IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 7, 2021, accepted August 28, 2021, date of publication August 30, 2021, date of current version September 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3109091

COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic

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

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

This work involved human subjects or animals in its research. The authors confirm that all human/animal subject research procedures and protocols are exempt from review board approval.

ABSTRACT Phishing is an online scam where criminals trick users with various strategies, with the goal of obtaining sensitive information or compromising accounts, systems, and/or other personal or organisational Information Technology resources. Multiple studies have shown that human factors influence the success of phishing attempts. However, these studies were conducted before the COVID-19 pandemic, which is significant because security reports show that the numbers of phishing attacks have been rapidly increasing since the start of COVID-19. This study investigates the extent to which users' fear, anxiety and stress levels regarding COVID-19, impact falling for common and COVID-19 themed phishing scams during the outbreak period. Prior studies have depicted the effects of human behaviour on phishing attacks before the pandemic, such as risk-taking preferences and users' demographic factors, hence this study also focuses on the effects of those factors on the likelihood of phishing victimisation. More concretely, we present the results of a scenario-based roleplay experiment to study the relationship between fear, anxiety, stress, risk-taking, and demographic factors and the success of phishing attacks during the pandemic. The findings indicate that fear of COVID-19 influences the success of COVID-19 specific themed phishing scams, while anxiety, stress, and risk-taking influences the success of both the COVID-19 themed and common phishing scams. Our findings also suggest that the users' education level impacts common phishing attacks during the pandemic.

INDEX TERMS Cyber security, phishing, human behavior, COVID-19, online scams.

I. INTRODUCTION

As individuals become more dependent on online services, such as e-shopping, e-government, online meetings, and various other forms of inter-personal interaction, they also become vulnerable to online fraud. This is demonstrated by statistics such as the fact that approximately 26 billion dollars' worth of losses due to Business E-mail Compromise (BEC) attacks were reported in 2019 [1]. One of the main cybersecurity challenges facing individuals and business is email security, as reports show 94% of malware was delivered via email and 32% of breaches involved phishing [2]. A phishing attack is a social engineering technique to steal users' sensitive information [3] and/or perform other attacks such as ransomware. The scammers involved in such action typically adopt different technical and psychological techniques [4] to convince the victim to click on a phishing link. Often, opening a phishing link opens a phishing website, asking the user to enter their sensitive information, or leads the user to an attachment including a link to a phishing website, or perhaps displays a fake invoice or a built-in malware.

Phishing attack numbers have been on a steady increase since the acceleration of the COVID-19 outbreak, starting from late 2019 [5]–[7]. Cyber attackers have taken advantage of the pandemic to target susceptible victims, using information and buzzwords that are specific to the virus.

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

For instance, users may receive emails with important and updated information about the Coronavirus situation in their location, with notices from international or national reliable health organisations, regarding self or family protection information [8]. This begs the question; what is the fundamental reason pushing users to click on phishing links or open attachments? Past studies investigated psychological and demographic root-causes of falling into phishing traps, such as risk-taking behaviour, decision making style, gender, age, and other human differences [4], [9]. These psychological factors are some of the root-causes of successful phishing attacks in the normal situation pre-COVID-19, but are there any specific reasons as to why people respond more to phishing in situations such as the pandemic?

In this paper, we have investigated the impacts of the COVID-19 outbreak on psychological factors, upon identifying that a change in these factors may be the reason for increased engagement with such phishing scams. Our research culminated in a survey with the intent to establish associations between clicking on common and COVID-19 themed phishing emails, and the possible psychological and demographic causes.

II. BACKGROUND AND RELATED WORK

It has been firmly established that cyber attackers use psychological techniques to design a phishing process that compromises victims. A person who is willing to take financial risks holds the potential to be an appropriate target for a financial phishing attack [10]–[12]. When an attacker incites a user to take immediate action, for instance, asking the user to enter their credentials so that the person's email account will not be disabled, the user may not pay sufficient attention to the phishing signs (such as the email sender, e.g., ''account-security-noreply@account protection-microsoft.com'' instead of ''account-security-noreply@accountprotection.microsoft.com''). Phishers often use ''time pressure'', or other psychological techniques, to reduce the user's cognitive resources, so that the user does not pay enough attention to the phishing email's clues to notice the discrepancies in their email, and rather, quickly responds to the phisher's request [13], [14]. Prior studies imply that personality traits can impact successful phishing detection [15]–[17]. For instance, a phisher can get the attention of the user by triggering their fears or desires, compelling the user to respond to the phisher's demands [18]. Effects of emotions such as anxiety, on the success of phishing scams and users, and thus the susceptibility to phishing, have been shown by several researchers [19]–[22]. However, a study found that a higher level of fear arousal may decrease response rate to a phishing attack, as the users' response may be influenced by the fear of providing login credentials to the scammer [22], but this depends on many factors, including the user's prior knowledge of phishing. Moreover, other fears such as fear of death, health problems, etc. that may have been aroused by the phishing content (e.g., a phishing email warns the user about a severe issue, such as a virus that is threatening people's lives), have not been considered by existing studies.

Hence, users' behaviour, in general, has the ability to impact the success of a phishing attack. We now turn to the scenario of a pandemic, in which the user's life and psychological wellbeing are under dramatic impact by a health crisis that has the potential to harm themselves and their families and friends' lives. Previous studies have neglected such situations in their discussions. COVID-19, first identified in China 2019, spread far and wide into neighbouring countries and eventually all over the world [23]. The number of the infected and deceased rapidly increased, and according to European Centre for Disease Prevention and Control (ECDC), since 31 December 2019 and as of early June 2021, over 174 million cases of COVID-19 have been reported and over 3.7 million of these individuals have passed away [24]. So, it is understandable and plausible that many people are afraid of infection with deadly impacts, or permanent debilitating, long-term health conditions. Surely, this fear and anxiety can cause other mental issues [25]. A study on 7,143 college students showed that around 24.9 percent of them experienced anxiety because of the COVID-19 situation [26]. Moreover, we can see that these psychological impacts were present even before the COVID-19 pandemic, for instance the prevalence of psychological distress issues when people had movement restrictions and were in quarantine during Australia's 2007 outbreak of equine influenza [27]. A study reviewed 3,166 publications related to the psychological impact of quarantine related to SARS, Ebola, the 2009 and 2010 H1N1 influenza pandemic, Middle East respiratory syndrome, and equine influenza, across 10 countries and found that the most reviewed studies reported negative psychological effects on people during those situations. The impacts included post-traumatic stress symptoms, confusion, and anger [28].

Several studies found that the pandemic has increased the level of psychological issues such as anxiety, stress, and fear of COVID-19 [29]–[37]. Phishers use the knowledge that people are expecting messages, news, alerts, etc. relating to the virus, and take advantage of this vulnerability to trick the users into clicking on phishing links or open malicious attachments. So, during the pandemic, users received both the common phishing emails (e.g., user password reset, charity donation, improved service, etc. [38]) and COVID-19 themed phishing emails (e.g., offering fast infection-tests, products to treat or prevent the disease, etc. [39]). Several studies explored the phishing issue during the pandemic [40]–[43]. Researchers have shown associations between users' behaviour, such as risk-taking, and common phishing attacks [4], [10], [44]–[46]. In accordance with the aforementioned analysis, the impact of users' traits and emotions, such as anxiety and fear, on the success of common phishing scams was also studied by researchers [44], [47]–[52], but to our knowledge, there is no study on the effects of these factors on phishing attacks

during the pandemic. To fill these knowledge gaps, the main questions of this research are:

- Are the psychological factors caused by COVID-19 (e.g., anxiety, stress, and fear of the virus) a reason why people fall for COVID-19 themed phishing scams? If so, do these factors also have an impact on user susceptibility to common phishing scams?
- Do the users' behaviour, such as risk-taking, still have an impact on falling victim to phishing emails during COVID-19?

Given that psychological factors can affect phishing attacks and considering the effects of COVID-19 on increasing peoples' anxiety, stress, and fear; and because evidence shows that phishing attempts have increased during COVID-19, we formulate the following hypothesis:

H1: Increasing anxiety, stress, and fear levels due to COVID-19 might increase the probability of falling for the COVID-19 themed and common phishing scams.

According to the Prospect Theory [53], [54] people's judgments and choices can be influenced by gains or losses. This theory explains how people might seek or avoid risk in their decision making under an uncertain situation (e.g., the COVID-19 crisis). Thus, users weigh the potential gains and losses of clicking on a link inside an email. As Kahneman and Tversky [53] suggested, people prefer the risk of loss over a sure loss. For instance, a user might click on a COVID-19 phishing link, in the pandemic situation, even if it is suspicious and this might lead to a money loss. They will still do so as they believe that the guaranteed loss when not clicking on the link could potentially be missing out on opportunities to prevent virus infection or even death. Given that the users' risk-taking level that COVID-19 can influence might impact a phishing attempt in the pandemic, we formulate the following hypothesis:

H2: General risk-taking level and/or a risk-taking preference (in one or more risk-taking domains) of people, can increase users' phishability[1] level of both the COVID-19 themed and common phishing scams, even during the pandemic.

Several studies show the effects of demographic factors, such as age, gender, and education on phishing attacks [10], [56]–[59]. We also want to investigate if these factors influence the success of phishing scams, both COVID-19 related phishing and common phishing, during the pandemic. So, we formulated the following hypothesis:

H3: Demographic factors (i.e., age, gender and education) have an impact on the result of the COVID-19 themed and common phishing attacks during the pandemic.

Figure 1 presents our research model which shows the selected behavioural, emotional, and demographic variables that are hypothesized to influence the phishability of a user (i.e., falling for a common and COVID-19 themed phishing attacks) during the pandemic. As illustrated in figure 1, the effects of stress, fear, and anxiety (H1), risk-taking (H2), and demographic (H3) factors on the success of both common and COVID-19 themed phishing emails will be investigated in this study. The research methods to measure these variables and to collect and analyze these data are explained in the next section.

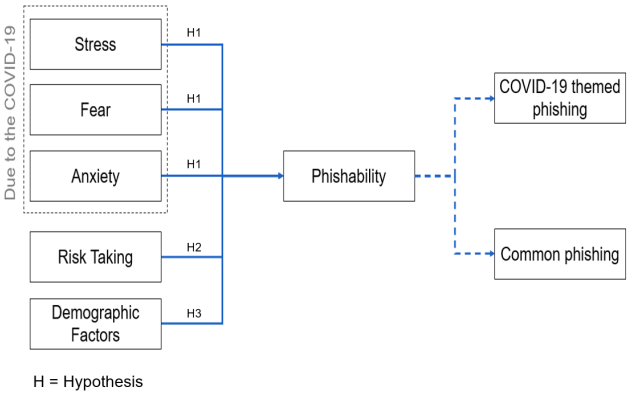

FIGURE 1. Research model.

III. METHODS

The aim of this research was to investigate the effects of increasing users' anxiety, stress, and fear caused by COVID-19 on the result of phishing attacks during the pandemic. We also aimed to find relations between users' general risk-taking, domain specific risk-taking preferences, and demographics on the success of COVID-19 and common phishing attacks in the coronavirus outbreak.

In this study, participants completed a roleplay task to measure their phishability by showing them 15 emails and asking them to identify which ones are COVID-19 phishing, common phishing, or legitimate emails. We also asked the participants to answer some questions related to demographics. The participant's COVID-19 anxiety, stress, and fear levels were measured by asking them to answer 48 questions of the Coronavirus Anxiety Scale (CAS), the Fear of COVID-19 Scale (FCV-195), and the COVID Stress Scale (CSS). We finally asked them to answer 31 questions to measure their domain specific risk-taking and general risk-taking levels by means of the Domain-Specific Risk-Taking (DOSPERT) and Dohmen risk-taking measures. We used Unipark[2] as our online survey tool.

A. RECRUITMENT

Participants were recruited through Amazon Mechanical Turk (MTurk[3]), a crowdsourcing marketplace that can be used to outsource tasks to those who can perform them virtually. There were some reasons of recruiting the participants through MTurk, such as:

- It broadly used for behavioural research [60], 61]

[1] "The likelihood of falling into phishing traps and becoming the victim of a phishing attack" [55].

[2] https://www.unipark.com
[3] https://www.mturk.com

- Samples are more varied than many other samples, such as university students [61], [62]
- We needed participants who regularly use the Internet and email. MTurk users meet this requirement [63].
- Our goal was to conduct a culture and country independent study, and on Internet users above 18 years old. MTruk users meet these requirements [64], [65].
- A previous study showed stability of participant demographics on the MTurk platform during the COVID-19 pandemic [66].

We, as the requester, posted the tasks under the category, HIT (Human Intelligence Tasks), and participants, as the ''workers'' who matched our qualification criteria, could complete the HIT. We paid 2 US dollars to those who completed the study and passed our qualification control. The qualification control method is explained in the following.

We told the participants that the aim of this questionnaire is to analyse how different people manage their emails. We asked the Workers to enter their Amazon worker ID at the first page. We also displayed a code at the end of the survey and asked them to enter the code on their MTurk dashboard to receive the survey credit. In total, 240 persons participated the survey but 42 of them failed the quality assessment. This resulted in a final sample size of 198.

The participants' data were anonymised. There was no link between participant's answers to the survey questions and their personal information, except their Amazon worker ID in the Unipark platform. The Unipark has a personal data protection feature that make a survey fully GDPR (General Data Protection Regulation)[4] compliant. We deleted all worker IDs from the Unipark platform right after conducting the qualification control and deleted all data after completing the study analyses. We debriefed the participants about the study and informed them that their data will be anonymised.

Qualification Control: To consider only participants who paid attention to the emails and questions, thus improving the reliability of the data, we performed a qualification control. We informed the participants that they need to carefully read the emails and appropriately answer the question for each mail (see section 3.2) to receive the credit in MTurk. After they answered this question for each email presented to them, we asked them to answer three multiple choice questions. One of the questions was very simple, ''who was the emails' recipient?'' (to which the correct answer was ''Alex''). The second and third questions were about the content of the emails. We qualified those who correctly answered two questions, as we felt that a person who carefully reads the emails could answer at least two of the mentioned questions. We asked them to answer the demographic questions beforehand, to reduce the likelihood of identifying the qualification control questions [67].

[4] https://ec.europa.eu/info/law/law-topic/data-protection_en

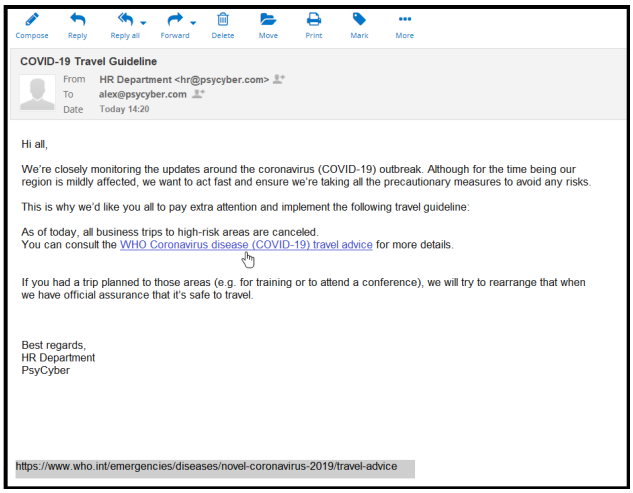

FIGURE 2. A legitimate email example.

B. ROLEPLAY

The participants were presented with images of emails and asked to identify how they would likely respond to the emails. They could choose one of four response options (see section 3.4.1). We asked them to play the role of 'Alex', an imaginary employee at Psycyber company. A total of 15 emails were shown, and they were instructed to decide how they would handle each one of them if they received these emails in their personal inbox, in real life. We asked them to choose the most appropriate answer, as the study data will be anonymised.

The 15 emails we created, were 5 COVID-19 related phishing emails, 5 common phishing emails, and 5 legitimate emails (each of them in the appropriate style), based on real phishing and regular email examples posted on different websites such as microsoft.com, google.com, who.int, cdc.gov, cisa.gov, and kaspersky.com. We registered psycyber.com as a domain name and created alex@psycyber.com email account. Henceforth, all emails for assessment were sent to this email address from various senders. Table 1 shows the emails subjects, their order, and their categories.

As presented in Table 1, the relation with COVID-19 / the coronavirus is readable from the subject of some emails (i.e., numbers 5, 10, 12 and 14). But this doesn't mean that these and only these emails were COVID-19 themed phishing (e.g., number 5 was a legitimate email). Further, for some COVID-19 themed phishing emails (i.e., the number 4 and 8), the relation to COVID-19 could not be inferred from the mail's subject. However, the content of these emails was related to COVID-19 as a lure. For instance, the phishing email with the ''Employee Starter Kit'' subject (i.e., number 4) was a fake email sent from the employer's human resources department asking the user to click on a link to download the company's COVID-19 policies, procedures and practices specific to their workplace.

We hovered a hand-pointer on the links (either a phishing or legitimate link) and displayed the URL in the email's left bottom corner. Figures 2, 3, and 4 are examples of the emails we used in the study.

TABLE 1. Simulated emails used in the survey.

#	Email subject	Category
1	Microsoft account password reset	Legitimate
2	Your Mailbox Will Shotdown Verify Your Account	Common Phishing
3	Fw: DHL World Wide Delivery/Parcel Arrival	Common Phishing
4	Employee Starter Kit	COVID-19 Phishing
5	COVID-19 Travel Guideline	Legitimate
6	Verify your email address	Legitimate
7	RE: [HSBC] Important Message Alert !!!!.. REF ID 233455	Common Phishing
8	I highly recommend you analyze and abide by the instructions attached	COVID-19 Phishing
9	Critical security alert	Legitimate
10	Important Coronavirus (COVID-19) Safety Measures	COVID-19 Phishing
11	Did You Just Sign In?	Common Phishing
12	Genuine Details Concerning COVID-19	COVID-19 Phishing
13	Microsoft account security alert	Legitimate
14	Increased Coronavirus Cases in your Area	COVID-19 Phishing
15	Important Information Regarding Your Account	Common Phishing

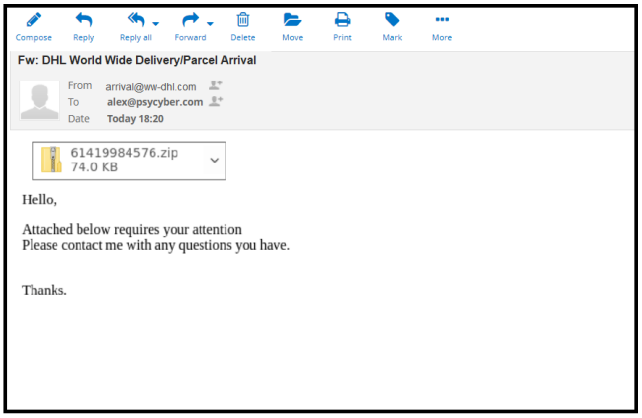

FIGURE 3. A common phishing email example.

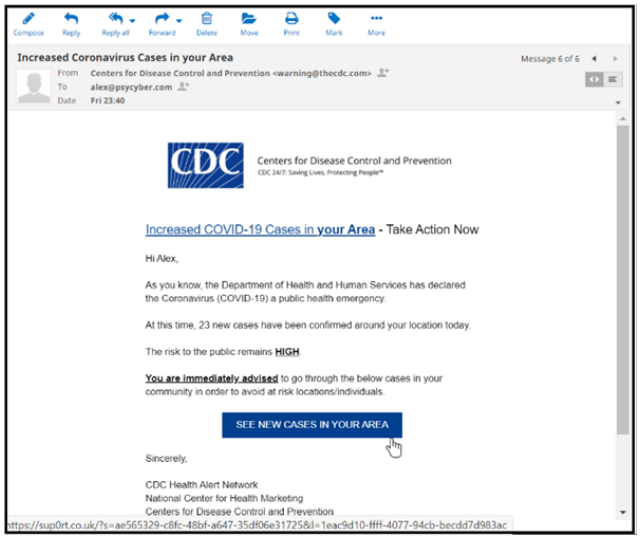

FIGURE 4. A COVID-19 themed phishing email example.

In each phishing email, one or more phishing signs taken from [59], [68]–[72] were considered, such as:

- The domain name is mimicked
- Grammatical and spelling errors
- Sense of urgency and/or demand for immediate action
- Unusual request from the employer or a public agency
- Link to a fake website (e.g., the email address and the link's domain names are inconsistent)
- Fake email address (e.g., it claims that the email is from the Centers for Disease Control and Prevention, but the domain name was thecdc.com instead of cdc.gov).

TABLE 2. Demographic information.

Variable	Frequency	Percent
Gender		
Male	124	62.6
Female	74	37.4
Education Level		
High school or less	21	10.6
Some college	37	18.7
Bachelor's degree	111	56.1
Master's degree	24	12.1
PhD degree	5	2.5
Age Range		
18-25	32	16.2
26-35	91	46
36-45	40	20.2
46-55	20	10.1
Above 56	15	7.6

C. DEMOGRAPHICS

Among the 198 qualified participants, 62.6 percent were male and 82.4 percent were between the age range 18-45. Table 2 summarises the demographic information of the participants.

Comparing Internet and MTurk users' age distribution, it is demonstrated in [73], [74] that MTurk users are younger than the worldwide internet users' population. This can justify why from our participants, 82.4 present were in the age range 18-45.

D. MEASURES

1) PHISHABILITY SCORE

To test the hypotheses of this research, we sought to find the phishability score of each user for both common phishing and COVID-19 themed phishing emails.

As explained above, we showed 15 emails to the participants and asked them to answer the following question for each email.

''You have received this email, what action would you take?''

As answer, they could choose one of the following options:

1. Emails with a link: ''Click on the link in the email (the one with a hand-pointer positioned over it)'' and emails with an attachment: ''Open the attachment''
2. Leave the email in my inbox for another time
3. Ignore and delete the email
4. Block the sender and delete the email

To calculate the users' phishability score we took the following assumptions into the account:

If the email was a phishing scam and the user chose the first option, the user was compromised. So, we added one to the user's total phishability score. If the email was a phishing scam but the user chose the second answer, the user is taking a risk, as the phishing email remains in the inbox and the user may click on the link (or open the attachment) in future. But the score is dependent on the user's ability to detect other phishing emails. This means that those who could detect at least one of our other phishing emails, could also detect this email (which was left in the inbox) in future, as the user has some phishing detection knowledge and by spending more time on this email in future, they will most likely detect a phishing indicator in the email. Deleting an email might be motivated by different reasons, for instance some users do not like to keep unknown, marketing emails, etc. in their inbox and opt to delete them. However, blocking the sender and then deleting the emails can indicate that the user has some knowledge of suspicious emails. So, if the user chose the second answer, and they could not correctly choose the fourth answer for any of the phishing emails, we added one to their total phishability score. We carried out the same calculation for both the common and COVID-19 themed phishing emails, so that we calculated each user's common phishability score and COVID-19 phishability score.

2) CORONAVIRUS ANXIETY SCALE (CAS)

To measure the participants' anxiety scale caused by COVID-19, we used the COVID-19 Anxiety Scale [75]. It is a five-item scale designed and developed to examine anxiety over COVID-19. The participants could get an overall score between the range of 5 to 25, where the higher score indicates a higher level of anxiety over COVID-19. The cut-off score of this scale is 9, meaning that people with a score of 9 or higher have COVID-19 dysfunctional anxiety.

3) THE FEAR OF COVID-19 SCALE (FCV-195)

The FCV-195 is a seven-item scale with robust psychometric properties that has been developed to examine people's fear of COVID-19. The participants could achieve an overall score ranging between 7 to 37, where a higher overall score indicates a more severe fear of COVID-19 [34].

4) COVID STRESS SCALES (CSS)

The CSS is a 36-item scale that is developed to examine COVID-19 related distress. The scale corresponds to the following sub-scales [76]–[78].

- Danger and contamination (DAN)

Fear of the dangerousness of COVID-19 and fear of contact with objects, surfaces, and other fomites.

- Socioeconomic consequences (SEC)

Concerns about the COVID-19 costs and its impacts on personal financial situation.

- Xenophobia (XEN)

Fear that foreigners are spreading the virus.

- Traumatic stress symptoms (TSS)

Traumatic exposure to the virus such as, ''nightmares, intrusive thoughts, or images'' related to COVID-19.

- Compulsive checking (CHE)

COVID-19-related compulsive checking and reassurance seeking

The DAN scale consists of 12 items and each one of the other four scales consists of six items. Each item is scored on a 5-point Likert scale, where a higher score indicates more related stress of COVID-19 and a higher CSS score (the overall score) indicates more overall stress about COVID-19. In each of the DAN, SEC, and XEN scales, the participants should answer the questions based on the extent to which they experienced COVID-19 related worries during the past week, while in the CHE and TSS scales, they should answer the questions considering how often they have ''engaged in compulsive checking or reassurance seeking behaviours, and how frequently they experience problems related to traumatic stress in the past week'' [76], [77].

5) DOMAIN-SPECIFIC RISK-TAKING (DOSPERT)

To test the participants' risk-taking behaviour in various domains, we used the DOSPERT scale. It is a 30-item scale which measures the participants' risk-taking in ethical, financial, health and safety, recreational, and social domains [79], [80]. This scale is used in several studies to examine the internet/computer users' risk-taking [10], [11], [44], [45], [81]–[83]. It is a 7-point rating scale, in which the participants could receive a score ranging between 6 to 42 for each domain, where a higher score indicates greater risk-taking behaviour in that domain.

6) DOHMEN RISK TAKING MEASURE

To measure the participant's general risk-taking behaviour, we used the one-item Dohmen scale. This scale asks the participants to rate the following question from 0 to 10: ''How do you see yourself: are you generally a person who is fully prepared to take risks or do you try to avoid taking risks?'', where the value 0 means: 'not at all willing to take risks' and the value 10 means: 'very willing to take risks' [84].

TABLE 3. Descriptive statistics.

Variables	Mean	S.D.	Skewness	Kurtosis
CAS	3.76	5.174	1.200	.088
FCV-195	18.35	7.760	.221	-1.064
CSS – DAN	21.71	12.62	.086	-.847
CSS – SEC	10.54	6.805	.184	-.947
CSS – XEN	7.14	7.388	.612	-1.016
CSS – TSS	5.98	6.850	.880	-.530
CSS – CHE	8.24	6.831	.488	-.924
DOSPERT – Social	27.88	7.277	-.513	.076
DOSPERT – Recreational	18.14	10.268	.538	-1.018
DOSPERT - Health/Safety	18.36	9.199	.478	-.853
DOSPERT – Financial	19.33	9.131	.402	-.675
DOSPERT - Ethical	16.51	8.897	.721	-.547
G-RT	6.34	2.579	-.170	-.918
COVID-19 Phishing Score	2.46	3.198	1.314	.436
Common Phishing Score	1.60	1.951	.815	-.982

IV. DATA ANALYSIS AND RESULTS

Several analyses were performed on the data to find out associations between the measured variables (i.e., their anxiety, fear, stress, risk-taking, and demographics) and their phishability (common and COVID-19). Statistical analyses were run in IBM SPSS Statistics 27.0 [85].

A. RELIABILITY TESTING

Reliability for each scale construct was analysed. Coronavirus anxiety α (Cronbach's alpha) =.959; Fear of COVID-19 $\alpha = .936$; COVID-19 Stress $\alpha = .981$ (DAN $\alpha = .951$; SEC $\alpha = .957$; XEN $\alpha = .956$; TSS $\alpha = .961$; CHE $\alpha = .937$); Domain-Specific Risk Taking $\alpha = .942$ (ethical $\alpha = .872$; financial $\alpha = .856$; health and safety $\alpha = .842$; recreational $\alpha = .900$; social $\alpha = .782$).

As Cronbach's alpha level between 0.70 and 0.90 considered "excellent reliability" and above 0.90 considered "high reliability" [86], all the reliabilities were acceptable. Thus, all scales had high internal consistency.

B. DESCRIPTIVE STATISTICS

Both the outcome variables (i.e., the COVID-19 and Common Phishing Scores) were not normally distributed, so we converted them to a normal distribution using Templeton's two-step transformation approach [87]. Table 3 presents descriptive statistics of the variables, after the transformations.

C. REGRESSION ANALYSIS

Multiple linear regression analyses were conducted with anxiety, stress, fear, risk-taking, and demographics predictor variables, and common phishability and COVID-19 phishability as outcome variables. The estimations of variance inflation factors (VIF) were performed on all the predictor variables to evaluate the data for multicollinearity issues. Variables with VIF values greater than 10 were considered as problematic variables [88], so the Socioeconomic consequences (SEC) variable which had high VIF was dropped from the analysis.

We defined eight regression models, four models for testing the users' response (phishability score) to common phishing emails and four models for testing the users' response to COVID-19 phishing emails. The results of regression models when the outcome variable was the users' response (score) to common phishing emails are presented in Table 4. In the first model, where the predictors were COVID-19 anxiety and fear, the COVID-19 anxiety score ($\beta = 0.117$, $p < 0.001$) had a significant effect on users' common phishability. In the second model, where the predictors were different types of COVID-19 stress levels, the compulsive checking stress (CHE) ($\beta = 0.088$, $p < 0.01$) had a significant effect on users' common phishability. As the DAN (initial VIF = 10.670) and SEC (initial VIF = 10.840) variables had collinearity issues, we dropped SEC (which had higher VIF value) from the analysis. In the third model, where the predictors were different domains of risk-taking, the ethical risk-taking ($\beta = 0.055$, $p < 0.01$) had a significant effect on users' common phishability. In the fourth model, where the predictors were demographic factors, education level ($\beta = 0.364$, $p < 0.01$) had a significant effect on users' common phishability.

The results of regression models when the outcome variable was the users' response (score) to COVID-19 phishing emails are presented in Table 5. In the first model, where the predictors were COVID-19 anxiety and fear, both the Coronavirus anxiety score ($\beta = 0.138$, $p < 0.01$) and fear of COVID-19 ($\beta = 0.070$, $p < 0.05$) had significant effect on users' COVID-19 phishability. In the second model, where the predictors were different types of COVID-19 stress levels, the danger and contamination (DAN) ($\beta = 0.044$, $p < 0.05$) and compulsive checking stress (CHE) ($\beta = 0.203$, $p < 0.001$) had a significant effect on users' COVID-19 phishability. As the DAN (initial VIF = 10.670) and SEC (initial VIF = 10.840) variables had collinearity issues, we dropped SEC (which had higher VIF value) from the analysis. In the third model, where the predictors were different domains of risk-taking, the social risk-taking ($\beta = -0.057$, $p < 0.05$) and ethical risk-taking ($\beta = 0.082$, $p < 0.05$) had a significant effect on users' COVID-19 phishability. In the fourth model, no demographic factor (age, gender, and education) had significant effect on users' COVID-19 phishability.

As figure 5 shows, these results partially support our H1, as users' anxiety and at least one type of stress influenced their phishability of both the common and COVID-19 phishing, but fear of COVID-19 only influenced their phishability of COVID-19 phishing, not the common phishing. These results partially support our H2, as an association can be found between at least one domain of the users' risk-taking preference and their common and COVID-19 phishability. We also found an association between the users' education level and susceptibility to falling for common phishing, which provides partially support for H3.

TABLE 4. Results from the multiple regressions predicting users' responses to common phishing emails (i.e., their phishability score).

Predictor	β	95% CI	t	SE	VIF	R^2	F
Model 1.1						.248	32.224***
Coronavirus Anxiety and COVID-19 Fear scores as the predictors							
CAS	.117***	[.061, .174]	4.093	.029	2.291		
FCV-195	.028	[-.009, .066]	1.491	.019	2.291		
Model 1.2						.236	14.944***
COVID-19 Stress DAN, SEC, XEN, TSS, and CHE scores as the predictors							
CSS - DAN	-.019	[-.042, .004]	-1.610	.012	2.256		
CSS - XEN	.033	[-.014, .079]	1.383	.024	3.079		
CSS - TSS	.021	[-.045, .088]	.625	.034	5.448		
CSS - CHE	.088**	[.029, .146]	2.931	.030	4.236		
Model 1.3						.287	12.817***
Domain-Specific Risk-Taking's Ethical, Financial, Health and Safety, Recreational, Social, and General Risk-Taking scores as the predictors							
DOSPERT - Social	-.018	[-.046, .011]	-1.213	.014	1.191		
DOSPERT - Recreational	.021	[-.010, .052]	1.326	.016	2.842		
DOSPERT - Health/Safety	-.019	[-.057, .019]	-.982	.019	3.370		
DOSPERT - Financial	.032	[-.004, .069]	1.741	.019	3.125		
DOSPERT - Ethical	.055**	[.016, .095]	2.744	.020	3.454		
General Risk-Taking	.049	[-.052, .149]	.953	.051	1.866		
Model 1.4						.042	10.568*
Age, Gender, and Education level as the predictors							
Age	-.008	[-.027, .011]	-.832	.010	1.026		
Gender	.192	[-.264, .648]	.832	.231	1.030		
Education	.364**	[.117, .610]	2.909	.125	1.008		

Age groups: 1. 18-25, 2. 26-35, 3. 36-45, 4. 46-55, 5. 55 and above
Gender: 0. Female, 1. Male
Educational level: 1. high school or less, 2. some college, 3. bachelor degree, 4. master degree, 5. PhD degree
*p<.05 **p<.01 ***p<.001

TABLE 5. Results from the multiple regressions predicting users' responses to COVID-19 phishing emails (i.e., their COVID-19 phishability score).

Predictor	β	95% CI	t	SE	VIF	R^2	F
Model 2.1						.182	21.719***
Coronavirus Anxiety and COVID-19 Fear scores as the predictors							
CAS	.138**	[.035, .241]	2.647	.052	2.291		
FCV-195	.070*	[.001, .138]	2.001	.035	2.291		
Model 2.2						.220	13.579***
COVID-19 Stress DAN, SEC, XEN, TSS, and CHE scores as the predictors							
CSS - DAN	-.044*	[-.085, -.003]	-2.119	.021	2.256		
CSS - XEN	.066	[-.017, .148]	1.575	.042	3.079		
CSS - TSS	-.024	[-.142, .094]	-.404	.060	5.448		
CSS - CHE	.203***	[.099, .308]	3.849	.053	4.236		
Model 2.3						.170	6.505***
Domain-Specific Risk-Taking's Ethical, Financial, Health and Safety, Recreational, Social, and General Risk-Taking scores as the predictors							
DOSPERT - Social	-.057*	[-.111, -.003]	-2.084	.027	1.191		
DOSPERT - Recreational	.050	[-.009, .109]	1.666	.030	2.842		
DOSPERT - Health/Safety	-.027	[-.098, .045]	-.731	.036	3.370		
DOSPERT - Financial	.028	[-.041, .097]	.795	.035	3.125		
DOSPERT - Ethical	.082*	[.007, .157]	2.150	.038	3.454		
General Risk-Taking	-.005	[-.195, .185]	-.050	.096	1.866		
Model 2.4						.021	1.416 (p = .239)
Age, Gender, and Education level as the predictors							
Age	-.003	[-.037, .030]	-.195	.017	1.026		
Gender	-.472	[-1.281, .337]	-1.151	.410	1.030		
Education	.359	[-.079, .797]	1.618	.222	1.008		

Age groups: 1. 18-25, 2. 26-35, 3. 36-45, 4. 46-55, 5. 55 and above
Gender: 0. Female, 1. Male
Educational level: 1. high school or less, 2. some college, 3. bachelor degree, 4. master degree, 5. PhD degree
*p<.05 **p<.01 ***p<.001

V. DISCUSSION

According to cyber security literature, investigating the effects of human and psychological factors on cybercrimes in general and in phishing attacks in particular, we can determine that factors such as risk-taking of users might impact the success of a phishing attack. However, the

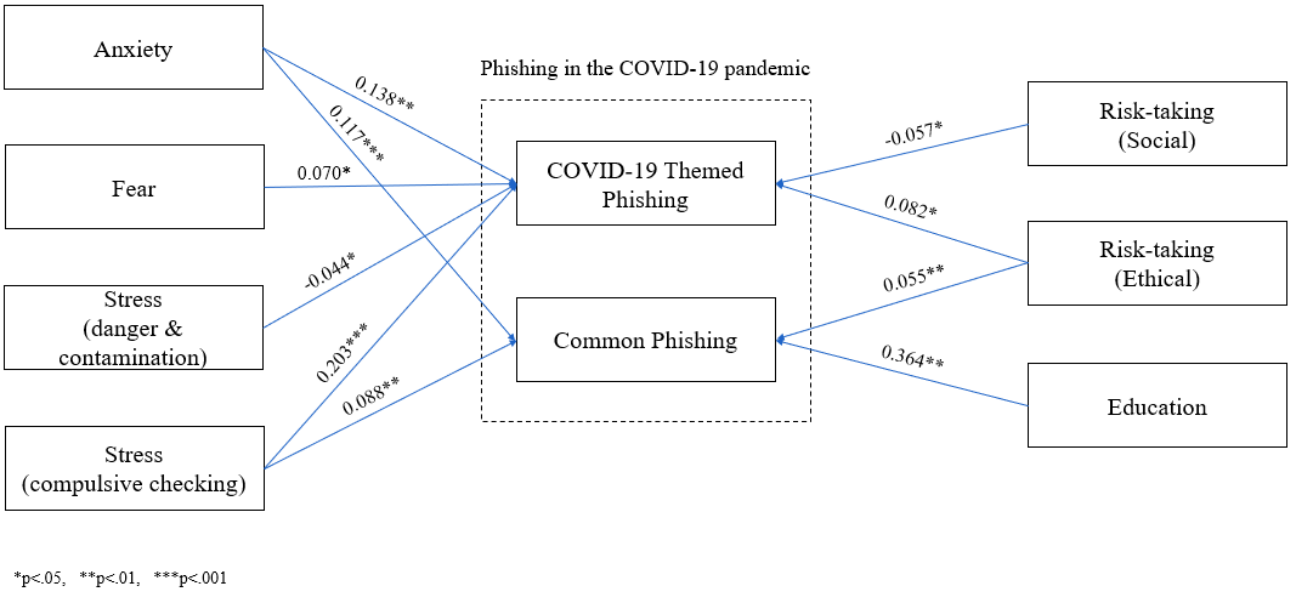

FIGURE 5. The results of the regression analyses (only statistically significant relationships shown).

studies were conducted before COVID-19, pre-pandemic, where the extremely high risk to human life and health was not present. In this situation, new psychological factors are introduced into the equation, ones that may play a more important role in rendering an individual a victim of phishing. To explore these possible factors, this study explored some of the contributing psychological factors and demographics.

As explained earlier in this paper, COVID-19 and its consequences had some psychosocial impacts, such as increased level of anxiety, fear, and stress. The results of our regression analysis indicate that having COVID-19 anxiety might increase the possibility of falling into both the common and COVID-19 themed phishing attacks. If a user's anxiety is increased due to the pandemic, the user may not detect phishing signs in an email and instead click on the harmful link or open the attachment, without consideration. The study also demonstrates that fear of coronavirus has an impact on the COVID-19 phishing scams, but no impact on the result of common phishing. Compulsive checking (CHE) stress also influences both the COVID-19 and common phishing attacks, but danger and contamination (DAN) stress negatively impacted COVID-19 themed phishing and had no impact on common phishing. The analysis also confirms that some risk-taking domains have an impact on falling into a phishing scam even during the pandemic. Ethical risk-taking influences both the common and COVID-19 phishing, while social risk taking negatively impacts the COVID-19 phishing with no impact on the common phishing. The result of an analysis on the association between demographic factors on response to phishing emails during the coronavirus situation demonstrates that only the education level of users can impact the extent to which a user is compromised by common phishing attacks. These results show that some human behaviour (i.e., the risk-taking preferences) causing the success of phishing prior to the pandemic can still play a role during the pandemic, but it seems that psychological factors as a result of COVID-19 can play an important role in an individual being victimised by phishing during the outbreak. However, some emotions can have more impact on the COVID-19 phishing emails, which can be used by scammers in designing those phishing campaigns.

Studies showed that anxiety can decrease attentional control while people perform tasks [89]–[91]. This can explain why a user with high levels of anxiety may pay less attention to phishing clues in an email and as a result, click on the compromising phishing link, for instance. When it comes to fear, the results present that the fear of COVID-19 was associated with falling into coronavirus phishing emails, not common phishing. This can happen because the users have a fear of coronavirus so they, for example, click on the link in an email which seems to be addressed from a reputable health agency (e.g., the WHO) to read the latest information about vaccination. Both fear and anxiety act as a danger or threat signal which can trigger appropriate responses [92]. Many scientists distinguish between fear and anxiety and believe that fear is related to known threats while anxiety acts as an unknown threat signal– that is, fear is focused on known external danger while anxiety is a ''response to an unknown threat or internal conflict'' [92]–[94]. This can be a reason why users with a high level of fear fell more into the phishing scam, as when they have a fear of coronavirus, they know what causes the fear (it is a known threat), therefore, they focus on the reason of the fear, hence COVID-19 related

emails gain their attention. But when users have high levels of anxiety, although it is caused by COVID-19, the reason is not very clear to them (it is unknown or less known), so they may fall into all types of phishing attacks. Studies showed that fear and anxiety can cause low certainty and low self-control [95], [96] which might be a reason as to why the high level of anxiety is significantly associated with responding to both types of phishing emails. One study demonstrated that less anxious people might allocate their full attention to a designed task, but the highly anxious cannot do this. They can allocate a part of their attention to the task [97]. So, this can be a reason as to why those users who have high level of anxiety, due to the COVID-19, cannot give the full attention required to detect the phishing signs in an email, despite knowing what those signs are and despite having phishing email detection skills.

The results suggest that those users who exhibit stress due to fear of contact with possibly contaminated objects or surfaces, clicked less on the COVID-19 phishing links or opened the attachment, while those who exhibit stress due to compulsive checking and reassurance seeking any possible threat that might be caused by the pandemic, can be susceptible to both common and COVID-19 phishing scams. It seems that stress can play an important role in becoming a victim of phishing. A user who had compulsive checking and reassurance seeking might want to address these needs by finding more information about COVID-19 (e.g., vaccination, latest status of infected people, etc.) by clicking on the COVID-19 phishing links. However, the results indicate that these stresses can cause falling into various types of phishing, and not only the COVID-19 related ones. The effects of different types of stress on phishing during the pandemic needs more research, to find out the root causes of these effects. For instance, it is not clear why those who have the fear of contact with contaminated objects are less likely to respond to phishing.

Some studies found an association between ethical and social risk-taking and security behaviour intentions of users [45] while other found that ethical and financial factors have this association [10], [98]. However, other studies did not find any association between ethical and social risk-taking behaviours and users' security behaviour but instead found a significant relationship between users' health and safety, and financial risk-taking and their security behaviour [44]. So, it seems that different risk-taking domains might be able to predict users' security behaviour, sometimes and probably in some social conditions, sometimes ethical, and sometimes financial. Our results showed that users' ethical risk-taking during the pandemic, can impact different types of phishing attacks' results but social risk-taking has a negative impact on falling for COVID-19 phishing.

The general risk-taking though, could not predict the success of a phishing scam. This can prove that some types of risk taking, especially those of ethical nature, play a greater role in the pandemic. Although, a previous study could find the effect of the users' general risk-taking on being victimised by a phishing before the pandemic [55], our results could not find such a relation during the pandemic.

While other studies demonstrated relationships between age and/or gender of users and their phishability [55], [99], [100], the results of this study did not show any relationship between them during the pandemic. Although a previous study conducted before the COVID-19 found that people with lower education levels tend to be more susceptible to phishing [10], our study results showed that those who are more educated are at greater risk of being victimised by common phishing during the outbreak. Further studies should investigate why the education level is positively associated with falling into a phishing attack during the outbreak. However, we should bear in mind that the previous study's participants were university students [10], and as younger students normally have lower education level, maybe the participants' age range had the main effect on falling into the phishing in that study. The association between the education level and age is not always positive in the general population [101].

The aforementioned results have practical implications. There are many technical anti-phishing solutions available that are preventing a huge number of phishing emails from reaching the users' inboxes. Although these solutions are becoming more and more advanced, for instance by using AI (artificial intelligence) powered and machine-learning based phishing detection and prevention techniques [102], [103], they cannot stop all phishing emails. Phishing is still successful, and scammers always find new ways to fool their victims by designing phishing attacks based on human weaknesses as it seems that the weakest link is human error [104]. Thus, many organisations spend a lot of time and effort on security training awareness campaigns to increase their employees phishing awareness, so that they can detect phishing emails (which passed through the anti-phishing solutions) [105]. However, as the results of this study show, it seems that the users' phishing detection skills might even be overshadowed by other factors such as fear of COVID-19 during the pandemic.

These results can help organisations to find their high-risk users, during a pandemic, by simply taking the CAS, FCV-195, and CSS test (or even one of them). By controlling their fear, stress, and/or anxiety, for instance by using psychological techniques, they can reduce the risk of being compromised by phishing attacks, as even a click on a phishing link or open a phishing attachment might cause their critical systems to face compromise by a malware (e.g., a ransomware). They can also prioritise their security training efforts and provide special and more phishing training to those users. In fact, all individuals can take these tests during the outbreak and, if for instance, their fear of COVID-19, anxiety, and/or stress score(s) is high, they will be at the risk of being hacked by a phishing attack. They should then concentrate more on all incoming emails and always bear in mind that they are more vulnerable than others, at least during the pandemic. Perhaps the best way to combat this, is to reduce those causes using psychological techniques.

This study is important because it explains how the individuals' emotions and behaviour is influenced by COVID-19, suggesting that future health crises can play an important role in the success of phishing attacks. Furthermore, it determines the idea that the results from other studies on the effects of human factors on phishing scams before or after a pandemic, can be overshadowed by some other factors that emerge during a pandemic. This, however, need further development, so researchers should deeply investigate the effect of COVID-19 on human factors, and thereafter, their impact on phishing. Through such research, other contributing factors may also be discovered. Moreover, effects of these factors might be different across different countries and cultures. We did not have any regional limitations for participation in this study but focusing on a specific country may highlight different results that can be used to minimise the success of phishing attempts in certain countries.

There are several limitations to this study. Firstly, the sample was drawn from Amazon mTurk users, so it cannot be considered as a representation of the behaviour of all email users. Secondly, we used images of the phishing emails in a role-play experiment and asked the participants how they would respond to the email if they were 'Alex'. So, they did not deal with a real-life scenario of receiving a mail themselves. Some of those who have a fear of COVID-19 or increased level of anxiety or stress, did not respond to the phishing emails in the study, but may have done so if they faced this situation in a non-monitored scenario. However, some other participants may even engage more in risky behaviour and respond to the phishing as they know that it is just an image and does not have any consequence. However, there is no reason to differentiate between the results of their role-play behaviour and their behaviour in the real world during the pandemic.

It is important to note that this study was conducted before people start receiving the COVID-19 vaccine, so results may vary after vaccination rollouts take place around the world. Future studies can investigate the effects of human factors on phishing scams during the pandemic since vaccination to find out if the effects are visible and sustainable.

VI. CONCLUSION

The main contribution of this study is new empirical evidence that anxiety, fear and stress related to the COVID-19 pandemic, affect falling to both common and COVID-19 themed phishing emails. These findings increase our knowledge of the human factors (e.g., risk-taking, education level) that impact the success of phishing attacks in pre-pandemic times.

Phishing attempts have increased after COVID-19 and have compromised a number of businesses and individuals. We know from previous studies that human behaviour and some demographic factors could impact falling for phishing before the pandemic, but are these factors still at play during the pandemic? More importantly, are there other, new factors, like COVID-19 related fear, anxiety and stress, that impact phishability, in particular related to COVID-19 themes phishing mails? Understanding the main reasons for why people follow the attackers during the outbreak will help us to focus on high-risk users and make an effective programme to mitigate the risk. We analysed the effect of some personal emotions, behaviours and demographic factors on both common and COVID-19 phishing. Future studies can focus more on these emotions and carry out lab and real-world experiments to further analyse their effects on different types of phishing and other cyber-attacks, and unearth how treating these emotions, e.g., fear of pandemic-scale viruses, can decrease the success of phishing. The studies can also investigate effects of other emotions and behaviours on phishing during the outbreak. These results can be useful to decrease the success of phishing during the COVID-19 pandemic and even possible future health crises.

The study's findings showed that the level of users' anxiety, level of stress caused by compulsive checking and reassurance-seeking, and ethical risk-taking could influence the different phishing types' success during the pandemic. Fear of COVID-19 can positively affect phishing success, while levels of stress caused by fear of COVID-19's danger and contact with objects that can carry and spread the virus, and social risk taking, can negatively impact the success of phishing attempts which use COVID-19 themes as a lure to fool the users. Furthermore, users' education level can influence the success of common phishing attempts during the pandemic – that is, those who are more educated might have more willingness to respond to a common phishing email.

This research is the first study on the effects of the human emotions which were impacted by COVID-19 on both common and COVID-19 themed phishing attempts. More in-depth research can be conducted on the effects of these emotions as well as the effects of other emotions and behaviour of phishing attacks during the pandemic. The results of this study and the proposed future studies can be used to minimise the success rate of phishing attempts during the COVID-19 outbreak and similar situations in future.

REFERENCES

[1] Federal Bureau of Investigation. (2021). *Business Email Compromise The 26 Billion Scam*. Accessed: Feb. 5, 2021. [Online]. Available: https://www.ic3.gov/Media/Y2019/PSA190910
[2] Verizon. (2019). *2019 Data Breach Investigations Report*. Accessed: Feb. 5, 2021. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/
[3] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in *Proc. Inf. Secfur. South Africa*, Aug. 2014, pp. 1–3.
[4] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing attacks root causes," in *Risks and Security of Internet and Systems* (Lecture Notes in Computer Science), vol. 10694. Cham, Switzerland: Springer, 2017, pp. 187–202, doi: 10.1007/978-3-319-76687-4_13.
[5] T. Kelly, *How Hackers are Using COVID-19 to Find new Phishing Victims*. Troy, MI, USA: BNP Media, 2021. Accessed: Feb. 5, 2021. [Online]. Available: https://www.securitymagazine.com/articles/92666-how-hackers-are-using-covid-19-to-find-new-phishing-victims
[6] Cision. (2021). *Phishing in a Pandemic: 1 in 4 Americans Received a COVID-19 Related Phishing Email*. Accessed: Feb. 5, 2021. [Online]. Available: https://www.prnewswire.com/news-releases/phishing-in-a-pandemic-1-in-4-americans-received-a-covid-19-related-phishing-email-301134037.html

[7] C. Crane. (2021). *Phishing Statistics: The 29 Latest Phishing Stats to Know in 2020*. Accessed: Feb. 5, 2021. [Online]. Available: https://securityboulevard.com/2020/04/phishing-statistics-the-29-latest-phishing-stats-to-know-in-2020/

[8] University of Pittsburgh. (2021). *COVID-19 Phishing Scams*. Accessed: Feb. 10, 2021. [Online]. Available: https://www.technology.pitt.edu/security/covid-19-phishing-scams

[9] A. K. Welk, K. W. Hong, O. A. Zielinska, R. Tembe, E. Murphy-Hill, and C. B. Mayhorn, "Will the 'Phisher-Men' reel you in?: Assessing individual differences in a phishing detection task," *Int. J. Cyber Behav., Psychol. Learn.*, vol. 5, no. 4, pp. 1–17, 2015.

[10] 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.*, 2010, pp. 373–382.

[11] 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.

[12] L. M. Bishop, P. L. Morgan, P. M. Asquith, G. Raywood-Burke, A. Wedgbury, and K. Jones, "Examining human individual differences in cyber security and possible implications for human-machine interface design," in *Proc. Int. Conf. Hum.-Comput. Interact.* Cham, Switzerland: Springer, 2020, pp. 51–66, doi: 10.1007/978-3-030-50309-3_4.

[13] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Syst.*, vol. 51, no. 3, pp. 576–586, 2011.

[14] M. Steves, K. Greene, and M. Theofanos, "Categorizing human phishing difficulty: A phish scale," *J. Cybersecurity*, vol. 6, no. 1, Jan. 2020, Art. no. tyaa009, doi: 10.1093/cybsec/tyaa009.

[15] M. Workman, "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security," *J. Amer. Soc. Inf. Sci. Technol.*, vol. 59, no. 4, pp. 662–674, 2008.

[16] T. Halevi, N. Memon, and O. Nov, "Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks," in *Phishing Self-Efficacy Vulnerability to Spear-Phishing Attacks*, vol. 2. 2015. [Online]. Available: https://ssrn.com/abstract=2544742, doi: 10.2139/ssrn.2544742.

[17] T. Halevi, J. Lewis, and N. Memon, "Phishing, personality traits and Facebook," 2013, *arXiv:1301.7643*. [Online]. Available: http://arxiv.org/abs/1301.7643

[18] W. Gao and J. Kim, "Robbing the cradle is like taking candy from a baby," in *Proc. Annu. Conf. Secur. Policy Inst. (GCSPI)*, vol. 4, 2007, pp. 23–37.

[19] N. LeFranc and A. Savoli, "Factors influencing employees'susceptibility to phishing emails: The role of emotions," in *Proc. 13th Medit. Conf. Inf. Syst. (MCIS)*, Naples, Italy, 2019, pp. 1–8.

[20] A. Falkenberg. (2019). *The Role of Cue Utilisation and Anxiety on Phishing Email Susceptibility*. [Online]. Available: http://hdl.handle.net/2440/128841

[21] X. Lu, M. Head, and J. Yang, "The impacts of individual emotional state and emotional framing of phishing attack on susceptibility to phishing: An emotional congruence perspective," in *Proc. 19th Annu. Pre-ICIS Workshop HCI Res. MIS, Virtual Conf. 16 (SIGHCI)*, 2020. [Online]. Available: https://aisel.aisnet.org/sighci2020/16

[22] D. House and M. K. Raja, "Phishing: Message appraisal and the exploration of fear and self-confidence," *Behav. Inf. Technol.*, vol. 39, no. 11, pp. 1204–1224, Nov. 2020.

[23] Y. Bao, Y. Sun, S. Meng, J. Shi, and L. Lu, "2019-nCoV epidemic: Address mental health care to empower society," *Lancet*, vol. 395, no. 10224, pp. e37–e38, Feb. 2020.

[24] ECDC. (Feb. 4, 2021). *COVID-19 Situation Update Worldwide, as of Week 4*. Accessed: Mar. 1, 2021. [Online]. Available: https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

[25] A. Amerio, D. Bianchi, F. Santi, L. Costantini, A. Odone, C. Signorelli, A. Costanza, G. Serafini, M. Amore, and A. Aguglia, "COVID-19 pandemic impact on mental health: A web-based cross-sectional survey on a sample of Italian general practitioners," *Acta Bio Med., Atenei Parmensis*, vol. 91, no. 2, p. 83, 2020.

[26] W. Cao, Z. Fang, G. Hou, M. Han, X. Xu, J. Dong, and J. Zheng, "The psychological impact of the COVID-19 epidemic on college students in China," *Psychiatry Res.*, vol. 287, May 2020, Art. no. 112934.

[27] M. R. Taylor, K. E. Agho, G. J. Stevens, and B. Raphael, "Factors influencing psychological distress during a disease epidemic: Data from Australia's first outbreak of equine influenza," *BMC Public Health*, vol. 8, no. 1, pp. 1–13, Dec. 2008.

[28] S. K. Brooks, R. K. Webster, L. E. Smith, L. Woodland, S. Wessely, N. Greenberg, and G. J. Rubin, "The psychological impact of quarantine and how to reduce it: Rapid review of the evidence," *Lancet*, vol. 395, no. 10227, pp. 912–920, Mar. 2020.

[29] N. Salari, A. Hosseinian-Far, R. Jalali, A. Vaisi-Raygani, S. Rasoulpoor, M. Mohammadi, S. Rasoulpoor, and B. Khaledi-Paveh, "Prevalence of stress, anxiety, depression among the general population during the COVID-19 pandemic: A systematic review and meta-analysis," *Globalization Health*, vol. 16, no. 1, pp. 1–11, Dec. 2020.

[30] S. M. Brown, J. R. Doom, S. Lechuga-Peña, S. E. Watamura, and T. Koppels, "Stress and parenting during the global COVID-19 pandemic," *Child Abuse Neglect*, vol. 110, Dec. 2020, Art. no. 104699.

[31] Y. Mo, L. Deng, L. Zhang, Q. Lang, C. Liao, N. Wang, M. Qin, and H. Huang, "Work stress among Chinese nurses to support Wuhan in fighting against COVID-19 epidemic," *J. Nursing Manage.*, vol. 28, no. 5, pp. 1002–1009, Jul. 2020.

[32] C. L. Park, B. S. Russell, M. Fendrich, L. Finkelstein-Fox, M. Hutchison, and J. Becker, "Americans' COVID-19 stress, coping, and adherence to CDC guidelines," *J. Gen. Internal Med.*, vol. 35, no. 8, pp. 2296–2303, Aug. 2020.

[33] C. A. Harper, L. P. Satchell, D. Fido, and R. D. Latzman, "Functional fear predicts public health compliance in the COVID-19 pandemic," *Int. J. Mental Health Addiction*, vol. 4, pp. 1–14, Apr. 2020.

[34] D. K. Ahorsu, C.-Y. Lin, V. Imani, M. Saffari, M. D. Griffiths, and A. H. Pakpour, "The fear of COVID-19 scale: Development and initial validation," *Int. J. Mental Health Addiction*, vol. 4, pp. 1–9, Mar. 2020, doi: 10.1007/s11469-020-00270-8.

[35] K. M. Fitzpatrick, C. Harris, and G. Drawve, "Fear of COVID-19 and the mental health consequences in America," *Psychol. Trauma, Theory, Res., Pract., Policy*, vol. 12, no. S1, pp. S17–S21, Aug. 2020.

[36] O. Rakhmanov and S. Dane, "Knowledge and anxiety levels of African university students against COVID-19 during the pandemic outbreak by an online survey," *J. Res. Med. Dental Sci.*, vol. 8, no. 3, pp. 53–56, 2020.

[37] O. Rakhmanov, A. Demir, and S. Dane, "A brief communication: Anxiety and depression levels in the staff of a Nigerian private university during COVID 19 pandemic outbreak," *J. Res. Med. Dent Sci.*, vol. 8, pp. 118–122, May 2020.

[38] K. Parsons, M. Butavicius, P. Delfabbro, and M. Lillie, "Predicting susceptibility to social influence in phishing emails," *Int. J. Hum.-Comput. Stud.*, vol. 128, pp. 17–26, Aug. 2019.

[39] CAFC. (2021). *COVID-19 Fraud*. Accessed: Feb. 5, 2021. [Online]. Available: https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm

[40] B. Collier, S. Horgan, R. Jones, and L. A. Shepherd, "The implications of the COVID-19 pandemic for cybercrime policing in scotland: A rapid review of the evidence and future considerations," Scottish Inst. Policing Res., Edinburgh, U.K., Tech. Rep., 2020, no. 1.

[41] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," *Internet Technol. Lett.*, vol. 4, no. 2, p. e247, 2021.

[42] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten deadly cyber security threats amid COVID-19 pandemic," Taylor's Univ., Selangor, Malaysia, Tech. Rep. techrxiv.12278792.v1, 2020, doi: 10.36227/techrxiv.12264722.v1.

[43] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, A. Erola, C. Maple, X. Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102248, doi: 10.1016/j.cose.2021.102248.

[44] 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.

[45] 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.*, 2015, pp. 2873–2882.

[46] B.-Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, Mar. 2009.

[47] J. L. Parrish, Jr., J. L. Bailey, and J. F. Courtney, "A personality based model for determining susceptibility to phishing attacks," Little Rock, Univ. Arkansas, Fayetteville, AR, USA, Tech. Rep., 2009, pp. 285–296.

[48] G. D. Moody, D. F. Galletta, and B. K. Dunn, "Which phish get caught? An exploratory study of individuals' susceptibility to phishing," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 564–584, Nov. 2017.

[49] V. Anandpara, A. Dingman, M. Jakobsson, D. Liu, and H. Roinestad, "Phishing IQ tests measure fear, not ability," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2007, pp. 362–366, doi: 10.1007/978-3-540-77366-5_33.
[50] M. Butavicius, K. Parsons, M. Pattinson, A. McCormac, D. Calic, and M. Lillie, "Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture," in *Proc. HAISA*, 2017, pp. 12–23.
[51] A. Ferreira and S. Teles, "Persuasion: How phishing emails can influence users and bypass security measures," *Int. J. Hum.-Comput. Stud.*, vol. 125, pp. 19–31, May 2019.
[52] 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.
[53] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica, J. Econ. Soc.*, vol. 47, no. 2, pp. 263–291, Mar. 1979, doi: 10.1142/9789814417358_0006.
[54] D. Kahneman, *Thinking, Fast and Slow*. New York, NY, USA: Macmillan, 2011.
[55] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process," *IEEE Access*, vol. 9, pp. 44928–44949, 2021, doi: 10.1109/ACCESS.2021.3066383.
[56] A. Darwish, A. E. Zarka, and F. Aloul, "Towards understanding phishing victims' profile," in *Proc. Int. Conf. Comput. Syst. Ind. Informat.*, Dec. 2012, pp. 1–5, doi: 10.1109/ICCSII.2012.6454454.
[57] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham, "School of phish: A real-word evaluation of anti-phishing training," in *Proc. 5th Symp. Usable Privacy Secur.*, 2009, pp. 1–12, doi: 10.1145/1572532.1572536.
[58] A. Diaz, A. T. Sherman, and A. Joshi, "Phishing in an academic community: A study of user susceptibility and behavior," *Cryptologia*, vol. 44, no. 1, pp. 53–67, Jan. 2020.
[59] D. M. Sarno, J. E. Lewis, C. J. Bohil, and M. B. Neider, "Which phish is on the hook? Phishing vulnerability for older versus younger adults," *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 62, no. 5, pp. 704–717, Aug. 2020.
[60] G. Paolacci, J. Chandler, and P. G. Ipeirotis, "Running experiments on Amazon mechanical Turk," *Judgment Decis. Making*, vol. 5, no. 5, pp. 411–419, 2010.
[61] W. Mason and S. Suri, "Conducting behavioral research on Amazon's Mechanical Turk," *Behav. Res. Methods*, vol. 44, no. 1, pp. 1–23, Mar. 2012.
[62] M. J. C. Crump, J. V. McDonnell, and T. M. Gureckis, "Evaluating Amazon's mechanical Turk as a tool for experimental behavioral research," *PLoS ONE*, vol. 8, no. 3, Mar. 2013, Art. no. e57410.
[63] P. G. Ipeirotis, "Demographics of mechanical Turk," NYU Work. Paper CEDER-10-01, 2010. [Online]. Available: https://ssrn.com/abstract=1585030
[64] K. Casler, L. Bickel, and E. Hackett, "Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-face behavioral testing," *Comput. Hum. Behav.*, vol. 29, pp. 2156–2160, Nov. 2013.
[65] M. J. Burnham, Y. K. Le, and R. L. Piedmont, "Who is Mturk? Personal characteristics and sample consistency of these online workers," *Mental Health, Religion Culture*, vol. 21, nos. 9–10, pp. 934–944, Nov. 2018.
[66] A. J. Moss, C. Rosenzweig, J. Robinson, and L. Litman, "Demographic stability on Mechanical Turk despite COVID-19," *Trends Cognit. Sci.*, vol. 24, no. 9, pp. 678–680, Sep. 2020.
[67] J. S. Downs, M. B. Holbrook, S. Sheng, and L. F. Cranor, "Are your participants gaming the system? Screening Mechanical Turk workers," in *Proc. 28th Int. Conf. Hum. Factors Comput. Syst.*, 2010, pp. 2399–2402.
[68] S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," *J. Assoc. Inf. Syst.*, vol. 18, no. 1, pp. 22–44, Jan. 2017.
[69] K. K. Greene, M. Steves, M. Theofanos, and J. Kostick, "User context: An explanatory variable in phishing susceptibility," in *Proc. Workshop Usable Secur.*, 2018, pp. 1–14.
[70] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: Taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, Feb. 2017.
[71] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, Apr. 2006, pp. 581–590, doi: 10.1145/1124772.1124861.
[72] NCSC. (2021). *Phishing Attacks: Defending Your Organisation*. Accessed: Feb. 14, 2021. [Online]. Available: https://www.ncsc.gov.uk/guidance/phishing
[73] J. Johnson, *Age Distribution of Internet Users Worldwide 2019*. Hamburg, Germany: Statista, 2021, Accessed: Aug. 1, 2021. [Online]. Available: https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/
[74] A. Moss, *Demographics of People on Amazon Mechanical Turk*. New York, NY, USA: Cloud Research, 2021. Accessed: Aug. 1, 2021. [Online]. Available: https://www.cloudresearch.com/resources/blog/who-uses-amazon-mturk-2020-demographics/
[75] S. A. Lee, "Coronavirus anxiety scale: A brief mental health screener for COVID-19 related anxiety," *Death Stud.*, vol. 44, no. 7, pp. 393–401, Jul. 2020.
[76] S. Taylor, C. A. Landry, M. M. Paluszek, T. A. Fergus, D. McKay, and G. J. G. Asmundson, "Development and initial validation of the COVID stress scales," *J. Anxiety Disorders*, vol. 72, May 2020, Art. no. 102232, doi: 10.1016/j.janxdis.2020.102232.
[77] S. Taylor, C. A. Landry, M. M. Paluszek, T. A. Fergus, D. McKay, and G. J. G. Asmundson, "COVID stress syndrome: Concept, structure, and correlates," *Depression Anxiety*, vol. 37, no. 8, pp. 706–714, Aug. 2020.
[78] S. Taylor, *The Psychology of Pandemics: Preparing for the Next Global Outbreak of Infectious Disease*. Newcastle Upon Tyne, U.K.: Cambridge Scholars, 2019.
[79] 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. 1–16, 2006.
[80] 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.
[81] 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.
[82] S. Bandi, "An empirical assessment of user online security behavior: Evidence from a university," M.S. thesis, Univ. Maryland, College Park, MD, USA, 2016, doi: 10.13016/M2BJ7X.
[83] M. Dove, "Predicting individual differences in vulnerability to fraud," University of Portsmouth, 2018.
[84] T. Dohmen, A. Falk, D. Huffman, U. Sunde, J. Schupp, and G. G. Wagner, "Individual risk attitudes: Measurement, determinants, and behavioral consequences," *J. Eur. Econ. Assoc.*, vol. 9, no. 3, pp. 522–550, Jun. 2011.
[85] *IBM SPSS Statistics for Windows*, IBM Corp, Armonk, NY, USA, 2020.
[86] P. R. Hinton, I. McMurray, and C. Brownlow, *SPSS Explained*. Evanston, IL, USA: Routledge, 2014.
[87] G. F. Templeton, "A two-step approach for transforming continuous variables to normal: Implications and recommendations for IS research," *Commun. Assoc. for Inf. Syst.*, vol. 28, no. 1, p. 4, 2011.
[88] J. F. Hair, *Multivariate Data Analysis, 7th ed. A Global Perspective*. Upper Saddle River, NJ, USA: Prentice-Hall, 2009.
[89] A. F. Stokes and K. Kite, *Flight Stress: Stress, Fatigue and Performance in Aviation*. Evanston, IL, USA: Routledge, 2017.
[90] S. J. Bishop, "Trait anxiety and impoverished prefrontal control of attention," *Nature Neurosci.*, vol. 12, no. 1, pp. 92–98, Jan. 2009.
[91] J. Allsop and R. Gray, "Flying under pressure: Effects of anxiety on attention and gaze behavior in aviation," *J. Appl. Res. Memory Cognition*, vol. 3, no. 2, pp. 63–71, Jun. 2014.
[92] T. Steimer, "The biology of fear-and anxiety-related behaviors," *Dialogues Clin. Neurosci.*, vol. 4, no. 3, p. 231, 2002.
[93] K. Craig, "Environmental factors in the etiology of anxiety," in *Proc. 4th Gener. Prog. Psychopharmacol.*, 1995, pp. 1325–1339.
[94] K. T. Strongman, *The Psychology of Emotion: Theories of Emotion in Perspective*. Hoboken, NJ, USA: Wiley, 1996.
[95] T. Brader and G. E. Marcus, "Emotion and political psychology," in *The Oxford Handbook of Political Psychology*, 2nd ed. New York, NY, US: Oxford Univ. Press, 2013, pp. 165–204.
[96] M. Wagner and D. Morisi, "Anxiety, fear, and political decision making," in *Proc. Oxford Res. Encyclopedia Politics*, 2019, pp. 1–24.
[97] M. R. Leon and W. Revelle, "Effects of anxiety on analogical reasoning: A test of three theoretical models," *J. Personality Social Psychol.*, vol. 49, no. 5, p. 1302, 1985.
[98] A. Mathur and M. Chetty, "Impact of user characteristics on attitudes towards automatic mobile application updates," in *Proc. 13th Symp. Usable Privacy Secur.*, 2017, pp. 175–193.
[99] 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, pp. 1–20, Dec. 2016.

[100] Z. Liu, L. Zhou, and D. Zhang, "Effects of demographic factors on phishing victimization in the workplace," in *Proc. PACIS*, 2020. [Online]. Available: https://aisel.aisnet.org/pacis2020/75
[101] *Adult Education Level*, OECD, Paris, France, 2018.
[102] S. Baadel and J. Lu, "Data analytics: Intelligent anti-phishing techniques based on machine learning," *J. Inf. Knowl. Manage.*, vol. 18, no. 1, 2019, Art. no. 1950005.
[103] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, Jan. 2021, doi: 10.1007/s11235-020-00733-2.
[104] LASTLINE. (2021). *Can You Stop Phishing Emails? Why What You're Doing Now is Failing*. Accessed: Feb. 6, 2021. [Online]. Available: https://www.lastline.com/blog/can-you-stop-phishing-emails-why-what-youre-doing-now-is-failing/
[105] T. Oesch. (2021). *Why Funding for Cybersecurity Training Is Growing*. Accessed: Feb. 6, 2021. [Online]. Available: https://trainingindustry.com/blog/compliance/why-funding-for-cybersecurity-training-is-growing/

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

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 at the Faculty of Architecture and Engineering, Ghent University. He is also an Associate Professor with the Faculty of Economics and Business Administration. He has published several articles on IT and SMEs and was a speaker at international academic and business conferences, which proceedings are published in different Springer series of LNBIP and AICT. His current research interests include IT governance in SME's, design science, IS failures, and IT security.

GEERT POELS is currently a Full Professor of management information systems with the Faculty of Economics and Business Administration, Ghent University, Ghent, Belgium, where he teaches intermediate and advanced courses on information systems, IT management, enterprise architecture, and service design. He also teaches in the Master of Enterprise ICT Architecture at IC Institute, Beerzel, Belgium. His recent research relates to 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. He also supervises Ph.D. research on digital marketplaces, cybersecurity, and GDPR. As academic service, he co-developed the COBIT 2019 framework for IT governance.

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 at the IDLab, Ghent University, in collaboration with IMEC. His research domain has evolved from the 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.