IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 19, 2021, accepted March 13, 2021, date of publication March 17, 2021, date of current version March 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3066383

Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process

HOSSEIN ABROSHAN[1], JAN DEVOS[2], GEERT POELS[1], AND ERIC LAERMANS[2], (Member, IEEE)
[1]Faculty of Economics and Business Administration, Ghent University, 9000 Gent, Belgium
[2]Faculty of Engineering and Architecture, Ghent University, 9000 Gent, Belgium

Corresponding author: Hossein Abroshan (hossein.abroshan@ugent.be)

ABSTRACT Prior studies have shown that the behaviours and attitudes of Internet users influence the likelihood of being victimised by phishing attacks. Many scammers design a step-by-step approach to phishing in order to gain the potential victim's trust and convince them to take the desired actions. It is important to understand which behaviours and attitudes can influence following the attacker in each step of a phishing scam. This will enable us to identify the root causes of phishing and to develop specific mitigation plans for each step of the phishing process and to increase prevention points. This study investigates to what extent people's risk-taking and decision-making styles influence the likelihood of phishing victimisation in three specific phishing steps. We asked participants to play a risk-taking game and to answer questions related to two psychological scales to measure their behaviours, and then conducted a simulated phishing campaign to assess their phishability throughout the three phishing steps selected. We find that the attitude to risk-taking and gender can predict users' phishability in the different steps selected. There are however other possible direct and indirect behavioural factors that could be investigated in future studies. The results of this study and the model developed can be used to build a comprehensive framework to prevent the success of phishing attempts, starting from their root causes.

INDEX TERMS Cyber security, phishing, human behaviour, individual differences, online scams.

I. INTRODUCTION

The digital world has increasingly become, for many of us, another 'real' world at the same level as the physical world that we inhabit. People do business on the Internet, share their knowledge and study online, make electronic bank and payments transfers, trade cryptocurrency, and carry out a range of other activities that used to only be possible in the physical world. The digital world is making our lives much easier by increasing the speed of communication, decreasing our travels, etc. But at the same time, this shift is causing a set of new challenges and potential problems. While many Internet attackers use technical methods such as exploiting vulnerabilities inherent in the design of applications and/or network security flaws to gain unauthorised access to the victims' sensitive and critical data, others use psychological tricks to fool people and gain their confidence, similarly to what scammers do in the physical world. Scams have existed since long before computers and the Internet, and they are unlikely to disappear, as scammers adapt and find new ways of fooling us. Phishing, which is a social engineering attack, is like other scams. Phishers use technical, social, and/or people's psychological vulnerabilities to acquire a victims' sensitive information [1] and use that information to steal their financial assets or launch other attacks, such as ICS (Industrial Control System) attacks [2], Smart Airports Attacks [3], etc.

Phishing usually starts with a scam email that is designed to lure a victim. Attackers send out millions of these scam emails every day, but not all of the phishing attempts end up successful [4], [5]. There are several technical solutions to block phishing emails before they are delivered to the users' email inbox. However, these solutions do not detect and prevent all phishing emails [6], [7], so it is the user's job to determine what email in the inbox is phishing and what is legitimate. This study focuses on the user's role in detecting and preventing phishing.

Previous studies [8], [9] showed that a scammer might use human cognitive and behavioural attributes to design their tricks and to fool victims. For instance, a scammer may send a

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inàcio.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

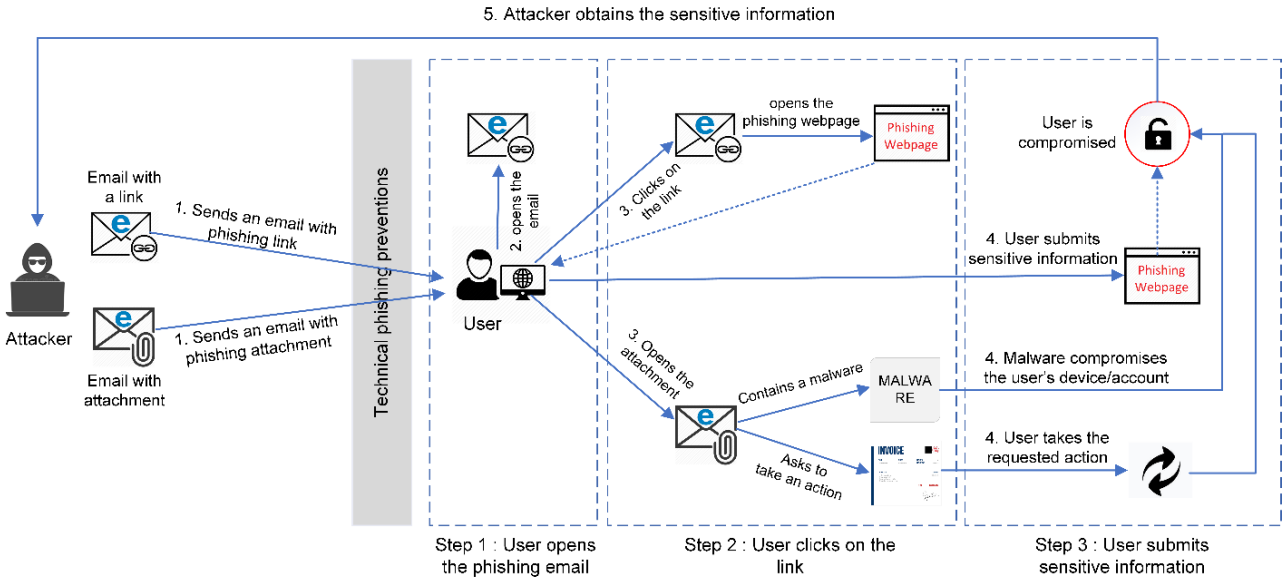


FIGURE 1. A common phishing attack process.

fake email that appears to come from a legitimate source and use the behavioural weaknesses of the victim to build trust. They can, for example, ask the recipient to click on a web link to win a prize. Some people's high risk-taking attitudes or a desire to gamble mean that they will click on the link, which opens a phishing website. Some of them might then decide to enter sensitive information on the webpage. As we go on to show in this paper, scammer uses psychological tricks to trap their victims. However, as of yet, little is known about which risk-taking behaviour and decision-making style[1] creates psychological vulnerabilities and how these are exploited in the different steps of the phishing process.

As presented in Figure 1, an attacker sends a phishing email to a user. The email might contain a phishing link or attachment (or both). The email might be detected and stopped by technical phishing prevention systems before it arrives in the user's inbox. The user receives and might open the phishing email if the technical systems do not prevent it, which is called the first step of the phishing process in this study. The second step of the process is when the user clicks on the phishing link in the email and/or opens the attachment. Clicking on the link usually opens a phishing webpage, on which the attacker uses various techniques to fool the user and obtain his/her sensitive information, such as bank account details. The attachment might contain built-in malware (e.g. ransomware, trojan, etc.) or a fake document asking the victim to take an action (e.g. a fake invoice, changing bank account payee details for a payment, etc.). The third step in the phishing process is when the user submits the sensitive information, takes the requested action, or when the built-in malware is not detected/prevented by any endpoint security system (e.g. antivirus software, mobile security, so on) and the malware compromises the user's device (i.e. computer, mobile phone, tablet, etc.) or account (i.e. email account, company account, etc.). In this study, we focused on the "clicking on the link" phishing method. Future research can focus on the "opening the phishing attachment" method, using the framework we developed in this study.

Researchers have studied the effects of demographic factors, such as age, gender, and education on falling for phishing [11]–[13]. However, to the best of our knowledge, no study focused on the effects of demographic factors and psychological traits on the phishability of users in the different steps of a phishing process. In the phishing process, presented in the Figure 1, a user takes actions such as clicking on the link and submitting the sensitive data on the phishing website. In fact, the user makes decisions (e.g. to click or not to click, to submit personal data or not) and takes risks (e.g. click on the link even when the email is suspicious because the phisher offers an "easily and quickly-achievable reward") throughout the phishing process [8], [9], [14]–[16].

This paper describes a study that was performed to assess the effects of risk-taking behaviour, decision-making style, and demographic factors (age, gender, and education) on how users respond to phishing attempts in the different steps of a phishing process. Based on this research, future studies and anti-phishing solutions can tackle the root causes of successful phishing attacks. Knowing these root causes allows focusing efforts on how to eliminate the sources of the phishing problem. For example, if a tendency for high-level risk-taking can increase the probability of falling victim to a phishing scam, we can investigate techniques to control or reduce this attitude in high-risk people to reduce their phishability. Of course, a risk-taking attitude can also be a valuable asset [17]. It is therefore important to understand which risk-taking behaviour makes people more vulnerable to phishing. Furthermore, discriminating the effects for the

[1]Decision-making style is defined as "the response pattern exhibited by an individual in a decision-making situation" [10]

different steps in the phishing process allows designing more specific solutions for these different steps.

The paper is structured as follows. First is the introduction followed by a literature review. Next, the three psychological tests and a phishing simulation carried out in this study are presented. The simulation aimed to assess the relationship between the phishability of a user and their risk-taking behaviour and decision-making style. Finally, the paper presents the results of the tests and simulation as well as proposals for future studies. The paper ends with a conclusion.

II. BACKGROUND AND HYPOTHESIS DEVELOPMENT

Several studies have shown a relationship between user behaviour,[2] personality,[3] and attitude[4] with regard to their cyber behaviour [21]–[27]. Some of them demonstrated the impacts of cyber activities on a user's behaviour [26], while others showed the effects of an individual's personality or behaviour on their cyber behaviour [23], [25]. Knowing which individual differences of Internet users might affect their cyber security behaviour can help us to develop better technical solutions and cyber security awareness programmes to prevent cyber-attacks. For instance, if we find that the risk-takers have poor cyber security behaviour, then we can provide more and specific training to those who take more risks. Studies have shown the relationship between individual differences and cyber security behaviour [9], [28]. They could, for instance, demonstrate that an individual's rational decision-making style is associated with their device securement behaviour [9] Alohali, *et al.* [29] used the BFI model [30] to investigate the relationship between personality traits such as extraversion, agreeableness, conscientiousness, neuroticism and openness to experience with 28 security behaviours such as clicking on email links and/or attachments, deleting suspicious emails, and keeping antivirus system up-to-date. Their findings suggested that personality traits are associated with the risk level of a user's security behaviour.

Other studies concentrated on phishing scams to identify the influence of individual differences and other factors, such as demographics, on a user's response to phishing attempts or phishing susceptibility [31]–[34]. While most of the studies investigated the effects of individual differences on a user's responses to phishing in general, the present study concentrates on the effects of user's behaviour during the different steps of a phishing process.

According to Stuart-Kotze, ''Ability and capability are not about traits, personality or genes – they are about behaviour. Unlike genetics or personality, behaviour can be described, observed, measured and changed. As a result, both ability and capability can be increased'' [35]. As we mentioned above, one of the usages of the result of this study would be to change the behaviour of vulnerable users (i.e. behaviours that are associated with their phishability) by using psychological techniques such as CBT [36]. This might take a long time but will tackle a root-cause of the person's vulnerability. Those behaviours may be shaped or influenced by different factors, such as the user's personality, attitude, emotions, thoughts, prior cyber-victimisation experiences [37]–[39], which can be used to change that behaviour.

A. RISK-TAKING BEHAVIOUR

Risk-taking is, in general, listed as one of the root causes of a successful phishing attack [8], [40], [41]. Other studies show that risk-taking is one of the causes of successful scams [9], [14], [42], [43], so it might impact people's phishability. In a phishing process, the attacker usually sends a phishing email to their targets and asks them to click on a phishing link or download an infected file. Clicking on the phishing link usually opens a phishing webpage asking the user to enter sensitive personal information or to download an infected file. For the purpose of this study, we define targets that open the phishing email as 'involved users', involved users that click on the link in the phishing e-mail 'risky users', and risky users that enter their personal data on the phishing webpage 'high-risk users'. Accordingly, we define phishability as the likelihood of falling into phishing traps and becoming the victim of a phishing attack, while the level of phishability is measured using an ordinal scale that ranges from low to high as: involved users – risky users – high-risk users.

As we are interested in phishability throughout the different steps of the phishing process, we formulate our first hypothesis as:

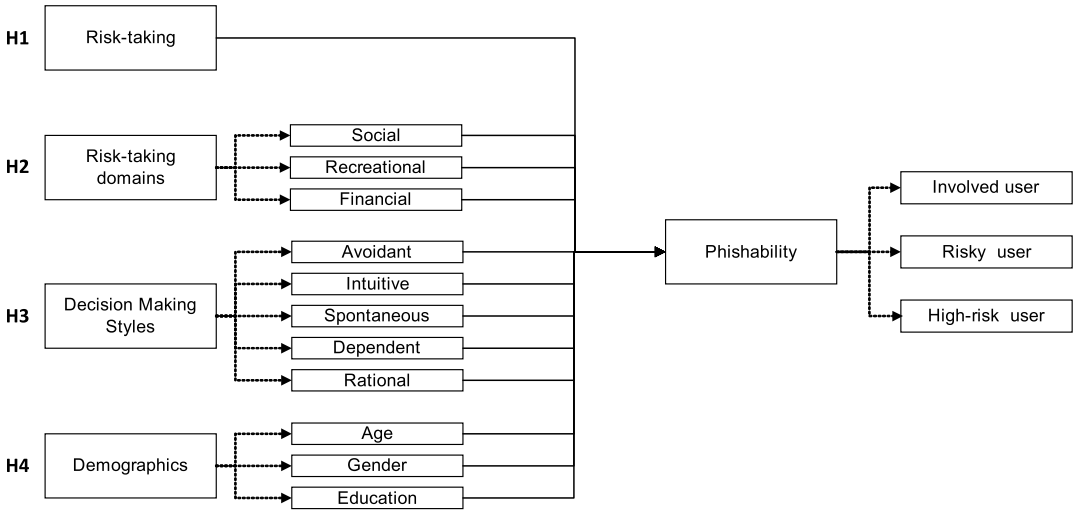
H1. Users' risk-taking behaviour affects their level of phishability in a phishing process.

Another study found that although people who exhibit greater financial risk-taking behaviour (i.e., risk-taking's financial domain) were more likely to become the target of scams, they were not necessarily being victimised [44], [45]. As a result, it is crucial to understand whether the risk-taking behaviour of an individual impacts their phishing victimisation or whether it is their domain-specific risk-taking behaviour (e.g. in the financial domain) that causes successful phishing attacks. Although previous research did not provide evidence that risk-taking in specific domains influences phishability or moderates the effect of general risk-taking behaviour on the level of phishability during the different steps of a phishing process, some studies demonstrated that a user's risk-taking preferences could influence their security behaviour [9]. Sheng, *et al.* [11] measured the financial investment risk reaction of users and found that the more risk-averse they were, the less likely they were to fall for a phishing scam. Therefore, we formulate the following hypothesis to confirm or refute these findings:

[2] ''Any action or function that can be objectively observed or measured in response to controlled stimuli''[18]

[3] ''The enduring configuration of characteristics and behavior that comprises an individual's unique adjustment to life, including major traits, interests, drives, values, self-concept, abilities, and emotional patterns''[19].

[4] ''A relatively enduring and general evaluation of an object, person, group, issue, or concept on a dimension ranging from negative to positive. Attitudes provide summary evaluations of target objects and are often assumed to be derived from specific beliefs, emotions, and past behaviors associated with those objects''[20]



H = Hypothesis

FIGURE 2. Research model.

H2. Users' domain-specific risk-taking behaviour (e.g. financial risk-taking) will affect their level of phishability in a phishing process.

B. DECISION-MAKING STYLE

As explained in this paper and based on the other studies mentioned [8], [45], people's decision-making style can be one of the factors in a successful phishing process. Sometimes scammers put their targets in a situation where they are more likely to make a poor decision, from the perspective of the victim. An error in decision-making can increase the chances of a successful scam [46]. However, a case of poor decision-making can happen for different reasons, such as ''episodic memory decline, particularly the loss of memory for details or source'' [47], which means that it may not be possible to avoid people ever making a poor decision during a phishing attack. A person's decision-making style and their security behaviour have been identified as some of the factors which can affect the result of scams [9], [48]. Even when the decision-making style is not the main cause of a successful phishing attack, it can be one of the factors that determine the success or failure of the attack. For instance, the target user might decide to share sensitive, personal information in one of the phishing steps [8], [49]–[51]. A target user might open a phishing email and click on the link as a result of their risk-taking behaviour but may submit their sensitive, personal information on the phishing website due to their decision-making style. Thus, we formulate the following hypothesis:

H3. User's decision-making style affects their level of phishability in the phishing process.

C. DEMOGRAPHICS

As mentioned earlier in this paper and based on other studies [9], [11]–[13], demographic factors might influence the phishability of users. Factors like age, gender, and education might directly or indirectly affect how people respond to a phishing attempt. For instance,..Sarno, *et al.* [52] investigated the relationship between age (range of 18-46) and gender differences with identifying an email as spam, authentic or dangerous. Their finding suggested that ''younger adults are more at risk to inauthentic emails than middle-aged adults'', but they could not find any significant difference between gender and identifying an email as spam.

Knowing the effects of these demographic factors on each phishing step and how they can influence the phishability of a user (i.e. to be an ''involved user, ''risky user'', or ''high-risk user'') can help us to build effective programmes and solutions to prevent phishing during the different steps. Therefore, we formulate the following hypothesis:

H4. Users' demographic factors affect their level of phishability in a phishing process.

As a result of this study, we aim to have an increased understanding of how and to what extent a user's behaviours impact the success of a phishing process. This knowledge should help mitigate a user's phishability by helping to change their risk-taking behaviour and/or decision-making style. Demographic factors might also affect the phishability of a user in each step of the process, which is analysed in this study.

Figure 2 presents a high-level research model which shows how behavioural variables (i.e. risk-taking, risk-taking domains, and decision-making styles) and demographic factors (i.e. age, gender, and education) might influence the phishability of a user in each step of phishing. These variables and their hypothesized effects on the dependent variable (user's phishability) are explained and analysed in the next sections.

III. RESEARCH METHOD

Cyber criminals use human cognitive and behavioural attributes to design phishing attacks and to trick their victims into taking the desired actions. Two such attributes were

identified by previous studies, as risk-taking behaviour and decision-making style [8], [9], both of which can play a role in causing people to fall into a phishing trap. We used three psychological measures in this study: the Balloon Analogue Risk Task test (BART) [53], the Domain-Specific Risk-Taking scale (DOSPERT) [54], and the General Decision-Making Style scale (GDMS) [55]. We then designed and executed a simulated phishing attack, with which we could determine the victims phishability levels by detecting those who opened the phishing email, those who clicked on the link provided, and those who entered their sensitive personal data on the phishing webpage. We analysed the effects of all the variables measured through the three psychological measures on the level of phishability to find out how general risk-taking behaviour, domain-specific risk-taking behaviour, and decision-making style predict phishability.

Since the participants of this study were from different parts of the country (Iran), and we wanted the simulation to appear like a real-life phishing attack, we decided to run the tests online rather than in a laboratory setting. Although both online and in-lab methods have their advantages and disadvantages, using the Internet is increasingly becoming a useful method for psychological research [56]–[58]. Another reason for doing the research online was that we did not want the participants to know when and how they would be subject to the simulated attack, as research has shown that informing participants that they are undertaking a phishing study effects the result [48]. In order to improve the study's quality, we followed the recommendations of previous Internet-based studies when designing and implementing our psychological tests. For instance, we clearly explained the study on the first page, explained each test before it started, and tested the survey platform several times to make sure that it was functioning correctly and was bug-free. We also tested the psychological tests and the phishing simulation on different Operating Systems such as Windows (XP, Vista, 7, 8, 10), Ubuntu, Mac OS, IOS, and Android, and different Internet browsers such as Internet Explorer, Google Chrome, and Safari. Moreover, we piloted the tests thoroughly to make sure that the system worked properly, that the information provided was both clear and comprehensive.

Several legal requirements and restrictions also needed to be taken into consideration before performing the online phishing simulation so as not to run into any legal issues [59], [60]. We had to design and run the simulation test in a way that actually sent phishing emails to the participants, we created and hosted a constructed phishing website, and we asked study participants to submit their personal information. As the simulation ran in Iran, we had to respect national regulations; however, we were not subject to other data protection regulations such as the EU GDPR.[5] We took into consideration the recommendations of previous studies in these matters and a roadmap to carry out ethical phishing [61]–[65]. We did not, for instance, store any data submitted by participants on the simulated phishing webpage, and we did not use any trademark. The participants were requested to opt-in to the study before it began. We also debriefed the participants about the study and provided them with opportunities to give their feedback.

Furthermore, the first author who played the primary role in designing the study, performing the tests, and communicating with the participants is Iranian, so the participants were recruited from a known culture.

A. DEMOGRAPHICS

The participants in the study were 62.2% female (84 participants) and 37.8% male (51 participants). Age ranged from 18 to 45 years old (three age groups of 18-25, 26-35, 36-45). All the participants were university students, researchers, or had recently completed one level of higher-level education and were preparing to continue their education. 45 participants (33.3%) were in areas of study within the social sciences, and the others 90 (66.7%) were in other fields. Sixteen participants (11.8%) held a bachelor's degree, five participants (3.7%) held a master's degree, 98 participants were bachelor students (72.6%), twelve participants were master students (8.9%), and four participants were PhD students (3%). All the participants regularly used online banking and/or online shopping.

As the participants were associated with academia (current/future students and/or researchers), the age and education level distributions were not balanced [66]. No one aged over 45 participated in this study. However, as mentioned earlier in this paper, previous studies found younger people more vulnerable to phishing attacks [1], [11], [67]; hence the imbalance in age distribution is not necessarily a drawback for our study. Moreover, on average, there have been more women than men in higher education in Iran over the last decade [68]–[70]. This explains the unbalanced gender distribution in our sample.

B. PSYCHOMETRIC TESTS

To measure the participants' real-world risk-taking behaviour, we used the BART test in our study. BART is widely used in different studies to measure risk-taking behaviour of participants [17], [71]–[74]. We also used DOSPERT to measure their risk-taking behaviour in financial, recreational, and social domains, with which we could analyse whether it was their overall risk-taking behaviour (based on the BART test) which affected phishability, or whether it was risk taking in a specific domain, for instance financial risk taking, which influenced the phishability level of a victim.

Studies show that a victim might take several decisions during the phishing process [8], [75], [76]. For instance, the person decides to click on the scam link in a phishing email or to close and delete the email instead. Another example is when the person decides to share or not their sensitive personal information with the phisher. There may well be other personal attributes of a potential victim or

[5]General Data Protection Regulation of the European Union; https://gdpr.eu/

different phishing techniques that influence the person's decision-making result; however, in this study, we wanted to find out what decision-making styles can impact on the victims' decisions in the phishing process. For this purpose, we used the GDMS scale, which measures the participant's ''Dependent'', ''Avoidant'', ''Intuitive'', and ''Spontaneous'' decision-making styles.

Both the DOSPERT and GDMS scales were available in English and in several other languages, but we could not find a good Farsi version of the scales. As we were going to use the scales in a new country (Iran) and translate them to a new language, we used a forward-backward standardised translation technique [77]–[79] to translate the tests to Farsi. In this technique, two native Iranians, both proficient in English and with different backgrounds, translated the tests to Farsi. They then worked together to synthesise the translations into one common translation. In the next step of the translation process, two other Iranian natives translated the common translation back to English. We set up an expert committee, including the translators and a psychologist, to review and finalise the translations. We finally pre-tested the translated version of the tests in a pilot phase, which is explained in this paper. The expert committee and the first author of this paper reviewed the translated questions based on the pilot feedback and discussions with the pilot participants to ensure that all the questions were clear and that they carried the same meaning as the original questions. One of the pilot participants was a native Iranian who was an English language lecturer with a master's degree in English language.

The DOSPERT and GDMS are well-established scales, but since we translated the questions and the sample questions were from another country with a different culture (the United States), a confirmatory factor analysis (CFA) was conducted on both scales. We used the following model fit indices and their criteria to examine the goodness-of-fit of the model with the given data set: goodness-of-fit index (GFI), comparative fit index (CFI), adjusted goodness-of-fit index (AGFI), normed fit index (NFI), Tucker-Lewis Index (TLI), and root mean square error of approximation (RMSEA) [80], [81]. After evaluating the model fit and analysing modification indices and standardised residual covariances, we improved the models and used the new ones for our further analyses.

1) BALLOON ANALOGUE RISK TASK (BART)

This test measures a person's risk-taking behaviour by examining their reward and loss potentials. In our study, the participants had 30 balloons. For each balloon they had two buttons on the page, ''pump'' and ''collect''. By clicking on the pump button, the balloon was inflated and 500 IRR (Iran Rial) were added to a counter-up until a random over-inflation point which caused the balloon to pop and set the counter back to zero. This meant that they could not earn any money for that period. They could, however, at any time before the balloon exploded have clicked on the collect button to collect whatever they had earned so far during the period. In this test, each click on the pump button means a greater risk-taking behaviour and a greater potential reward. We used the most common calculation method of BART, whereby we measured each person's risk-taking score based on the average number of pumps on the balloons that not exploded [82].

2) DOMAIN-SPECIFIC RISK-TAKING (DOSPERT)

To test the participants' risk-taking behaviour in different domains, we used the DOSPERT scale. The refined version of DOSPERT [54], [83] has 30 questions in ethical, financial, health and safety, recreational, and social domains. We choose eighteen questions in the financial, recreational, and social domains as these domains were more relevant to online scams, especially phishing attacks [14], [44], [84]–[86]. We did not include any health and safety or ethical questions in our study due to legal restrictions [87], [88] and cultural differences [89]. For example, participants would probably not have been comfortable answering questions that included ''Drinking heavily at a social function'' as Iran is an Islamic country where drinking alcohol is prohibited by law. Moreover, as the tests were not anonymous and the questions pertaining to the ethical domain were related to a person's unethical activities, university students would probably not provide reliable answers because of fear of possible negative consequences.

We asked all participants to answer the eighteen translated questions. Each question had seven ratings which participants needed to select from: ''Extremely Unlikely'' with a score of 1; ''Moderately Unlikely'' (score 2); ''Somewhat Unlikely'' (score 3); ''Not Sure'' (score 4); ''Somewhat Likely'' (score 5); ''Moderately Likely'' (score 6); and the ''Extremely Likely'' (score 7).

3) GENERAL DECISION-MAKING STYLE (GDMS)

As explained before in this paper, we decided to identify participants' decision-making styles to analyse their relationships with their phishability. For this purpose, we used the GDMS scale [90], which is a self-reporting questionnaire, to identify how the participants approach situations where they must make decisions. It includes 25 questions, such as ''my decision making requires careful thought'', using 5-point ratings from ''Strongly Disagree'', with a score of 1, to ''Strongly Agree'' with a score of 5. The questionnaire identifies the following styles: ''Rational'': ''thorough search for and logical evaluation of alternatives''; ''Intuitive'': ''use of hunches and feelings in decision making''; ''Dependent'': ''reliance on the advice of others''; ''Avoidant'': ''attempts to avoid decision-making''; and ''Spontaneous'': ''sense of immediacy and desire to complete decision-making as soon as possible''[91].

C. TEST PLATFORMS

We evaluated several online survey systems and finally selected unipark.de for our study. We based our decision on good reviews, user-friendliness, and the possibility to add and use scripts. The BART test is a computerised measurement, so we needed an online platform to run our JavaScript on. We customised a BART script used in another study [92], and

translated its buttons and other contents, such as ''Click to Collect the Money'' and ''Pump the Balloon'' to Farsi.

For the phishing simulation platform, we compared several open source and commercial systems, such as KnowBe4,[6] SET,[7] SPT,[8] PhishMe,[9] PhishingBox,[10] and GoPhish,[11] and based our decision on our own selected criteria. These included how easy it was to customise the landing page and phishing email, whether the system supported Farsi language and the cost. Furthermore, the emails should not end up in participants' spam folders and the possibility of sending emails to public emails such as Gmail, Yahoo, etc., were also important considerations. In the end, we chose the GoPhish open-source phishing simulator. The technical details are provided in Appendix A.

D. PILOT PHASE

The study was piloted with five participants in order to make sure that all the tests were clear and comprehensive, that the online questionnaire and phishing simulator system worked properly, to get participants' feedback on the content and translation of the questions, and in general, to improve the study and fix any possible issues. All pilot participants had university level education (bachelor, master, or PhD level) in social sciences or engineering and had some research experience. They were also between 35 and 48 years old. One pilot participant was a person educated in the English language, and another was a psychologist with a research background. Both participants could thus help us to verify the accuracy of the translations and the meaning of the questions. They were informed that they would receive a financial contribution equal to what they earned in the balloon game (BART).

The test structure:

1) The first page explained the goal of the study and what participants should do in the next pages. We informed them that they will play a game (BART) in which they will earn some money that will be transferred to their bank account afterwards. The number of questions, which was 43, and the estimated time to complete the tests, 20 minutes, was mentioned on this page.
2) The second page asked participants to fill in a form. They had to enter their name and personal email address. They were also requested to select their gender, age group (18-25, 26-35, 36-45, 46-55), and level of education (bachelor student, bachelor graduated, master student, master graduated, PhD student) and the subject of study. They were asked to give their consent to sharing their personal data with the researchers of this study and were informed that it would only be used for the purpose of the study. They also had to give their consent for the use of their information in future tests and steps of this research project and were informed that their personal information would be not shared outside of this research project. We informed them that we would use their email address to settle the payment (what they would earn by participating in the BART test). We could thereby assume that they would provide a correct email address that they regularly check. This email address could then be used in the phishing simulation.
3) The third page was the BART test, which is described in the Psychological Tests section of this paper. After completing the test, they had a total amount of money in their wallet, which was the sum of what they had collected from each balloon that they had earned during the game.
4) The fourth page asked them to answer the eighteen questions of the DOSPERT test, described in the Psychological Tests section of this paper.
5) The fifth page asked them to answer 25 GDMS questions, explained in the Psychological Tests section of this paper.
6) The last page thanked them for participating and asked them to contact us if they had any questions. A dedicated email address was given on this page.

Once the five participants had completed the pilot tests, we asked them seven questions. Based on their answers, we found that the tests are well designed, and the questions are easy to understand. They believed that the payment system of the balloon game worked well and the amount of money was enough to take the game seriously. The questions, the reasoning behind each question, and conclusions based on our assessment of their answers to each question are provided in Appendix B.

E. FULL-SCALE PHASE

After completing the pilot phase, we removed all the pilot data from the system and built a final version of the tests that included all the fixes and improvements made as a result of the pilot phase.

Our participants were invited to participate in our study either via university announcements or posts on specific social media channels[12] aimed at Iranian university students and researchers from different universities. The invitations were announced and posted by reputable persons (e.g. professors and known researchers) to ensure that they will be perceived as completely trustworthy. The use of trustworthy communication channels was meant to reduce the selection bias towards more risk-taking individuals. The requirements were that participants should be familiar with the use of computers, email, and the web and regularly use their personal email address. We drew attention to some rules, such as the ''only one-time rule'', whereby participants can take the test only once. The invitation was sent to over 3,000 university

[6] https://www.knowbe4.com
[7] https://github.com/trustedsec/social-engineer-toolkit/
[8] https://github.com/chris-short/sptoolkit
[9] https://www.cofense.com
[10] https://www.phishingbox.com/
[11] https://getgophish.com/

[12] Such as an academic researchers' channel on Telegram and an Iranian university students' group on Facebook.

students and graduates, and in total, 148 persons participated in the study via a web link.

Every other week, we sent a thank you email to each person who had participated in the study during that period of time, and informed them of the amount of money that they had earned in the balloon game. We also asked them to send us their own bank account details (this could not be someone else's bank account). This helped us to verify the person's name and to make sure that each person participated only once and that no one could use the study to earn more money than allowed in the framework of the study. We sometimes received email error autoreplies (from email servers) informing us that the email address did not exist. One person did not reply to our email and did not share their bank account details with us. We, however, fixed some of the email addresses that had been entered incorrectly, for instance, by changing username@domainname.con to username@domainname.com. We made a spreadsheet and documented all their responses, wrong emails, and so on. We transferred the money that they had earned, by using Internet banking, to their bank account and informed them that the payment had been made. We finally cleaned the participants' list, for example, by removing the persons who used the same email address and those who provided a wrong email address. By the end of this process, we had collected 135 participants for the next phase of our study.

F. PHISHING SIMULATION

We imported the participants' information, including their first name, last name, and email address to the phishing simulator (GoPhish), and created a phishing campaign. The system sent an email to all the users, which encouraged them to click on a link to win 100 million IR Tomans (approximately 8,000 USD, at the time of doing the phishing simulation). The email contained this message (in Farsi): ''Dear Student/Researcher, you are invited to win 100 million Tomans. Please click on the below link to enrol in the lottery.'' This was followed by a link to the phishing webpage. Clicking on the link opened the www.100million.live webpage for the user (our phishing webpage), which asked them to enter their name and bank account information. Clicking on the submit button of the webpage showed them a message that you enrolled in the lottery. However, as we explained before in this paper, the system did not store the information they entered on the phishing webpage, but it only detected and stored who opened the email, who clicked on the link, and who pressed the button on the webpage after entering the personal information. We assumed that they would enter their real information as they wanted to get the money.

We continually monitored the responses and stopped the campaign after one month, when there had been no new records for a few days. Among those 135 participants, 97 persons opened the phishing email and can thus be regarded as ''involved users''. To identify the reason(s) why those remaining 38 people did not open the email, we did a random check[13] after closing the campaign and found different reasons such as the person did not see the email, or they were not interested in the subject of the mail (which was ''win 100 million Tomans'' in Farsi), or they found the email to be suspicious. However, some of them were not sure if they had seen the email or not. We know that some of those emails might ended-up in their spam folder or even stopped by phishing prevention systems. This could also happen in real life (with real phishing emails), so we considered all of them as participants in our study, even though they had not opened the phishing email.

IV. DATA ANALYSIS AND RESULTS

Several analyses were performed on the data. For each step of the phishing process, we performed: (1) a factor analysis; (2) reliability testing; (3) multicollinearity analyses; (4) common method variance; and (5) multiple exact logistic regression analyses.

Table 1 summarises the demographics of the sample in three phishing process steps. Of the 97 involved users, 22 were risky users. Of these 22 risky users, 10 were high-risk users.

We performed a confirmatory factor analysis (CFA) on both the DOSPERT and GDMS tests. In our DOSPERT test, we had three constructs, and we wanted to see if the question items of each construct (i.e. risk-taking domain) load together. We did the same for the GDMS to analyse whether the items related to each decision-making style load together. Answering all the scales' questions was mandatory, so we had no missing values, which meant that there could be no missing items in our statistical analysis.

To explore factors that could help predict the phishability of the participants (as a result of the phishing simulation), multiple exact logistic regression analyses were conducted with the predictor variables of risk taking (BART), Risk-taking domains (DOSPERT), decision-making styles (GDMS), and the outcome variable of phishability in each step (i.e. email opened, link clicked, data submitted). IBM SPSS

Statistics 25.0 [93] was used to analyse the data and SAS 9.4 (SAS Inc., Cary, NC, USA) was used to carry out exact regression models.

A. FACTOR ANALYSIS

We used AMOS 22.0 to conduct a confirmatory factor analysis (CFA) on both the DOSPERT and GDMS scales. Multiple studies considered a sample size of 100 as the minimum sample size for conducting structural equation modeling (SEM) and CFA [94]–[97]. However, other studies [98], [99] show that five times the number of latent variables is an acceptable sample size for a SEM, although ten times would be better. Our DOSPERT model had three latent variables, and the GDMS model had five latent variables. Thus, our sample size

[13]By sending them an email from the email address which was used for the study communications and mentioned as the contact email on the survey.

TABLE 1. Demographic summary in three steps of phishing process.

Demographic Factor	Category	Total (n=135)	Email opened – involved users (n=97)	Link clicked – risky users (n=22)	Submitted Data – high-risk users (n=10)
Age					
	18-25	74%	80%	82%	90%
	26-35	18%	12%	9%	10%
	36-45	8%	8%	9%	0%
Gender					
	Male	38%	38%	18%	30%
	Female	62%	62%	82%	70%
Education					
	Bachelor student	72%	75%	82%	80%
	Bachelor graduated	12%	14%	0%	0%
	Master student	9%	5%	14%	20%
	Master graduated	4%	3%	0%	0%
	PhD student	3%	3%	4%	0%

of 135 should be enough to conduct factor analyses in this study.

1) DOSPERT FACTOR ANALYSIS

Factor loadings of the initial CFA for the three factors of DOSPERT scale (social, recreational, and financial) are presented in Figure 3. The model fit indices were as follows: χ 2 = 229.04, df = 132, p<.001, GFI = 0.833, CFI = 0.845, AGFI = 0.784, NFI = 0.707, TLI = 0.821, and RMSEA = 0.074. As it is presented in the Table 2, F2_Q4 and F6_Q11 have weak loadings on the financial factor. According to guidelines found in the literature, factor loadings below 0.3 should be dropped from the model [83], [97], [100], [101]. We therefore removed those two items from the model and the result of the model fit changed to: χ 2 = 143.26, df = 101, p<.005, GFI = 0.883, CFI = 0.925, AGFI = 0.843, NFI = 0.791, TLI = 0.911, and RMSEA = 0.056. Table 2 also presents the new factor loadings and Figure 4 presents the new model.

2) GDMS FACTOR ANALYSIS

Factor loadings of the initial CFA for the five factors of the GDMS scale are presented in Figure 5. The model fit indices were as follows: χ 2 = 563.98, df = 256, p<.001, GFI = 0.730, CFI = 0.780, AGFI = 0.669, NFI = 0.661, TLI = 0.752, and RMSEA = 0.074. Table 3 presents the initial factor loadings. To enhance the model fit, Standardised Residual Covariance and Modification Indices were inspected and problematic items (e.g. those with above 2.5 residual covariance with other items [101]) and those with loads below 0.3 were dropped from the model [97], [100], [101]. We ended up with 20 items (three items removed from the Intuitive, one from the Dependent, and one from Spontaneous factors). After this enhancement, the CFI and TLI achieved desirable values and the GFI, AGFI, and NFI scores were close to satisfactory [102], and RMSEA went down. The new model is presented in Figure 6, and the model fit indices were as follows: χ 2 = 248.68, df = 158, p<.001, GFI = 0.850, CFI = 0.922, AGFI = 0.801, NFI = 0.817, TLI = 0.906, and RMSEA = 0.065. Table 3 presents the new factor loadings.

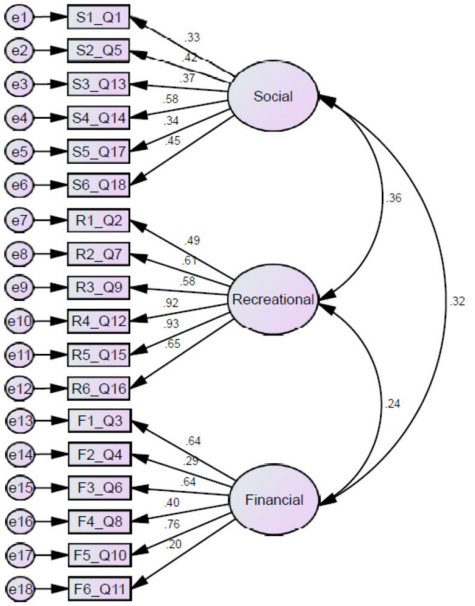


FIGURE 3. Initial factor model of DOSPERT.

We used the enhanced DOSPERT and GDMS models for the next analysis in this study.

B. RELIABILITY TEST

To ensure the internal consistency of the variables, reliability testing was performed on the subscales of DOSPERT and GDMS. The observations for the GDMS subscales were as follows: Cronbach's Alpha of Intuitive = 0.711 (0.735 after three items were deleted for model enhancement), Dependent α = 0.777 (0.840 after one item was deleted for model enhancement), Rational α = 0.812, Avoidant α = 0.783, and Spontaneous α = 0.731 (0.815 after one item was deleted for model enhancement). The observations for DOSPERT subscales were as follows: Cronbach's Alpha of Social = 0.547, Recreational α = 0.858, and Financial α = 0.681 (0.692 after two items were deleted for model enhancement). The results demonstrated good internal consistency for all the variables except for the DOSPERT's social subscale, which is poor but still shows moderate reliability [103].

TABLE 2. The initial and new factor loadings of the DOSPERT scale.

ID	Factor and Initial Loading			Factor and New Loading		
	S	R	F	S	R	F
S1-Q1	0.326	0	0	0.326	0	0
S2-Q5	0.424	0	0	0.423	0	0
S3-Q13	0.368	0	0	0.361	0	0
S4-Q14	0.582	0	0	0.588	0	0
S5-Q17	0.339	0	0	0.340	0	0
S6-Q18	0.449	0	0	0.448	0	0
R1-Q2	0	0.489	0	0	0.488	0
R2-Q7	0	0.610	0	0	0.610	0
R3-Q9	0	0.579	0	0	0.579	0
R4-Q12	0	0.917	0	0	0.917	0
R5-Q15	0	0.925	0	0	0.925	0
R6-Q16	0	0.654	0	0	0.654	0
F1-Q3	0	0	0.640	0	0	0.641
F2-Q4	0	0	0.287	0	0	0
F3-Q6	0	0	0.642	0	0	0.647
F4-Q8	0	0	0.403	0	0	0.342
F5-Q10	0	0	0.756	0	0	0.797
F6-Q11	0	0	0.204	0	0	0

The number after Q in the ID column identifies the question number in our questionnaire.
The questions and their order are based on the DOSPERT scale [54]. The full survey instrument and each ID's question can be found in the Appendix C.
S = Social, R = Recreational, F = Financial

TABLE 3. The initial and new factor loadings of the GDMS scale.

ID	Factor and Initial Loading					Factor and New Loading				
	I	D	R	A	S	I	D	R	A	S
I1_Q1	0.389	0	0	0	0	0	0	0	0	0
I2_Q3	0.447	0	0	0	0	0	0	0	0	0
I3_Q12	0.812	0	0	0	0	0.631	0	0	0	0
I4_Q16	0.584	0	0	0	0	0	0	0	0	0
I5_Q17	0.683	0	0	0	0	0.927	0	0	0	0
D1_Q2	0	0.279	0	0	0	0	0	0	0	0
D2_Q5	0	0.699	0	0	0	0	0.699	0	0	0
D3_Q10	0	0.864	0	0	0	0	0.868	0	0	0
D4_Q18	0	0.726	0	0	0	0	0.724	0	0	0
D5_Q22	0	0.745	0	0	0	0	0.741	0	0	0
R1_Q4	0	0	0.745	0	0	0	0	0.758	0	0
R2_Q7	0	0	0.581	0	0	0	0	0.530	0	0
R3_Q11	0	0	0.816	0	0	0	0	0.814	0	0
R4_Q13	0	0	0.676	0	0	0	0	0.680	0	0
R5_Q25	0	0	0.570	0	0	0	0	0.533	0	0
A1_Q6	0	0	0	0.672	0	0	0	0	0.672	0
A2_Q14	0	0	0	0.506	0	0	0	0	0.506	0
A3_Q19	0	0	0	0.846	0	0	0	0	0.848	0
A4_Q21	0	0	0	0.798	0	0	0	0	0.797	0
A5_Q23	0	0	0	0.445	0	0	0	0	0.442	0
S1_Q8	0	0	0	0	-0.138	0	0	0	0	0
S2_Q9	0	0	0	0	0.528	0	0	0	0	0.490
S3_Q15	0	0	0	0	0.919	0	0	0	0	0.941
S4_Q20	0	0	0	0	0.794	0	0	0	0	0.779
S5_Q24	0	0	0	0	0.529	0	0	0	0	0.490

The number after Q in the ID column identifies the question number in our questionnaire.
The questions and their order are based on the GDMS scale [55]. The full survey instrument and each ID's question can be found in the Appendix C.
I = Intuitive, D = Dependent, R = Rational, A = Avoidant, S = Spontaneous

C. MULRICOLLINEARITY ANALYSES

We performed a Pearson correlation analysis and examined the Variance Inflation Factors (VIF) on all the predictor variables to detect a possible issue of multicollinearity in our study [104]. The results indicated that no multicollinearity problem within the regression models (Maximum VIF in all the phishing steps and models is below 4 [105]). The tests results can be found in Appendix D.

D. COMMON METHOD VARIANCE

To examine the potential impact of common method bias, we conducted Harman's single-factor test on both the DOSPERT and GDMS models [106]. The single-factor test on the DOSPERT indicated that 23.6% of the variance was explained by one item, and the test on the GDMS indicated that 24.0% of the variance was explained by one item. These results showed that no single factor accounted for most of

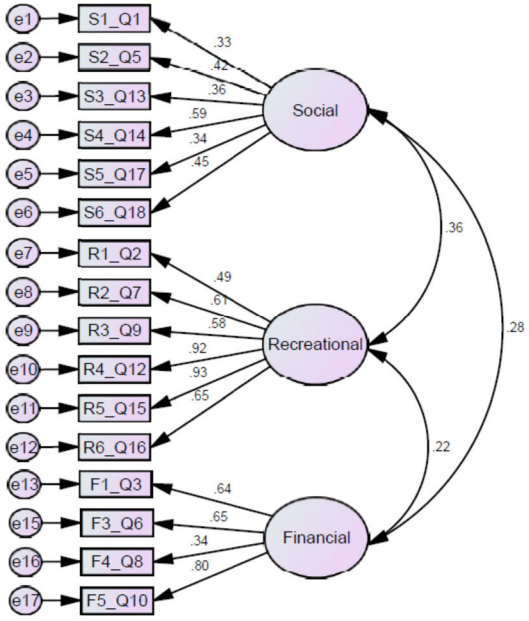


FIGURE 4. Improved factor model of DOSPERT.

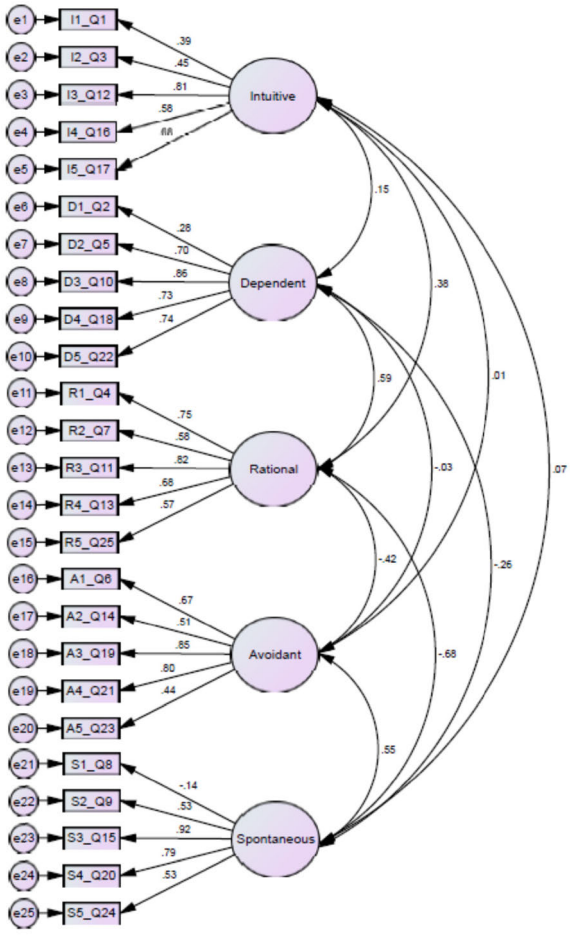


FIGURE 5. Initial factor model of GDMS.

the variance in the variables of the DOSPERT and GDMS models [106], [107].

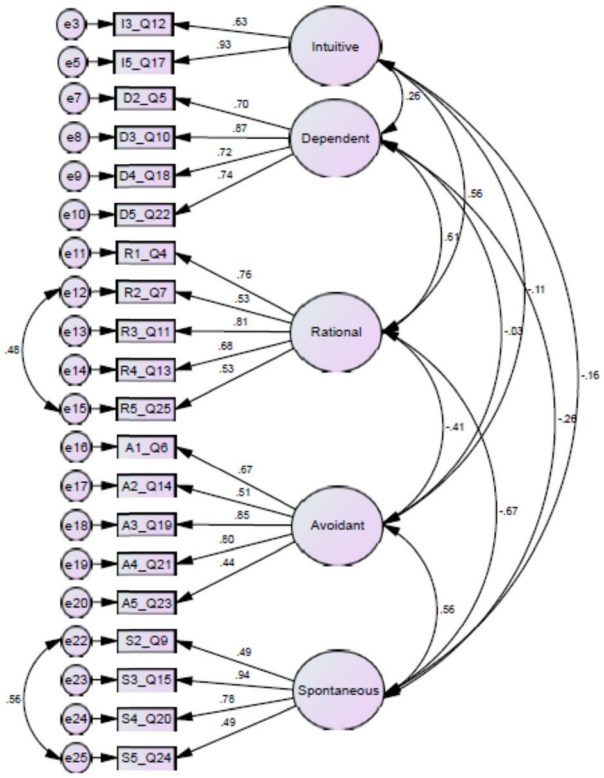


FIGURE 6. Improved factor model of GDMS.

E. EXACT LOGISTIC REGRESSIONS

Our dichotomous dependent variable in each step (i.e. involved users, risky users, and high-risk users), needs the use of logistic regression. We used multiple exact logistic regression in this study, as it is the appropriate method for small and unbalanced samples [108]. The predictive power of each of the risk-taking behaviours, decision-making styles, and demographic factors are shown in Table 4, which presents the results from several exact logistic regressions (coefficients with odds ratios in parentheses). The results show that the measures are not significant predictors of opening the phishing email and submitting data (i.e. involved users in the first step and high-risk users in the third step of the phishing process). However, the risk-taking behaviour (BART) ($\beta = 0.074$, $p < 0.05$) and gender ($\beta = 1.267$, $p < 0.05$) do significantly predict clicking on the phishing link (risky users) in the second step of the phishing process.

These results support our H1, as users' risk-taking behaviour influenced their level of phishability in a phishing process. More specifically, the results show that general risk-taking behaviour increases the likelihood to become a risky user (i.e. clicking the link, which happens in the second step of the phishing process). The results show no effect of risk-taking in recreational, social and financial domains on the level of phishability, hence H2 is not supported. Likewise, there is no support for H3 as we did not find an effect of decision-making style on the level of phishability. We also did not find any association between age and education

TABLE 4. Results from the exact logistic regressions predicting users' responses to each phishing step.

Measures	Step 1 (n=135) Email Opened?	Step 2 (n=97) Link Clicked?	Step 3 (n=22) Data Submitted?
Model 1. Risk-taking			
Risk-taking (BART)	-0.034 (0.966)	0.074* (1.077)	0.021 (1.021)
Social Risk-taking (DOSPERT)	-0.021 (0.979)	-0.004 (0.996)	-0.004 (0.996)
Recreational Risk-taking (DOSPERT)	0.022 (1.022)	-0.019 (0.981)	0.053 (1.054)
Financial Risk-taking (DOSPERT)	0.064 (1.066)	-0.012 (0.988)	0.002 (1.002)
Model 2. Decision-making Styles			
Avoidant (GDMS)	-0.016 (0.984)	0.033 (1.034)	-0.159 (0.853)
Intuitive (GDMS)	0.189 (1.208)	-0.052 (0.949)	-0.150 (0.861)
Spontaneous (GDMS)	-0.054 (0.947)	0.109 (1.115)	-0.138 (0.871)
Dependent (GDMS)	-0.036 (0.965)	0.044 (1.045)	-0.004 (0.996)
Rational (GDMS)	-0.101 (0.904)	-0.033 (0.967)	0.045 (1.046)
Demographic Factors			
Age	-0.029 (0.757)	-0.193 (0.824)	-0.937 (0.392)
Gender	-0.008 (0.992)	1.267* (3.551)	-1.153 (0.316)
Education	-0.151 (0.860)	0.061 (1.063)	0.407 (1.502)

The numbers shown are coefficients with odd ratios in parentheses from the logistic models.
Age groups: 1. 18-25, 2. 26-35, 3. 36-45
Gender: 0: Male, 1. Female
Educational level: 1. Bachelor student, 2. Bachelor graduated, 3. Master student, 4. Master graduated, 5. PhD student
Opening the phishing email: involved users, clicking on the link in the phishing email: risky users, and submitting data in the phishing website: high-risk users
*significant at 5%

factors and level of phishability, but the results show an effect of gender on clicking on the phishing link, which provides support for H4 as far as gender is concerned.

V. DISCUSSION

The findings from this study show that users' response to a phishing attack can be influenced by their risk-taking behaviour. We also found that gender is a predictor of clicking on a phishing link. Specifically related to the aim of our study, these effects occur in the second step of the phishing process, so general risk-taking behaviour and gender influence the likelihood of involved users to become risky users. Figure 7 shows a high-level summary of our findings.

These results suggest that the risk-taking behaviour of the users could affect their phishability level in the second step of the phishing process. There was no evidence of a satisfactory significant effect of risk-taking behaviours and decision-making styles on opening a phishing email, clicking on a phishing link in the email, and submitting sensitive data on a phishing website.

Moreover, our findings show that women can be slightly more phishable than men in the second step of the phishing process. This, however, could demonstrate that there might

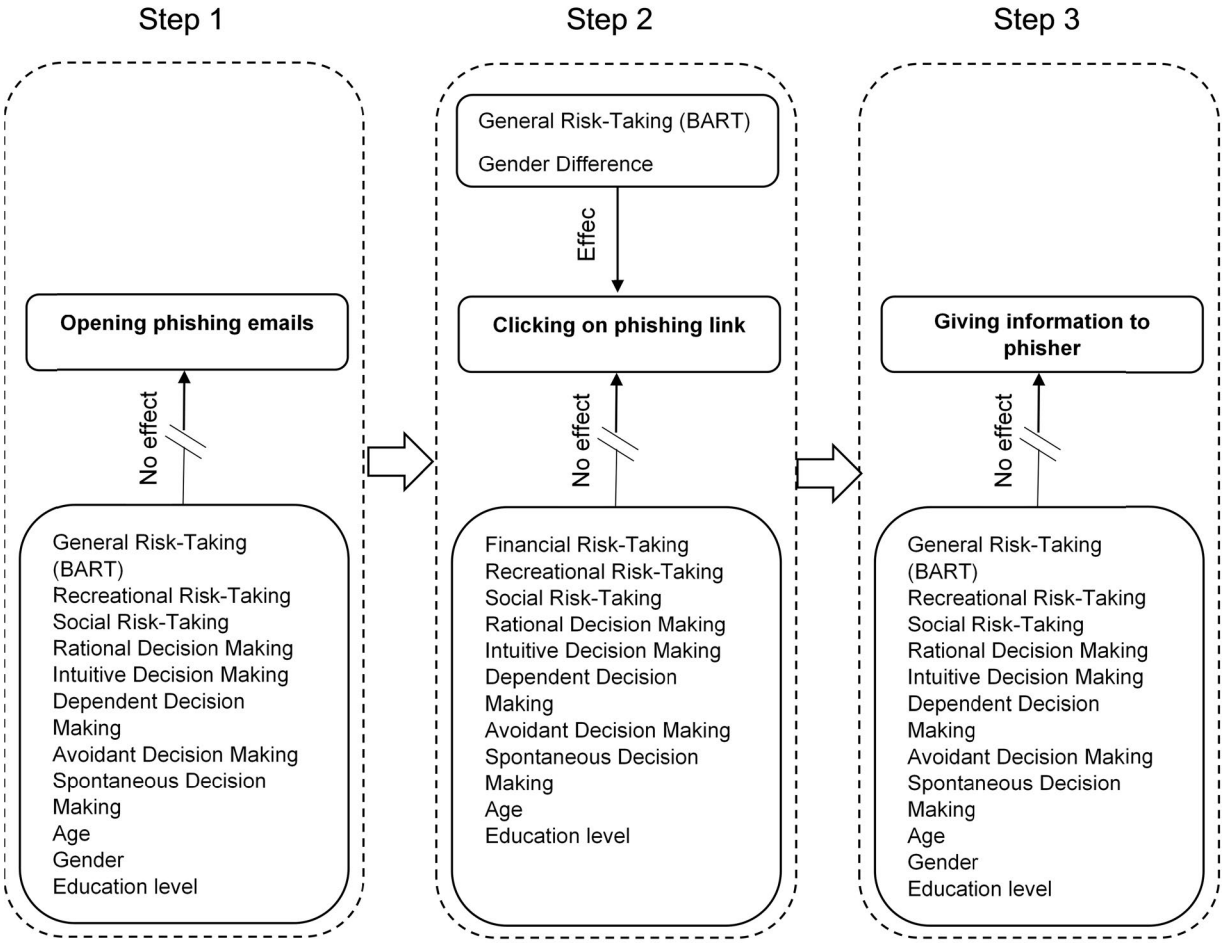


FIGURE 7. Effects of behaviors and demographic factors on each phishing step.

be other psychological reasons, for instance, gender-specific behaviours [109], [110], that might indirectly or directly impact the level of phishability. Further work is needed to learn more about the possible effects of female-related traits or behaviours on their level of phishability.

The aim of this study was to identify the effect of behaviour during the different steps of a phishing attack. We assessed some possible psychological root causes of what can make a phishing scam successful when a user receives a phishing email. Opening these emails is usually safe, especially if we view the email in plain text or HTML mode, but it might infect our computer if our email client allows scripting [111]. Furthermore, attackers might spoof an email to send email appearing to be from someone else. Although organisations and Internet/email service providers can reduce the email account spoofing risks by using solutions such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) [112], but according to the technical report [113] of the Joint Research Centre (JRC), many users do not follow anti-spoofing standards and solutions. Employees in an organisation may open an email from known names, e.g. their manager or the CEO. Our study did not show any effect of risk-taking behaviour and decision-making style on opening a phishing email, but there might be other reasons such as an attractive email subject that uses the Visceral Influence tactic [8], [114], an email from a known person (spoofed email), or a sense of urgency in the user which might lead an individual to open the email. One of the main issues with opening such emails is that the scammer might use email tracking techniques [115] which makes them sure that the email address belongs to a real person. In this case, the scammer will probably focus on the victim and use different tactics, for example, by using sophisticated spear phishing techniques [8], [116]–[121], to successfully attack that person. Focusing on deploying technical phishing email detection and prevention solutions [122] is therefore considered favourable to prevent phishing emails from reaching users in the first place.

A phishing message is designed to look genuine, usually using the same format as that of the real organisation, including their logo. Scammers use different techniques to convince the user to open an infected attachment or click on a link [8], [123]. Opening the attachment might infect the user's computer, and then an organisation's servers for example, with a malware such as ransomware [124], [125].

Clicking on the link and opening the phishing website can cause several problems, such as infecting the user's computer with a malware [124], attracting the user to submit sensitive information on the website, downloading an infected file from a website or cloud file hosting service (e.g. Dropbox). This study shows that a user who takes more risks will most likely click on a phishing link. Previous researches [9], [126] have shown a relationship between risk-taking and people's responses to cyber-attacks in general and phishing. However, knowing that the general risk-taking attitude of the user, and not necessarily a specific risk-taking attitude, has a stronger effect in one step of a phishing attack (i.e. based on this study, clicking on the link in step 2) can help us to develop successful mitigation strategies and solutions, especially for the risk takers. For example, it is possible to measure the risk-taking style of an organisation's employees and deliver focused trainings to employees with a high risk-taking score (e.g. to increase their awareness and knowledge about the dangers linked with clicking on links) and/or to implement an adequate technical solution [127]–[130]. Another way to reduce a users' likelihood of clicking on phishing links can be to use psychotherapy techniques to reduce negative risk-taking [17], [131]. This could be deliverable through Internet-based psychotherapies such Internet-based Cognitive Behavioural Therapy (iCBT) [36], [132], [133].

We however did find that gender is a significant (but not strong) unique predictor in step 2 of the phishing process, i.e. clicking on the link. Multiple studies have also showed that gender can affect a user's cybersecurity behaviour, such as avoiding reusing passwords for different accounts, proactive awareness (such as paying attention to indicators in a website or email), applying security patches [9], and falling prey to a phishing scam [1], [11]. A previous study [11] suggested that gender had effects on falling prey to a phishing attack and showed that women were more likely to click on phishing links than men. The study [11] showed that gender can have an indirect effect on falling prey to a phishing attack, as a result of a lack of technical knowledge and a lack of training of users. We believe that further work is needed to shed some light on other indirect effects of gender on each step of the process of a phishing attack, especially in clicking on phishing links, as we found a significant effect in this step. However, these indirect effects may be inconsistent in other countries, male and female traits and behaviours differ across cultures [110]. Thus, it is possible that users' behaviours in clicking on phishing links are subject to cultural differences.

Many phishing emails contain a hyperlink to a phishing website. The link looks like a legitimate hyperlink, but it is, in fact, a disguised link to a criminal website, which could install a malware on the victims' device or steal the individual's sensitive and confidential data [134], [135]. In this study, we measured the effects of risk-taking, decision-making, and demographics (age, gender, and level of education) on submitting information on a phishing website, which can compromise the victim's bank account, access to personal or organisational confidential data, so on and so forth. We could not find any significant effect of the mentioned psychological behaviours related to risk and decision-making on submitting information on the phishing website.

There were, however, several limitations in our study. We conducted the tests in a real-world setting to increase the appeared veracity of the phishing simulation. We tried to control some of the real-world experimental limitations such as by providing an incentive to participants (the BART reward). The possible effects of not having an incentive to provide feedback or continue completing a test have been mentioned in a previous study [136]. However, this incentive caused some issues and limitations, such as:

- We are not sure whether the reason that some participants did not open the email was that they did not want to take the risk or because they did not see the email, etc.
- We are not aware of any extraneous variables for each participant and could, therefore, not control and minimise those effects. For instance, the impact of a stressful situation or the mood of a participant was not considered. Such variables could affect the results of our tests, especially in the phishing simulation.
- We had to end the simulation as soon as possible; otherwise, our website could be listed in phishing databases and/or filtered by phishing prevention systems. This meant that the duration of the exercise was limited.
- We do not know if a participant had a client issue (e.g. browser issues, high security protections if they were connected to a secure network or used email/client anti-phishing features), which could prevent users from taking action in the simulated phishing.

Having no control over the participants' environments gave us little visibility on other factors that could influence clicking or not clicking on the phishing link. We believe this to be an intrinsic limitation of online studies.

Moreover, only one type of phishing attack (i.e., lottery scam) was used in this study. Participants might respond differently to other types of phishing attacks. Future studies can investigate the effects of users' behaviour and demographics for other types of phishing.

Another limitation of our study was the number of participants, as our overall response rate was only 5%. However, a low response rate to online studies shown by researchers [137], [138].

Finally, we could not include all the questions of the DOSPERT scale due to some limitations in Iran [87], [88] and cultural differences [89]. This meant that we could not measure the effect of all risk-taking attitudes on the phishing process. In addition to that, our participants were university students, researchers, and those who were preparing to continue their education, meaning that the sample is not representative of the overall Internet population.

All in all, the results of this study did not show any effect of risk-taking domains and decision-making style on all three steps of the phishing process. Therefore, we might be able to assume that a user will not necessarily be deemed phishable because, for example, their financial risk-taking is high

TABLE 5. Questions asked after the pilot tests.

#	Question	Reason	Conclusions based on the Answers
1	Do you remember how much money you earned in the balloon game?	We wanted to know if the money earned was important for this person and how consciously and seriously the person had participated in the test. The overall feedback from the persons with correct answers to this question were more important for us. The second purpose of this question was to make sure that the script[14] and system worked probably.	They mentioned an amount close to what was recorded by the system. The money earned was not very important for the pilot participants, but they did say that they wanted to do their best to win more. The game could be a good tool to be used in our full-scale test (the next phase). However, because the amounts mentioned were not the exact amounts recorded in the system, we tested the system several times, after the pilot, to ensure that it recorded the correct amount each time.
2	How clear were the questions?	This was done to check whether the translations were clear and simple to understand and to ensure that the participants of the full-scale test would not be in doubt regarding the meaning of the questions.	All the questions were judged to be clear and simple to understand.
3	Did you come across any errors (typo, technical issue, etc.)? Do you have any suggestions for improvement?	This was asked to make sure that the system worked properly and to fix any possible typos or other errors.	One typo was found in the test explanation text, which was fixed after the pilot. No technical issues were observed.
4	Would you have participated in the study, done the tests correctly and shared your information with us if you had not known us?	This was asked to ensure that we had designed a sound strategy for inviting people to participate in the study in a way that inspired confidence. We also needed their full trust to ensure that their answers were correct.	They could not see any reason for sharing wrong information. However, one participant mentioned that some people might consider it to be a fake study and would not believe that they would in fact receive the money promised, as there are an increasing number of online scams these days.
5	Was the money (cash per pump) enough to encourage you to take the balloon game seriously and to show your real risk-taking level? Which reward method do you prefer: small individual rewards per pump or a big reward to the overall winner (who has earned the highest number of points)?	This was asked to ensure that the amount of money offered for each pump was tempting enough, and answers would also help identify their attitude to risk taking.	They believed that the pay per pump system worked best and that the amount of money offered was enough, and even deemed very tempting by some students. In general, participants confirmed that the balloon game and its reward system was very interesting and attractive. For instance, one of them mentioned a genuine sense of engagement in the balloon game and expressed the desire to want to acquire more points.
6	What do you think about the number of questions? Are there too many questions?	This was designed to ensure that the number of questions was satisfactory and not excessive, to avoid the risk of participants answering randomly.	All participants were satisfied with the number of questions.
7	How accurately do you think that you answered the questions? Did your responses reflect your real behaviour in everyday life?	Answers to this question could strengthen our belief that the chosen tests, their translations, and the whole test package were satisfactory for our needs.	Participants had tried to answer the questions accurately and participate in the tests in an honest fashion. Their impression was that the tests were good and that they could reflect their real behaviour.

(at least in a similar phishing process as used in this study). High risk-taking behaviour can lead users to click on a phishing email, but not their risk-taking in a specific domain, as measured by the DOSPERT scale. The same result was found for the decision-making style of users (opening a phishing email, clicking on a phishing link, and submitting data in a phishing website), is unlikely to be related to a user's rational decision-making skills.

In this study, we have developed a unique methodology to find associations between human behaviours (i.e. risk-taking and decision-making in this study) and the phishability of users. This methodology can be used to investigate the effects of other human behaviours on phishability by using different psychological scales (to measure those behaviours).

VI. CONCLUSION

In this study, we analysed the effects of risk-taking, decision-making, age, gender, and the level of education on the success of a phishing attack. Phishing is usually a process in which scammers try to gain a victim's trust and encourage them to open a phishing email, click on a link (or open an infected attachment) and finally share sensitive information on a phishing website, such as bank account details or confidential information about their organisation. If we understand the main reasons why people follow the attacker in each phishing step, this will help us to make an effective programme to block phishing attacks each step of the way. These programmes can work alongside existing technical solutions to increase the level of phishing prevention both in our private and public lives. We analysed the effect of

TABLE 6. Correlations in the first phishing step (email opened).

Variables	RT	S-RT	R-RT	F-RT	A-DM	I-DM	S-DM	D-DM	R-DM	Age	Gender	Education
RT	1	0.256**	0.165	0.289**	0.101	-0.114	0.098	-0.047	-0.100	-0.080	-0.126	0.124
S-RT	0.256**	1	0.301**	0.188*	0.043	0.074	0.172*	-0.057	-0.002	0.005	0.135	0.070
R-RT	0.165	0.301**	1	0.174*	-0.046	0.002	0.052	0.000	-0.023	-0.267**	-0.092	-0.168
F-RT	0.289**	0.188*	0.174*	1	0.078	-0.188*	0.115	-0.127	0.000	-0.106	-0.058	-0.023
A-DM	0.101	0.043	-0.046	0.078	1	-0.011	0.377**	0.014	-0.316**	-0.190*	-0.177*	-0.176*
I-DM	-0.114	0.074	0.002	-0.188*	-0.011	1	0.098	0.210*	0.400**	0.125	0.110	0.032
S-DM	0.098	0.172*	0.052	0.115	0.377**	0.098	1	-0.162	-0.426**	-0.015	0.051	-0.092
D-DM	-0.047	-0.057	0.000	-0.127	0.014	0.210*	-0.162	1	0.480**	-0.134	-0.061	0.078
R-DM	-0.100	-0.002	-0.023	0.000	-0.316**	0.400**	-0.426**	0.480**	1	0.087	0.049	0.225**
Age	-0.080	0.005	-0.267**	-0.106	-0.190*	0.125	-0.015	-0.134	0.087	1	0.122	0.398**
Gender	-0.126	0.135	-0.092	-0.058	-0.177*	0.110	0.051	-0.061	0.049	0.122	1	-0.033
Education	0.124	0.070	-0.168	-0.023	-0.176*	0.032	-0.092	0.078	0.225**	0.398**	-0.033	1

RT: Risk-taking (BART), S-RT: Social Risk-taking (DOSPERT), R-RT: Recreational Risk-taking (DOSPERT), F-RT: Financial Risk-taking (DOSPERT),
A-DM: Avoidant (GDMS), I-DM: Intuitive (GDMS), S-DM: Spontaneous (GDMS), D-DM: Dependent (GDMS), R-DM: Rational (GDMS)
**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

TABLE 7. Correlations in the second phishing step (link clicked).

Variables	RT	S-RT	R-RT	F-RT	A-DM	I-DM	S-DM	D-DM	R-DM	Age	Gender	Education
RT	1	0.231*	0.167	0.378**	0.123	-0.103	0.182	-0.076	-0.166	-0.060	-0.131	0.108
S-RT	0.231*	1	0.208*	0.199	0.095	0.085	0.294**	-0.102	-0.076	0.076	0.102	0.154
R-RT	0.167	0.208*	1	0.174	-0.010	-0.072	0.145	-0.052	-0.149	-0.186	-0.151	-0.158
F-RT	0.378**	0.199	0.174	1	0.110	-0.133	0.228*	-0.150	-0.048	-0.023	0.030	-0.014
A-DM	0.123	0.095	-0.010	0.110	1	0.001	0.323**	0.002	-0.328**	-0.180	-0.192	-0.046
I-DM	-0.103	0.085	-0.072	-0.133	0.001	1	0.067	0.244*	0.441**	0.112	0.006	0.046
S-DM	0.182	0.294**	0.145	0.228*	0.323**	0.067	1	-0.168	-0.409**	0.002	0.012	0.068
D-DM	-0.076	-0.102	-0.052	-0.150	0.002	0.244*	-0.168	1	0.472**	-0.175	-0.126	0.029
R-DM	-0.166	-0.076	-0.149	-0.048	-0.328**	0.441**	-0.409**	0.472**	1	0.097	-0.024	0.150
Age	-0.060	0.076	-0.186	-0.023	-0.180	0.112	0.002	-0.175	0.097	1	0.075	0.380**
Gender	-0.131	0.102	-0.151	0.030	-0.192	0.006	0.012	-0.126	-0.024	0.075	1	-0.049
Education	0.108	0.154	-0.158	-0.014	-0.046	0.046	0.068	0.029	0.150	0.380**	-0.049	1

RT: Risk-taking (BART), S-RT: Social Risk-taking (DOSPERT), R-RT: Recreational Risk-taking (DOSPERT), F-RT: Financial Risk-taking (DOSPERT),
A-DM: Avoidant (GDMS), I-DM: Intuitive (GDMS), S-DM: Spontaneous (GDMS), D-DM: Dependent (GDMS), R-DM: Rational (GDMS)
**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

some personal behaviours and demographic factors in each of the three phishing steps described. Future studies can use a similar model to identify the effect of other possible phishing root causes (i.e. human and psychological factors), which can help us to build a holistic framework to proactively prevent the success of phishing scams.

We found that a high level of general risk-taking can increase the possibility of clicking on a phishing link, and

TABLE 8. Correlations in the third phishing step (data submitted).

Variables	RT	S-RT	R-RT	F-RT	A-DM	I-DM	S-DM	D-DM	R-DM	Age	Gender	Education
RT	1	0.387	0.306	0.342	0.200	0.030	0.038	0.103	-0.029	0.027	0.109	-0.131
S-RT	0.387	1	0.033	0.217	-0.223	0.159	0.187	0.120	0.086	0.314	0.407	0.356
R-RT	0.306	0.033	1	0.283	-0.012	0.095	0.008	-0.193	-0.185	-0.170	-0.176	-0.266
F-RT	0.342	0.217	0.283	1	-0.020	-0.402	0.057	-0.084	-0.078	0.010	0.454*	-0.254
A-DM	0.200	-0.223	-0.012	-0.020	1	-0.028	0.011	-0.278	-0.344	-0.281	0.155	-0.363
I-DM	0.030	0.159	0.095	-0.402	-0.028	1	0.031	0.332	0.432*	0.318	-0.191	0.261
S-DM	0.038	0.187	0.008	0.057	0.011	0.031	1	-0.354	-0.422	0.316	0.136	0.319
D-DM	0.103	0.120	-0.193	-0.084	-0.278	0.332	-0.354	1	0.768**	-0.150	-0.140	-0.049
R-DM	-0.029	0.086	-0.185	-0.078	-0.344	0.432*	-0.422	0.768**	1	0.106	-0.255	0.102
Age	0.027	0.314	-0.170	0.010	-0.281	0.318	0.316	-0.150	0.106	1	0.209	0.662**
Gender	0.109	0.407	-0.176	0.454*	0.155	-0.191	0.136	-0.140	-0.255	0.209	1	0.208
Education	-0.131	0.356	-0.266	-0.254	-0.363	0.261	0.319	-0.049	0.102	0.662**	0.208	1

RT: Risk-taking (BART), S-RT: Social Risk-taking (DOSPERT), R-RT: Recreational Risk-taking (DOSPERT), F-RT: Financial Risk-taking (DOSPERT),

A-DM: Avoidant (GDMS), I-DM: Intuitive (GDMS), S-DM: Spontaneous (GDMS), D-DM: Dependent (GDMS), R-DM: Rational (GDMS)

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

that women seem to be more prone to clicking on a phishing link. We realise, however, that these findings can vary across cultures and countries. Future research could focus on gender-specific behaviours and other psychological reasons that might indirectly or directly impact the level of phishability.

The strength of this study is that it was conducted in a manner that reflects what happens in the real world. Furthermore, it analysed two types of human behaviour, when it comes to risk-taking and decision-making. These two predictors of user behaviour form a basis for future research with the aim of finding a holistic approach to tackling phishing attacks. The findings described in this paper have implications for security management in organisations. For example, assessing the risk-taking behaviour of an organisation's employees and adapting company policy to include specific security and anti-phishing training opportunities (especially for risky users and high-risk users, for example) are two ways to help prevent successful phishing attacks and the dangers that they incur both for a user and their employer.

Moreover, the methodology we developed in this study can be used to investigate relationships between different human behaviours and phishability.

APPENDIX A
PHISHING SIMULATOR TECHNICAL DETAILS

We installed and configured the GoPhish system on a Windows 2016 Virtual Private Server (VPS) hosted by time4vps.com. The server had a 2.60 GHz CPU, with 2 GB RAM, 20 GB storage and 2 TB bandwidth per month. We then registered the 100million.live domain name for one year and created the win@100million.live email address. The domain name was registered in private mode, so that in case the participants searched the domain in a ''Whois'' online service, they would not be able to find our names as the domain owners, which could make it suspicious to the participants and compromise our results. We also created a phishing webpage which asked visitors to enter their full name and bank card number in order to enrol in a 100,000,000 IRT (Iran Toman, which is equal to one billion IRR) lottery. The webpage was hosted on the VPS mentioned above, and its IP address registered as the www hostname in the DNS of the 100million.live domain name, so that the www.100million.live URL opened the phishing webpage. We tested the URL from different places in Iran to make sure that it was accessible from different Internet Service Providers, including mobile operators.

We had to ensure that the domain name and IP address would not be blacklisted as a phishing IP or domain [8], [139], [140] or be blocked by web filtering and other security systems. We also had to make sure that the simulated phishing emails would not be blocked by anti-spam and anti-phishing software. For this purpose, the phishing webpage was hosted by GoPhish and was only available during the period where we were running the phishing simulation. It was, therefore, only available for a short period of time, which decreased the chance of it being blacklisted [141], [142]. We also used techniques such as using a Meta Robots tag [143] to hide the webpage from web search engines. We also used Search Engine Optimisation (SEO) techniques [144] to make the page unsearchable and thus

TABLE 9. Variance Inflation Factors (VIF) in three phishing steps.

Variables	Step 1 (n=135) Email Opened	Step 2 (n=97) Link Clicked	Step 3 (n=22) Data Submitted
Model 1. Risk-taking			
Risk-taking (BART)	1.149	1.210	1.373
Social Risk-taking (DOSPERT)	1.165	1.103	1.204
Recreational Risk-taking (DOSPERT)	1.122	1.073	1.166
Financial Risk-taking (DOSPERT)	1.120	1.197	1.196
Model 2. Decision-making Styles			
Avoidant (GDMS)	1.257	1.234	1.210
Intuitive (GDMS)	1.333	1.383	1.371
Spontaneous (GDMS)	1.460	1.365	1.366
Dependent (GDMS)	1.354	1.334	2.444
Rational (GDMS)	2.061	2.097	3.250
Demographic Factors			
Age	1.214	1.181	1.797
Gender	1.023	1.013	1.055
Education	1.197	1.177	1.797

prevent it from being indexed by search engines, which would have increased the visibility of the webpage to all users of the search engines.

APPENDIX B
PILOT PHASE QUESTION

See Table 5.

APPENDIX C
SURVEY INSTRUMENTS

A. DOSPERT SURVEY INSTRUMENT

S1-Q1 Admitting that your tastes are different from those of a friend.
S2-Q5 Disagreeing with an authority figure on a major issue.
S3-Q13 Choosing a career that you truly enjoy over a more secure one.
S4-Q14 Speaking your mind about an unpopular issue in a meeting at work.
S5-Q17 Moving to a city far away from your extended family.
S6-Q18 Starting a new career in your mid-thirties.
R1-Q2 Going camping in the wilderness.
R2-Q7 Going down a ski run that is beyond your ability.
R3-Q9 Going whitewater rafting at high water in the spring.
R4-Q12 Taking a skydiving class.
R5-Q15 Bungee jumping off a tall bridge.
R6-Q16 Piloting a small plane.
F1-Q3 Betting a day's income at the horse races.
F2-Q4 Investing 10% of your annual income in a moderate growth mutual fund.

[14]BART's JavaScript

F3-Q6 Betting a day's income at a high-stake poker game.
F4-Q8 Investing 5% of your annual income in a very speculative stock.
F5-Q10 Betting a day's income on the outcome of a sporting event.
F6-Q11 Investing 10% of your annual income in a new business venture.

B. GDMS SURVEY INSTRUMENT

I1_Q1 When I make decisions, I tend to rely on my intuition.
I2_Q3 I rarely make important decisions without consulting other people.
I3_Q12 When I make a decision, it is more important for me to feel the decision is right than to have a rational reason for it.
I4_Q16 I double-check my information sources to be sure I have the right facts before making decisions.
I5_Q17 I use the advice of other people in making my important decisions.
D1_Q2 I put off making decisions because thinking about them makes me uneasy.
D2_Q5 I make decisions in a logical and systematic way.
D3_Q10 When making decisions I do what feels natural at the moment.
D4_Q18 I generally make snap decisions.
D5_Q22 I like to have someone steer me in the right direction when I am faced with important decisions.
R1_Q4 My decision making requires careful thought.
R2_Q7 When making a decision, I trust my inner feelings and reactions.
R3_Q11 When making a decision, I consider various options in terms of a specified goal.
R4_Q13 I avoid making important decisions until the pressure is on.
R5_Q25 I often make impulsive decisions.
A1_Q6 When making decisions, I rely upon my instincts.
A2_Q14 I generally make decisions that feel right to me.
A3_Q19 I often need the assistance of other people when making important decisions.
A4_Q21 I postpone decision making whenever possible.
A5_Q23 I often make decisions on the spur of the moment.
S1_Q8 I often put off making important decisions.
S2_Q9 If I have the support of others, it is easier for me to make important decisions.
S3_Q15 I generally make important decisions at the last minute.
S4_Q20 I make quick decisions.
S5_Q24 I usually have a rational basis for making decisions

APPENDIX D
MULTICOLLINEARITY ANALYSES RESULTS

Correlations in the phishing process steps, Variance Inflation Factors (VIF) examination. See Table 6–9.

REFERENCES

[1] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, 2007.
[2] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," Electr. Inf. Sharing Anal. Center (E-ISAC), Washington, DC, USA, Tech. Rep., vol. 388, 2016.
[3] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, Dec. 2018.
[4] Kaspersky. (2020). *Phishing Attacks More Than Doubled in 2018 to Reach Almost 500 Million*. Accessed: Mar. 15, 2020. [Online]. Available: https://www.kaspersky.com/about/press-releases/2019_phishing-attacks-more-than-doubled-in-2018
[5] GetCyberSafe Canadian Centre for Cyber Security. (2020). *Phishing: How Many Take the Bait?* Accessed: Mar. 15, 2020. [Online]. Available: https://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx
[6] K. Pfeffel, P. Ulsamer, and N. Müller, "Where the user does look when reading phishing mails—An eye-tracking study," presented at the Int. Conf. Hum.-Comput. Interact., 2019.
[7] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, Sep. 2018.
[8] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing attacks root causes," in *Proc. Int. Conf. Risks Secur. Internet Syst.* Dinard, France: Springer, 2017, pp. 187–202.
[9] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018.
[10] P. Thunholm, "Decision-making style: Habit, style or both?" *Personality Individual Differences*, vol. 36, no. 4, pp. 931–944, Mar. 2004.
[11] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proc. 28th Int. Conf. Hum. Factors Comput. Syst. (CHI)*, 2010, pp. 373–382.
[12] C. Iuga, J. R. C. Nurse, and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Hum.-Centric Comput. Inf. Sci.*, vol. 6, no. 1, p. 8, Dec. 2016.
[13] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham, "School of phish: A real-world evaluation of anti-phishing training," in *Proc. 5th Symp. Usable Privacy Secur.*, 2009, pp. 1–12.
[14] S. Egelman and E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (SeBIS)," in *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst.*, Apr. 2015, pp. 2873–2882.
[15] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: An empirical study of the effectiveness of Web browser phishing warnings," in *Proc. 26th Annu. CHI Conf. Hum. Factors Comput. Syst. (CHI)*, 2008, pp. 1065–1074.
[16] L. F. Cranor, "A framework for reasoning about the human in the loop," in *Proc. Conf. Usability, Psychol., Secur.* Berkeley, CA, USA: USENIX Association, 2008, pp. 1–15.
[17] K. L. Humphreys, S. S. Lee, and N. Tottenham, "Not all risk taking behavior is bad: Associative sensitivity predicts learning during risk taking among high sensation seekers," *Personality Individual Differences*, vol. 54, no. 6, pp. 709–715, Apr. 2013.
[18] American Psychological Association. *Behavior*. Accessed: Sep. 21, 2020. [Online]. Available: https://dictionary.apa.org/behavior
[19] American Psychological Association. *Personality*. Accessed: Sep. 21, 2020. [Online]. Available: https://dictionary.apa.org/personality

[20] American Psychological Association. *Attitude*. Accessed: Sep. 21, 2020. [Online]. Available: https://dictionary.apa.org/attitude

[21] J. D. Russell, C. F. Weems, I. Ahmed, and G. G. Richard, "Self-reported secure and insecure cyber behaviour: Factor structure and associations with personality factors," *J. Cyber Secur. Technol.*, vol. 1, nos. 3–4, pp. 163–174, Oct. 2017.

[22] M. Eşkisu, R. Hoşoğlu, and K. Rasmussen, "An investigation of the relationship between Facebook usage, big five, self-esteem and narcissism," *Comput. Hum. Behav.*, vol. 69, pp. 294–301, Apr. 2017.

[23] D. Liu and R. F. Baumeister, "Social networking online and personality of self-worth: A meta-analysis," *J. Res. Personality*, vol. 64, pp. 79–89, Oct. 2016.

[24] C. D. Pornari and J. Wood, "Peer and cyber aggression in secondary school students: The role of moral disengagement, hostile attribution bias, and outcome expectancies," *Aggressive Behav.*, vol. 36, no. 2, pp. 81–94, Mar. 2010.

[25] S. Pabian, C. J. S. D. Backer, and H. Vandebosch, "Dark triad personality traits and adolescent cyber-aggression," *Personality Individual Differences*, vol. 75, pp. 41–46, Mar. 2015.

[26] C.-H. Ko, J.-Y. Yen, S.-C. Liu, C.-F. Huang, and C.-F. Yen, "The associations between aggressive behaviors and Internet addiction and online activities in adolescents," *J. Adolescent Health*, vol. 44, no. 6, pp. 598–605, Jun. 2009.

[27] G. Dhillon, Y. Y. A. Talib, and W. N. Picoto, "The mediating role of psychological empowerment in information security compliance intentions," *J. Assoc. Inf. Syst.*, vol. 21, no. 1, p. 5, 2020.

[28] R. van Bavel, N. Rodríguez-Priego, J. Vila, and P. Briggs, "Using protection motivation theory in the design of nudges to improve online security behavior," *Int. J. Hum.-Comput. Stud.*, vol. 123, pp. 29–39, Mar. 2019.

[29] M. Alohali, N. Clarke, F. Li, and S. Furnell, "Identifying and predicting the factors affecting end-users' risk-taking behavior," *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 306–326, Jul. 2018.

[30] P. Costa and R. McCrae, "Professional manual of the revised NEO personality inventory and NEO five-factor inventory," Psychol. Assessment Resour., Odessa, FL, USA, Tech. Rep. 61, 1991.

[31] J.-H. Cho, H. Cam, and A. Oltramari, "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," in *Proc. IEEE Int. Multi-Disciplinary Conf. Cognit. Methods Situation Awareness Decis. Support (CogSIMA)*, Mar. 2016, pp. 7–13.

[32] I. Alseadoon, M. Othman, and T. Chan, "What is the influence of users' characteristics on their ability to detect phishing emails?" in *Advanced Computer and Communication Engineering Technology*. Berlin, Germany: Springer, 2015, pp. 949–962.

[33] S. R. Curtis, P. Rajivan, D. N. Jones, and C. Gonzalez, "Phishing attempts among the dark triad: Patterns of attack and vulnerability," *Comput. Hum. Behav.*, vol. 87, pp. 174–182, Oct. 2018.

[34] J. Wang, T. Herath, R. Chen, A. Vishwanath, and H. R. Rao, "Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email," *IEEE Trans. Prof. Commun.*, vol. 55, no. 4, pp. 345–362, Dec. 2012.

[35] R. Stuart-Kotze, *Performance: The Secrets of Successful Behaviour*. London, U.K.: Pearson Education, 2006.

[36] C. N. Lorian, N. Titov, and J. R. Grisham, "Changes in risk-taking over the course of an Internet-delivered cognitive behavioral therapy treatment for generalized anxiety disorder," *J. Anxiety Disorders*, vol. 26, no. 1, pp. 140–149, Jan. 2012.

[37] R. Adolphs, "Cognitive neuroscience of human social behaviour," *Nature Rev. Neurosci.*, vol. 4, no. 3, pp. 165–178, Mar. 2003.

[38] A. Bateman, Peter, and P. Fonagy, *Psychotherapy for Borderline Personality Disorder*. Oxford, U.K.: Oxford Univ. Press, 2004.

[39] H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Comput. Secur.*, vol. 28, no. 8, pp. 816–826, Nov. 2009.

[40] M. Abdelhamid, "The role of health concerns in phishing susceptibility: Survey design study," *J. Med. Internet Res.*, vol. 22, no. 5, May 2020, Art. no. e18394.

[41] R. Ayyagari and A. Crowell, "Risk and demographics' influence on security behavior intentions," *J. Southern Assoc. Inf. Syst.*, vol. 7, no. 1, pp. 1–13, 2020.

[42] C. M. White, M. Gummerum, S. Wood, and Y. Hanoch, "Internet safety and the silver surfer: The relationship between gist reasoning and adults' risky online behavior," *J. Behav. Decis. Making*, vol. 30, no. 4, pp. 819–827, 2017.

[43] E. J. Williams, A. Beardmore, and A. N. Joinson, "Individual differences in susceptibility to online influence: A theoretical review," *Comput. Hum. Behav.*, vol. 72, pp. 412–421, Jul. 2017.

[44] J. Van Wyk and M. L. Benson, "Fraud victimization: Risky business or just bad luck?" *Amer. J. Criminal Justice*, vol. 21, no. 2, pp. 163–179, Mar. 1997.

[45] K. Holtfreter, M. D. Reisig, T. C. Pratt, and R. E. Holtfreter, "Risky remote purchasing and identity theft victimization among older Internet users," *Psychol., Crime Law*, vol. 21, no. 7, pp. 681–698, Aug. 2015.

[46] S. Lea, P. Fischer, and K. Evans. (2009). *The Psychology of Scams: Provoking and Committing Errors of Judgement*. [Online]. Available: https://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

[47] E. L. Glisky, "Changes in cognitive function in human aging," in *Brain Aging: Models, Methods, and Mechanisms*. Boca Raton, FL, USA: CRC Press, 2007, pp. 3–20.

[48] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "Phishing for the truth: A scenario-based experiment of users' behavioural response to emails," in *Proc. IFIP Int. Inf. Secur. Conf.* Auckland, New Zealand: Springer, 2013, pp. 366–378.

[49] A. N. Shaikh, A. M. Shabut, and M. A. Hossain, "A literature review on phishing crime, prevention review and investigation of gaps," in *Proc. 10th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*, Dec. 2016, pp. 9–15.

[50] A. Zamir, H. U. Khan, T. Iqbal, N. Yousaf, F. Aslam, A. Anjum, and M. Hamdani, "Phishing Web site detection using diverse machine learning algorithms," *Electron. Library*, vol. 38, no. 1, pp. 65–80, 2020.

[51] M. S. Jalali, M. Bruckes, D. Westmattelmann, and G. Schewe, "Why employees (still) click on phishing links: Investigation in hospitals," *J. Med. Internet Res.*, vol. 22, no. 1, 2020, Art. no. e16775.

[52] D. M. Sarno, J. E. Lewis, C. J. Bohil, M. K. Shoss, and M. B. Neider, "Who are phishers luring?: A demographic analysis of those susceptible to fake emails," in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 61, no. 1. Los Angeles, CA, USA: Sage, 2017, pp. 1735–1739.

[53] C. W. Lejuez, J. P. Read, C. W. Kahler, J. B. Richards, S. E. Ramsey, G. L. Stuart, D. R. Strong, and R. A. Brown, "Evaluation of a behavioral measure of risk taking: The balloon analogue risk task (BART)," *J. Experim. Psychol., Appl.*, vol. 8, no. 2, p. 75, 2002.

[54] A.-R. Blais and E. U. Weber, "A domain-specific risk-taking (DOSPERT) scale for adult populations," *Judgment Decis. Making*, vol. 1, no. 1, pp. 1–15, 2006.

[55] S. G. Scott and R. A. Bruce, "Decision-making style: The development and assessment of a new measure," *Educ. Psychol. Meas.*, vol. 55, no. 5, pp. 818–831, 1995.

[56] M. H. Birnbaum, "Human research and data collection via the Internet," *Annu. Rev. Psychol.*, vol. 55, no. 1, pp. 803–832, Feb. 2004.

[57] F. Dandurand, T. R. Shultz, and K. H. Onishi, "Comparing online and lab methods in a problem-solving experiment," *Behav. Res. Methods*, vol. 40, no. 2, pp. 428–434, May 2008.

[58] B. E. Hilbig, "Reaction time effects in lab-versus Web-based research: Experimental evidence," *Behav. Res. Methods*, vol. 48, no. 4, pp. 1718–1724, 2016.

[59] B. Pakzad and G. Ghassemi, "Cybercrimes in Iran: Perspectives, policies and legislations," in *Proc. ISP C*, 2012, p. 139.

[60] A. 19. (2020). *Computer Crimes in Iran: Online Repression in Practice*. Accessed: Apr. 11, 2020. [Online]. Available: https://www.article19.org/data/files/medialibrary/38039/Risky-Online-Behaviour–final-English.pdf

[61] C. Soghoian, "Legal risks for phishing researchers," in *Proc. eCrime Res. Summit*, Oct. 2008, pp. 1–11.

[62] P. Finn and M. Jakobsson, "Designing and conducting phishing experiments," *IEEE Tech. Soc. Mag.*, vol. 26, no. 1, pp. 46–58, 2007.

[63] R. S. El-Din and L. Sugiura, "To deceive or not to deceive! Legal implications of phishing covert research," *Int. J. Intellectual Property Manage.*, vol. 6, no. 4, pp. 285–293, 2013.

[64] F. Hassandoust, H. Singh, and J. Williams, "The role of contextualization in users vulnerability to phishing attempts," *Australas. J. Inf. Syst.*, vol. 24, Sep. 2020, doi: 10.3127/ajis.v24i0.2693.

[65] D. B. Resnik and P. R. Finn, "Ethics and phishing experiments," *Sci. Eng. Ethics*, vol. 24, no. 4, pp. 1241–1252, Aug. 2018.

[66] MSRT Ministry of Science Research and Technology. *Statistics-2019*. Accessed: Sep. 21, 2020. [Online]. Available: https://www.msrt.ir/en/page/20/statistics-2019

[67] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, no. 2, pp. 1–31, May 2010.
[68] F. Parsa. *The Role of Women in Building Iran's Future*. Middle East Institute. Accessed: Sep. 21, 2020. [Online]. Available: https://www.mei.edu/publications/role-women-building-irans-future
[69] Z. M. Elmi, "Educational attainment in Iran," *The Middle East Institute Viewpoints: The Iranian Revolution at 30*. Jan. 2009, pp. 62–69.
[70] ICEF. (2021). *Iran's University Enrolment is Booming. Now What?* Accessed: Feb. 12, 2021. [Online]. Available: https://monitor.icef.com/2015/12/irans-university-enrolment-is-booming-now-what/
[71] B. Lang, "A comparison of risk-taking measures," *J. Undergraduate Res.*, vol. 11, no. 1, p. 3, 2011, Art. no. 3.
[72] S. Mishra, M. L. Lalumière, and R. J. Williams, "Gambling as a form of risk-taking: Individual differences in personality, risk-accepting attitudes, and behavioral preferences for risk," *Personality Individual Differences*, vol. 49, no. 6, pp. 616–621, Oct. 2010.
[73] T. J. Crowley, K. M. Raymond, S. K. Mikulich-Gilbertson, L. L. Thompson, and C. W. Lejuez, "A risk-taking 'set' in a novel task among adolescents with serious conduct and substance problems," *J. Amer. Acad. Child Adolescent Psychiatry*, vol. 45, no. 2, pp. 175–183, 2006.
[74] O. Schürmann, R. Frey, and T. J. Pleskac, "Mapping risk perceptions in dynamic risk-taking environments," *J. Behav. Decis. Making*, vol. 32, no. 1, pp. 94–105, Jan. 2019.
[75] H. Alqahtani and M. Kavakli-Thorne, "Does decision-making style predict individuals' cybersecurity avoidance behaviour?" in *HCI for Cybersecurity, Privacy and Trust*. Cham, Switzerland: Springer, 2020, pp. 32–50.
[76] J. Nicholson, Y. Javed, M. Dixon, L. Coventry, O. D. Ajayi, and P. Anderson, "Investigating teenagers' ability to detect phishing messages," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, Sep. 2020, pp. 140–149.
[77] D. E. Beaton, C. Bombardier, F. Guillemin, and M. B. Ferraz, "Guidelines for the process of cross-cultural adaptation of self-report measures," *Spine*, vol. 25, no. 24, pp. 3186–3191, Dec. 2000.
[78] C. Acquadro, K. Conway, A. Hareendran, and N. Aaronson, "Literature review of methods to translate health-related quality of life questionnaires for use in multinational clinical trials," *Value Health*, vol. 11, no. 3, pp. 509–521, May 2008.
[79] O. Behling and K. S. Law, *Translating Questionnaires and Other Research Instruments: Problems and Solutions*. Newbury Park, CA, USA: Sage, 2000.
[80] R. B. Kline, *Principles and Practice of Structural Equation Modeling*. New York, NY, USA: Guilford Publications, 2015.
[81] B. M. Byrne, *Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming* (Multivariate Applications Series), vol. 396. New York, NY, USA: Taylor & Francis Group, 2010, p. 7384.
[82] M. Koscielniak, K. Rydzewska, and G. Sedek, "Effects of age and initial risk perception on balloon analog risk task: The mediating role of processing speed and need for cognitive closure," *Frontiers Psychol.*, vol. 7, p. 659, May 2016.
[83] E. U. Weber, A.-R. Blais, and N. E. Betz, "A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors," *J. Behav. Decis. Making*, vol. 15, no. 4, pp. 263–290, 2002.
[84] M. Tischer, Z. Durumeric, E. Bursztein, and M. Bailey, "The danger of USB drives," *IEEE Secur. Privacy*, vol. 15, no. 2, pp. 62–69, Mar. 2017.
[85] S. Bandi, "An empirical assessment of user online security behavior: Evidence from a university," M.S. thesis, Univ. Maryland, College Park, MD, USA, 2016.
[86] M. Dove, "Predicting individual differences in vulnerability to fraud," Doctoral thesis, Dept. Psychol., Univ. Portsmouth, Portsmouth, U.K., Feb. 2018.
[87] B. Al-Ansari, A.-M. Thow, M. Mirzaie, C. A. Day, and K. M. Conigrave, "Alcohol policy in Iran: Policy content analysis," *Int. J. Drug Policy*, vol. 73, pp. 185–198, Nov. 2019.
[88] M. Tamadonfar and R. B. Lewis, "Religious regulation in Iran," in *Oxford Research Encyclopedia of Politics*. London, U.K.: Oxford Univ. Press, 2019.
[89] R. Fallahchai, M. Fallahi, and M. Badiee, "Intent, attitudes, expectations, and purposes of marriage in Iran: A mixed methods study," *Current Psychol.*, pp. 1–11, Oct. 2019, doi: 10.1007/s12144-019-00477-6.
[90] D. P. Spicer and E. Sadler-Smith, "An examination of the general decision making style questionnaire in two UK samples," *J. Managerial Psychol.*, vol. 20, no. 2, pp. 137–149, Mar. 2005.
[91] R. Loo, "A psychometric evaluation of the general decision-making style inventory," *Personality Individual Differences*, vol. 29, no. 5, pp. 895–905, Nov. 2000.
[92] T. Gnambs. (2019). *Balloon Analogue Risk Task (BART)*. Accessed: May 1, 2019 [Online]. Available: https://timo.gnambs.at/research/bart
[93] *IBM SPSS Statistics for Windows*, IBM Corp, Armonk, NY, USA, 2017.
[94] H. E. A. Tinsley and D. J. Tinsley, "Uses of factor analysis in counseling psychology research," *J. Counseling Psychol.*, vol. 34, no. 4, pp. 414–424, Oct. 1987, doi: 10.1037/0022-0167.34.4.414.
[95] J. C. Anderson and D. W. Gerbing, "Structural equation modeling in practice: A review and recommended two-step approach," *Psychol. Bull.*, vol. 103, no. 3, p. 411, May 1988.
[96] L. Ding, W. F. Velicer, and L. L. Harlow, "Effects of estimation methods, number of indicators per factor, and improper solutions on structural equation modeling fit indices," *Struct. Equation Model., Multidisciplinary J.*, vol. 2, no. 2, pp. 119–143, Jan. 1995, doi: 10.1080/10705519509540000.
[97] B. G. Tabachnick, L. S. Fidell, and J. B. Ullman, *Using Multivariate Statistics*. Boston, MA, USA: Pearson, 2007.
[98] P. M. Bentler and C.-P. Chou, "Practical issues in structural modeling," *Sociol. Methods Res.*, vol. 16, no. 1, pp. 78–117, Aug. 1987, doi: 10.1177/0049124187016001004.
[99] H. E. A. Tinsley and R. A. Kass, "The latent structure of the need satisfying properties of leisure activities," *J. Leisure Res.*, vol. 11, no. 4, pp. 278–291, Sep. 1979.
[100] A. Field, *Discovering Statistics Using IBM SPSS Statistics*. Newbury Park, CA, USA: Sage, 2013.
[101] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham, *Multivariate Data Analysis*, no. 3. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.
[102] B. M. Byrne, "Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument," *Int. J. Test.*, vol. 1, no. 1, pp. 55–86, Mar. 2001.
[103] P. R. Hinton, I. McMurray, and C. Brownlow, *SPSS Explained*. Evanston, IL, USA: Routledge, 2014.
[104] J. Pallant, *SPSS Survival Manual*. New York, NY, USA: McGraw-Hill Education, 2013.
[105] J. F. Hair, R. E. Anderson, B. J. Babin, and W. C. Black, *Multivariate Data Analysis: A Global Perspective*, vol. 7. Upper Saddle River, NJ, USA: Pearson, 2010.
[106] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *J. Appl. Psychol.*, vol. 88, no. 5, p. 879, 2003.
[107] H. A. Richardson, M. J. Simmering, and M. C. Sturman, "A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance," *Organizational Res. Methods*, vol. 12, no. 4, pp. 762–800, Oct. 2009.
[108] C. R. Mehta and N. R. Patel, "Exact logistic regression: Theory and examples," *Statist. Med.*, vol. 14, no. 19, pp. 2143–2160, Oct. 1995.
[109] M. Powell and D. Ansic, "Gender differences in risk behaviour in financial decision-making: An experimental analysis," *J. Econ. Psychol.*, vol. 18, no. 6, pp. 605–628, Nov. 1997.
[110] P. T. Costa, A. Terracciano, and R. R. McCrae, "Gender differences in personality traits across cultures: Robust and surprising findings," *J. Personality social Psychol.*, vol. 81, no. 2, p. 322, 2001.
[111] CISA Department of Homeland Security. (2019). *Virus Basics*. Accessed: Apr. 7, 2020. [Online]. Available: https://www.us-cert.gov/publications/virus-basics
[112] National Cyber Security Centre (NCSC). (2019). *Email Security and Anti-Spoofing*. Accessed: Mar. 15, 2020. [Online]. Available: https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing
[113] G. Draper-Gil and I. Sanchez, "My email communications security assessment (MECSA): 2018 results," EUR 29674 EN, Publications Office Eur. Union, Luxembourg, Tech. Rep. JRC115217, 2019, doi: 10.2760/166203.
[114] D. MacFarlane, M. J. Hurlstone, and U. K. H. Ecker, "Protecting consumers from fraudulent health claims: A taxonomy of psychological drivers, interventions, barriers, and treatments," *Social Sci. Med.*, vol. 259, Aug. 2020, Art. no. 112790.

[115] S. Stahly, K. Fertig, and D. Miller, "Phishing for users," in *Proc. Midwest Instruct. Comput. Symp.*, 2017. [Online]. Available: http://www.micsymposium.org/mics_2017_proceedings/docs/MICS_2017_paper_41.pdf
[116] Pentestgeek. (2019). *How do I Phish?—Advanced Email Phishing Tactics*. Accessed: Apr. 15, 2020. [Online]. Available: https://www.pentestgeek.com/phishing/how-do-i-phish-advanced-email-phishing-tactics
[117] S. Waterman. *Hackers Using Pixel Tracking to Build Data for Better Phishing Practices*. CYBERSCOOP. Accessed: Mar. 16, 2020. [Online]. Available: https://www.cyberscoop.com/pixel-tracking-hacking-checkpoint/
[118] J. Thomas, "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks," *Int. J. Bus. Manage.*, vol. 12, no. 3, pp. 1–23, 2018.
[119] TrendLabsSM. (2021). *Spear-Phishing Email: Most Favored APT Attack Bait*. Accessed: Feb. 12, 2021. [Online]. Available: https://www.trendmicro.nl/media/misc/spear-phishing-email-apt-attack-research-paper-en.pdf
[120] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing: Exploring user research through a systematic literature review," 2019, *arXiv:1908.05897*. [Online]. Available: http://arxiv.org/abs/1908.05897
[121] A. Binks, "The art of phishing: Past, present and future," *Comput. Fraud Secur.*, vol. 2019, no. 4, pp. 9–11, Apr. 2019.
[122] S. Chanti and T. Chithralekha, "Classification of anti-phishing solutions," *Social Netw. Comput. Sci.*, vol. 1, no. 1, p. 11, Jan. 2020.
[123] S. Mansfield-Devine, "The ever-changing face of phishing," *Comput. Fraud Secur.*, vol. 2018, no. 11, pp. 17–19, Nov. 2018.
[124] S. I. Popoola, S. O. Ojewande, F. O. Sweetwilliams, S. John, and A. Atayero, "Ransomware: Current trend, challenges, and research directions," in *Proc. World Congr. Eng. Comput. Sci.*, San Francisco, CA, USA, vol. 1, 2017, pp. 169–174.
[125] CISA Department of Homeland Security. (2019). *Ransomware*. Accessed: Jul. 4, 2020. [Online]. Available: https://www.us-cert.gov/Ransomware
[126] F. Schulte, *Fleeced!: Telemarketing Rip-offs and How to Avoid Them*. Amtierst, NY, USA: Prometheus Books, 1995.
[127] J. Chen and C. Guo, "Online detection and prevention of phishing attacks," in *Proc. 1st Int. Conf. Commun. Netw. China*, Oct. 2006, pp. 1–7.
[128] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Syst. Appl.*, vol. 117, pp. 345–357, Mar. 2019.
[129] M. Reddy, "Intelligent phishing website detection and prevention system by using link guard algorithm," *IOSR J. Comput. Eng.*, vol. 14, no. 3, pp. 28–36, Sep./Oct. 2013.
[130] Microsoft. (2020). *ATP Safe Links*. Accessed: Jul. 4, 2020. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links?view=o365-worldwide
[131] S. Fischer and G. T. Smith, "Deliberation affects risk taking beyond sensation seeking," *Personality Individual Differences*, vol. 36, no. 3, pp. 527–537, 2004.
[132] A. J. Winzelberg, D. Eppstein, K. L. Eldredge, D. Wilfley, P. Dev, R. Dasmahapatra, and C. B. Taylor, "Effectiveness of an Internet-based program for reducing risk factors for eating disorders," *J. Consulting Clin. Psychol.*, vol. 68, no. 2, p. 346, 2000.
[133] L. A. Kiropoulos, B. Klein, D. W. Austin, K. Gilson, C. Pier, J. Mitchell, and L. Ciechomski, "Is Internet-based CBT for panic disorder and agoraphobia as effective as face-to-face CBT?" *J. Anxiety Disorders*, vol. 22, no. 8, pp. 1273–1284, Dec. 2008.
[134] C. Parulekar, "Minimize phishing attacks: Securing spear attacks," *Int. Res. J. Eng. Technol.*, vol. 6, no. 6, pp. 3054–3058, 2019.
[135] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," presented at the SIGCHI Conf. Hum. Factors Comput. Syst., Montreal, QC, Canada, 2006.
[136] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Lessons from a real world evaluation of anti-phishing training," in *Proc. eCrime Researchers Summit*, Oct. 2008, pp. 1–12.
[137] W. Fan and Z. Yan, "Factors affecting response rates of the Web survey: A systematic review," *Comput. Hum. Behav.*, vol. 26, no. 2, pp. 132–139, Mar. 2010.
[138] C. Steinmetz, S. Thompson, and N. Marshall, "Surveying international university students: The case of the 5% response rate," *Issues Educ. Res.*, vol. 30, no. 3, pp. 1105–1125, 2020.
[139] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. Automated cybersecurity anti-phishing techniques," *Comput. Sci. Rev.*, vol. 29, pp. 44–55, Aug. 2018.
[140] M. Adil and A. Alzubier. (2019). *A Review on Phishing Website Detection*. EasyChair. Accessed: Apr. 15, 2020. [Online]. Available: https://easychair.org/publications/preprint/m2gw
[141] T. Thakur and R. Verma, "Catching classical and hijack-based phishing attacks," in *Proc. Int. Conf. Inf. Syst. Secur.* Cham, Switzerland: Springer, 2014, pp. 318–337.
[142] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An empirical analysis of phishing blacklists," in *Proc. 6th Conf. Email Anti-Spam*, Mountain View, CA, USA, Jul. 2009.
[143] R. Fishkin. (2019). *12 Ways to Keep Your Content Hidden From the Search Engines*. Accessed: Mar. 15, 2020. [Online]. Available: https://moz.com/blog/12-ways-to-keep-your-content-hidden-from-P. Devthe-search-engines
[144] J. B. Killoran, "How to use search engine optimization techniques to increase website visibility," *IEEE Trans. Prof. Commun.*, vol. 56, no. 1, pp. 50–66, Mar. 2013.

HOSSEIN ABROSHAN received the master's degree in business administration. He is currently pursuing the Ph.D. degree with Ghent University. He has over 20 years of experience in the IT and information security fields in financial, telecom, maritime, manufacturing, and research sectors. He also worked as a university Lecturer, teaching internet engineering, information security, and expert systems. He holds several professional certifications, including Certified Information Security Manager (CISM) and ISO 27001 Lead Auditor. He has had a technical and management roles on numerous cyber-security and data protection projects. His research interests include social engineering and psychological aspects of cyber-security.

JAN DEVOS received the master's degree in engineering and applied mathematics from KU Leuven, in 1984, the M.B.A. degree from Vlerick Leuven Gent Management School, in 1992, and the Ph.D. degree in engineering from Ghent University, in 2011. He is currently an Assistant Professor with the Faculty of Architecture and Engineering, Ghent University. He is also an Associated Professor with the Faculty of Economics and Business Administration. He has published several articles on IT and SMEs. His current research interests include IT governance in SME's, design science, IS failures, and IT Security. He was a speaker at international academic and business conferences, which proceedings are published in different Springer series of LNBIP and AICT.

GEERT POELS is currently a Full Professor of Management Information Systems with the Faculty of Economics and Business Administration, Ghent University, Gent, Belgium, where he teaches intermediate and advanced courses on information systems, IT management, enterprise architecture, and service design. He also teaches with the Master of Enterprise ICT Architecture, IC Institute, Belgium. He supervises Ph.D. research on digital marketplaces, cyber-security, and GDPR. As academic service, he co-developed the COBIT 2019 framework for IT governance. His recent research interests include conceptual modeling (as research method) and enterprise modeling (as research domain) with a focus on business process architecture mapping, ArchiMate, value modeling, and NLP-based automated generation of conceptual models out of user requirements documents.

ERIC LAERMANS (Member, IEEE) received the master's degree in engineering physics and the Ph.D. degree in electrical engineering from Ghent University, Belgium, in 1994 and 1999, respectively. He is currently a Professor with the IDLab, Ghent University, Belgium, in collaboration with imec. His research interests include electromagnetic modeling of high-speed interconnection structures (with special attention to via holes) and reverberation chambers to data analysis and machine learning, more specifically, surrogate modeling and experimental design.