https://doi.org/10.54483/sajaar.2023.25.1.4

South Africans' susceptibility to phishing attacks

Mariska C Wannenburg
https://orcid.org/0000-0002-5362-9342
Department Economic and Financial Sciences, Akademia, Pretoria, South Africa

Annamart Nieman
https://orcid.org/0000-0002-3145-7316
Department of Auditing, University of Pretoria, Pretoria, South Africa

Blanche Steyn
https://orcid.org/0000-0003-0632-6346
Department of Auditing, University of Pretoria, Pretoria, South Africa

Daniel G Wannenburg
https://orcid.org/0000-0002-6280-478X
First National Bank, Pretoria, South Africa

ABSTRACT

Purpose: The purpose of the study is to assess the phishing susceptibility of individuals in South Africa, across industries related to financial services, education, legal services, and fraud- and forensic businesses.

Design/Methodology/Approach: This was an empirical, quantitative research study that collected anonymised data on simulated phishing attacks, using a survey. The results were statistically analysed to identify factors that were significantly related to the phishing score generated.

Findings: This was the first South African study to develop a phishing susceptibility score. The following demographic categories demonstrated a higher likelihood of phishing susceptibility: the legal industry; Gen Z and Alpha; females; and participants with matric as the highest educational level. The only two variables that were found to be significantly related to the phishing susceptibility score were gender (with females more susceptible) and the variable relating to prior reporting of phishing attacks (rendering such reporters less susceptible).

Research Limitations/Implications: The data collected from the online survey represents the perceptions of the individual respondents. The results of this research are valuable, not only to the participants in this study but also to organisations within other industries, as it highlights phishing susceptibility risks.

Originality/Value: This study provides insight into factors influencing phishing susceptibility. For future research purposes, this study could be replicated within other industries in South Africa.

Key words

Phishing susceptibility, demographic information, phishing training, phishing awareness, phishing reporting, industry, generations, gender, educational level, simulated phishing training

1 INTRODUCTION

"Phishing", as a type of social engineering, is characterised by deceit, impersonation, and fake communication designed to lure victims to click on a malicious link, so as to elicit sensitive information. The channels used are email, WhatsApp, short message services (SMSs), or other means of electronic communication, and the object is to commit digital theft (Ashiru 2021:176-177; Shaw 2020:27). Phishing can also enable the installation of malicious software in order to trigger a system intrusion, identity theft, and/or immobilise an organisation's systems as part of a ransomware attack (Ravi, Shillare, Bhoir & Charumathi 2021:355-356). Given the widespread risks of a phishing attack, this study assessed the phishing susceptibility of individuals.

The impact of phishing is not confined to money; it also destroys the fragile bond of trust that organisations develop with its customers (De Bona & Paci 2020:1). Phishing attacks cause substantial losses in terms of money, time, and resources, as it results in penalties and compensatory payments to customers for inconvenience or consequential loss suffered (Okpa, Ajah & Igbe 2020:472). Additionally, organisations suffer losses in company value and intellectual property and are adversely affected by the disruption

of operational activities (Smith, Jones, Johnson & Smith 2019:47). Phishing remains an information security risk, despite the use of numerous defence technologies and despite end-user education to detect and prevent it (Yang *et al*. 2022:2).

Thus, the question that arises is: who succumbs to phishing attacks (Australian Competition and Consumer Commission 2020:18)? Approximately 32% of untrained individuals fall for phishing attacks, according to KnowBe4, a security awareness training and phishing simulation organisation (KnowBe4 2022a:6; 2022b). This means that one in three untrained individuals is likely to click on a suspicious email link or comply with fraudulent requests (KnowBe4 2022a:7). Phishing constitutes the fourth most common cause of security incidents—it is ranked as the main cause of data breaches and has the highest success rate of any form of cyber-attack (Verizon 2022:34, 84). Verizon, a technology and communication services organisation, reported the clicked rate of phishing emails as 2.9%, breaching 1,154,259,736 personal records (Verizon 2022:34) across Europe, the Middle East, Africa, and North- and South America. If this data resulted only from email address breaches, this would translate to a risk of 2.9% or 33,473,532 additional phished email accounts (Verizon 2022:34).

Although phishing susceptibility across industries has been previously researched internationally, there is a lack of literature on similar research in South Africa. This constitutes a gap in the literature. In addition, the legal-, fraud- and forensic industries have not been included in previous international, phishing susceptibility research studies.

The purpose of this study was to assess the phishing susceptibility of individuals in South Africa, across the financial service-, education-, legal-, fraud- and forensic industries. This phishing susceptibility score considered common phishing attacks that can be directed to people in South Africa *via* emails, SMSs or WhatsApp messages. However, to identify the variables that are positively related to a higher level of phishing susceptibility, demographic information was collected. The instrument (Appendix A) included an informed permission question, 6 demographic questions and 14 phishing susceptibility questions. Figure 1 shows the demographic data gathered from participants, in relation to the following variables: (1) industry; (2) age; (3) gender; (4) education; (5) phishing training before entering the workforce; (6) phishing training and awareness levels; and (7) reporting of phishing attacks. The results showed that the group most susceptible to a phishing attack are females, whilst people who previously reported phishing attacks are least susceptible.

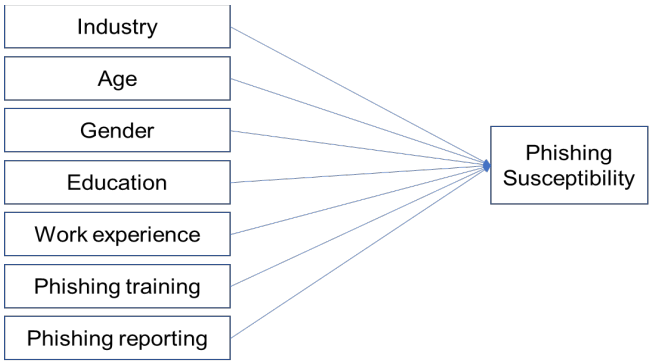


Figure 1: Variables for phishing susceptibility factors

(Source: Compiled by the authors)

This paper is organised as follows: section 2 presents a literature review; section 3 describes the research methodology; section 4 discusses the results; and section 5 concludes the study.

2 LITERATURE REVIEW

Most organisations are just one click away from a possible cyber disaster. Failure to effectively train employees on phishing, renders them unprepared and vulnerable to social engineering attacks (Ashiru 2021:176-177). The continuously high success rate of phishing attacks is attributable to phishers' ability to exploit human vulnerabilities (Bhadane & Mane 2018:15). Human capital—not technology—presents the ultimate line of defence against phishing (Alohali, Clarke, Li & Furnell 2018:307). Phishing susceptibility reflects the degree to which individuals interact with phishing attacks (Yang *et al.* 2022:2).

Predictably, phishers also attempt to take advantage of users working from home (Georgiadou, Mouzakitis & Askounis 2022:495). KnowBe4 found that only 38% of respondents have returned to their workplace on a full-time basis or are using an office network, post-COVID-19, whereas 55% continued to work from home (KnowBe4 2022a:19). Of the respondents that have continued to work from home, 72% indicated that they lack even a basic understanding of typical cyber threats to which they may be exposed (KnowBe4 2022a:19). Georgiadou *et al.* (2022:504) reported that 53% of employees across thirteen European countries have not received any security guidelines from their employers regarding working from home, highlighting the risk to organisations and individuals.

Organisations are encouraged to identify employees who are highly susceptible to phishing, in order to mitigate data breaches (Abroshan, Devos, Poels & Laermans 2021:2). In addition to industry type, demographic factors, such as age, gender, and educational level are key indicators used by organisations in determining which employees are susceptible to phishing (Abroshan *et al.* 2021:2), as these factors are distributed differently across various industry types (Mannix, Petric, Eriksen, Paglia & Roer

2022:71). Whilst many studies focus on employees in a specific industry, in regions such as Bangalore (India), Switzerland, Italy, Washington D.C. and Maryland (United States of America), little research data is currently available that directly compares different industries (Lain, Kostiainen, & Capkun 2022:1; Warda & Samaddar 2022:59; De Bona & Paci 2020:3; Diaz, Sherman & Joshi 2020:4; Li *et al*. 2020:2242). In addition, no previous phishing susceptibility literature for South Africa was found on the library databases of the University of Pretoria. This was, consequently, identified as a gap in the literature. Another gap, similarly identified, is that limited research results exist to assess the phishing susceptibility of students with little or no work experience.

The outcomes of previous phishing susceptibility studies, based on demographic information, are discussed in Table 1 below. Demographic and phishing awareness information on participants in relation to the following variables, formed the basis for the assessment of phishing susceptibility in this study: (1) industry; (2) age; (3) gender; (4) education; (5) phishing training before entering the workforce; (6) phishing training and awareness levels; and (7) reporting of phishing attacks.

Table 1: A summary of the demographic variables and phishing awareness of previous susceptibility studies

Demographic variables and phishing awareness	Outcomes
Industry	The construction-, healthcare-, and pharmaceutical industries are more susceptible to phishing, when compared to the education- and financial services industries (Mannix *et al.* 2022:72). However, a second study, in the USA, found that click rates of simulated phishing attacks in the financial services industry were higher (20%) in comparison to those in the non-financial industries (8%) (Tian, Jensen & Durcikova 2018:9). The second study included non-financial industries, such as manufacturing, biotechnology, energy, and retail (Tian *et al*. 2018:9).
Age	Older people, belonging to the baby boomer generation, are not always familiar with information technology practices and the frequent changes in current technologies and, therefore, are more susceptible to phishing (Li *et al.* 2020:2248; Taib, Yu, Berkovsky, Wiggens, & Bayl-Smith 2019:12). In contrast, a Swiss susceptibility study confirmed a strong relationship between phishing susceptibility and younger generations, in particular Gen Z (Lain *et al*. 2022:8). Castillo (2021:47), Diaz *et al*. (2020:4), and Unchit, Das, Kim and Camp (2020:7) agreed that younger generations—25 years and younger—are more susceptible to phishing attacks.
Gender	Gender susceptibility is dependent on the amount of technical knowledge possessed by individuals (Zhuo, Biddle, Koh, Lottridge & Russello 2022:6). Males were found to be significantly more susceptible to phishing attacks than females, within a university environment (Diaz *et al.* 2020:5; Li *et al.* 2020:2248). Lin *et al*. (2019:12) argued that older females (4.1%) are more susceptible to phishing than older males (2.3%). Meanwhile, according to Daengsi, Pornpongtechavanich and Wuttidittachotti (2022:4747), these inconsistencies in phishing susceptibility—as related to gender—are attributable to the level of phishing awareness.
Education	According to De Bona and Paci (2020:7-8), susceptibility to phishing is slightly higher for employees with a high school education (25.9%) than for employees with a university degree (21.7%). Other researchers concluded that employees that hold only a bachelor's degree are less confident in their ability to correctly identify phishing attacks and legitimate uniform resource locators (URLs), than those employees that hold a doctoral or master's degree (Sumner, Yuan, Anwar & McBride 2022:975). The educational level of an individual influences their predicted level of caution regarding phishing, and individuals with a higher level of education have been found to be more cautious and less likely to be phished (De Bona & Paci 2020:7-8). This suggests that there is a strong relationship between reduced phishing susceptibility and being highly qualified.
Phishing training prior to entering the workforce	There is not much information in the literature on the phishing awareness of employees with limited work experience, including students with no work experience (Pósa & Grossklags 2022:509). A German study of university students with work experience found that those students had a higher level of phishing awareness than students who did not have any work experience (Pósa & Grossklags 2022:509). In addition, a Norwegian study reported that students were less likely to identify a spear phishing email accurately, compared to a general phishing email (Berre, Eggemoen, Haugrud, Le & Sandnes 2022:4). The Norwegian study did not indicate whether the students had any work experience.
Phishing training and awareness levels	Improving people's awareness of phishing through ongoing training improves their ability to detect phishing attacks (De Bona & Paci 2020:1). Research studies conducted in Switzerland and Italy (Europe), Beijing (China), Maryland (USA), and Bangalore (India) supported this hypothesis (Lain *et al.* 2022:11; Warda & Samaddar 2022:59-79; Yang *et al*. 2022:1-11; De Bona & Paci 2020:1; Diaz *et al*. 2020:1-7). The likelihood of phishing susceptibility reduces significantly when an individual's phishing awareness increases (Warda & Samaddar 2022:69; Castillo 2021:47). Participants who received training quarterly and monthly, were less susceptible to phishing attacks (Schuetz, Lowry, Pienta & Thatcher 2020:21; Nowitz 2018:16).

continued/

Demographic variables and phishing awareness	Outcomes
Phishing reporting	A study conducted in Switzerland, investigated the effect of a crowd-sourced phishing reporting mechanism (Lain *et al*. 2022:10). "Crowd-sourced phishing reporting" is the use of secondary applications to distinguish between clearly benign emails, spam and phishing emails (Lain *et al*. 2022:2-3). A study in Arizona, found that individuals do not report phishing attacks, as they believe that the organisations are unable to do anything about the attacks (Sun 2022:125). Bidgoli, Knijnenburg, Grossklags and Wardman (2019:7) demonstrated that individuals' personal preferences regarding the way to report phishing attacks, influence the frequency with which these attacks are reported.
Simulated phishing attack campaigns	A common approach, adopted by organisations in Italy, is to train employees to identify phishing attacks via an embedded phishing training method (De Bona & Paci 2020:1). "Embedded phishing training" helps to create phishing awareness in a more effective manner using conditioning (Yeoh, Huang, Lee, Jafari & Mansson, 2022:808). Castillo (2021:138) reported a level of overconfidence in employees who had undergone simulation training, and recommended promoting personal accountability, as a control (Castillo 2021:138). Volkamer, Sasse and Boehm (2020:17) argued that negative consequences for phished employees, such as compulsory phishing training, reduce the reporting rates of phishing attacks, that only increases its potential for damage. Wokabi (2019:3) found that simulation phishing campaigns do not always enable organisations to perform a knowledge assessment of employees based only on click rates, leading to an inability to identify training gaps amongst the employees.

(Source: Compiled by the authors)

The motivation for the phishing susceptibility variables is discussed next.

The Protection Motivation theory (PMT) was applied, to determine individual factors in people who succumb to phishing attacks (Shahbaznezhad, Kolini & Rashidirad 2021:539). This theory explains the impact of persuasive communication on protective behaviour, whilst emphasising cognitive mechanisms that mediate fear and behavioural changes (Marikyan & Papagiannidis 2023:3). The PMT considers the motivation to adopt the recommended behaviour to be an attitude change, predicted by cognitive processes mediating the effect of fear (Marikyan & Papagiannidis 2023:4). This emphasises the need for training. This theory is widely applied and a meta-analysis of studies employing PMT has demonstrated that the theory is robust in terms of explaining the behaviour of individuals facing threats, such as phishing attacks (Marikyan & Papagiannidis 2023:3).

Previous phishing susceptibility studies have produced inconclusive results on the precise demographic factors that influence an individual's likelihood of falling prey to phishing attacks. Industry type, age, and gender are frequently researched; however, the outcomes of these studies have proved inconsistent. More highly qualified individuals are consistently less susceptible to phishing. Individuals who receive phishing training prior to commencing employment, appear to be less susceptible. Several studies have found that increased exposure to phishing training diminishes phishing susceptibility, through improved awareness. Increased levels of phishing reporting are often associated with reduced susceptibility, as supported by the results of simulated phishing campaigns.

3 RESEARCH METHODOLOGY

The next section outlines the research methodology followed in this study and includes the approach, method, participation, susceptibility measures and data analysis.

3.1 Approach

This was an empirical, quantitative research study, that collected survey data using simulated phishing attacks. Quantitative research is "a systematic investigation of phenomena by gathering quantifiable data and performing statistical, mathematical, or computational techniques to derive the results" (Khatri & Karki 2022: 71). Online surveys are one of the structured tools used to gather actionable quantitative data from participants (Khatri & Karki 2022:73). The survey gathered demographic information from participants by using Qualtrics, an online survey tool. Qualtrics ensures that responses from participants are completely anonymised and also facilitates the extraction of the responses into a Microsoft Excel spreadsheet (Qualtrics 2022). The statistical analysis was performed using SPSS, to objectively interpret the survey results.

3.2 Method

The survey was divided into four parts, namely sections A, B, C, and D. Section A obtained the consent of each participant, by acknowledging that participation was both voluntary and anonymous. Section B gathered the following demographic information from participants: industry, gender and age. Age was categorised based on the following generations: Gen Z and Alpha (25 years old and younger), millennials (26 to 41 years old), Gen X (42 to 57 years old), baby boomers (58 to 67 years old), and the silent generation (68 years and older).

Section C was aimed at determining the extent of phishing awareness training undergone by the participants prior to starting a professional career, their frequency of exposure to phishing awareness training, and whether the participants had ever reported a phishing attack that was sent to their work email address. Section D was administered so as to determine participants' ability to identify a phishing attack correctly, and to establish whether participants were knowledgeable regarding what to do when they had been phished. The survey questions comprised emails, SMSs and websites, depicted in Appendix A.

The survey questions were adopted from security awareness platforms created by Cisco, Google, SonicWall, TechTarget, Surfshark and the cyber awareness website of the Australian government (Cisco 2022; Google 2022; SonicWall 2022; Cosio

2021; Powers 2018). The adopted phishing emails were modified to include the name of a fictitious person, namely Kirsten Cruise. Participants were required to assume the identity of Kirsten Cruise during completion of the survey questions. Participants were also made aware of the need to examine the uniform resource locator (URL) when evaluating emails, SMSs and websites. Fictitious websites, used for phishing purposes, use fake URLs that appear to be very similar to the URL of the real and valid website of the organisation that is being impersonated (Afandi & Hamid 2021:288). In verifying the URLs of websites and email links, participants are likely to identify a phishing attack. The red flag signals that were included in the phishing attacks in the survey were: (1) the greeting; (2) suspicious URLs with a deceptive name or internet protocol address; (3) requests for urgent action by financial institutions; (4) receiving emails from individuals known by the recipient; (5) requests to change usernames and passwords; and (6) COVID-19 related SMSs.

3.3 Participants

Participants were drawn from two organisations within the financial services industry, a private higher education institution, and members of two fraud- and forensic institutions. The legal industry participants were working students from a private higher education institution. The dataset comprised 210 participants, three of whom opted out of the study and were, therefore, not included in the results. Gen Z and Alpha (25 years and younger) presented the highest proportion of participants (50%), whilst the silent generation (68 years and older) and the baby boomer generation (58 to 67 years) had the smallest proportion (2%) of participants, compared to the other generations. The aforementioned two generations were thus combined, for data analysis purposes.

Of the 207 participants to the survey study, 38% were males and 62% were females. Since the response rates of males and females could not be individually determined, a level of bias does exist in this sample. To resolve the sampling bias, an Anova analysis was used to statistically compare patterns and trends across different sample sizes, encountered in this study.

Table 2 summarises key demographic and phishing awareness information, per industry.

Table 2: Detailed summary of industry-linked demographic and phishing awareness information

	Financial services industry (N=52)	Education industry (N=45)	Legal industry (N=22)	Fraud and forensic industry (N=11)	Other (N=77)	Total (N=207)
Gender						
- Male	19	13	10	6	30	78
- Female	33	32	12	5	46	128
- Prefer not to say	-	-	-	-	1	1
Age						
- Gen Z and Alpha (25 years and younger)	31	16	12	-	45	104
- Millennials (26 to 41 years old)	13	15	7	5	17	57
- Gen X (42 years and older)	8	14	3	6	15	46
Education						
- Matric	22	7	8	2	38	77
- Undergraduate	14	6	10	-	20	50
- Graduate	5	2	3	1	10	21
- Postgraduate	11	6	-	6	8	31
- Prefer not to say	-	24	1	2	1	28
Received phishing training before entering the workforce						
- Yes	10	7	3	3	5	28
- No	40	38	18	8	68	172
-Answer not provided	2	-	1	-	4	7
Phishing training and awareness levels						
- Never	24	21	9	1	51	106
- Annually	4	3	2	-	5	14
- More than once a year	6	1	2	3	4	16
- Randomly	18	20	9	7	16	70
- Answer not provided	-	-	-	-	1	1
Phishing reporting						
- Yes	25	23	11	9	28	96
- No	20	21	11	2	39	93
- Answer not provided	7	1	-	-	10	18

(Source: Compiled by authors)

3.4 Susceptibility measure

The survey responses were reviewed to ensure the reasonableness of every submission prior to its inclusion in the data set. Validity was confirmed by ascertaining that none of the surveys reflected responses that were all answered as "yes", "no", or "I don't know". In addition, validity was also assessed to ensure that the questions were appropriate for this study. The development of the survey was an interactive process, to ensure that completing the questions would achieve the objective of this study.

Susceptibility was scored using the correct or ideal responses. The interpretation of the susceptibility score was as follows: the higher the score, the less susceptible the participant, since the participant answered the questions correctly in the survey. The highest obtainable susceptibility score was 14, whilst the lowest possible score was 0.

3.5 Data analysis

The cross-tabulation shows the demographic information and phishing awareness obtained from 207 participants, as depicted in Table 2. The demographics, respectively, indicated that the majority of the respondents were female (128), from Generation Z and Alpha (104), with matric (77), with no phishing training preceding workforce entrance (172), with no phishing training (106), and reflects phishing reporting (96).

The survey resulted in an average score of 8, as shown in Table 3. The susceptibility score was calculated using the correct or ideal answers to the phishing questions. Thus, a high score indicated a low level of susceptibility, whereas a low score suggested a high level of susceptibility.

Table 3: Descriptive statistics of the phishing susceptibility score

Participants (=N)	Mean	Standard deviation	Median	Skewness	Kurtosis	Minimum	Maximum
207	8.169	2.084	8	0.11	-0.2	3	14

(Source: Compiled by the authors)

The sample taken for this study produced a normal distribution, that was approximately symmetrical. The kurtosis result was considered acceptable to prove a normal distribution (Kunnan & Liao 2019:704).

Table 4 summarises the susceptibility scores across the various demographic groupings and phishing awareness variables.

Table 4: Summary of susceptibility scores

Demographic variable (N=207)	Subsections per demographic and phishing awareness factors	Participants (=N)	Average susceptibility score	Median
Industry	Fraud- and forensic industry	11	**9.36**	10
	Education industry	45	8.36	8
	Other	77	8.08	8
	Financial services industry	52	8.02	8
	Legal industry	22	*7.86*	8
Age	Gen X, baby boomers and the silent generation (42 years and older)	46	**8.52**	9
	Millennials (26 to 41 years old)	57	8.25	8
	Gen Z and Alpha (25 years and younger)	104	*7.97*	8
Gender	Males	78	**8.85**	9
	Females	128	*7.77*	8
	Prefer not to say	1	6.00	8
Education	Graduate	21	**8.57**	8
	Postgraduate	31	8.55	9
	Prefer not to say	28	8.32	8
	Undergraduate	50	8.20	8
	Matric (National Senior Certificate)	77	*7.83*	8
Phishing training before entering the workforce	Answer not provided	7	**8.71**	9
	Yes	28	8.36	8
	No	172	*8.12*	8

continued/

Demographic variable (N=207)	Subsections per demographic and phishing awareness factors	Participants (=N)	Average susceptibility score	Median
Phishing training and awareness levels	Answer not provided	1	12.00	-
	More than once a year	16	**8.63**	8
	Annually	14	8.57	9
	Randomly	70	8.50	9
	Never	106	*7.79*	8
Phishing reporting	Yes	96	**8.75**	9
	Answer not provided	18	7.72	8
	No	93	*7.66*	7
(Legend: **least susceptible**; *most susceptible*)				

(Source: Compiled by the authors)

The results showed that the following are the most susceptible (score in italics) to phishing attacks: The legal industry, Generation Z and Alpha, females, people with matric as their highest qualification, people untrained prior to entering the workforce, and people with no phishing awareness training, who do not report phishing. To assess the statistical significance of the relationship between the demographic, phishing awareness factors and the phishing score, an analysis of variance (ANOVA) was performed. Only two factors were significant, namely gender and reporting of phishing attacks (both p=<.001).

To further assess the relationship between the different demographic variables and phishing awareness variables, a two-phase Ordinary Least Square (OLS) regression analysis was used on the phishing susceptibility score (the dependent variable), in SPSS. The key demographic variables were entered first and included gender, industry, and generation. Table 5 indicates that the results were significant (p=<.001) but shows limited predictability, with R = 0.273, R square at 0.075, and adjusted R square at 0.016. The only variable that showed an individual significant relationship was gender (beta -1.085; p=<.001).

Table 5: Regression results – Phase 1

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.273[a]	.075	.061	2.019	.075	5.443	3	202	.001

a. Predictors: (Constant), Gender, Generation, Industry

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	8.613	.498		17.279	<,001					
	Industry	-.058	.087	-.046	-.668	.505	-.037	-.047	-.045	.981	1.020
	Generation	.246	.176	.095	1.398	.164	.102	.098	.095	.987	1.014
	Gender	-1.085	.291	-.253	-3.729	<,001	-.250	-.254	-.252	.994	1.007

a. Dependent Variable: Sscore_raw

(Source: Compiled by the authors)

Table 6 reflects the second phase, namely when the education and phishing variables were entered on top of the previous OLS, by adding the following: the highest level of education, whether phishing attack education was received before entering employment, frequency of phishing training received, and level of phishing reported.

The additional variables improved the model, however, it still showed poor prediction levels, even though the results were significant (p=<.001). The result of the OLS showed R = 0.346; R square = 0.119 and adjusted R square at 0.088. The variables that showed individual significance in the second phase, were gender (beta=-1.027; p=<.001), and the reporting of phishing attacks (beta=.692, p=<.005). Thus, gender and the level of phishing reported were significantly related to the phishing susceptibility score.

Table 6: Regression results – Phase 2

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.288[a]	.083	.069	1.999	.083	6.064	3	201	<,001
2	.346[b]	.119	.088	1.978	.036	2.041	4	197	.090

a. Predictors: (Constant), Gender, Generation, Industry

b. Predictors: (Constant), Gender, Generation, Industry, Frequence of phishing training received, Highest level of education, Received phishing training before starting with work, Reporting of phishing attacks

Coefficients[a]

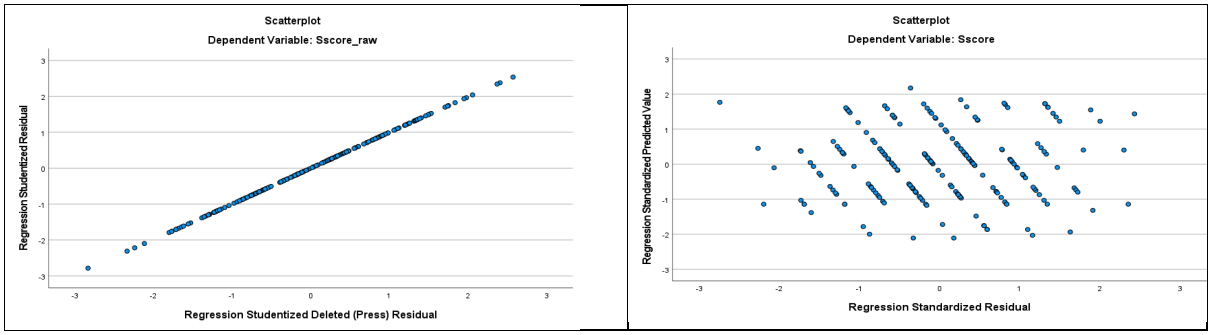
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	8.626	.493		17.483	<,001	7.653	9.599					
	Industry	-.073	.086	-.058	-.848	.397	-.243	.097	-.047	-.060	-.057	.981	1.020
	Generation	.267	.175	.104	1.532	.127	-.077	.612	.112	.107	.103	.988	1.013
	Gender	-1.125	.289	-.264	-3.898	<,001	-1.694	-.556	-.260	-.265	-.263	.993	1.007
2	(Constant)	7.777	1.196		6.505	<,001	5.419	10.135					
	Industry	-.059	.088	-.046	-.669	.504	-.232	.114	-.047	-.048	-.045	.926	1.080
	Generation	.076	.186	.029	.407	.685	-.292	.443	.112	.029	.027	.850	1.177
	Gender	-1.027	.291	-.241	-3.534	<,001	-1.601	-.454	-.260	-.244	-.236	.959	1.043
	Highest level of education	.027	.103	.018	.259	.796	-.176	.229	.012	.018	.017	.965	1.036
	Received phishing training before starting with work	-.278	.370	-.052	-.751	.453	-1.008	.452	.020	-.053	-.050	.940	1.064
	Frequence of phishing training received	-.024	.170	-.009	-.139	.889	-.359	.312	.014	-.010	-.009	.975	1.025
	Reporting of phishing attacks	.692	.245	.210	2.824	.005	.209	1.176	.249	.197	.189	.806	1.240

a. Dependent Variable: Sscore_raw

(Source: Compiled by the authors)

The OLS was valid, as there was no multicollinearity, given a VIF score of around 1. Figure 2 illustrates the scatterplot on the standardised residual on the dependent variable, highlighting that the regression adhered to the normality requirement. In addition, Figure 2 also shows the second scatterplot, where there was no heteroscedasticity. Transforming the phishing susceptibility score into a ratio or percentage score, yielded the same results. Despite the validity of the model, the low betas and poor predictability suggested a need for further analysis.

Figure 2: Scatterplots



(Source: Compiled by the authors)

For a robustness test, the same variables were entered into a stepwise regression. The results of the stepwise model were also significant at p=<.001, with gender the only significant variable in the first model, followed by gender and reporting of phishing attacks as the significant variables in the second model. Although the non-significant variables were excluded by the stepwise process, the overall predictability of the model remained low. Table 7 indicates that gender had a negative relationship, whilst reporting of phishing attacks had a positive relationship, in both types of regression models.

For additional robustness tests, the Andrew Hayes process (Hayes 2022) in SPSS regression was run, to assess whether certain variables moderated the effect of other independent variables. With the phishing susceptibility score as the dependent variable, and gender as the independent variable, the other variables were tested as mediator variables, using the Hayes process. During the various iterations, gender remained a significant variable with the only significant moderator being reporting on phishing attacks.

Table 7: Stepwise regression

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.260[a]	.067	.063	2.006	.067	14.694	1	203	<,001
2	.337[b]	.114	.105	1.960	.046	10.540	1	202	.001

a. Predictors: (Constant), Gender

b. Predictors: (Constant), Gender, Reporting of phishing attacks

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	59.109	1	59.109	14.694	<,001[b]
	Residual	816.579	203	4.023		
	Total	875.688	204			
2	Regression	99.602	2	49.801	12.962	<,001[c]
	Residual	776.086	202	3.842		
	Total	875.688	204			

a. Dependent Variable: Score

b. Predictors: (Constant), Gender

c. Predictors: (Constant), Gender, Reporting of phishing attacks

(Source: Compiled by the authors)

3.6 Study limitations

This study presented two notable limitations. Firstly, the literature reviewed was limited to available English language academic journals and peer-reviewed papers in the online library of databases of the University of Pretoria. Secondly, the data collected from the online survey represents the perceptions of the individual respondents and is not necessarily representative of the views of the wider population of the industries involving financial services, education, law, fraud, and forensics.

The extent to which historical data from simulated phishing campaigns could be used was limited, on account of the considerable variation in the type of phishing simulations that were sent to employees across the two organisations within the financial services industry. It should be borne in mind that different simulation phishing emails were sent to employees and there was little standardisation regarding the language, content, or length of emails sent at different times. This can make it difficult to compare response behaviour over time, across different organisations or message types, in view of differences in motivating factors, such as degree of relevance, interest, or perceived authenticity.

4 CONCLUSION

The purpose of the study was to assess the phishing susceptibility of individuals in South Africa, across the financial services-, education-, legal-, fraud-, and forensic industries. In the course of the study, primary data was collected from surveys across these industries, and anecdotal and anonymised data from simulated phishing attacks was collected from two organisations in the financial services industry.

Previous literature review studies revealed a variety of findings, when assessing demographic information to determine phishing susceptibility. In some instances, non-financial services industries were found to be less susceptible to phishing, compared to the financial services industry. A number of studies indicated that older individuals are more susceptible than younger people, but other studies contradicted these findings. The same goes for gender: a number of inconclusive results exist on the question whether females are more susceptible to phishing, than males. Prior studies concluded that the higher an individual's level of education, the less susceptible they are to phishing. Similarly, the more exposure to phishing training individuals receive prior to starting their professional career, and the more frequently they are made aware of phishing, the less susceptible they are to phishing. When individuals report phishing attacks, the likelihood that they will be phished decreases significantly.

The results of this study indicated that the legal industry; Gen Z and Alpha (25 years and younger); females; individuals holding only a matric qualification; individuals that did not receive phishing training prior to entering the workforce; individuals that have never received phishing awareness training; and those who did not report phishing attacks, are the most susceptible. This suggests that these individuals are most susceptible to phishing. In addition, the results of the study pointed to a statistically significant contribution by two demographic categories, namely (1) gender and (2) people who do not report phishing attacks in the workplace. In South Africa, therefore, females who do not report phishing attacks can be considered to be more susceptible to phishing.

Overall, the results of this research are valuable, not only for the participants in this study but also for organisations within other industries. Organisations can benefit from the susceptibility score developed by this study, in order to identify individuals who are likely to be susceptible to phishing.

The findings of the study should be considered in the light of the limitations. The literature included was limited to available English-language academic journals and peer-reviewed papers in the online library of databases of the University of Pretoria. The data collected from the online survey represents the perceptions of the individual respondents.

For future research purposes, this study could be replicated within other industries in South Africa, and could also assess why individuals are susceptible to phishing.

REFERENCES

Abroshan, H., Devos, J., Poels, G. & Laermans, E. 2021. COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, *9*:121916-121929. https://doi.org/10.1109/ACCESS.2021.3109091

Afandi, N.A. & Hamid, I.R.A. 2021. Covid-19 phishing detection based on hyperlink using k-nearest neighbor (KNN) algorithm. *Applied Information Technology and Computer Science*, *2*(2):287-301. [Online]. https://publisher.uthm.edu.my/periodicals/index.php/aitcs/article/view/2317/1288 (Accessed 30 October 2023).

Alohali, M., Clarke, N., Li, F. & Furnell, S. 2018. Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information and Computer Security*, *26*(3):306-326. https://doi.org/10.1108/ICS-03-2018-0037

Ashiru, A. 2021. Identifying phishing as a form of cybercrime in Nigeria. *Journal of International Law and Jurisprudence*, *12*(2):176-186.

Australian Competition and Consumer Commission. 2020. *Targeting scams 2019: A review of scam activity since 2009.* [Online]. ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-2019-a-review-of-scam-activity-since-2009 (Accessed: 10 September 2022).

Berre, T.T., Eggemoen, V., Haugrud, T.D., Le, W.H. & Sandnes, M. 2022. *Phishing awareness among students at NTNU.* [Online]. NTNU. https://folk.idi.ntnu.no/baf/eremcis/2022/Group17.pdf (Accessed: 12 September 2022).

Bhadane, A. & Mane, S.B. 2018. State of research on phishing and recent trends of attacks. *I-Manager's Journal on Computer Science*, *5*(4):14-35. https://dx.doi.org/10.26634/jcom.5.4.14608

Bidgoli, M., Knijnenburg, B.P., Grossklags, J. & Wardman, B. 2019. Report now. Report effectively. Conceptualizing the industry practice for cybercrime reporting*. Proceedings of the 2019 Anti-Phishing Working Group Symposium on Electronic Crime Research (eCrime), Pittsburgh, November 13-15*. 1-10. [Online]. IEEE. https://ieeexplore.ieee.org/document/9037577 (Accessed: 5 November 2022).

Castillo, D. 2021. One click from disaster: An exploratory study of the impact of employees' perception of email protection on phishing susceptibility. PhD thesis. St. Thomas University: Miami Gardens. [Online]. ProQuest. https://www.proquest.com/openview/649284a7f1c7f163a9aa6750e5de75e2/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y (Accessed: 28 September 2022).

Cisco. 2022. *What is phishing?* [Online]. Cisco Systems, Inc. [Online]. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#:~:text=Phishing%20is%20the%20practice%20of,malware%20on%20the%20victim's%20device (Accessed: 27 August 2022).

Cosio, N. 2021. *Are you smarter than a hacker?* [Online]. Surfshark. https://surfshark.com/blog/phishing-quiz (Accessed: 27 August 2022).

Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. 2022. Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*, *27*:4729-4752. https://doi.org/10.1007/s10639-021-10806-7

De Bona, M. & Paci, F. 2020. A real world study on employees' susceptibility to phishing attacks*. Proceedings of the 15th International Conference on Availability, Reliability and Security, Dublin, August 25-28*. [Online]. ACM Digital Library. https://dl.acm.org/doi/abs/10.1145/3407023.3409179 (Accessed: 9 September 2022).

Diaz, A., Sherman, A.T. & Joshi, A. 2020. Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, *44*(1):53-67. https://doi.org/10.1080/01611194.2019.1623343

Georgiadou, A., Mouzakitis, S. & Askounis, D. 2022. Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal*, *35*:486-505. https://doi.org/10.1057/s41284-021-00286-2

Google. 2022. *Can you spot when you're being phished?* [Online]. Google. https://phishingquiz.withgoogle.com/ (Accessed: 27 August 2022).

Hayes, A.F. 2022. *Introduction to mediation, moderation, and conditional process analysis. A regression-based approach*. 3rd ed. New York, NY: Guilford Press.

Khatri, K.K. & Karki, D. 2022. Uses and limitations of quantitative research in English language education. *Bouddhik Abhiyan*, *7*(1):70-75. https://doi.org/10.3126/bdkan.v7i1.47565

KnowBe4. 2022a. *Phishing by industry benchmarking report.* [Online]. KnowBe4. https://www.knowbe4.com/hubfs/2022-Phishing-by-Industry-Benchmarking-Report.pdf?hsCtaTracking=5545cbd3-4d37-4ec2-a8120b2830feefbb%7C753ae012-a008-46ca-ade5-5035e74f6667 (Accessed: 10 September 2022).

KnowBe4. 2022b. *Who we are.* [Online]. KnowBe4. https://www.knowbe4.com/about-us/ (Accessed: 29 September 2022).

Kunnan, A.J. & Liao, C.L. 2019. Modeling relationships among young learners' self-assessment, learning attitude, and language test performance. *The Journal of Asia TEFL*, *16*(2):701-710. http://dx.doi.org/10.18823/asiatefl.2019.16.2.18.701

Lain, D., Kostiainen, K. & Capkun, S. 2022. Phishing in organizations: Findings from a large-scale and long-term study. *Proceedings of the 2022 IEEE Symposium on Security and Privacy, San Francisco, May 22-26*. 842-859. [Online]. IEEE. https://ieeexplore.ieee.org/abstract/document/9833766 (Accessed: 7 November 2022).

Li, W., Lee, J., Purl, J., Greitzer, F.L., Yousefi, B. & Laskey, K.B. 2020. Experimental investigation of demographic factors related to phishing susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Science*, Maui, 7-10 January 7-10. 2240-2249. [Online]. University of Hawai'i at Mānoa Library. https://scholarspace.manoa.hawaii.edu/items/fd80b2a4-e51d-4704-bd8a-d2377a5d00aa (Accessed: 29 September 2022).

Lin, T., Capecci, D.E., Ellis, D.M., Rocha, H.A., Dommaraju, S., Oliveira, D.S. & Ebner, N.C. 2019. Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction*, *26*(5):1-28. https://doi.org/10.1145/3336141

Mannix, T., Petric, G., Eriksen, A., Paglia, J. & Roer, K. 2022. Phishing susceptibility across industries. In: Schmorrow, D.D. & Fidopiastis C.M. (Eds.) *Augmented cognition.* Cham: Springer. https://doi.org/10.1007/978-3-031-05457-0_6

Marikyan, D. & Papagiannidis, S. 2023. *Protection motivation theory: A review*. [Online]. TheoryHub. https://open.ncl.ac.uk/theory-library/protection-motivation-theory.pdf (Accessed: 12 April 2023).

Nowitz, J. 2018. *A modern perspective on phishing: An investigation into susceptibility to phishing attacks between mobile and desktop email clients*. Master's thesis. Victoria University of Wellington: Wellington. [Online]. Victoria University of Wellington. http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/7907/thesis_access.pdf?sequence=5 (Accessed: 26 September 2022).

Okpa, J.T., Ajah, B.O. & Igbe, J.E. 2020. Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology*, *14*(2):460-478. https://doi.org/10.5281/zenodo.4770111

Pósa, T. & Grossklags, J. 2022. Work experience as a factor in cyber-security risk awareness: A survey study with university students. *Journal of Cybersecurity and Privacy*, *2*(3):490-515. https://dx.doi.org/10.3390/jcp2030025

Powers, J. 2018. *Test your phishing security knowledge with this quiz.* [Online]. TechTarget. https://www.techtarget.com/searchenterprisedesktop/quiz/Test-your-phishing-security-knowledge-with-this-quiz (Accessed: 27 August 2022).

Qualtrics. 2022. *Projects*. [Online]. Qualtrics. https://qfreeaccountssjc1.az1.qualtrics.com/Q/MyProjectsSection (Accessed: 9 September 2022).

Ravi, R., Shillare, A.A., Bhoir, P.P & Charumathi, K.S. 2021. URL based email phishing detection application. *International Research Journal of Engineering and Technology*, *8*(4):355-360.

Schuetz, S.W., Lowry, P.B., Pienta, D.A. & Thatcher, J.B. 2020. The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, 37(3):723-757. https://doi.org/10.1080/07421222.2020.1790187

Shahbaznezhad, H., Kolini, F. & Rashidirad, M. 2021. Employees' behaviour in phishing attacks: What Individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6):539-550. https://doi.org/10.1080/08874417.2020.1812134

Shaw, C. 2020. *Why phishing works and the detection needed to prevent it.* Master's dissertation. Utica College: Utica. [Online]. ProQuest. https://www.proquest.com/docview/2446039541?pq-origsite=gscholar&fromopenview=true (Accessed: 25 June 2022).

Smith, K.T., Jones, A., Johnson, L. & Smith, L.M. 2019. Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1):42-60. https://doi.org/10.1108/JICES-02-2018-0010

SonicWall. 2022. *Sonicwall phishing IQ test.* [Online]. SonicWall. https://www.sonicwall.com/phishing-iq-test-landing/ (Accessed: 27 August 2022).

Sumner, A., Yuan, X., Anwar, M. & McBride, M. 2022. Examining factors impacting the effectiveness of anti-phishing trainings. *Journal of Computer Information Systems*, *62*(5):975-997. https://doi.org/10.1080/08874417.2021.1955638

Sun, Z. 2022. *In the light and in the shadows: Human-centred analysis in cybercrime.* PhD thesis. Arizona State University: Phoenix. [Online]. ASU Library. https://keep.lib.asu.edu/items/168600 (Accessed: 2 October 2022).

Taib, R., Yu, K., Berkovsky, S., Wiggens, M. & Bayl-Smith, P. 2019. Social engineering and organisational dependencies in phishing attacks. *Proceedings of the 17th IFIP Conference on Human-Computer Interaction, Paphos, September 2-6*. 564-584. [Online]. Springer Nature. https://link.springer.com/chapter/10.1007/978-3-030-29381-9_35 (Accessed: 25 September 2022).

Tian, C., Jensen, M.L. & Durcikova, A. 2018. Phishing susceptibility across industries: The differential impact of influence techniques. *Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, December 13*. 1-16. [Online]. AIS eLibrary. https://aisel.aisnet.org/wisp2018/25/ (Accessed: 1 October 2022).

Unchit, P., Das, S., Kim, A. & Camp, L.J. 2020. Quantifying susceptibility to spear phishing in a high school environment using signal detection theory. *Proceedings of the 14th International Symposium on Human Aspects of Information Security and Assurance*, *Lesbos, July 8-10*. 109-120. [Online]. Cornell University. https://arxiv.org/pdf/2006.16380.pdf (Accessed: 8 September 2022).

Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z. & Wang, X. 2022. Predicting user susceptibility to phishing based on multidimensional features. *Computational Intelligence and Neuroscience*, (January):1-11. https://doi.org/10.1155/2022/7058972

Verizon. 2022. *Data breach investigations report.* [Online]. Verizon. https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 10 September 2022).

Volkamer, M., Sasse, M.A. & Boehm, F. 2020. Analysing simulated phishing campaigns for staff. *Proceedings of the 25th European Symposium on Research in Computer Security, Guildford, September 14-18*. 1-16. https://doi.org/10.1007/978-3-030-66504-3_19

Warda, A. & Samaddar, J. 2022. A primary study on user perception of phishing in the banking sector. *SJCC Management Research Review*, *12*(1):59-79.

Wokabi, F.M. 2019. *Employee awareness on social engineering threats in the financial sector.* Master's dissertation. Strathmore University: Nairobi. [Online]. Strathmore University. http://su-plus.strathmore.edu/handle/11071/6784 (Accessed: 7 November 2022).

Yeoh, W., Huang, H., Lee, W.S., Al Jafari, F. and Mansson, R., 2022. Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems*, *62*(4):802-821. https://doi.org/10.1080/08874417.2021.1919941

Zhuo, S., Biddle, R., Koh, Y.S., Lottridge, D. & Russello, G. 2022. SoK: Human-centered phishing susceptibility. *Arxiv*, (February):1-18. https://doi.org/10.48550/arXiv.2202.07905

APPENDIX A - PHISHING SURVEY

Section A

Question 1

Dear Participant

You are invited to participate in an academic cybercrime research study conducted by an MPhil Fraud Risk Management student from the Department of Auditing at the University of Pretoria. The purpose of the study is to determine susceptibility to phishing attacks.

Please note the following:

- The participants benefit from this survey by increasing their awareness about phishing attacks and will receive the results of the findings on request.
- This is an anonymous study survey as your name will not appear on the survey. The answers you give will be treated as strictly confidential as you cannot be identified in person based on the answers you give.
- Your participation in this study is very important to us. You may, however, choose not to participate and you may also stop participating at any time without any negative consequences.
- Please answer the questions in the attached survey as completely and honestly as possible. This should not take more than 15 minutes of your time.
- The results of the study will be used for academic purposes only and may be published in an academic journal.
- Please contact my supervisor if you have any questions or comments regarding the study.
- In research of this nature, the supervisor may wish to contact respondents to verify the authenticity of data gathered by the researcher. It is understood that any personal contact details that you may provide will be used only for this purpose, and will not compromise your anonymity or the confidentiality of your participation.

Please indicate:

- Yes, I have read and provided consent.
- No, I don't provide consent.

Section B

Question 2

In which industry are you employed?

- Education industry
- Financial services industry
- Legal industry
- Fraud and forensic industry
- Other

Question 3

Please indicate your age:

- 25 years old and younger (Gen Z and Alpha)
- 26–41 years old (Millennials)
- 42–57 years old (Gen X)
- 58–67 years old (Baby Boomers)
- 68 years old and older (Silent Generation)
- Prefer not to disclose

Question 4

Please indicate your gender:

- Male
- Female
- Prefer not to disclose

Section C

Question 5

Please indicate whether you received phishing training before you started your professional career:

- Yes
- No
- I don't know

Question 6

Please indicate the frequency of phishing awareness training at your organisation:

- Never
- Randomly
- Annually
- Bi-annually
- Quarterly
- Monthly

Question 7

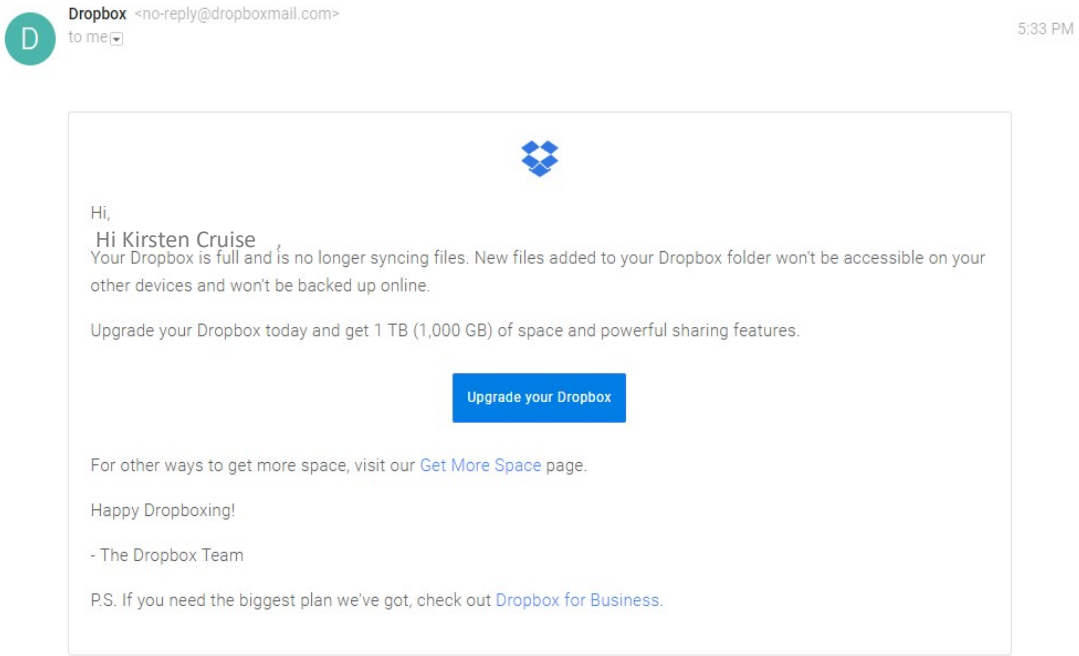
Please indicate whether you have ever reported a phishing attack when it was sent to your work email address:

- Yes
- No
- I don't know

Section D

For the rest of the survey, assume you are Kirsten Cruise. This is a fictitious name created for this survey. *Please take note of the abbreviation Uniform Resource Locators (URL).*

Question 8 - Dropbox

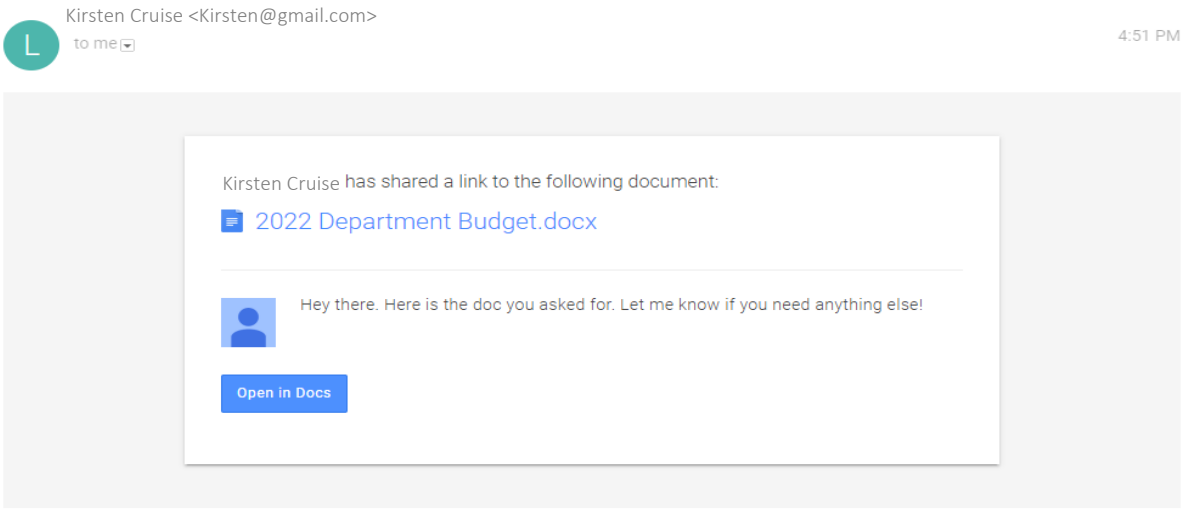


Uh no, looks like you are out of storage! If you hover over the "Get More Space" link the URL is as follows: https://www.dropbox.com/help/space/get-more-space. The URL for the "Dropbox for Business" is https://www.dropbox.com/business.

Is this a phishing attack?

- Yes
- No
- I don't know

Question 9 - Departmental Budget

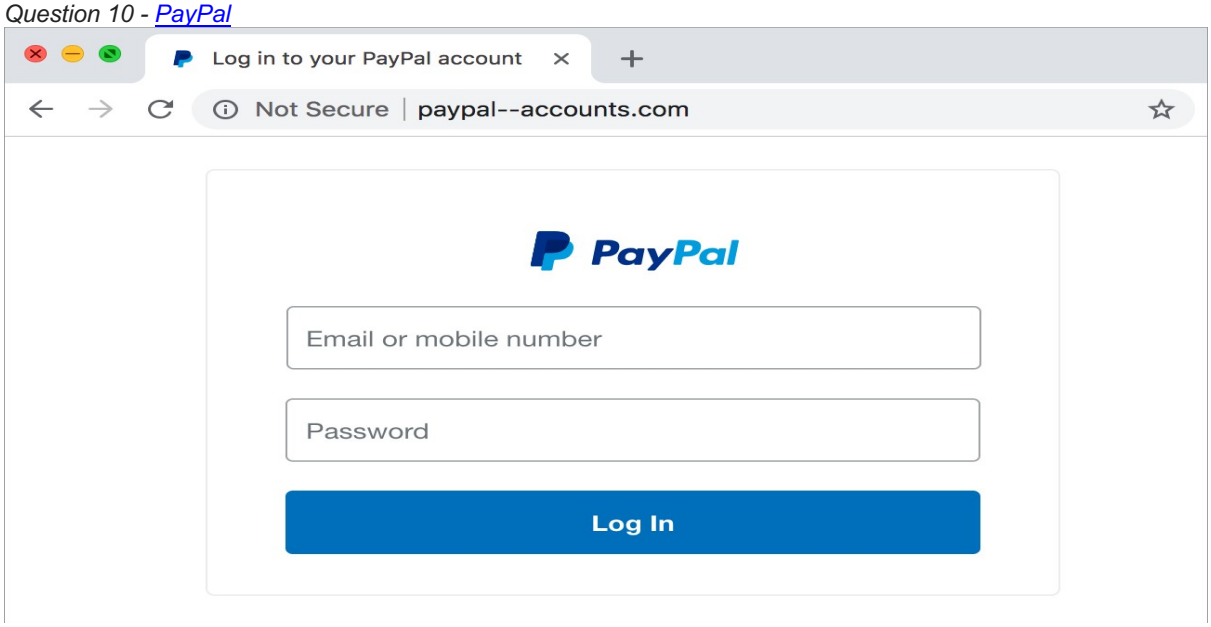


You are part of the department's budgeting team and you received this email from Google Docs. If you hover over the link "2022 Department Budget.docx" then the URL is as follows: http://drive--google.com/kirsten.smith.

Is this a phishing attack?

- Yes
- No
- I don't know

Question 10 - PayPal

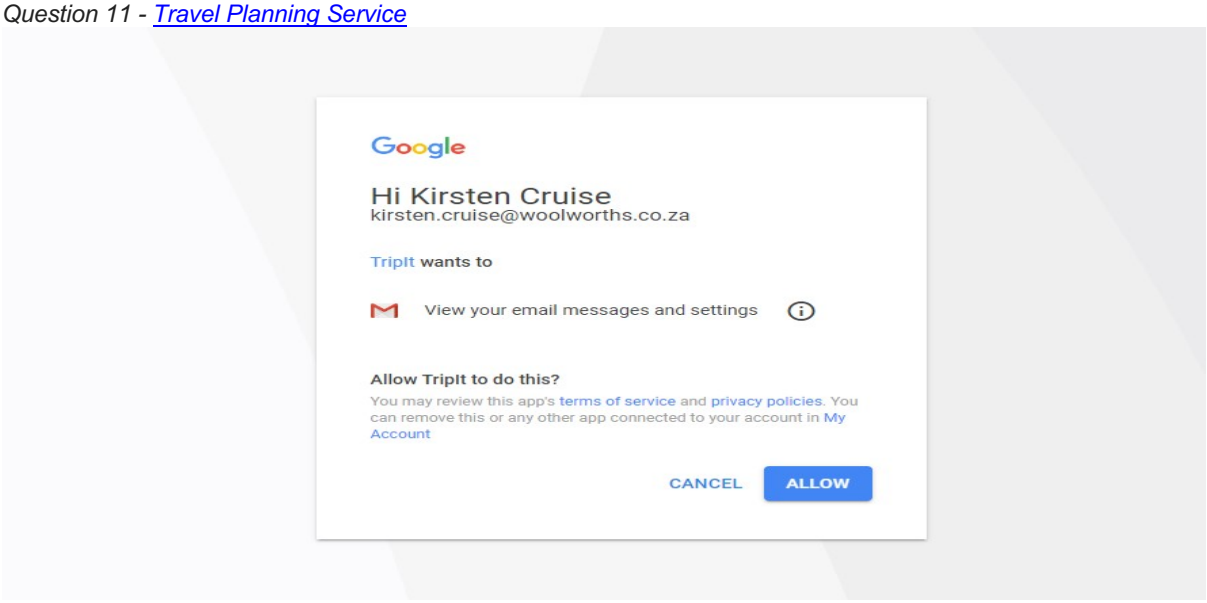


You are buying concert tickets online and you are about to make an online payment through PayPal.

Is this a phishing attack?

- Yes
- No
- I don't know

Question 11 - Travel Planning Service



You have signed up for a travel planning service. There is no URL available for the "TripIt" link. There are three other URLs available:

“terms of reference”: https://www.tripit.com/uhp/userAgreement

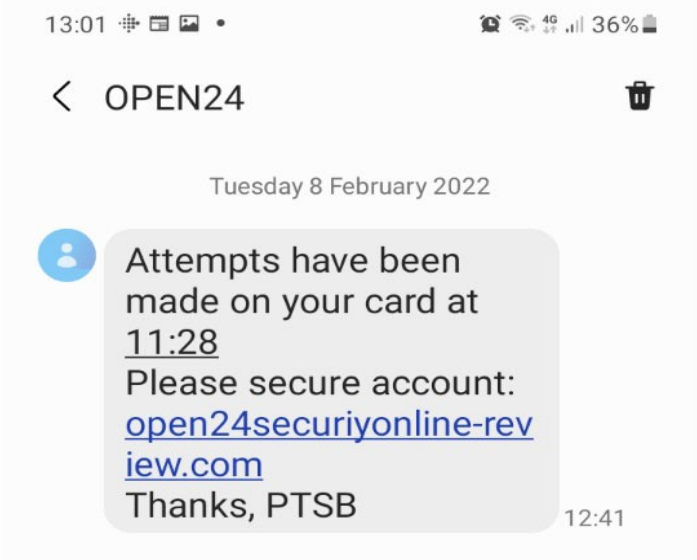
“privacy policies”: https://www.tripit.com/uhp/privacyPolicy

“My Account”: https://security.google.com/settings/security/permissions

Is this a phishing attack?

- Yes
- No
- I don’t know

Question 12 - PTSB Bank

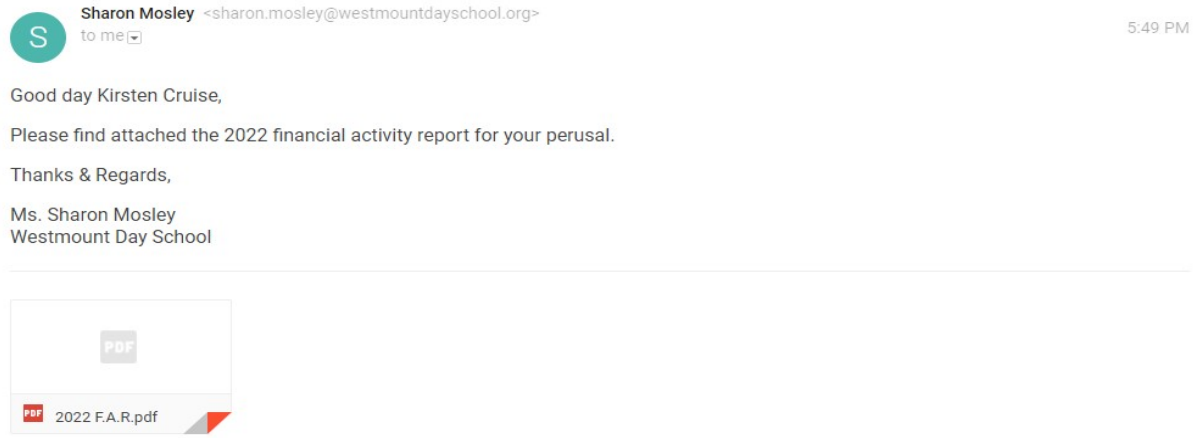


You bank with PTSB Bank and they send you a text message.

Is this a phishing attack?

- Yes
- No
- I don’t know

Question 13 - School

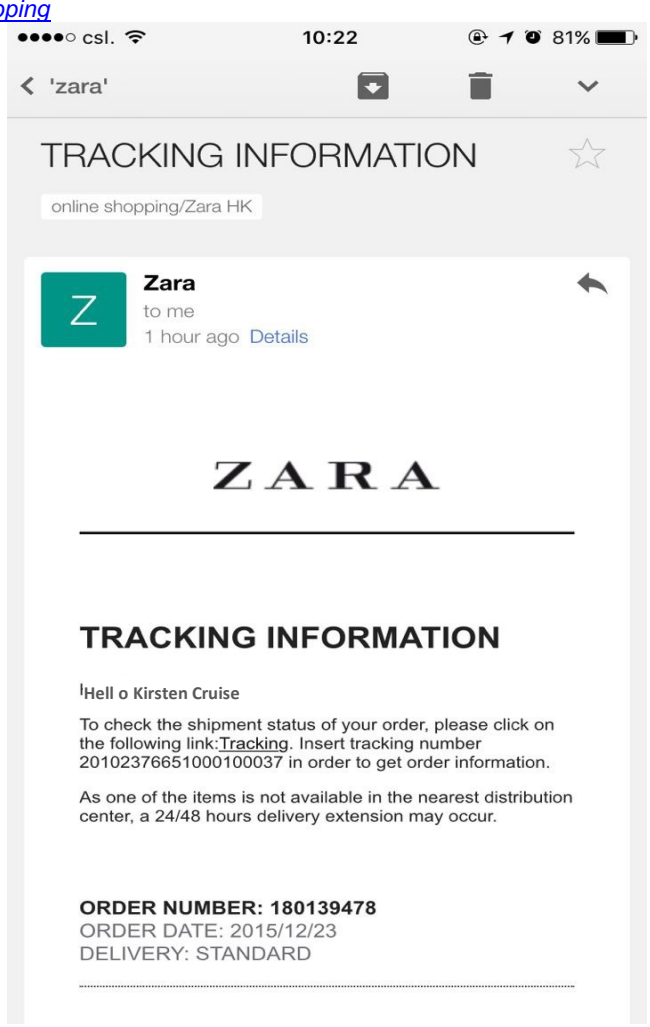


You have received a new kind of report from the school. Usually, their emails come from sharon.mosley@westmountschool.org.

Is this a phishing attack?

- Yes
- No
- I don't know

Question 14 - Online shopping

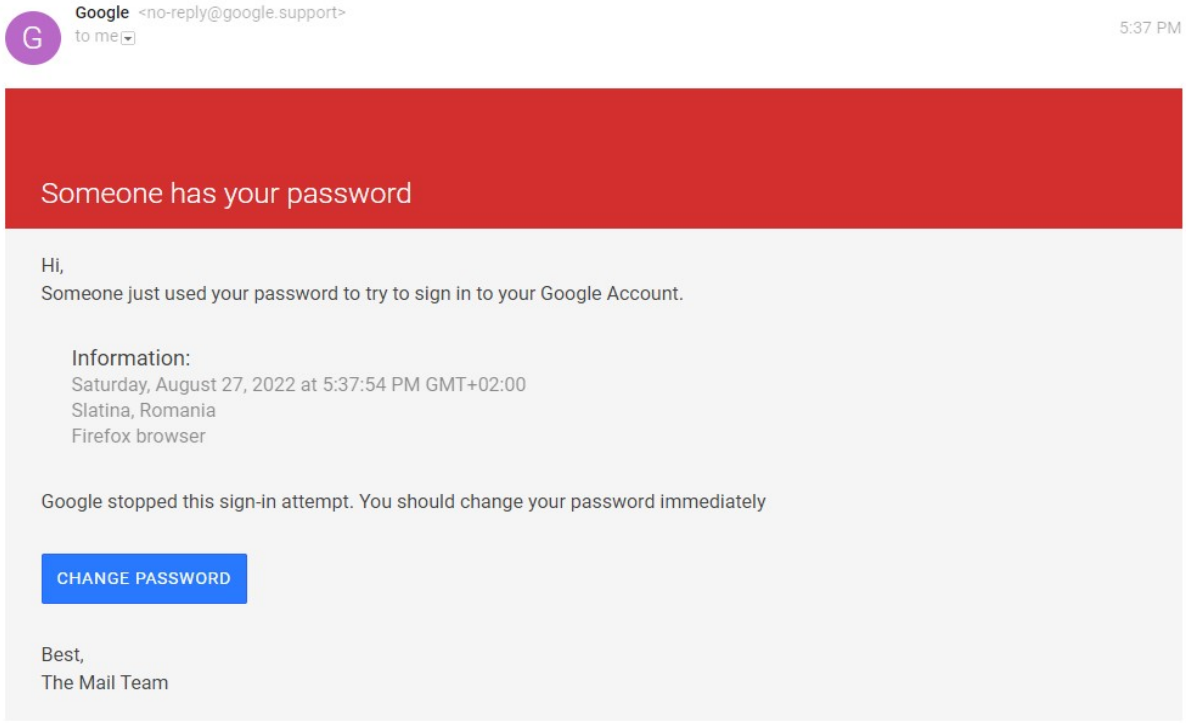


You have done online shopping from Zara. Your order number is 20102376651000100037.

Is this a phishing attack?

- Yes
- No
- I don't know

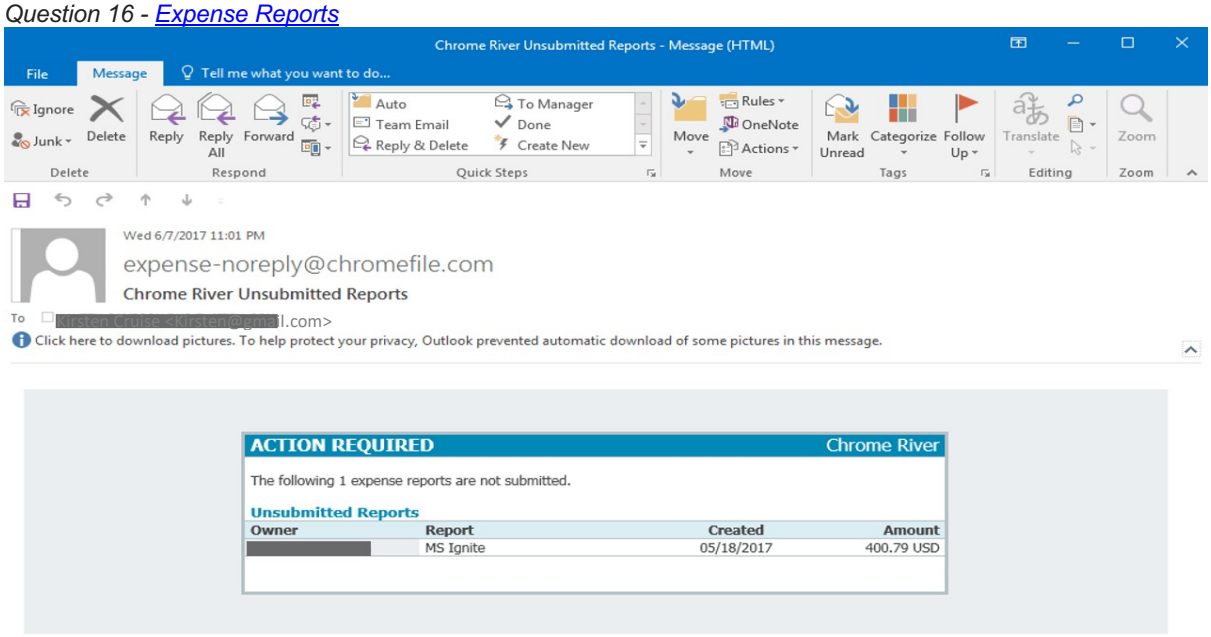
Question 15 - Google Account



Someone has been trying to access your account. The URL on the "change password" button is as follows: http://myaccount.google.com-securitysettingpage.mlsecurity.org/signonoptions/ Is this a phishing attack?

- Yes
- No
- I don't know

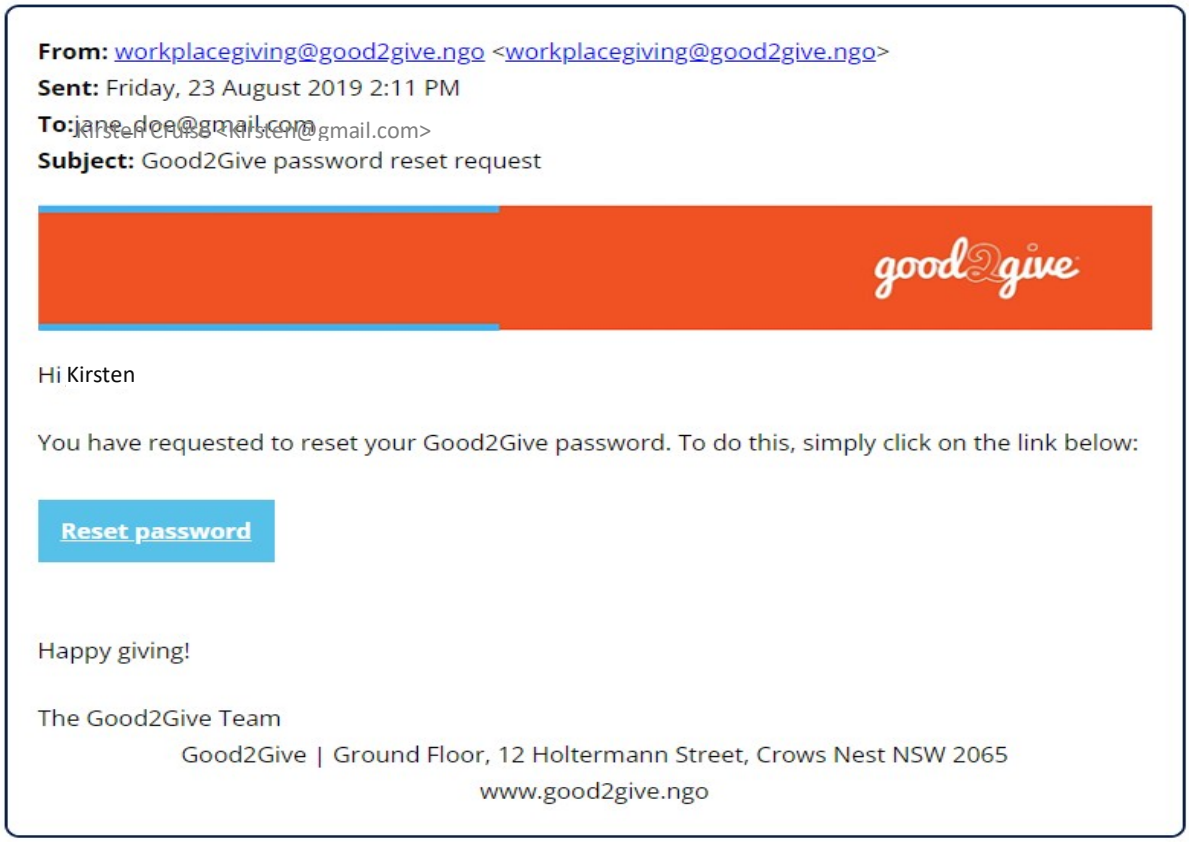
Question 16 - Expense Reports



Is this a phishing attack?

- Yes
- No
- I don't know

Question 17 - Donation



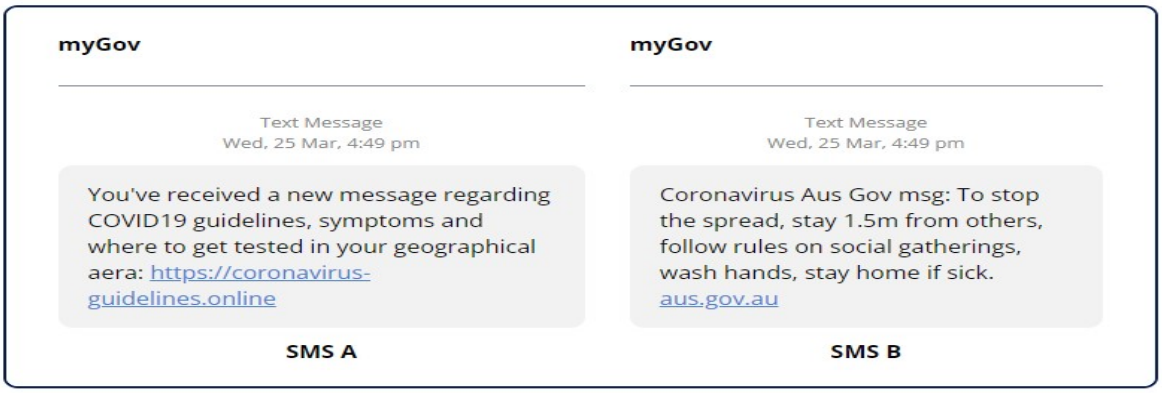
You are about to donate; the URL of the "Reset password" button is as follows: https://signin.good2give.ngo/Account/ResetPassword?userId=6b4551bc-3f7e-20049642-&code=CfDJ8KKFSWQ9ffF4yvvZEi

Is this a phishing attack?

- Yes
- No
- I don't know

Question 18 - COVID-19

Select which one of these SMS notifications is a phishing attack.



- A
- B
- I don't know

Question 19 - KnowBe4

KnowBe4 specialises in cybercrime awareness training. The URL to activate your account is as follows: https://eu.knowbe4.com/ui/users/signup/user_details/ZKg4enpNqJYKTKk1zxbz Is this a phishing attack?

- Yes
- No
- I don't know

Question 20

An email from your line manager asks for the names, addresses, and banking information of your organisation's top clients. The email says it's urgent and asks you to please reply right away. You should reply right away.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

Question 21

If you fall for a phishing attack, what should you do to limit the damage?

- Delete the phishing email.
- Unplug your computer. This will deactivate the installation of possible malware.
- Change any compromised usernames and passwords.

Thank you for your participation. This is the end of the survey.