threats in the KSA. Alzubaidi also found that the KSA has seen a considerable increase in such threats. As of 2018, the country recorded over 160,000 online attacks on its systems each day. The rise was accompanied by a 4% increase in malware attacks and an incredible 378% increase in ransomware instances [8]. However, it should be noted that we only required participants to report up to three threats per day, but most participants on most days were not reporting the maximum number of threats, so we assume there were not a lot of threats going unreported. However, it would have been useful to ask participants to report the total number of threats they received that day, but then document up to three in detail.

By far the most frequently reported threat type was phishing, which accounted for nearly 70% of all threats reported. Within this category, email phishing and spear phishing were the most frequently reported types, which agrees with previous research with Saudi participants [6, 8, 9].

To categorise the cues which participants used, we started by using the categories proposed by the Phish Scale [18]. However, it became clear that the categories and subcategories in that Scale, while useful, did not describe all the cues being reported by participants. This is undoubtedly because the range of online security threats has proliferated since the Phish Scale was developed, with threats now being sent by SMS, WhatsApp, and online voice channels. Thus, we expanded the number of sub-categories in the Phish Scale categories, and we added one more major category, Prior Knowledge. We were able to include this category as we had asked participants how they detected the threat, information which is not always available to researchers. It

was also interesting that a number of sub-categories from the Phish Scale were never reported by our participants.

While cues relating to visual presentation [19] and technical indicators [20] have been highlighted in previous research with European participants as important cues for users to detect threats, while the Saudi participants in this study relied most frequently on cues related to language and content, although cues related to visual presentation were the second most frequently reported. These results partly agree with those found by Aleroud et al. [10], who conducted research with an Arab sample (although they were Jordanian, not Saudi) and found that participants trusted the simulated phishing websites because of the logos, but they did not notice the technical indicator of the missing padlock sign. Another study by Algarni et al. [6] which also investigated Arab participants (in this case Saudi participants), found that credibility of the source was an important factor to identify fake accounts on Facebook. This supports the findings from the present study that Saudi participants reported using technical indicators such as unknown phone or SMS numbers, email addresses and sender name to detect a threat.

In conclusion, the findings of this study provide useful insights in the types of online security threats received by a sample of young Saudi participants and the cues they use to detect those threats. Although the frequency of threats reported was not high, they were clearly irritating, time wasting, and in some cases, distressing for participants, and in one instance involved financial loss. Therefore, more needs to be done to support people in all countries in this area. Further research is required to address the wide range of cybersecurity threats and establish a set of approaches to support people in dealing with the increasing number of threats that combines technology improvements, educational activities, and behavioural interventions.

Acknowledgments. We would like to thank the participants who took part in this study. This work is supported by King Khalid University, Kingdom of Saudi Arabia, as part of the first author's PhD research conducted at the University of York in the United Kingdom.

Disclosure of Interests. The authors declare that they have no competing interests.

References

1. Federal Bureau of Investigation (FBI). Internet Crime Report 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2023IC3Report.pdf (2023).
2. Office for National Statistics. Telephone-Operated Crime Survey for England and Wales, 2020-2021. UK Data Service. SN: 9198, DOI: http://doi.org/10.5255/UKDA-SN-9198-1 (2024).
3. Rosnow, R.L., Rosenthal, R. People studying people: artifacts and ethics in behavioral research. Freeman (1997, re-issued 2009).
4. Flores, W.R., Holm, H., Svensson, G., Ericsson, G. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Information Management and Computer Security, 22(4), 393 – 406, (2014).

5. Sommestad, T., Karlzén, H. A meta-analysis of field experiments on phishing susceptibility. APWG Symposium on Electronic Crime Research (eCrime). pp. 1-14, doi: 10.1109/eCrime47957.2019.9037502. (2019).
6. Algarni, A., Xu, Y., Chan, T.: An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. European Journal of Information Systems, *26*(6), 661–687 (2017).
7. Innab, N., Al-Rashoud, H, Al-Mahawes, R., Al-Shehri, 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), IEEE, pp.1–5, (2018).
8. Alzubaidi, A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7, e06016, (2021).
9. Aldaraani, N., Petrie, H., Shahandashti, S. (2023). Online security attack experience and worries of young adults in the Kingdom of Saudi Arabia. In S. Furnell & N. Clarke (Ed.,), Human Aspects of Information Security and Assurance, 17th IFIP WG 11.12 International Symposium (HAISA 2023). Springer.
10. Aleroud, A., Abu-Shanab, E., Al-Aiad, A., Alshboul, Y.: An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. Journal of Information Security and Applications, 55 (2020).
11. 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).
12. Kumaraguru, P. Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., Pham, T. School of Phish: A Real-World Evaluation of Anti-Phishing Training. In the Proceedings on Usable Privacy and Security, (2009).
13. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., Downs, J.: 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 systems pp. 373-382 (2010).
14. Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., Ebner, N. C.: Susceptibility to Spear-Phishing Emails. ACM Transactions on Computer-Human Interaction, *26*(5), 1–28 (2019).
15. Sarno, D. M., Lewis, J. E., Bohil, C. J., Neider, M. B.: Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human Factors*, *62*(5),704–717 (2020).
16. Lazar, J., Feng, J.H., Hochheiser, H. Research methods in human-computer interaction. Wiley (2010).
17. Rosnow, R.L., Rosenthal, R. Beginning behavioral research: a conceptual primer (7th Edition), (2012).
18. Steves, M., Greene, K., Theofanos, M.: Categorizing human phishing difficulty: A Phish Scale. *Journal of Cybersecurity*, *6*(1) (2020).
19. Blythe, M., Petrie, H., Clark, J. A.: F for Fake: Four studies on how we fall for Phish. *CHI* '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 3469–3478 (2011).
20. Furnell, S.: Phishing: can we spot the signs? Computer Fraud & Security, 10–15 (2007). https://doi.org/10.1016/S1361-3723(07)70035-0