Information & Management 60 (2023) 103858

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model

Edwin Donald Frauenstein [a], Stephen Flowerday [b], Syden Mishi [c], Merrill Warkentin [d,*]

[a] Department of Information Technology, Faculty of Science, Engineering and Technology, Walter Sisulu University, PO Box 1421, East London 5241, South Africa
[b] School of Cyber Studies, University of Tulsa, 800 S. Tucker Dr., Tulsa, OK 74104, USA
[c] Department of Economics, Nelson Mandela University, South Campus, P O Box 77000, Summerstrand, Gqeberha 6031, South Africa
[d] Department of Management & Info Systems, College of Business, Mississippi State University, 302 V McCool Hall, P.O. Box 9581, Mississippi State, MS 39762-9581 USA

ARTICLE INFO

Keywords:
Phishing
Big Five
Personality traits
Habit
Social media
Heuristic processing
Systematic processing
Heuristic-systematic processing model

ABSTRACT

Frequent and habitual engagement with social media can reinforce certain activities such as sharing, clicking hyperlinks, and liking, which may be performed with insufficient cognition. In this study, we aimed to examine the associations between personality traits, habits, and information processing to identify social media users who are susceptible to phishing attacks. Our experimental data consisted of 215 social media users. The results revealed two important findings. First, users who scored high on the personality traits of extraversion, agreeableness, and neuroticism were more likely to engage in habitual behaviors that increase their susceptibility to phishing attacks, whereas those who scored high on conscientiousness were less likely. Second, users who habitually react to social media posts were more likely to apply heuristic processing, making them more susceptible to phishing attacks than those who applied systematic processing.

1. Introduction

The proliferation of collaborative web technologies has introduced new forms of internet communication, such as instant messengers, video conferencing, cloud services, blogs, really simple syndication, wikis, podcasting, and social networking sites (SNSs). This shift has resulted in a culture of user-generated content with considerably more collaboration amongst users [1]. In particular, the explosion of SNSs has fostered a virtual community that encourages its members to share information, with an estimated 4.7 billion people using SNSs worldwide [2]. SNSs, including their messaging functionalities that mimic email, have become a primary means of electronic communication [3]. Some popular online SNSs include Facebook, Twitter, Instagram, LinkedIn, Snapchat, Pinterest, TikTok, YouTube, ResearchGate, and Xing. Among these, Facebook is the most popular, with an estimated 2.9 billion active monthly users worldwide [4].

SNSs attract members from different cultures and backgrounds, each possessing their own religious beliefs, ethnicity, education, political views, and social class, and are not restricted by geographical boundaries. SNSs encourage their members to create and curate a public profile, share their interests, ideas, photos, music, and videos with other registered users. By design, this social interaction satisfies an innate need to belong [5] and an innate desire to be part of a community [6]. Because SNSs are popular and have afforded users these opportunities, this same environment inadvertently cultivates certain behaviors that give threat agents an opportunity to target vulnerable users.

The Anti-Phishing Working Group (APWG), a global consortium, defines phishing as “a crime employing both *social engineering* and *technical subterfuge* to steal consumers’ personal identity data and financial account credentials” [7]. Phishing is typically carried out through email with the source usually impersonating a financial institution recognizable by the target [8]. The user is persuaded, by a convincing story described in the phishing email, to click on a hyperlink or open a malicious file contained in the email. The link subsequently diverts the user to an external fake webpage, unbeknownst to the user, imitating the original website. The user submits their login information, which is captured by the phisher and subsequently used to carry out their criminal objectives [9]. Phishing remains one of the biggest cybersecurity threats and affects millions of Internet users, causing substantial monetary losses for both organizations and individuals [10]. According to the APWG report [7], in the third quarter of 2022, APWG observed a record 1270,883 phishing attacks, making it the worst

[*] Corresponding author.
E-mail address: m.warkentin@msstate.edu (M. Warkentin).

https://doi.org/10.1016/j.im.2023.103858
Received 17 June 2021; Received in revised form 5 September 2023; Accepted 6 September 2023
Available online 9 September 2023

quarter for phishing that APWG has ever observed. Phishers take advantage of seasonal events in crafting their messages, which make it difficult for unsuspecting users. For example, security company Netwrix [11], discovered that nearly half (48%) of the organizations surveyed reported phishing attacks during the first three months of the coronavirus pandemic. Phishing is generally known to be email-based, but it can also be occur in other environments such text messages and on SNSs [9,12]. Krombholz, Hobel, Huber, and Weippl [13] point out that users' awareness of phishing on SNSs is still comparatively low compared with emails. However, a study by Diaz et al. [14] found that even users with knowledge and awareness of phishing were susceptible to phishing.

Since Facebook's inception[1] in the international market in September 2006, its once plain and minimalistic design has continued to evolve, incorporating new features to enhance the user experience while also using persuasive techniques to increase interaction and user retention [15]. Over the past fifteen years, some prominent features introduced into the Facebook interface include advertisements and Facebook "pages" (November 2007), the "like" function (February 2009), instant messenger (August 2011), timeline (September 2011), safety check (October 2014), like reactions/emoticons (February 2016), the marketplace (October 2016), Messenger rooms (July 2020), and Facebook Reels (September 2021). Although these technical features enhance the user experience, they can be used effectively by social engineers to create and spread deceitful posts such as controversial videos, conspiracy theories, fake news, and advertisements that are of interest or benefit to the user [16]. Moreover, they are used to create fake accounts, fake apps and groups, and to distribute malicious content [17]. Kahimise and Shava [18] reported the most common threats on SNSs are phishing, social engineering (SE), spamming, cyberbullying/cyberstalking, data leakage, and malware attacks. Of these threats, social engineers and phishers can influence users that allow them to obtain users' personal information through phishing attacks. Smartphone users also tend to be complacent in their security behavior and demonstrate high levels of trust toward their apps [19]. This also poses a risk because SNSs, in particular Facebook, are mainly accessed via smartphone apps [20].

While the technological features embedded in SNS platforms can be leveraged by social engineers, these features bring out certain behaviors of their user base that can be exploited. Owing to individual characteristics such as *personality traits*, the posts on SNSs can effectively trigger the emotions of certain users, luring them into performing actions that can put them at risk of phishing [21]. Furthermore, the frequent use of clicking on and sharing links, liking posts, copying and posting messages, and uploading and downloading media content may have the potential to unintentionally lead to the formation of undesirable *habits* [22]. A "habitual mind-set" can make an individual less attentive to new information and courses of action [23]. As a result, as users are repeatedly performing a behavior out of habit on these sites, they can become lax and unintentionally click on or share phishing messages because they do not apply sufficient *cognitive processing* [24]. To reduce phishing susceptibility, ideally, users must apply a *systematic* mode of information processing when presented with phishing messages. However, as users receive a proliferation of information on SNSs, originating from different sources at any given time, they are inclined to apply a *heuristic* mode of processing to resourcefully save time and effort. As a result, users might not spend adequate time and apply enough effort to analyze a persuasive message, and consequently may overlook suspicious characteristics in a malicious message that could help identify the message as phishing. Social media users might also not *perceive any risks* on these sites [25] or they may think that risks will be more likely to happen to others [26,27]. Moreover, some users might not make an effort or have the aptitude to verify the validity and authenticity of the origins of messages. To elaborate, some users may not have the required *computer self-efficacy* to go outside the realm of Facebook to search other websites to verify the authenticity of the message. Because of *social norms*, some Facebook users post messages with the intention of being perceived in a favorable light (hence the usefulness of the "like" feature), but do not think about the unintended consequences of what they are posting, misjudging the culture and social norms of their social circles [28]. This also has the potential to cause users to overlook malicious posts on SNSs because they might not spend enough cognitive effort to think about the reason for their sharing or posting of content or messages even if it might be fake news [29]. Each of these potential areas of concern subsequently increases the risk of overlooking phishing attacks. The main research question for this study is: To what extent will dispositional factors such as personality traits, habits, and information processing on Facebook influence susceptibility to phishing attacks? Consequently, this study aims to examine the influences of each of these areas on one another, subsequently identifying users who are at risk to phishing attacks.

2. Background

A growing body of research has primarily focused on two approaches to protect users from phishing, namely a technological approach and a behavioral approach [30]. For several years, countermeasures used to mitigate phishing have largely focused on technological controls that have continued to make gains in phishing prevention for end users [31]. However, although these technological measures can help mitigate phishing, relying solely on technical measures has been widely criticized as insufficient because phishing techniques evolve as technology evolves [30,32].

While having a trusting disposition is generally a good personal characteristic because it facilitates communication [33], such a quality is often frowned on in the information security domain and pointed out as a "weakness" that requires fixing [34]. The "blame-the-victim" approach has resulted in scholars frequently citing humans as the "weakest link" in the security chain [35] and, as such, has led researchers to turn their attention to exploring behavioral vulnerabilities and their interrelationships and to develop interventions to address these vulnerabilities [36]. As a result, research efforts were directed toward educating the human element to change their current behavior [37]. Other scholars also explored financial incentives to encourage improved anti-phishing attentiveness [38]. Persuasion techniques, such as fear appeals, has shown to encourage compliance with information security policies [39].

In the context of SNSs, Facebook offer no phishing countermeasures to protect its users, apart from general security advice through their online Help center. Under the section "What steps can I take to protect myself from phishing on Facebook?" users are informed to: "Look out for suspicious emails or messages, Do not click suspicious links, Do not respond to these emails, and Get alerts for unrecognized logins" [40]. Exactly the same advice is provided for Instagram users. To a certain extent, these interventions have not yielded the desired results because studies have shown that users who consider themselves to be aware of phishing have not demonstrated this in their behavior [14,41].

Security scholars have identified, used, or adapted popular behavioral theories pertaining to attitudinal change such as the theory of reasoned action, the theory of planned behavior, protection motivation theory, technology acceptance model, social learning theory, social cognitive theory, and general deterrence theory to gain new insights into the behavioral problems of users [19,42–45]. However, as pointed out by Kearney and Kruger [44], behavioral theories on their own do not provide adequate solutions to adverse behavior. Because individuals each possess their own unique set of vulnerabilities, addressing these by means of a one-size-fits-all approach has limitations. This has prompted many researchers to explore individual differences in characteristics and to examine their influence on user susceptibility to SE and phishing

[1] For the purposes of this research, we use Facebook as an example of SNSs, a choice that allows us to provide a relevant context for exploration of this phenomenon. However, our results can also apply to other SNSs.

[46–55]. In particular, prior literature has shown that certain people with particular personality traits exhibit behaviors that can make them more vulnerable to phishing than others [56–59]. This is to be expected: prior research has shown that different personalities exhibit certain internet behaviors [60]. Gratification can also result from performing certain behaviors on SNSs [61]. In this regard, as users frequently engage on SNSs, this could lead to the formation of certain habits that might make some users vulnerable to deception [62]. Prior literature has also shown that the mode in which users cognitively process information could also put them at risk of phishing attacks [63–66]. In this regard, certain habits may influence the mode in which the user will cognitively process the information they receive on these sites.

All of these aforementioned aspects mentioned highlight the susceptibility of social media users to phishing attacks. A systematic review and meta-analysis conducted by Parker and Flowerday [67] confirmed the variables of personality traits, habits, and information processing to be factors that can make users susceptible to phishing on SNSs. Moreover, a study by Alotaibi [68] also considered that these components can make LinkedIn users susceptible to SE attacks. By examining the previously mentioned relationships, this study proposes a theoretical model that can help identify users who are vulnerable to phishing; this serves as the objective for this study. Previous research by Frauenstein and Flowerday [12] investigated the Big Five personality traits and their influence on information processing which, depending on the processing mode, were shown to have an effect on phishing susceptibility. The Big Five comprises the five overarching domains of openness, conscientiousness, extraversion, agreeableness, and neuroticism [69], which are usually represented by the acronym OCEAN or CANOE. This study builds upon the research conducted by Frauenstein and Flowerday [12] by examining the influence of the habit construct and its mediating role between personality traits and information processing. Furthermore, this study investigates the impact of other behavioral factors, such as perceived risk, social norms, and computer self-efficacy, on susceptibility to phishing. The contribution of this study is novel because no prior study has combined these different variables into a single model. This study also uniquely explores the impact of the integration of email functionality into social media. By doing so, this study provides a comprehensive, clearer view of characterizing individuals at risk to the phishing deception process measuring phishing in a unique way. Accordingly, the following section discusses each of the variables considered to be influential in phishing susceptibility and serves as the theoretical foundation for this study.

3. Theoretical foundation

3.1. Social network phishing

Vishwanath [24] alludes to email-based phishing attacks as simple and one dimensional because they typically involve a one-step attack process. Anecdotal evidence suggests users should be made aware of the following interventions they can use to mitigate email-based phishing: (1) do not trust emails that do not specifically mention the recipient by name, (2) look out for spelling and grammatical errors and the domain name, (3) understand that personal or sensitive information (i.e., account numbers, passwords) should not be given out via email or phone, (4) check whether the website connection is secure by looking for Hypertext Transfer Protocol Secure (HTTPS) and the padlock icon in the web address bar, (5) hover the cursor over a suspicious link to see where it is directed to and (6) do not click on links or attachments originating from unknown sources. In addition, Binks [70] puts forward the most obvious point (but perhaps not so obvious to a victim), that is, when an offer is too good to be true, it almost certainly is a scam. However, some of these areas have their own limitations. For example, Schneier [34] states that educating users not to click on links is futile, as for decades users have been trained to click on links, which is necessary for navigating websites. Vishwanath et al. [52] state that education and training may be ineffective when users' online habits determine their likelihood of being deceived. Moreover, educating users to positively identify legitimate websites by looking out for HTTPS can be a pointless exercise. Phishers are aware of this and thus more than half of all phishing sites (as of end of first quarter of 2019) use HTTPS [71]. Users are also educated to be mindful of certain organizations that are frequently impersonated, particularly financial institutions, government agencies and e-commerce organizations. In this regard, a study conducted by Frauenstein [72] found that most users, despite receiving no formal training, were more suspicious of phishing emails impersonating financial institutions than of phishing emails emanating from Facebook. As such, and pointed out by Chou et al. [73], it is insufficient for security education and training programes to merely identify the technical characteristics of phishing messages, such as source of email, grammar, spelling and the email subject. All of these precautions are also predicated on the premise that the user's intention is to look out for these characteristics.

In contrast, phishing attacks conducted on SNS are multistaged, with users receiving friend requests often followed by messages [9]. More recently, Vishwanath [24] referred to these attacks as involving a two-level attack process. Compared with email-based phishing, SNSs offer phishers more opportunities for impersonation, tools, and techniques to conduct phishing attacks. Moreover, phishing conducted on SNSs present fewer clues about its deceptive intent [24]. While the default tendency for humans to believe that others are honest helps facilitate cooperation and communication between people, it can also make people vulnerable to the occasional deception [33]. Facebook engenders a greater sense of trust among its users compared with other popular SNSs [26,74]. Moreover, SNSs have fewer limitations on who can be impersonated because an attacker can impersonate a legitimate user, page, or group. By means of SE techniques, the attacker can then use these avenues to further build trust and establish a relationship with the victim. Because there are no restrictions on geographical boundaries on these platforms, the videos, comments, and pictures posted allow phishers to reach a much broader audience, made possible by the sharing feature. Cialdini [75] devised six key principles of persuasion, namely, reciprocity, commitment or consistency, social proof or conformity, authority, liking, and scarcity. Certain persuasion principles incorporated in email-based phishing have been shown to be effective on certain individuals [76] and can also be executed on SNSs [7,12,77]. Much like we judge the trustworthiness of people based on their physical appearance and other cues, users react similarly to SNS posts based on the appearance; this is further enhanced by the aforementioned persuasion principles. Phishing attacks typically combine techniques that leverage on normative commitment, scarcity, and authority in one scenario [54]. Authority is the most used and most effective technique for convincing victims to trust the message [78]. As such, users might not try to verify the validity and authenticity of messages' origins. Prior research has shown that Big Five personality traits influence information-seeking behavior [79].

3.2. Personality traits

SNSs are predominantly used as a tool for self-expression with users frequently posting information about their daily activities, "selfies", and their thoughts and opinions on a variety of topics. To an extent, the information that social network users share reveals certain things about them and their behavior. Social media, by its very nature, encourages a community of openness, participation, and connectedness [80]. Owing to the influence of social norms, some observable behaviors are common across different cultures and age groups, such as the use of emotion icons (or emojis) and internet slang (e.g., lol, omg, lmfao). However, while this might indicate that social media users tend to behave similarly, not all users behave in exactly the same way. For example, some users may post information frequently, whereas others observe passively. Some users may be impulsive, clicking on links that attract their interest and attention while others may do this when in an emotional state, under the influence of alcohol, or acting out on their frustrations [81]. Some may be inclined to be helpful, open, and trusting of others. These disparities in user behavior have motivated the need to categorize these behaviors more uniformly, leading to the development and adoption of personality trait scales. In view of this, it is not surprising that a large body of literature has investigated personality traits and their influence on social media usage [82–88].

The five-factor model of personality, consisting of the "Big Five" personality traits, is the most widely used and extensively researched model of personality [89]. Behaviors associated with particular personality traits appear to remain predominantly stable after the age of 30 years [90]. However, a more recent, ground-breaking, longitudinal study conducted by Damian, Spengler, Sutu, and Roberts [91] over a 50-year period, using the Big Five measures of John and Srivastava [92], demonstrated that personality traits remain stable and malleable from the age of 16 to 66 years. The characteristics for each of the traits of the five-factor model of personality are broadly described in Table 1 as follows:

Researchers have found that certain persuasion strategies, incorporated in phishing messages, can be effective on certain personality types [95–99]. For example, persuasive messages that incorporate the *urgency* principle may be more effective on impulsive users, targeting users who possess the extraversion trait. The effectiveness of security awareness campaigns for individuals may vary based on their personality traits [100]. While various empirical studies have shown that personality traits have an influence on the outcome of a phishing attack, they have also been criticized for their contradictory findings on certain traits [57]. For example, Moody et al. [51] found that personality traits had no general effects on phishing susceptibility, in contrast to many others studies showing significant relationships. The personality trait model is descriptive and cannot explain *why* humans differ in personality [101]. As such, it is important to consider other behavioral influences that can help explain the differences or variables that can have an effect.

3.3. Habit

Gardner [102] defines habitual behavior as "any action, or sequence of actions, that is controlled by habit". Habit is a learned behavior that can be triggered by a particular context and can begin as intentional and goal-directed behavior (e.g., eating particular foods for weight loss) which could ultimately develop into a healthy routine. Habits are widely considered for the prediction and explanation of human behavior in relatively stable situations [102,103]. According to Verplanken and Aarts [23], habits are "learned sequences of acts that have become automatic responses to specific cues, and are functional in obtaining certain goals". In the context of using information systems, habit refers to the "extent to which people tend to perform behaviors automatically because of learning" [104].

Table 1
Big Five personality trait characteristics [93,94].

Trait	Characteristics
Openness to Experience	Open-minded, independent of judgement, inquisitive, intellectual, creative, seeks new experiences, open to risky behavior, active imagination, non-judgemental, higher cognitive abilities, appreciation for art, nature and different ideas and beliefs
Conscientiousness	Honest, thorough, cautious, trustworthy, organized, hardworking, self-disciplined, responsible, strong-willed, goal-oriented, prudent, follows rules, standards and procedures
Extraversion	Friendly, enthusiastic, excitement, sociable, energetic, talkative, assertive, impulsive, dominant, needs stimulation
Agreeableness	Self-conscious, influenceable, tolerant, compassionate, accepting, modest, polite, cooperative and trusting of others, respect for other people's beliefs and convention
Neuroticism	Emotionally unstable, withdrawal, sensitive, impulsive, need for belongingness, experiences negative emotions (e.g., sadness, anger, fear, pessimism, low-self-esteem, disgust, and guilt)

In the information systems (IS) domain, prior literature on the influence of "habits" has focused on many areas including password management [105–107], social media usage [62,108–113], information systems usage [104], payments using e-commerce [114], e-commerce continuance [115], mobile internet usage [116], and information security policy compliance [117]. Recently, habits have emerged as an area of interest in phishing research [9,30,52,62,118,119].

Social media users do not expect to be faced with phishing attacks [120]. Thus, if they feel that in general the SNS environment poses a low risk to them, they are likely to continue using SNSs frequently [121]. According to Vishwanath [62], users who habitually engage on Facebook are more at risk to falling victim to a social media phishing attack. Vishwanath [62] identified three antecedents for Facebook habits, namely, *consumption frequency, gratifications*, and *automaticity.* The more frequently a habit is performed, the more *automated* the choice process will become [122,123]. The example Vishwanath [9] uses is that habit can be viewed as a lack of awareness or attention and performing the habit could range from being completely conscious (i.e., aware) and intentional at times (checking email on a smartphone) to being unconscious and automatic at other times (checking email while driving). The automaticity aspect of habits offers an advantage by reducing the cognitive effort needed to perform certain activities [122]. In this regard, Turel and Serenko [113] refer to people as "cognitive misers". A variety of cues may *trigger* habit performance, including aspects of the physical environment, other people, and preceding actions in a sequence [124]. Such situational cues may thus trigger the performance of a habit automatically in that context [23,125]. In the context of the present study on SNSs, situational cues may, for example, be boredom, low self-esteem, app notifications, or fear of missing out (FoMO). As a result of the user's repetitive and frequent interaction on SNSs, it is possible for habits to develop from seemingly innocuous behaviors which might include:

- Seeking attention, recognition, or rewards by posting messages, photos, and videos, and then regularly checking to see if members have responded and/or reacted to the post in the form of likes, emojis, comments or receiving newly added followers/subscribers.
- Persistently "liking" or sharing posts on social media platforms.
- Watching videos on Facebook reels, stories, etc.
- FoMO, leading to regularly checking to see what others have posted (i.e. updates, news, memes), checking the Messenger inbox, checking for likes, and checking the notification icon.
- Seeking self-beneficial opportunities, for example goods for sale, discounted goods, competitions, companionship and employment opportunities.

Most of these behaviors appear self-promoting and superficial and are associated with the narcissism trait, one of the Dark Triad personality traits, which consists of narcissism, Machiavellianism, and psychopathy [126]. These behaviors could also, to a certain extent, relate to users with low self-esteem who will thus be more engaged and active in promoting themselves on Facebook to fill this void [126]. Moreover, these behaviors also highlight the three primary antecedents of habit, namely satisfaction, usage and frequency of prior behavior [104]. The reflexive or habitual liking of posts presents another concern – "like-farming" also known as "like-harvesting". Personality traits have been found to have an influence on the "liking" of posts on Facebook [127]. Moreover, prior literature has shown that habits can lead to clicking "likes" or to reactions such as interpreting such cues as social support from others [128]. Like-farming is performed mostly on Facebook and is used by commercial entities and scammers to raise the popularity of a site with the intention of making it go viral around the world [129]. Similar to click-bait, like-farmers rely on users to click habitually or share attention-grabbing topics such as animal welfare, competitions and the like. Phishers can transform these popular posts so that they lead to spoofed websites and trick the user into divulging personal information.

Habits can be formed and strengthened through associative and reward-learning mechanisms [124]. For example, the gratification that arises from frequent participation on SNSs can develop into a habit [109]. If the user experiences an enjoyable emotion when interacting on SNSs, they are likely to develop stronger habits [130]. This supports Turel and Serenko's [113] finding that on SNSs, perceived enjoyment is a key antecedent of habit. In this regard, some features or activities on SNSs could stimulate the gratification gained from receiving appreciation for sharing a post, compliments on photos, tagging friends, the prospect of winning a competition, watching videos, or gaining likes and more friends or followers. The outcomes stemming from these types of behaviors may encourage a user to continue performing them, potentially also on other platforms, thereby forming and reinforcing the habit. In some cases, excessive use of the habitual behavior can develop into a dependency such as Facebook addiction [131–133].

The present study posits that habit (i.e., clicking and/or sharing of posts on SNSs) presents a potential risk to users as their habitual behaviors may influence them to overlook phishing messages. Therefore, given the behavioral concerns on SNS discussed earlier, investigating habits is an important consideration for the current study.

3.4. Information processing

Today, the distinction between professional and social communication is often blurred because both streams of information can originate from various channels such as email, social media, communication apps, and instant messenger apps. Employees have more workload and expectations than before and, as such, are prone to making mistakes and being deceived [134]. Situational events, for example the Covid-19 period, may present users with an even larger volume of messages stemming from the various platforms, thereby increasing the cognitive effort needed to identify and respond to messages. Social media users are particularly prone to information overload because of the constant attention needed to be given to the large volume of information on these sites [135]. For example, the structure of the Facebook news feed/timeline could potentially cause information overload [136]. In this regard, depending on what the user has subscribed to (i.e., follow), a news feed/timeline can contain a mixture of content stemming from friends, pages, groups, and unsolicited advertisements. The use of certain emoji reactions on Facebook has a behavioral influence on whether a user will choose to comment, share, or like on that particular post [137]. Moreover, a user could simultaneously be dividing their attention between SNSs or online tasks such as emailing, viewing websites, or working on open documents, thereby increasing the demands on their attention. As such, they may not be motivated to consider the security aspects associated with that threat [138]. As a result, to save time and effort, users may resort to other forms of "cognitive shortcuts" when attempting to make decisions about a message. This poses another risk, as cognitive load is an important indicator in recognizing deception [139] and presents an opportunity for phishers to take advantage of users' lack of attention to detail.

Buller and Burgoon [140] state that identifying the verbal and non-verbal leakage cues in social interactions is key to detecting deception. However, in an online environment, email-based phishing and social network phishing involve no direct physical interaction. As a result, to judge the authenticity of messages, users have to resort to other cues such as the content, language, and design [141]. However, although researchers note that some of the previously mentioned characteristics of phishing messages should be obvious for users to identify, prior literature has nevertheless shown that not all users will pay attention to these cues or comply with the security indicators, even those who have computer experience. This is because users do not approach phishing emails with similar cognitive processes or capabilities [142]. To elaborate, a study by Lin et al. [143] found that certain people paid attention to different elements of the browsing interface to judge a website's legitimacy. Some based their decisions on (1) institutional brand, (2) content as presented in the main pane of the browser, (3) input information requested and (4) information in the address bar and other security indicators. However, others, when evaluating information online, will use heuristics and cues [144]. Consequently, Sterrett et al. [145] suggest that people are likely to use two cues, namely: (1) who shared the information and (2) the original reporting source of the story.

Given these concerns, researchers have turned to the cognitive processing paradigm, where the lack of systematic processing is viewed as the sole reason why individuals do not notice the aforementioned deceptive clues [30,146]. A dual-process theory associated with this paradigm is the Heuristic-Systematic Model (HSM) of information processing [147]. This particular model has motivated scholars to attempt to predict human behavior when presented with phishing [12,24,48,63,65,66,73,142,148]. In persuasive contexts in which users have to perform an evaluation, the HSM hypothesizes two modes of information processing: heuristic or systematic. At one end of the information-processing continuum is *systematic processing*, which requires considerable effort and motivation as it is analytically orientated. In this mode, users will carefully scrutinize, compare, and relate arguments [149]. In contrast, at the other end of the continuum, *heuristic processing* is an efficient but information insufficient form of processing in which individuals use limited cognitive resources, relying on superficial cues and "simple decision rules" potentially developed from past experiences on which to base their judgement of the validity of a message [149]. Phishers will use persuasion techniques to influence the user to respond quickly and without deliberation. In this regard, perceived credibility, likeability, or the attractiveness of the message source encourage heuristic processing [54]. Moreover, as previously mentioned, owing to the risk of information overload on SNSs, users have a tendency to apply heuristic processing to save time and effort [78].

It is possible that systematic and heuristic processing operate simultaneously, either independently or interactively [150]. Luo et al. [64] suggest that phishing could be most effective if the message stimulates both the heuristic and systematic processing modes.

4. Research model and hypothesis development

4.1. Influence of personality traits on habits

A plethora of research has empirically tested to what extent personality traits directly influence phishing detection [50,58], yet no empirical research has rigorously examined linkages between personality traits and habits, especially in the phishing context [151,152]. The personality trait literature on phishing reveals a persistent trend of scholars justifying their contradictory results when explaining their findings. This indicates that personality traits may be influenced by variables such as the culture, specific situations, environments, and other behavioral factors in terms of which are investigated. Moreover, Bandura [153] states that personality traits are essentially clusters of habitual behaviors, which may indicate possible linkages between habits and personality traits. The self-representation of social media users can be linked to the Big Five traits, with an underlying social purpose that might predispose them to satisfying certain needs [84], as characterized by Maslow's hierarchy of needs which consist of physiological, safety, love and belonging, esteem, and self-actualisation. Section 3.3 established that gratification stemming from repeated behavior may satisfy a particular need, thereby fostering a habit. Thus, it could be argued that depending on the personality trait, augmented by the differing needs and motives of individuals, the need for satisfaction could be the force driving the habitual behavior. McCloskey & Johnson [151] is of the view that should an association exist between personality and behavioral automaticity, it could stem from “perceived rewards”. This is plausible, as a study by Amichai-Hamburger and Ben-Artzi [154] has shown that the relationships between personality traits and internet use, and moreover loneliness, are important indicators of psychological well-being. This study considers the behavior of clicking or sharing a social media post, as requested by a friend, that is of interest to the user to be a habit and as such an undesirable behavior that could potentially put users at risk to phishing attacks. For example, a hoax post shared by a friend stating “I am Elon Musk, if you click and share this link, I will give you $10,000.00″. This can be likened to a phishing email whereby the victim is enticed to click on a link to confirm or verify something. Thus, in this study, it is proposed that a habit, manifesting from characteristics inherent in certain personality traits, makes SNS users vulnerable to phishing.

Lawson et al. [96] found that incorporating a combination of persuasion techniques in a phishing email made those with the extraversion trait more susceptible. In the context of SNSs, extraverted Facebook users have been found likely to participate in risky behaviors [82], tend to spend more time using Facebook [83,84,87,155–157], have more Facebook friends [82,155,158,159] and could potentially comment on or “like” other people’s pictures or selfies [160]. This trait also has an influence on their sharing preferences [161]. In contrast to these findings, Ross et al. [86] found the fact that a person was an extravert had no effect on the number of Facebook friends, time spent online, or the use of Facebook features. From the perspective of social norms and phishing susceptibility, we expect that extraverts would be more likely to act out of habit because they are more engaged on SNSs and receive gratification from the views and opinions of others on SNSs. This frequent engagement and interaction by these enthusiastic users might reinforce the behavior of clicking and sharing links originating from their friends. As such, we hypothesize:

H1a: Extraversion trait is positively related to habit on social networking sites.

Modic and Lea [162] found highly agreeable people are more susceptible to phishing because they are more inclined to trust in uncertain situations. Similar results by Cho et al. [56] found agreeableness to have a significant effect on perceived trust and risk in terms of phishing vulnerability. Cusack and Adedokun [57] also reported that people who display the agreeableness trait are susceptible to SE techniques. In the context of Maslow’s needs, recent personality trait research has seen belongingness emerge as the strongest need [101]. According to Mancinelli et al. [84], the agreeableness trait is associated with belongingness and people with this trait are more prone to accept friend requests on Facebook [158]. Van der Schyff, Flowerday, Kruger, and Patel [163] found people with this trait use Facebook extensively. Given prior literature on the vulnerability of the agreeableness trait to phishing susceptibility and that belongingness might encourage agreeable users to engage more with the online community, we expect that users with this trait may develop a habit of clicking and sharing links, influenced by their compliant behavior to “fit in”. Given the latter, this study hypothesizes:

H1b: The agreeableness trait is positively related to habit on social networking sites.

As individuals with the conscientiousness trait are more cautious (e.g. noticing an absence of typographical and grammatical errors) and generally more risk averse, they may be less likely to perform risky behaviors [164]. Pattinson, Jerram, Parsons, McCormac, and Butavicius [21] found less impulsive users were better at managing phishing emails, as they were likely to spend more time deliberating before making a decision on whether to open them or not. In the context of SNSs, Wehrli [159] found highly conscientious people tend to refrain from participation on SNSs. Similarly, Sumner et al. [158] found people with this trait were less likely to join Facebook groups. Gou et al. [161] found Twitter users with the conscientiousness trait to be less likely to share their preferences regarding their values and needs. Given the thoughtfulness and cautious nature of the conscientious user, we expect that such users will be less prone to engage in clicking and sharing links at a habitual level. Accordingly, we therefore hypothesize:

H1c: The conscientiousness trait is negatively related to habit on social networking sites.

The opposite of emotional stability is neuroticism. Prior literature has it that the neuroticism trait in individuals may decrease a user’s willingness to trust a system [165], increase computer anxiety [166], promote a strong desire to avoid using the internet [167], and increase resistance to adopting new technologies such as smartphones [168] and instant messenger apps [169]. In the context of phishing, Halevi et al. [58] found neuroticism to be the trait most at risk to responding to a phishing emails, with gender-based differences in the responses. Owing to the distrusting nature and lack of technology adoption associated with the neuroticism trait, we expect such a user to be less likely to engage frequently on SNSs and thus unlikely to develop a habit of sharing and clicking links. We thus hypothesize:

H1d: The neuroticism trait is negatively related to habit on social networking sites.

The curiosity, open-mindedness, and explorative nature of individuals possessing the openness trait can raise behavioral concerns. For example, Johnston et al. [35] found that individuals with this trait are likely to violate information security policies. Alseadoon, Othman, and Chan [47] found that openness is closely related to high phishing susceptibility. In an SNS context, individuals possessing the openness trait both posted more information on Facebook and had less strict privacy settings [58]. Studies have also shown that Facebook users are friends with others who share similar values or traits, particularly with those who possess the openness trait [170]. This is a similar result to that of Amichai-Hamburger and Vinitzky [82], who found users with high openness to be likely to spend more time with, and have more, friends. This is not surprising as the nature of SNSs is to encourage open interactions. Given the description of users with the openness trait being very active in a social network context, they might be more willing to share posts and click on links which could develop into a habit. As such, we hypothesize:

H1e: The openness trait is positively related to habit on social networking sites.

4.2. Influence of habit on information processing

Gardner [102] depicts habit on an impulsive pathway, such that the perception of cues activates low-level context–behavior associations. Habits thus streamline behavior to such an extent that such users repeat what they have done in the past to save mental effort. As noted earlier, Turel and Serenko [113] describe people who perform habitual behaviors as “cognitive misers”, as they tend to be economical with the amount of cognitive effort they allocate to tasks. This description closely resembles the characteristics of *heuristic* processing. Vishwanath [9] points out the conundrum that likening habits to mental scripts implies that “email” habits and heuristic processing may be part of the same process as they both lead to phishing susceptibility. Owing to the *automaticity* aspect associated with habits, which allows users to reduce their cognitive effort when performing tasks, it is anticipated that habits will have a positive relationship with heuristic processing and an opposing relationship with systematic processing. Because an individual who uses a systematic mode of processing applies deep thinking and critically evaluates information, we expect that habit will not affect this form of cognitive processing. A paucity of research in this area creates an opportunity to examine the effect habits have on heuristic and systematic processing. We therefore hypothesize the following:

H2a: Habit is negatively related to the systematic processing of phishing stimuli on social networking sites.
H2b: Habit is positively related to the heuristic processing of phishing stimuli on social networking sites.

4.3. *Influence of habit on phishing susceptibility*

Following an investigation of the effect habits have on both modes of information processing (as hypothesized in H2a and H2b), by examining the direct relationship that habits, stemming from Facebook behavior, have to phishing susceptibility it can be determined whether habits are an independent or parallel process to information processing, specifically heuristic processing. According to Robbins and Costa [171], the concept of habits refers not so much to "how the behavior is performed" but to "which stimuli prompt the behavior", both of which involve aspects of automaticity. As numerous studies by Vishwanath[9],[62],[24] have shown, users acting out of habit are at risk of phishing. Accordingly, we hypothesize:

H3: Habit is positively related to phishing susceptibility.

4.4. *Influence of information processing on phishing susceptibility*

As this study considers information processing as a variable that can influence susceptibility to phishing on SNSs, the aesthetics and functions offered on SNSs may have an influence on user behavior, in particular how they perceive and interpret information. Although a lack of knowledge is considered a factor that influences phishing susceptibility, an individual's capacity for interpreting information and their motivation play a role in how users will react to risk [172]. Moreover, a study conducted by Vishwanath et al. [30] found that participants with domain-specific knowledge did not conclusively yield the expected results in terms of processing information in depth. Within the context of phishing on SNSs, we posit that the snap judgements that users often make, based on a superficial cues in posts, will lead them to overlook some of the cues that could raise suspicion. We hypothesize that:

H4: Systematic processing is negatively related to phishing susceptibility.
H5: Heuristic processing is positively related to phishing susceptibility.

4.5. *Influence of social norms on phishing susceptibility*

Although the literature has used various terms for subjective norm constructs, in this study, the term social norms is used. Social norms share the common notion that individual behavior is influenced by perceptions of what people think others expect from them. Social norms develop and evolve as a result of the interaction between individuals in social groups [173]. Users may adjust their behavior based on the perceived expectations of others [174]. Compared with email-based phishing in which an individual deals with one particular person (i.e., email) at a time, users of SNSs may be influenced by a community of members to behave in a particular way. Accordingly, in the context of SNS, users may be motivated, pressured, or perceive themselves as being pressured by their friends into performing certain behaviors such as sharing posts, responding to posts or liking posts. The user might possibly gain gratification, in the form of likes, as a form of approval for their behavior. This explanation resembles the reciprocity persuasion principle of Cialdini (2001), also related to normative commitment, which stems from the sense of obligation that people may feel when they are given something to exchange for something similar in return. Workman [54] found individuals who were higher in normative commitment would succumb to SE techniques. For the purposes of marketing, some legitimate organizations on Facebook offer the public a chance to win a prize if they, for example, like their page, share the post with friends, copy and paste, or tag two or more friends. As a result, users become accustomed to following these "rules" and seeing this behavior performed by others. Such willingness to meet the expectations of others increases the riskiness, especially if the posts are malicious. In addition, if the user has not made an effort to validate the authenticity of the message, it may lead to an increase in the spread of hoax messages. As such, we hypothesize:

H6: Social norms are positively related to phishing susceptibility.

4.6. *Influence of computer self-efficacy on phishing susceptibility*

Computer self-efficacy (CSE) refers to the user's judgement of their capability to use computers to achieve a particular purpose [175]. The more time an individual spends on the internet, the more likely they are to acquire experience or information about threat agents and therefore be better equipped to identify them [51]. Yao, Rice, and Wallis [176] found that internet users with high CSE are confident in their abilities to handle online threats and secure their privacy and are thus better at avoiding phishing attacks [21,55,177,178]. However, this confidence can also present other risks, as high levels of CSE can to also lead to high levels of actual confidence about how to proceed when presented with system errors [179]. This presents another concern as prior research has shown that users ignore phishing warnings that might indicate that they are less motivated to pay attention to warnings, especially in environments they frequently engage in. Moreover, Vishwanath et al. [30] found that both CSE was negatively related to users examining a phishing message closely. This indicates that individuals who consider themselves to be technological sophisticated are just as likely to be phished as those who are not. If users do not have the motivation or perceive themselves as lacking the capabilities associated with computer usage, this could prevent them from performing tasks related to detecting phishing [180]. Examples of such tasks include recognizing file extensions of attachments in emails or checking the security indicators of a website to determine whether it is safe or not. As pointed out by Cox [181], people will avoid an action if they do not believe they have the ability to complete the action and achieve their desired results. It is thus necessary to investigate the influence CSE has on users when presented with phishing. As such, we hypothesize:

H7: Computer self-efficacy is negatively related to phishing susceptibility.

4.7. *Influence of perceived risk on phishing susceptibility*

Pavlou and Gefen [182] explain perceived risk as "the subjective belief that there is some probability of suffering a loss in pursuit of the desired outcome". Perceived risk can be described as a dispositional factor that can help predict an individual's likelihood to accept risk in an uncertain situation and context. Perceived risk or perceived susceptibility is typically viewed as a product of two variables: the perceived likelihood of an event and perceived damage if the event takes place [25]. Empirical studies have suggested that in a particular situation in which people perceive a potential threat as severe and likely, they will adjust their behavior in a more cautious manner that they think will be effective in preventing that threat from causing them harm [53,179,183,184]. Similarly, Rogers' [185] protection motivation theory postulates that when individuals perceive they are more at risk of security threats, and when the threats are more severe, they are more likely to adopt a recommended response to the threat and adjust their behavior according to the amount of risk they are willing to accept or tolerate. This "trade-off" is also known as risk homeostasis [186]. Pattinson and

Anderson [187] suggest that perceptions of security risks are generally influenced by factors such as the individual's disposition at the time, recent media reports, past experiences, and prior knowledge of technical aspects. Sheng, Holbrook, Kumaraguru, Cranor, and Downs [188] found that risk-averse users were less likely to fall for phishing. In addition, Wright and Marett [55] found individuals who are suspicious of others and display general distrust toward people are less susceptible to phishing.

People have a tendency to have biased insights, overestimating the likelihood of positive events and underestimating the likelihood of negative events – known as optimism bias [189]. Similar to "optimism bias", users may be aware of security threats and the techniques associated with phishing, but may be of the view that falling victim could not happen to them personally [26,27] and, as such, believe that organizations and others are the main targets of attackers [190,191]. This perception of "it won't happen to me" [25] can potentially put users more at risk of phishing because they are less prepared to deal with it. In addition, and similar to CSE, some users may be overconfident in their ability to detect phishing messages [51]. As individuals have different propensities for risk, it is important to consider perceived risk as yet another contributing factor that influences human behavior and phishing susceptibility [192]. We therefore hypothesize that:

H8: Perceived risk is positively related to phishing susceptibility.

This study also measured aspects related to: (1) Demographics, including gender, age, and course of study; (2) duration and hours spent on SNSs; (3) motivation/reasons for visiting SNSs; and (4) dependency on SNSs. However, while some of the demographic data was reported, its role within the theoretical model was excluded because it was not the primary focus of this study.

To conclude, the proposed model in Fig. 1 posits that personality traits each have particular characteristics that can render individuals prone to developing habits on SNSs. These habits in turn can cause a user to pay insufficient attention or to overlook key aspects associated with distinguishing phishing messages. The model also proposes that other behavioral factors related to social norms, computer self-efficacy, and perceived risk can also influence susceptibility to phishing.

5. Methodology

5.1. Sample size and data collection

The determination of an appropriate sample size has been remarked as a contentious issue for studies employing structural equation modeling (SEM) [193,194]. Weston and Gore [194] recommend a minimum sample size of 200 for any SEM, provided the researcher anticipates no complications with the data. This study used a convenience sample of final-year undergraduate students from a university located across three different sites. SurveyMonkey®, an online survey tool, was used to collect primary data. The total population consisted of 477 final-year students. Students were chosen because 65% of Facebook users are typically under the age of 35 years, are actively engaged on SNSs [195], and are driven by the need for social presence and entertainment value [6]. Before data collection, ethical approval was granted by the university where the target sample was located. Because our study aimed to achieve a 95% confidence level, a minimum of 213 users were required [196]. We intended to collect as many responses as possible, ultimately managing to collect data from 285 respondents. Early analysis detected 70 cases to have incomplete responses and these were therefore removed. The final sample consisted of a total of 215 respondents, of which 114 were male (53%) and 101 were female (47%). Respondents had a mean age of 22.6 years (*S.D.* = 4.41).

5.2. Variable descriptions and measures

The materials in the survey instrument were presented in the following order to the respondents: demographics (age, course of study), computer self-efficacy, personality traits, perceived risk, information processing (six stimuli), phishing email, social norms, and habit. The

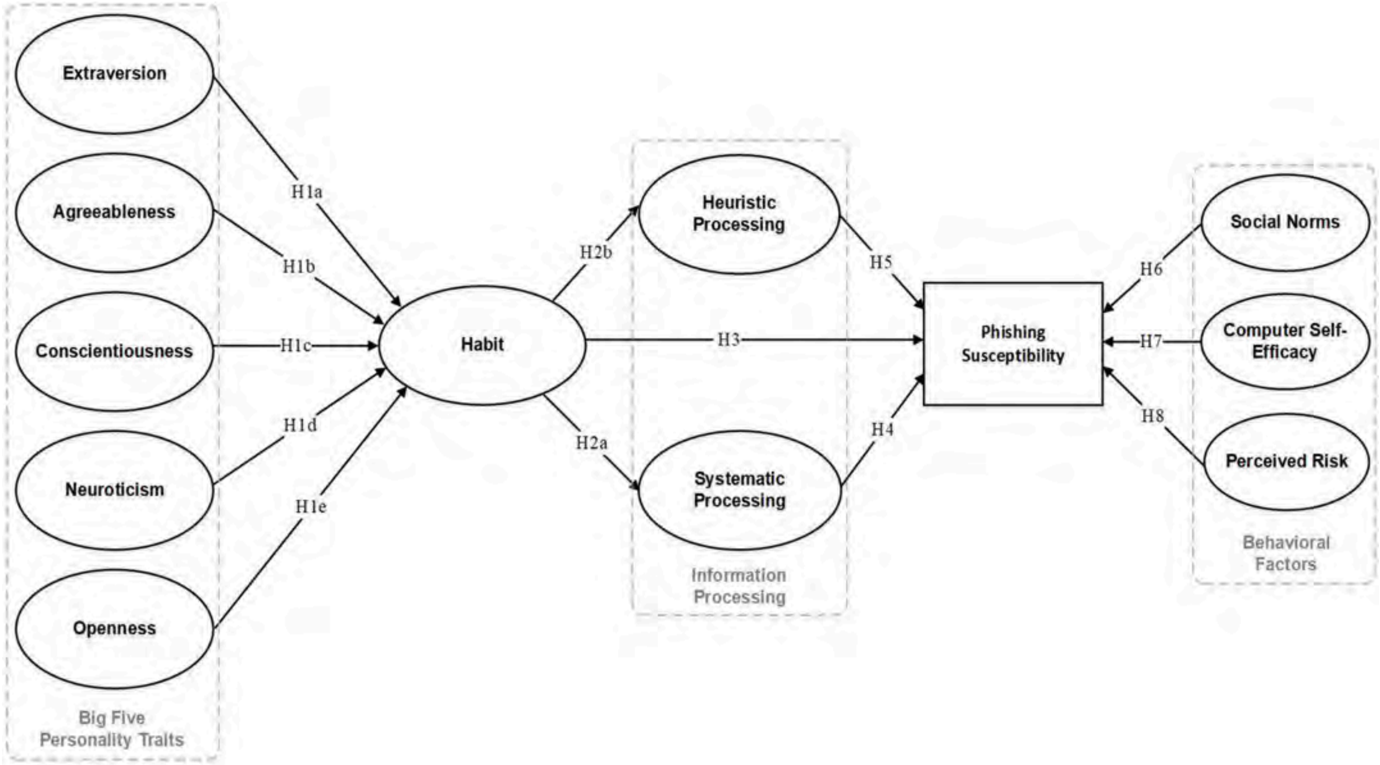


Fig. 1. Proposed model.

measurement items and description for each of the variables are discussed next.

5.2.1. Personality traits

The public domain instrument known as the Big Five Inventory scale test by John and Srivastava [92] was used to determine into which of the five traits a person's personality predominantly fits. This instrument (see Appendix A) consists of 44 items scored on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). Boudreaux and Ozer [197] who, in their comparison of numerous Big Five scales, state that the Big Five Inventory by John and Srivastava [92] is considered highly reliable (Cronbach alpha coefficients range from 0.75 to 0.90, with an average above 0.80), stable over time (3-month retest coefficients range from 0.80 to 0.90, with a mean of 0.85), and possess convergent and discriminant validity with respect to other Big Five instruments. Moreover, this particular instrument has been adopted in other phishing experiments [21,198].

5.2.2. Habit

Verplanken and Aarts [23] recommend that researchers focus on habitual mindsets and automatic cue-response links instead the associations between past and future behavior. Accordingly, the 12-item Self-Report Habit Index of habit strength (SRHI) scale was used in this study to measure habit with the main focus on capturing *automaticity* [199]. As discussed in Section 3.3, many behaviors are performed in a social network environment. As such, we considered the habitual behavior of clicking, opening, or sharing a link, requested by a friend to carry out (as a form of compliance), a potential risk to phishing. Items were scored on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). This instrument can be found in Appendix B. Apart from the scale's popularity in the health psychology and medicine discipline, it was also adapted by Vance et al. [117] in the context of compliance with information security policies. This scale was also used in the context of social media usage [200] and phishing [9].

5.2.3. Information processing

The survey instrument assessed respondents on six persuasive stimuli/images related to social network phishing found on Facebook and personally obtained by the researcher. Considering that 98.3% of Facebook users access the site via their smartphone [20], actual screenshots of stimuli were derived from the Facebook smartphone app. This ensured that the context of the stimuli was relevant to the audience [201]. Although not part of Cialdini's principles, most of our stimuli fitted the "curiosity" technique, which is very effective in phishing [8,51]. The screenshots illustrated that a particular action was required from the user (e.g., to click on play). More detailed descriptions for each of these stimuli can be found in Appendix C and the actual visual samples used in the survey can be found in Appendix I. The purpose of including a variety of different stimuli was to address respondents' potential bias as they might give more attention to some messages than others based on their interests or prior encounters. In an attempt to use stimuli that are of interest or liked by the respondents, South African content that the respondents would be familiar with and potentially would be interested in clicking was used. This supports Petty and Cacioppo's [201] assertion that persuasion is increased if the message is relevant to the audience. This was also confirmed in a study by Hassandoust et al. [202], which found that respondents used heuristic processing when the messages they received were specific to their context. Heuristic processing was measured by adopting a four-item scale (see Appendix D) used in prior research [148,203]. Systematic processing was measured using a three-item scale (see Appendix D) adapted from prior research [148,203]. Both the heuristic and systematic items were scored on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). The items in each stimulus were combined, thus consisting of a total of seven items per stimulus. Separating items according to whether they were heuristic or systematic could potentially influence respondents to respond in a way that they may consider morally acceptable rather than reflecting their true behavior [204].

5.2.4. Social norms

Our scale consisted of six items (see Appendix E) scored on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). Respondents were required to rate their decision based on when to share a post of a friend if they requested them to share it. Sample items include: "If it is my friend, then it is the friendly thing to do"; "If the post is popular (i.e., trending) and I know others will also find it interesting".

5.2.5. Computer self-efficacy

Compeau and Higgins [205] developed a ten-item measure for CSE; however, this measure is several years out of date and focused mainly on the use of general computer tasks and not on tasks related to phishing avoidance. Hocevar et al. [206] developed social media self-efficacy scales that focused on an average of a person's (1) perceived social media skill, (2) confidence in ability to successfully find information online, (3) level of social media content production and (4) level of social media content consumption. While the latter scale fits our context, it was also deemed not appropriate for our study. Subsequently, we defined our CSE scales as more aligned to our context and considered items related to the user's computer experience, general computer self-efficacy, and their knowledge of some technical features required to protect or evaluate potential phishing attacks. This view is supported by Marakas, Johnson, and Clay [207], who state that measures for CSE should be redesigned with articulated alignment to the situation under study. Our scale consisted of eight items scored on a five-point Likert scale (1 = very poor to 5 = excellent) and required respondents to evaluate their abilities to perform certain tasks a using a computer system (see Appendix F).

5.2.6. Perceived risk

Our scale consisted of four items (see Appendix G) measured on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). Sample items include: "There is little risk in sharing posts which instruct you to share to your profile (e.g., share this post and R100 will be donated to a charity)" and "There is little risk in accepting friend requests from strangers, as I can remove them later if I want to". Van Schaik et al. [208] suggest that most behavioral research on SNSs has focused primarily on privacy and not on security. Our scale focused on the risks related to phishing in an SNS context from a dispositional perspective. To elaborate, respondents might be optimistic about the SNS environment and thus complacent to potential threats [27]. Certain measures of the scale were informed by Van Schaik et al. [208], for example, items related to social media behavior, such as obliging with the sharing of posts and accepting friend requests from strangers. Another item (see Perceived risk item 3) measured respondents' overall awareness of risks pertaining to some form of personal loss that could potentially originate from SNSs (e.g., identity theft, reputational and financial loss). Two "control" items (see Perceived risk items 2 and 4 in Appendix G), informed by Van Schaik et al. [208] and Nilsson [209], and were also used to ascertain whether the respondents perceived themselves as able to mitigate potential risks.

5.2.7. Phishing susceptibility

A screenshot of a real-world phishing email purportedly originating from Facebook, containing an attachment, was used to test susceptibility to phishing (see Appendix J). The email is designed to appear as if it originated from Facebook, with the address being update@facebookmail.com. It also employs the blue theme typically associated with Facebook branding. Our dependent variable (DV) was measured on a binary scale coded as 0 = Not susceptible and 1 = Susceptible. The items: "Reply to the email" and "Check the attachment because I am interested to know what my friend has to say" were considered to be items related to phishing susceptibility. Not susceptible was represented by the items: "Immediately delete the email", "Ignore the email", and "I do not trust this email". The item "Unsure" was indeterminate and therefore was not included in the analysis because it does not inform the exact position of the respondent's choice. The decision to measure the DV in a different context from the independent variables of personality traits, habits, and information processing was motivated by several factors. First, the stimuli used to measure the independent variables were modeled after actual phishing attempts in SNSs, and having the DV measure within the same social media environment could potentially contaminate the measures, as respondents could "learn" through prior survey questions, thus biasing their responses to the other measures. Therefore, a change of context was necessary while still retaining the appropriate SNS context. Second, no literature exists that measures SNS phishing in this way, despite the phishing email used in this study originating from the SNS. Third, this approach enables the study to capture the ubiquitous nature of SNSs and their interdependency with other platforms, such as emails, which can further compromise users. Finally, measuring the DV in a different context from the independent variables ensures that the approach is not serially correlated with the independent variables, while still measuring the outcome of the behavior.

6. Analysis and results

The statistical software packages Stata 14 and R were used to perform the data analysis. As this study aimed to develop a theoretical model that entails examining the causal effect variables have on each other, SEM was identified as the appropriate statistical technique. SEM is a collection of statistical procedures allowing for theory building and model testing. SEM can be considered a hybrid of *factor analysis* and *path modeling,* with factor analysis used to examine the interrelationships among the variables and path analysis used to test the hypothesized relationships among constructs [194]. In this regard, SEM consists of two primary components, the measurement model and the structural model, and is discussed next.

6.1. Measurement model evaluation

The measurement model of SEM allows the researcher to evaluate how well the observed (measured) variables combine to identify underlying hypothesized constructs. We performed confirmatory factor analysis to test the reliability and validity of the measurement model. First, we assessed the reliability by calculating the composite reliability of each construct. Owing to the alpha limitations, it is technically more useful for researchers to apply composite reliability values as these take into consideration the different outer loadings of the indicator variables [210]. Similar to Cronbach's alpha requirements, constructs exceeding 0.7 are deemed acceptable for internal reliability. This evaluation ascertained whether our research instrument produced consistent results. As reported in Appendix H, apart from the agreeableness trait, our variables exceeded the recommended level of 0.7, thereby establishing good reliability for the scales. In terms of validating the measurement model, we assessed both the convergent validity and the discriminant validity. For convergent validity, we first inspected the individual item loadings of the constructs and their associated items (as indicated in Appendix H) and second we computed the Average Variance Extracted (AVE) scores. Factor loadings exceeding 0.5 were deemed acceptable, whereas those below 0.5 were subsequently dropped from our model. Apart from the heuristic processing variable, the AVE values of our constructs were above the recommended threshold of 0.5, thus indicating good convergent validity [211]. According to Fornell and Larcker [212], even if the AVE for a construct is below 0.5, if the composite reliability is higher than 0.6, then the convergent validity of the construct is still adequate. To assess discriminant validity, we used the Fornell-Larcker criterion [212] as presented in Table 2, in the form of a correlation matrix. This test is used to evaluate whether the square root of the AVE of each variable (on the diagonal) is greater than the correlation coefficients it shares with other variables in the same measurement model. Our results show the square root of all the AVE values was above 0.70, except for the systematic processing variable where the square root of the AVE equals 0.694. However, this construct maintains discriminant validity as the diagonal value is above the off-diagonal values. In accordance with the guidelines by Weston and Gore [194], we included the means and standard deviations in the matrix. This allows others to duplicate the results and independently assess model fit.

Because a self-report questionnaire was used to collect primary data from the same participants in a single sitting, we assessed the model for the prospect of common method variance (CMV). CMV is "attributable to the measurement method rather than to the constructs the measures represent" [204]. Procedural remedies (ex-ante techniques) were used to control for CMV before administering the survey to the respondents. In this regard, we pilot tested the research instrument to establish whether it could be considered reliable, included synonyms in parenthesis (where necessary) to ensure questions was clear and unambiguous, and assured anonymity and confidentiality. In respect of statistical remedies (an ex-post technique), we performed two statistical tests

Table 2
Correlation matrices and discriminant validity.

Variable	Mean	S.D	1	2	3	4	5	6	7	8	9	10	11	12
1. Extraversion	3.519	0.721	**0.708**											
2. Agreeableness	3.978	0.715	0.156*	**0.720**										
3. Conscientiousness	3.691	0.854	0.321*	0.352*	**0.833**									
4. Neuroticism	2.661	0.701	−0.303*	−0.388*	−0.437	**0.756**								
5. Openness	3.610	0.277	0.410*	0.119*	0.338	−0.192*	**0.951**							
6. Heuristic	2.901	0.290	0.021	0.048	0.031*	0.002	0.093	**0.760**						
7. Systematic	3.080	0.565	0.361*	0.017	−0.013	0.027	0.187*	0.491*	**0.694**					
8. Habit	3.908	0.256	0.005*	0.117*	−0.139*	−0.130	0.029*	0.146*	0.223*	**0.710**				
9. Computer self-efficacy	3.394	0.490	0.229*	0.049	0.231*	−0.050	0.315*	0.068	0.029	−0.057	**0.819**			
10. Social norms	2.649	0.599	−0.007	−0.097	−0.100*	0.145*	0.038	0.073*	0.119*	0.308*	−0.040	**0.800**		
11. Perceived risk	2.093	0.160	0.015*	0.110	0.350	0.040*	−0.024	−0.104*	−0.093*	0.312*	0.100*	0.039	**0.783**	
12. Phishing susceptibility	0.651	0.053	0.170*	0.031*	−0.121*	0.033	0.122*	0.047	0.022	0.093	−0.143*	0.003*	0.051	**1**

Note: the square root of the AVEs is presented in bold, appearing down the diagonal.

* Indicates significant correlation coefficients $p < 0.05$.

during the empirical stage to ascertain whether CMV posed any concerns. First, we used the Harman's single-factor test to check whether variance in the data can be largely attributed to a single factor [204]. If the total variance for a single factor is less than 50%, it suggests CMV is of no concern. Our results show that the largest variance explained by a single factor in our model was 10.31%, indicating that none of the emergent factors could explain the majority of the covariance. Second, Bagozzi, Yi, and Phillips [213] suggest that CMV can have an effect on the discriminant validity of the constructs. In this regard, we used the procedure by Pavlou, Liang, and Xue [214] and examined the correlation matrix (shown in Table 2) to determine whether any of the correlations between any pair of constructs exceeded 0.9 – of which all the correlations were below 0.9. Based on our examination and the results presented in Appendix H and Table 2, it was concluded that our measurement model was both reliable and valid as it satisfied the requirements from a convergent and discriminant perspective.

6.2. *Structural model evaluation*

Because the measurement model demonstrated sufficient construct validity and reliability, we conducted path modeling analysis. The structural model specifies the hypothesized relationships among latent variables representing the causal and consequent constructs of a theoretical proposition [215]. Depending on *p*-values as a sole means to justify significance has received criticism [216]. Although significance tests are important, it is also recommended that effect sizes (f^2) should be reported because it offers insight into the magnitude of the actual size of an effect [217] and therefore helps researchers assess the overall contribution of a research study [218]. The guidelines for assessing Cohen's f^2 are values of 0.02–0.14, 0.15–0.34, and 0.35 and above, which respectively represent small, medium, and large effects of an exogenous latent variable on an endogenous latent variable [219]. Effect size values of less than 0.02 indicate that there is no effect.

Based on the results of our path coefficient analysis, presented in Table 3, apart from openness ($\beta = 0.183$, $p > 0.10$, no effect), the remaining Big Five traits of extraversion, agreeableness, conscientiousness, and neuroticism show statistically significant relationships with habit. Extraversion revealed a positive influence on habit ($\beta = 0.245$, $p < 0.05$, small effect) thus supporting H1a. Although statistically significant, agreeableness had a negative influence on habit ($\beta = -0.161$, $p < 0.05$, small effect), thus H1b is rejected. Conscientiousness was also found to have a negative influence on habits ($\beta = -0.167$, $p < 0.05$, small effect), thereby supporting H1c. Our study shows that neuroticism ($\beta = 0.227$, $p < 0.01$, small effect) positively influences habits. Although this relationship is statistically significant, its direction does not support our hypothesis; thus, H1d is not supported. Hypothesis 2a posited that habit will have a negative influence on systematic processing and H2b that habit will have a positive effect on heuristic processing. Our results show habit to have a negative influence on systematic processing ($\beta = -0.269$, $p < 0.001$, small effect) and is positively related to heuristic processing ($\beta = 0.207$, $p < 0.01$, small effect), thus providing support for both H2a and H2b. Habit is shown to have a positive effect on phishing susceptibility ($\beta = 0.209$, $p < 0.001$, small effect) thus supporting H3. Systematic processing had a negative influence on phishing susceptibility ($\beta = -0.277$, $p < 0.001$, small effect), whereas heuristic processing had a positive effect ($\beta = 0.172$, $p < 0.05$, small effect), thus supporting both H4 and H5. Other behavioral factors (i.e., control variables) were examined pertaining to their influence on phishing susceptibility. Hypothesis 6 is supported as social norms has a positive effect on phishing susceptibility ($\beta = 0.098$, $p < 0.05$, small effect). Computer self-efficacy was found to have a negative effect on susceptibility to phishing ($\beta = -0.118$, $p < 0.01$, small effect), thus supporting H7. Hypothesis 8 was rejected as perceived risk was found to be not statistically significant ($p > 0.10$). Overall, the results of our path analysis support nine of the 13 hypotheses proposed in our study.

Following the hypotheses tests and outcomes presented in Table 3, a structural model was created and is depicted in Fig. 2.

Fig. 2, depicted as a path diagram, presents the theoretical model demonstrating the predictors of phishing susceptibility in terms of personality traits, habits, information processing, as well as other behavioral factors. The model also indicates the model coefficients (β) and significance of the relationships (*) between the variables. In addition, the mediating role of the habit construct was ascertained. Following the guidelines of Baron and Kenny [220], as well as those of Sun et al. [178], the indirect effects of personality traits on information processing were estimated. Table 4 presents the results.

Unlike in Sun et al. [178], given the multiplicity of our constructs, it was not possible to model all the direct effects without compromising the model or leading into convergence problems. Nonetheless, it can be observed, through habit, that extraversion has a positive indirect effect on heuristic processing and consequently on phishing susceptibility. On the other hand, extraversion has a negative indirect effect on systematic processing. Agreeableness has a negative indirect effect on heuristic processing and consequently on phishing susceptibility, and a positive indirect effect on systematic processing. Conscientiousness has a negative indirect effect on heuristic processing and phishing susceptibility, and a positive indirect effect on systematic processing. Neuroticism, through habit, has a positive indirect effect on heuristic processing and phishing susceptibility, and a negative on systematic processing. Because of the openness trait not having statistical significance, it has no indirect effect on information processing and phishing susceptibility.

According to Weston and Gore [194], researchers should evaluate fit in terms of the significance and strength of estimated parameters and how well the overall model fits the sample data. Pertaining to model fit, there has been considerable disagreement and debate over what constitutes acceptable threshold values for adjudicating acceptable fit in SEM. Barrett [221] controversially advocates for an outright ban on approximate fit indexes and suggests that "the chi-square test is the ONLY statistical test for SEM models". This view is supported by Kline [193], who recommends that researchers should at the very least report

Table 3
Path analysis and hypotheses outcomes.

Test	Path	β	S.E.	*t*-value	*p*-value	Effect size	Outcome
H1a	Extraversion→Habit	0.245	0.093	2.624	0.010	0.064	Supported
H1b	Agreeableness→Habit	−0.161	0.072	−2.242	0.022	0.024	*Not Supported*
H1c	Conscientiousness→Habit	−0.167	0.076	−2.202	0.030	0.045	Supported
H1d	Neuroticism→Habit	0.227	0.070	3.256	0.001	0.051	*Not Supported*
H1e	Openness→Habit	0.183	0.165	1.109	0.125	0.000	*Not supported*
H2a	Habit→Systematic	−0.269	0.065	−4.083	0.000	0.078	Supported
H2b	Habit→Heuristic	0.207	0.062	3.339	0.001	0.046	Supported
H3	Habit→Phishing Susceptibility	0.209	0.078	2.685	0.007	0.068	Supported
H4	Systematic→Phishing Susceptibility	−0.277	0.071	−3.916	0.000	0.072	Supported
H5	Heuristic→Phishing Susceptibility	0.172	0.038	4.514	0.020	0.109	Supported
H6	Social norms→Phishing Susceptibility	0.098	0.018	2.105	0.035	0.023	Supported
H7	Computer self-efficacy→Phishing Susceptibility	−0.118	0.039	−3.005	0.003	0.081	Supported
H8	Perceived risk→Phishing Susceptibility	0.152	0.149	1.020	0.109	0.004	*Not supported*

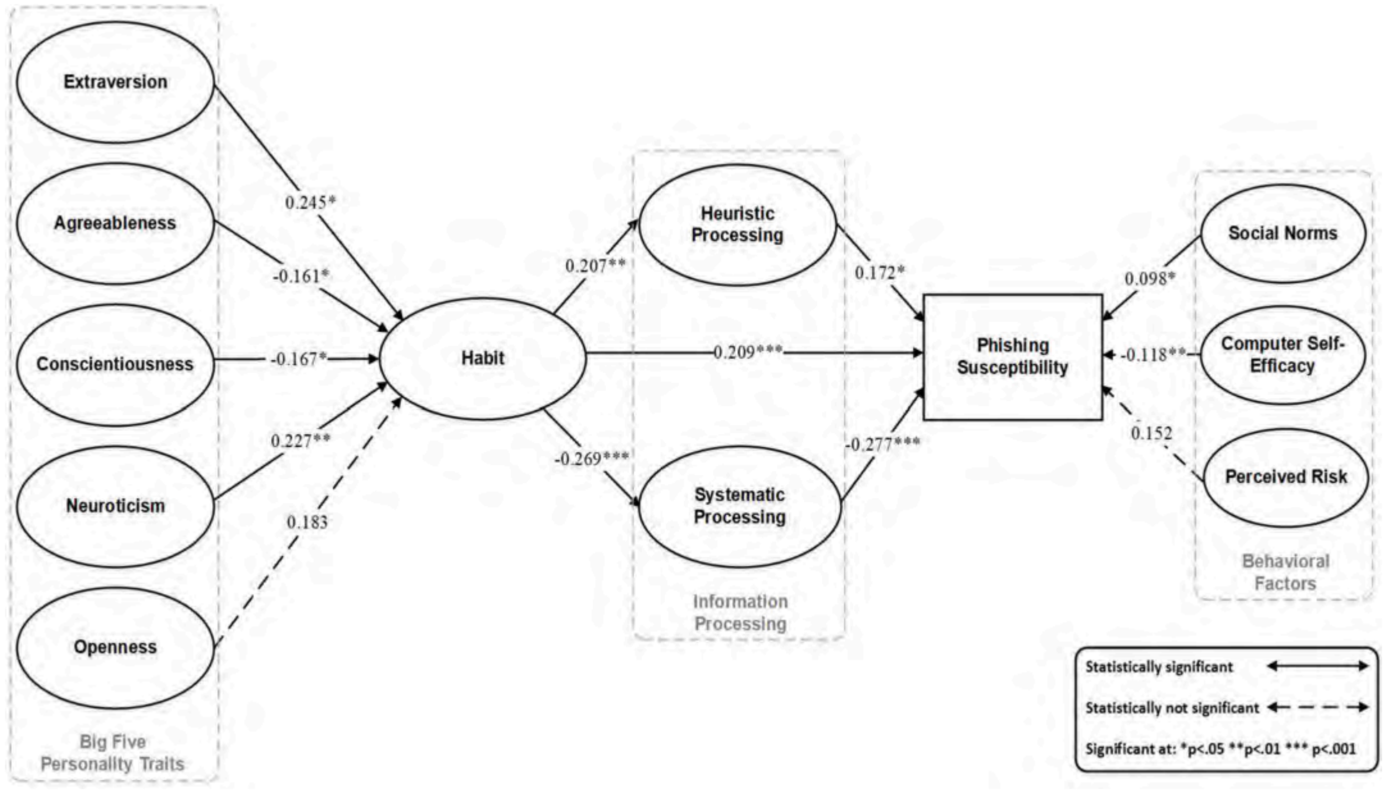


Fig. 2. The Personality-Habit-Information Processing (PHIP) model.

Table 4
Mediating effects of the habit construct.

Trait	Indirect effect to Heuristic Processing	Indirect effect to Systematic Processing
Extraversion	0.051*	−0.066**
Agreeableness	−0.033*	0.043*
Conscientiousness	−0.035*	0.045**
Neuroticism	0.047**	−0.061***
Openness	0.038	−0.050

Statistical significance:
* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

on the following fit indices: the model chi-square (χ^2) test with its degrees of freedom (*df*) and *p*-value, the root mean square error of approximation (RMSEA), the standardized root mean square residual (SRMR), and the comparative fit index. The χ^2 test can be described as an accept–support test with a "significant" result indicating that the model does not fit the sample data [193]. Thus, in contrast to the traditional significance measures, a non-significant χ^2 result at the > 0.05 threshold is desired to achieve a good fit between the variance and covariance matrix [221]. As depicted in Table 5, the χ^2 test in this study did not achieve an acceptable fit: $\chi^2 = 3700.386$, $df = 1794$ and $p < 0.05$. As reported in Sun et al. [178], χ^2 is affected by sample size. In terms of goodness-of-fit measures, RMSEA is an absolute fit index which evaluates the extent to which a hypothesized model differs from a perfect model. An RMSEA value of 0.00 indicates that the model exactly fits the data [193]. SRMR is an approximate fit index that tests the difference between the observed correlation and the model implied correlation matrix. Similar to the RMSEA, an SRMR value of zero indicates perfect fit [222] and a value as high as 0.08 is deemed an acceptable fit [223]. The comparative fit index is an incremental fit index and compares the sample covariance matrix with the null model. To ensure misspecified models are not accepted, a value exceeding 0.9 is required. Table 5 summarizes the fit index measures with their associated acceptable thresholds.

Table 5
Fit indices of the model.

Fit indices	Measurement model	Structural model	Acceptable standard
χ^2 (*df*)	5227.470 (1891); $p <$ 0.05)	3700.386 (1794); $p <$ 0.05)	$P > 0.05$
RMSEA	0.050	0.044	< 0.08
SRMR	0.079	0.051	< 0.08
CFI	0.999	0.903	≥ 0.9

The values for all the goodness of fit indices satisfied the required criteria thus validating that our model fits the data satisfactorily. In addition, the unshared variance, which reveals measurement errors of the latent construct, were extracted. In this study, this measurement error is likely non-random given that the respondents could have agreed with attitudinal statements regardless of the content of the question. For example, it is possible that some respondents may have responded in terms of the statement in general rather than the context. The correlated residuals were not dropped because it would have negatively affected the loadings leading to misestimation of the parameters. Significant correlated error terms were found under habit (unique variance = 103.72; SE = 10.01; *p*-value < 0.001) and heuristic processing constructs (unique variance = 142.32; SE 13.73; *p*-value < 0.001). Single item error correlations were computed, and two significantly correlated errors items pairs were found under the *habit* construct as follows: items 2 and 8, coe]f. = −0.0230, *p*-value = 0.036; items 4 and 11, coef. = 0.431, *p*-value = 0.051. One pair under the *heuristic* processing construct were found: items 1 and 2, coef. = −0.199, *p*-value 0.049.

7. Discussion

In this study, we aimed to develop a model that can help identify the individual and behavioral characteristics that make users =susceptible to phishing. We examined the influence of the Big Five personality traits and their effect on habits. Moreover, we examined the extent to which habits influence information processing, which served as the theoretical foundation for the underlying problem of phishing susceptibility. We also considered other behavioral factors and their influence on phishing susceptibility. Our study subsequently yielded many statistically significant findings, which are discussed next.

Given the absence of research investigating the influence of the Big Five personality traits on habit and their relationship on phishing susceptibility, we leveraged literature stemming from Facebook usage. In this regard, much of the literature on Facebook usage, which included personality traits, discussed concerns pertaining to Facebook addiction, dependency, or intensity. The literature in this area highlights that excessive frequency and performance of a behavior (i.e., habits) on SNSs can potentially lead to a form of addiction or dependency. In addition, we leveraged on recent literature drawing on some of Maslow's hierarchy of needs and its relationship to the Big Five traits, in which we argue that satisfying certain needs could encourage habitual behavior. This may also bear some resemblance to the uses and gratifications theory, which asserts that the use of a particular media is goal-directed to satisfy certain wants and needs [224].

Because *extraverts* are typically positively disposed, social, and enthusiastic, we anticipated that they would be more likely to develop habits from their frequent engagement with other users on Facebook. Our results support this view and align with the findings of Van der Schyff, Flowerday, Kruger, et al. [163], who found people with the extraversion trait to develop an intensive use of Facebook. Wehrli [159] and Correa et al. [83] likewise found extraversion to be positively related to the use of SNSs. Facebook specifically gratifies those with a need to engage in self-promoting and superficial behavior [87]. As extraversion is strongly correlated with esteem [101], we argue that individuals with the extraversion trait are prone to spending more time on SNSs, posting photos of themselves, interacting with their friends, and regularly checking for notifications. As a result, this behavior could develop into a habit and, more concerning, intensive usage might potentially lead to a more addictive behavior.

In view of the fact that *agreeable* individuals are trusting, friendly, and respecting of others' feelings and beliefs, and that this trait is strongly correlated with belongingness [101], we expected that users' with this trait would likely develop habits to satisfy this need on the SNS community. Contrary to our expectations, however, our results revealed that agreeableness was negatively related to habits. This result is similar to that of Ross et al. [86] and Amichai–Hamburger and Vinitzky [82], who found no relationship between this trait and Facebook usage. Rajesh and Rangaiah [225] found that agreeableness is not related to Facebook addiction. This indicates that this trait might be less susceptible to forming habitual behaviors on SNSs. Rolland [226] found agreeableness to be unique to the cultural background of the individual, which may explain why our results found agreeableness to have a negative correlation to habit. Furthermore, negative experiences may have an adverse effect on agreeableness as well as on phishing susceptibility [164]. Thus, it is possible that the background or current circumstances of the participants may have had an influence on their disposition at the time of their participation.

Conscientious users are generally risk adverse and less prone to SNS addiction [131,227]. McCloskey and Johnson [151] found conscientiousness was negatively associated with behavioral automaticity. As such, we anticipated these users to be less likely to develop a habit. We found that the conscientiousness trait negatively correlated to habit thus supporting our hypothesis.

Because individuals who are *neurotic* are typically depressed, lack self-esteem, and are anxious, it was expected that they would have a tendency to resist adopting technologies [168]. Although Halevi et al. [58] found this trait most at risk of email-based phishing, as our context involved SNSs and prior literature has shown, this trait to be less engaged with technology, we expected neurotic individuals to be less likely to be habitually engaged on SNSs. On the contrary, our results showed this not to be the case. This might indicate that while the neurotic trait might be risk averse to privacy concerns, such as sharing information, this does not necessarily indicate that they will have no interaction on SNSs. This explanation would also support Mehdizadeh's [126] finding that users with low self-esteem are more engaged and active in promoting themselves on Facebook. This is because the neurotic trait relates to the narcissism trait in terms of self-promotional content on Facebook [126]. A study by McCloskey and Johnson [151] found that neuroticism positively predicted automaticity even for behaviors not performed more frequently by neurotic individuals. Moreover, Hughes, Rowe, Batey, and Lee [228] found neuroticism to be positively associated with Facebook usage. This also supports the findings of Wehrli [159] who, contrary to expectations, found neuroticism to be associated with more participation on StudiVZ, a German-based SNS. Ross et al. [86] found that individuals higher in neuroticism were less willing to share personal information on Facebook, and those low in neuroticism preferred posting photos on their Facebook wall. Sumner et al. [158] found that the more neurotic a person is, the more photo albums they have on Facebook. These similar findings may indicate that due to emotional instability, users with this trait will be motivated to use SNSs to compensate for their lack of interpersonal skills [85] and in addition to avoid loneliness by garnering a sense of belongingness on SNSs [229]. More concerning, loneliness was found to be positively related to Facebook addiction [225]. As with extraverts, this too could potentially lead to developing addictions as a result of excessive habit performance.

Openness is associated with individuals who have an appreciation for new experiences and different ideas and beliefs [99]. As this trait is associated with being sociable on Facebook [86], we expected high engagement leading to the development of habits. Although our relationship showed a positive association, our hypothesis was rejected as our results were found not to be statistically significant. In terms of Maslow's needs, openness was not significantly correlated with the physiological and the safety and security needs [101]. Given that our context involves protecting against phishing attacks, this might explain why we also had a non-significant result in our study. In the context of SNSs, Van der Schyff, Flowerday, Kruger et al. [163] also found openness having no significant relationship with Facebook usage.

Prior literature has shown that all the Big Five traits, apart from conscientiousness, have certain vulnerabilities that can be exploited by deception. Empirical research has also revealed that the extraversion and agreeableness traits share very similar characteristics, particularly in terms of Facebook engagement. Our results show that extraversion and neuroticism, although polar opposites in their characteristics, may be driven by very similar goals or needs which might potentially reinforce the habit. For example, extraverts have a natural social need to be involved and engaged with other Facebook users. On the other hand, neurotic users might develop habits because of their loneliness in the physical world, and thus may be more motivated to fulfill this need on SNSs. Moreover, SNSs could help them overcome their lack of self-esteem, finding SNSs a safer place to interact with others without physical interaction [230]. As such, loneliness and a quest for belonging, as related to Facebook usage, might tie these two traits together in terms of susceptibility to habits [154].

Overall, our results on the relationship between personality trait and habit closely resemble those of Tang et al. [227], who found agreeableness and conscientiousness to be negatively associated with Facebook addiction. These same traits were also found to be negatively related to increased Facebook usage [87,231,232]. Ideally, personality characteristics that support reserved behavior, low impulsivity, and distrust are less at risk of phishing [50]. However, as context can influence the way people react (e.g., SNSs, emails, text messages), an individual who may be considered a "low-risk" personality profile may be just as likely to fall victim to phishing when particular persuasion principles are used or they are put under pressure.

The findings also lend support to the HSM and phishing susceptibility. Vishwanath [9] maintained that the "impact of habit and information processing on phishing deception is unclear". This study investigated the relationship between habit and information processing and the direct effect of habit on phishing susceptibility, of which both were found statistically significant and support our hypotheses. By doing so this offered some interesting insights. Habit is positively related to heuristic processing which results in phishing susceptibility, and habit is directly related to phishing susceptibility. This supports Vishwanath's [9] suggestion of a possible joint influence of habit and cognitive processes and essentially answers Vishwanath's concern that habit and heuristic processing could essentially be measuring the same process; that is, if you are performing a behavior out of habit, you are actually applying heuristic processing. In both cases, one is likely to be susceptible to phishing. Coincidentally, the coefficient value and *p*-values for these two relationships show strong similarity as they have almost identical values. Habit was found to be negatively related to systematic processing that also supports our hypothesis. This suggests that if users are performing out of habit, they will not make a considerable cognitive effort to evaluate the authenticity of the message and therefore will be more susceptible to phishing.

Workman [54] found that individuals who are high in normative commitment feel obligated to reciprocate SE requests incorporated in phishing attacks, such as receiving free gifts or divulging confidential company and user information. Our results support the notion that *social norms* positively influence phishing susceptibility. As such, users who feel obligated to share posts, or have a tendency to comply with requests from others on SNSs, are more at risk to phishing.

Our results supported our hypotheses that individuals with *computer self-efficacy* will be less at risk from phishing. This indicates that individuals who have the competency to perform certain tasks and other validation checks in determining the authenticity of phishing messages, will be less susceptible. This result contradicts that of Dhamija, Tygar, and Hearst [233], who found in their study that neither previous experience nor hours of computer usage had any effect on users distinguishing legitimate and spoofed websites. However, Wright and Marett [55] are of the view that internet experience and increased security knowledge resulting from training should make users less susceptible to phishing. Algarni, Xu, and Chan [234] and Albladi and Weir [46] found that computer and security knowledge decreases a user's susceptibility to phishing attacks. Phishing on SNSs provokes different risk perceptions compared to email-based phishing attacks [118]. This might explain why we found no statistically significant relationship with perceived risk.

8. Contribution

8.1. Contribution to theory

This is the first empirical study, in one comprehensive model, investigating the relationship between the Big Five personality traits and habit and its effect on information processing, which can influence susceptibility to phishing on SNSs. In addition, the model included other behavioral factors such as social norms, perceived risk and computer self-efficacy. Much like all theoretical models, including the theory of planned behavior and the technology acceptance model, the study allows other researchers to expand on these models or theories to include other variables such as gender, culture, and the like, which could potentially offer further insights into phishing susceptibility and contribute to the body of knowledge. As prior literature has shown that psychological aspects stemming from Maslow's hierarchy of needs, such as "belongingness" and "esteem", has a relationship to the Big Five traits, this study argued that identifying certain needs associated with a particular trait could bring to light factors that contribute to habit formation. Classifying potential motivating factors such as self-esteem, loneliness and a need to belong (belongingness) as leading factors for performing a habit on SNSs offers interesting prospects for future research. Literature on phishing and security education, training, and awareness (SETA) interventions has focused predominantly on email-based phishing and spoofed websites, and hence a lack of attention has been given to phishing conducted on SNSs [62]. As such, the context of the study also offers a contribution. There is a lack of studies investigating the influence of personality traits on both habit and information processing. This study extends a prior model developed by Frauenstein and Flowerday [12] and shows that, by including habits, the model reveals new perspectives that individuals with certain personality traits can be prone to exhibiting risky habitual behaviors, with implications for phishing susceptibility. This is also expressed by Wood [152], who states that "habit is largely missing from modern social and personality psychology" and by Vishwanath [9], who states that the "impact of habit and information processing on phishing deception is unclear". This study showed that habits put users directly at risk of phishing. Interestingly, this study revealed that habit uses a form of heuristic processing due to the automaticity aspect of the behavior. As a result, the inclusion of the habit construct in this study also makes a contribution. Valecha et al. [65] state that there is a need for future research to investigate whether social media users assess the validity of a phishing message using systematic or heuristic or a combined approach. This study addressed this and found that the mode of processing, particularly heuristic processing, may reduce rational logic by the user to detect phishing.

8.2. Contribution to practice

Ultimately, having some effect on human behavior will require education and training interventions. As mentioned by Lawson, Pearson, Crowson and Mayhorn [235], it is not possible to develop and subsequently use a phishing susceptibility model to protect potential targets without first identifying the areas of greatest susceptibility. As prior literature has criticized the effectiveness of SETA interventions as being too general, the findings of this study may assist organizations in the customization of an individual anti-phishing training program to target specific dispositional factors in vulnerable users [236]. By using an instrument similar to the one used in this study, pre-assessments or simulated attacks could be used determine and classify certain risk profiles. Similarly, Mitnick and Simon [237] suggest that organizations should carry out "auditing and testing" on employees to determine their susceptibility to SE attacks. Organizations could examine employees' preferences to, for example, determine their interest in free gifts, movie genres, employment opportunities, financial stability, and the like. These preferences could help to identify potential behavioral vulnerabilities that phishers could use to persuade victims in both emails and on SNSs. Once identified, more targeted and explicit training interventions could be conducted with the associated vulnerable groups to address employees' personal sets of vulnerabilities with consideration of their personality traits. This approach has also been recommended by Mayhorn et al. [50] and Chou et al. [73]. Jensen et al. [238] introduced "mindfulness" techniques into training programes as an approach to teach individuals to allocate attention "dynamically" during message evaluation and anticipate judgement of suspicious messages. Cue-based training may be another means for improving phishing detection [239]. Ultimately, such training interventions are aimed at improving systematic processing in order to better detect phishing [240].

It is possible that social media users develop certain habitual behaviors transferred from home or which develop in their personal time. As a result, organizations could overlook habitual behaviors and also neglect this aspect in their training interventions, as they may not be able to detect or observe these behaviors (e.g., duration spent on Facebook) in the work environment, thus bringing security risks [241]. Organizations can use the knowledge of habit formation to break the cycle of habitual behavior. In this regard, SETA programes may assist in replacing the insecure behavior and establishing better behaviors by inserting a new routine between the cue and reward [242]. Other individual factors such as age, gender, and technical expertise may also have an impact on the type of training that yields the best results [243]. In addition, Gardner [102] states that self-regulatory skills training may be a valuable addition to interventions aimed at modifying habits via reflective motivation change. The importance of considering educational interventions aimed at improving users' cognitive skills to avoid internet deception has been identified in early work [146]. On the contrary, strong habits are not easily changeable by mere informational interventions but also involve disrupting the environmental factors that automatically prompt habit performance [244].

Harrison et al. [63] recommend that anti-phishing interventions be developed in such a way to also include educating individuals on the use of richness and presence cues in emails and the risks these could impose. In this regard, training users to become more vigilant with regard to graphics, logos, and other elements may assist the user to judge the authenticity of an email. However, this study pointed out, as reported in the study by Vishwanath et al. [30], that this could have an adverse effect in terms of which the user may focus only on systematic processing and thereby neglect the role of heuristics. From the literature, it is apparent that both modes of processing have a role to play if one is to conduct a thorough assessment of a phishing message. As a result, the stance taken in this study was to focus on the behavioral perspective, instead of the user interface perspective, which might help to identify to what extent the former would influence the two modes of processing.

9. Limitations and future research

Although this study makes an important theoretical contribution and offers interesting insights into various spheres of behavioral research, its limitations must be mentioned. This study used a cross-sectional design that involved collecting data from students within one particular university in one country. Personality traits are shown to differ across some cultures [245]. Accordingly, the behavior of the respondents in their context must be noted. The statistical classifications derived from our sample do not imply any judgement toward a particular class of individual or personality trait profile. In addition to increasing our sample size, it would be interesting to research an international population to determine whether our model could be generalized across social and cultural contexts. Distinctions between cultures could also be explored; Guo et al. [246] suggest a theoretical approach for exploring social network use across cultures. Demographics, such as age and gender, continue to be an area of contention in phishing studies where there remains disparate findings [247]. Although Diaz et al. [14], Moody et al. [51], Benenson et al. [3] and Mohebzada et al. [248] suggested gender was not conclusive in predicting attack susceptibility, it would be interesting to see if certain personality traits performing a habit would be influenced by their gender and age. This is not inconceivable because prior literature has shown that females habitually practice security compliance in their workplace [249]. As surveys and observations have been shown to capture different factors concerning security behaviors in phishing experiments [250], a multimethod approach might be more suitable for this study design, in particular to observe behaviors such as habit and to narrow down the particular habits users are performing, for example liking, sharing, and clicking on links. The stimuli used to test information processing in our study originated from the researcher's Facebook account. Although we informed respondents in the survey to treat the stimuli as though it originates from their friend, prior literature indicated that individuals are more likely to respond to posts from their actual friend connections than from unknown entities. In addition, our instrument assessed respondents on a single stimulus at a time. In reality, a Facebook user would be exposed to a greater number of posts at once on a timeline containing both textual and graphic elements. In this regard, time pressures were also not assessed which can influence the mode processing [239]. Our stimuli contained mostly graphics that trigger heuristic processing and have been shown to be more effective for phishing attacks [24]. Because the 44-item personality trait instrument took a long time for the participants to complete, other shortened versions, while still reported reliable, like the 10-item shortened personality trait scale, could be considered [251]. There are thus future opportunities to test a wide variety of behavioral variables and their effect on information processing. For example, Spottswood and Hancock [252] found social norms on SNSs can trigger heuristic processing.

10. Conclusion

This study aimed to identify users who are susceptible to phishing by developing a theoretical model that examined the influence of personality traits, habits, and information processing, as well as social norms, computer self-efficacy, and perceived risk on phishing susceptibility. The results of SEM analysis on data collected from 215 participants revealed several significant findings that contribute to the growing body of research in this area. Our study showed that all of the Big Five traits, except for openness, exhibited significant relationships with habits and other variables. Habit was also found to have a significant effect on heuristic and systematic processing, which can affect phishing susceptibility. Owing to the direct influence of habit on phishing susceptibility, the study has also shown that habit and heuristic processing may be part of the same process, as they involve some aspects of *automaticity*, which allows individuals to use limited cognitive resources when engaging in a task.

The study also found that phishing attacks on Facebook can have a significant impact on email phishing susceptibility, highlighting the importance of mitigating phishing risks on social media platforms. With just one careless click, an entire organization could be at risk, emphasizing the need to explore behavioral factors that could hinder phishing detection efforts. Prior literature has suggested that a variety of behavioral factors, including personality traits, habits, threat perceptions, and self-efficacy, could influence phishing detection. Individual differences and characteristics are, therefore, an area of ongoing exploration among scholars in the information security domain [35,50, 253–255].

As social media platforms continue to blur the boundaries between personal and professional settings, the priming effect of users' behavior on these platforms could make them less attentive to and cautious of malicious posts. This, in turn, increases the risk of data breaches in the workplace. In conclusion, our study has contributed to a better understanding of the factors that influence phishing susceptibility, highlighting the need for further research in this area to help organizations protect themselves and their employees from cyber threats.

CRediT authorship contribution statement

Edwin Donald Frauenstein: Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing. **Stephen Flowerday:** Conceptualization, Methodology, Writing – review & editing, Supervision. **Syden Mishi:** Formal analysis, Data curation, Writing – review & editing. **Merrill Warkentin:** Writing – review & editing, Supervision, Project administration.

Appendix A – BFI Personality Trait Scale (John and Srivastava, 2009)

Items measured (1 = strongly disagree to 5 = strongly agree)		
Construct	Item No:	Description
Extraversion	1	Is talkative
	6	Is reserved (R)
	11	Is full of energy
	16	Generates a lot of enthusiasm
	21	Tends to be quiet (R)
	26	Has an assertive (i.e. confident) personality
	31	Is sometimes shy, inhibited (R)
	36	Is outgoing, sociable
Agreeableness	2	Tends to find fault with others (R)
	7	Is helpful and unselfish with others
	12	Starts quarrels (i.e., arguments) with others (R)
	17	Has a forgiving nature
	22	Is generally trusting
	27	Can be cold and aloof (i.e., distant) (R)
	32	Is considerate and kind to almost everyone
	37	Is sometimes rude to others (R)
	42	Likes to cooperate with others
Conscientiousness	3	Does a thorough job
	8	Can be somewhat careless (R)
	13	Is a reliable worker
	18	Tends to be disorganized (R)
	23	Tends to be lazy (R)
	28	Perseveres until the task is finished
	33	Does things efficiently
	38	Makes plans and follows through with them
	43	Is easily distracted (R)
Neuroticism	4	Is depressed, blue
	9	Is relaxed, handles stress well (R)
	14	Can be tense (i.e., nervous, anxious)
	19	Worries a lot
	24	Is emotionally stable, not easily upset (R)
	29	Can be moody
	34	Remains calm in tense situations (R)
	39	Gets nervous easily
Openness	5	Is original, comes up with new ideas
	10	Is curious about many different things
	15	Is ingenious (i.e., clever), a deep thinker
	20	Has an active imagination
	25	Is inventive
	30	Values artistic (i.e., beauty), esthetic experiences
	35	Prefers work that is routine (i.e. procedure) (R)
	40	Likes to reflect, play with ideas
	41	Has few artistic interests (R)
	44	Is sophisticated in art, music, or literature

(R) = denotes reverse scaled items.

Appendix B – Habits [199]

Items measured (1 = strongly disagree to 5 = strongly agree) When a friend posts a link (e.g., could contain a video, image, news article) on Facebook timeline that is of interest to me, and requests me to share it, I click/open/share it as this is something:
I do frequently/often
I do automatically
I do without having to consciously remember
That makes me feel weird if I do not do it
I do without thinking
That would require effort not to do it
That belongs to my (daily, weekly, monthly) routine
I start doing before I realize I'm doing it
I would find hard not to do it
I have no need to think about doing
That's typically 'me'
I have been doing for a long time

Appendix C – Description of stimuli used to measure information processing

Stimuli #	Description of Stimuli	Action Required from User	Persuasion Technique
Stimulus (S1)	Presents an opportunity to win a free store voucher worth R1500 (ZAR). The voucher contains an expiry date.	Click/Share	Authority and scarcity
Stimulus (S2)	The source is giving an opportunity for others to win a silver Mercedes-Benz vehicle. Two lucky giveaways. The draw claims to take place in the next two days.	Comment, Like and Share	Scarcity and social proof
Stimulus (S3)	Breaking News of a famous local athlete Caster Semenya died in a car accident. The video claims to show actual footage of the accident.	Click link	Curiosity
Stimulus (S4)	Opportunity to have financial freedom. Image shows a proof of payment received.	Comment with personal info (i.e., contact number)	Scarcity and social proof
Stimulus (S5)	Video thumbnail showing a person appearing to be robbed. The video indicates that it has been viewed 11 810 727 times.	Click play	Curiosity
Stimulus (S6)	Video thumbnail showing an altercation between workers at Marikana mines.	Click play	Curiosity

Appendix D – Information Processing [30,203]

Items measured (1 = strongly disagree to 5 = strongly agree)
Your Facebook friend posts the image seen **above** on their/your timeline, select the action **YOU** would most likely take:

Construct	Items
Heuristic	I skimmed (i.e., moved quickly) through the Facebook message
Heuristic	I briefly looked at the sender/source of the message
Heuristic	The message is attractive to me as I am interested in the benefits it has to offer
Heuristic	I ignored the message content
Systematic	I thought about the action I took based on what I saw in the Facebook message
Systematic	I spent some time thinking about the request before I made my decision
Systematic	I found myself making connections between the message request and what I have heard about on social networks requesting such information

Appendix E – Social norms

Items measured (1 = strongly disagree to 5 = strongly agree) When a friend posts a status update and asks me to also "share" it, I will consider sharing it based on:
If it is my friend, then it is the friendly thing to do
It depends on what it is that I must share
If it is a topic of interest to me personally
The post is very popular (i.e., trending) and I know others will also find it interesting
If I can see many of my friends or others have also already liked it
If it could get me noticed with some likes from my friends

Appendix F – Computer Self-efficacy

Items measured (very poor, poor, average, good, excellent) Please evaluate your abilities based on the following:
Using a desktop computer to type a document (e.g., assignment, CV, report)
Using a web browser (e.g., Chrome, Explorer, Firefox) to search for information on the Internet
Using the features of an email client app (e.g., Gmail, Yahoo) to send/receive messages and download/upload attachments
Identifying different file extensions (e.g., docx, pdf, .rar, .zip)
Using social network websites (e.g., Facebook, Twitter, Instagram) to post and interact with other users
Checking the security settings of a website to determine if it can be trusted as safe/original
Identifying safe web links/URLs
Installing software on a desktop/laptop computer

Appendix G – Perceived risk

Items measured (1 = strongly disagree to 5 = strongly agree) To what extent do you agree/disagree with the following statements:
There is little risk in sharing posts which instruct you to share to your profile (e.g. share this post and R100 will be donated to a charity)
There is little risk in accepting friend requests from strangers, as I can remove them later if I want to
There is little risk that I can be personally affected on social networking websites (e.g., losing money, identity theft)
I am able to protect myself against threats on social network websites as I have control of my account

Appendix H – Construct descriptive statistics

Variable	Item No.	Mean	S.D.	Loading	CR	AVE
Extraversion	1	3.76	1.18	0.522	0.70	0.502
	6	3.56	1.17	0.828		
	11	4.15	0.94	0.566		
	16	3.74	0.94	0.751		
	21	2.66	1.39	0.660		
	26	4.10	0.96	0.716		
	31	2.43	1.31	0.743		
	36	3.56	1.28	0.681		
Agreeableness	2	3.53	1.24	0.882	0.57	0.518
	7	4.48	1.02	0.793		
	12	4.31	0.91	0.835		
	17	4.35	0.99	0.697		
	22	3.84	1.11	0.806		
	27	3.04	1.34	0.796		
	32	4.39	0.89	0.671		
	37	3.95	1.38	0.749		
	42	4.25	0.91	0.632		
Consciousness	3	3.95	1.01	0.727	0.70	0.694
	8	2.95	1.30	0.659		
	13	4.31	0.91	0.597		
	18	3.59	1.29	0.562		
	23	3.33	1.39	0.629		
	28	4.17	0.99	0.754		
	33	4.15	0.79	0.677		
	38	3.84	1.07	0.740		
	43	2.83	1.43	0.796		
Neuroticism	4	2.02	1.20	0.865	0.73	0.572
	9	2.04	1.15	0.673		
	14	3.41	1.26	0.656		
	19	3.44	1.43	0.674		
	24	2.27	1.34	0.674		
	29	2.82	1.47	0.735		
	34	2.12	1.14	0.707		
	39	3.08	1.46	0.556		
Openness	5	4.09	0.96	0.599	0.72	0.904
	10	4.43	0.78	0.749		
	15	3.79	0.99	0.650		
	20	4.34	0.82	0.619		
	25	3.51	1.02	0.662		
	30	3.91	1.10	0.739		
	35	2.04	1.08	0.875		
	40	3.96	1.00	0.479*		
	41	2.59	1.25	0.779		
	44	3.38	1.35	0.733		
Systematic	S7_5	3.37	1.42	0.530	0.90	0.578
	S7_6	3.33	1.58	0.465*		
	S7_7	3.28	1.51	0.547		
	S8_5	3.36	1.45	0.675		
	S8_6	3.40	1.57	0.675		
	S8_7	3.20	1.49	0.720		
	S9_5	3.21	1.39	0.624		
	S9_6	3.13	1.55	0.575		
	S9_7	3.07	1.53	0.568		
	S10_5	3.11	1.60	0.590		
	S10_6	3.00	1.66	0.639		
	S10_7	2.90	1.62	0.610		
	S11_5	3.02	1.57	0.614		
	S11_6	2.64	1.56	0.624		
	S11_7	2.69	1.54	0.662		
	S12_5	2.99	1.55	0.633		
	S12_6	2.83	1.56	0.638		
	S12_7	2.84	1.56	0.698		
Heuristic	S7_1	1.78	1.41	−0.013*	0.84	0.482
	S7_2	3.86	1.27	0.484*		
	S7_3	3.01	1.58	0.527		
	S7_4	2.27	1.51	0.296*		
	S8_1	1.87	1.53	0.022*		
	S8_2	3.76	1.38	0.492*		
	S8_3	3.30	1.57	0.557		
	S8_4	2.44	1.51	0.284*		
	S9_1	1.84	1.47	0.045*		
	S9_2	3.65	1.38	0.527		
	S9_3	2.70	1.54	0.465*		
	S9_4	2.48	1.44	0.356*		

(*continued on next page*)

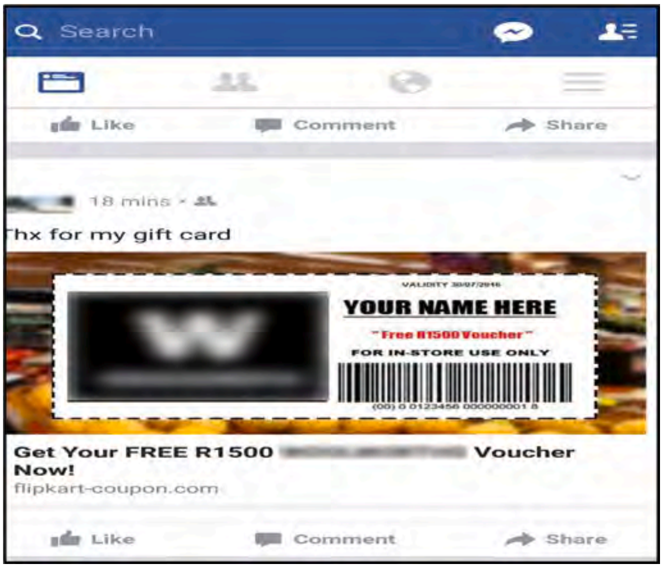
(*continued*)

Variable	Item No.	Mean	S.D.	Loading	CR	AVE
	S10_1	1.72	1.61	0.103*		
	S10_2	3.35	1.56	0.563		
	S10_3	2.73	1.62	0.577		
	S10_4	2.13	1.60	0.462*		
	S11_1	1.81	1.58	0.032*		
	S11_2	3.22	1.60	0.629		
	S11_3	2.27	1.48	0.552		
	S11_4	2.15	1.65	0.402*		
	S12_1	1.73	1.58	−0.013*		
	S12_2	3.27	1.56	0.638		
	S12_3	2.36	1.52	0.584		
	S12_4	2.33	1.54	0.397*		
Habit	1	3.43	1.28	0.443*	0.88	0.504
	2	2.74	1.33	0.622		
	3	2.78	1.31	0.652		
	4	2.27	1.26	0.561		
	5	2.33	1.36	0.663		
	6	2.36	1.21	0.361*		
	7	2.58	1.33	0.623		
	8	2.30	1.28	0.703		
	9	2.47	1.34	0.742		
	10	2.74	1.36	0.501		
	11	2.56	1.34	0.791		
	12	2.65	1.42	0.770		
Social norms	1	3.40	1.43	0.500	0.70	0.640
	2	4.45	1.04	0.021*		
	3	4.21	1.07	0.151*		
	4	3.60	1.34	0.632		
	5	2.89	1.47	0.843		
	6	2.61	1.46	0.651		
Perceived risk	1	3.05	1.62	0.723	0.73	0.613
	2	3.26	1.64	0.801		
	3	3.15	1.72	0.784		
	4	3.83	1.30	0.224*		
Computer self-efficacy	1	4.17	0.84	0.470*	0.79	0.671
	2	4.37	0.70	0.431*		
	3	4.07	0.90	0.544		
	4	3.61	0.96	0.580		
	5	4.37	0.79	0.301*		
	6	3.13	0.97	0.823		
	7	2.97	0.97	0.771		
	8	3.47	1.23	0.500		

Note: *indicates the items with less than 0.5 factor loading were dropped from the model.

Appendix I – Information processing stimuli

Information Processing – Stimulus (S1)



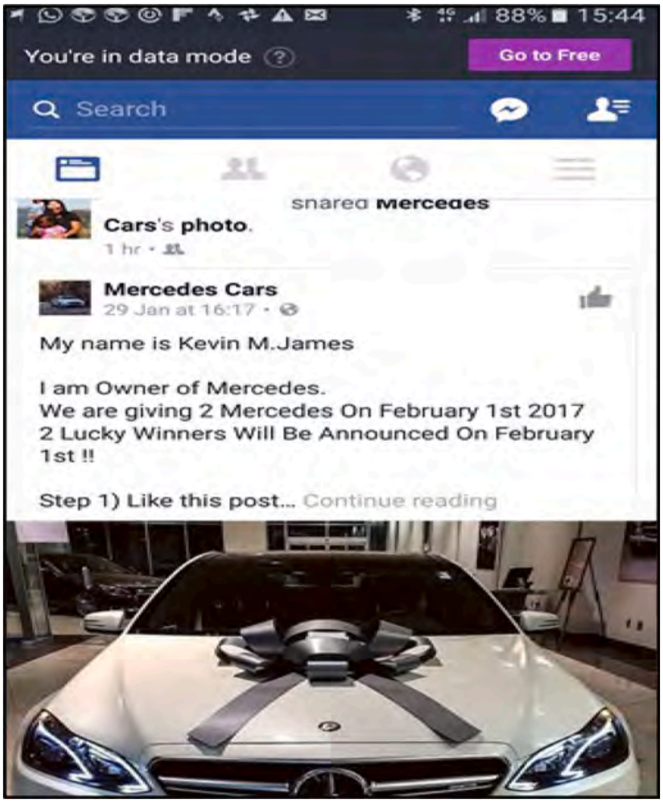
18 mins ·

hx for my gift card

Get Your FREE R1500 [redacted] Voucher Now!

flipkart-coupon.com

Information Processing – Stimulus (S2)



shared Mercedes Cars's photo.

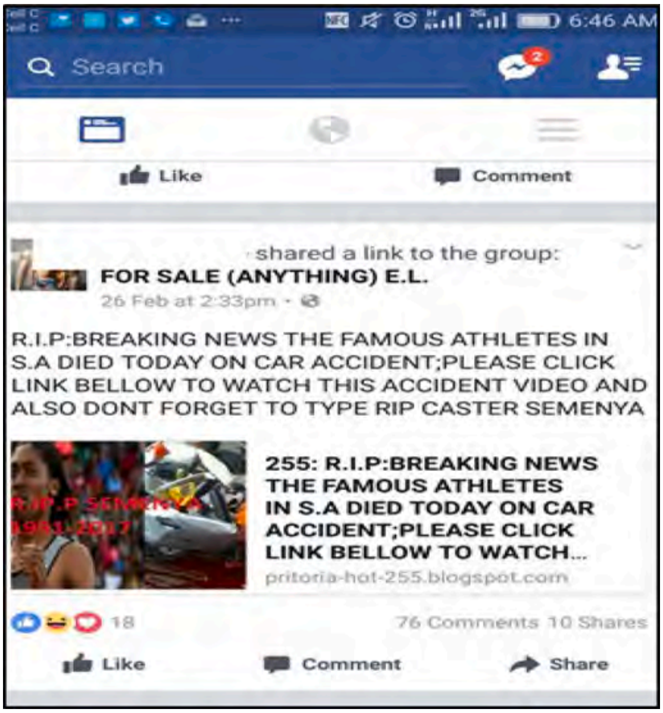
Mercedes Cars

My name is Kevin M.James

I am Owner of Mercedes.
We are giving 2 Mercedes On February 1st 2017
2 Lucky Winners Will Be Announced On February 1st !!

Step 1) Like this post...

Information Processing – Stimulus (S3)



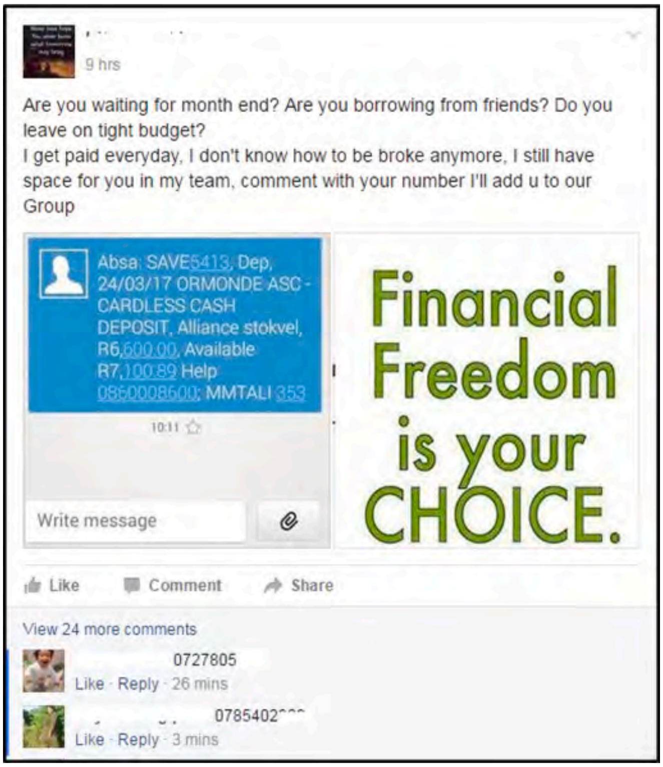
shared a link to the group: FOR SALE (ANYTHING) E.L.

R.I.P:BREAKING NEWS THE FAMOUS ATHLETES IN S.A DIED TODAY ON CAR ACCIDENT;PLEASE CLICK LINK BELLOW TO WATCH THIS ACCIDENT VIDEO AND ALSO DONT FORGET TO TYPE RIP CASTER SEMENYA

255: R.I.P:BREAKING NEWS THE FAMOUS ATHLETES IN S.A DIED TODAY ON CAR ACCIDENT;PLEASE CLICK LINK BELLOW TO WATCH...

pritoria-hot-255.blogspot.com

Information Processing – Stimulus (S4)



9 hrs

Are you waiting for month end? Are you borrowing from friends? Do you leave on tight budget?
I get paid everyday, I don't know how to be broke anymore, I still have space for you in my team, comment with your number I'll add u to our Group

Absa: SAVE5413, Dep, 24/03/17 ORMONDE ASC - CARDLESS CASH DEPOSIT, Alliance stokvel, R6,500.00, Available R7,100.89 Help 0850008600; MMTALI 353

10:11

Write message

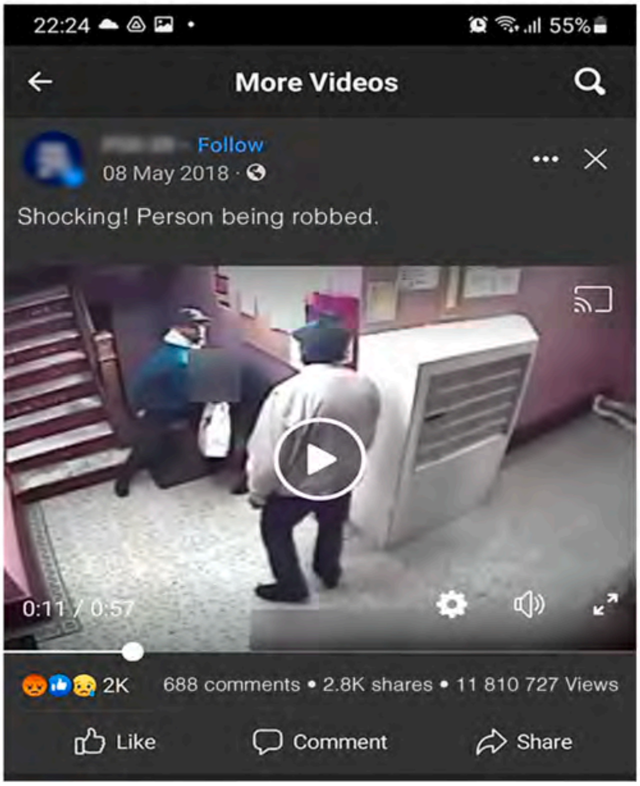
Financial Freedom is your CHOICE.

View 24 more comments

0727805
Like · Reply · 26 mins

0785402
Like · Reply · 3 mins

Information Processing – Stimulus (S5)

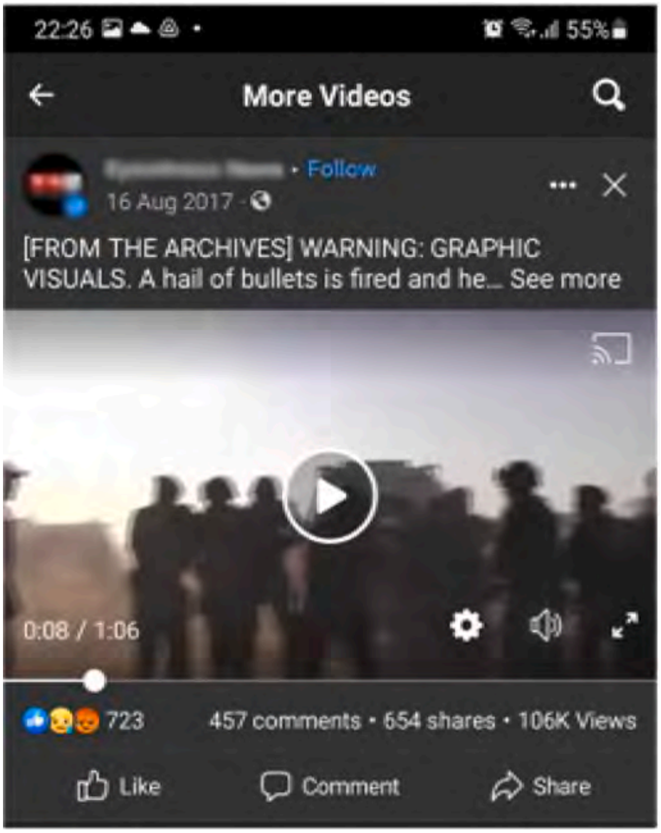


08 May 2018 ·

Shocking! Person being robbed.

2K 688 comments • 2.8K shares • 11 810 727 Views

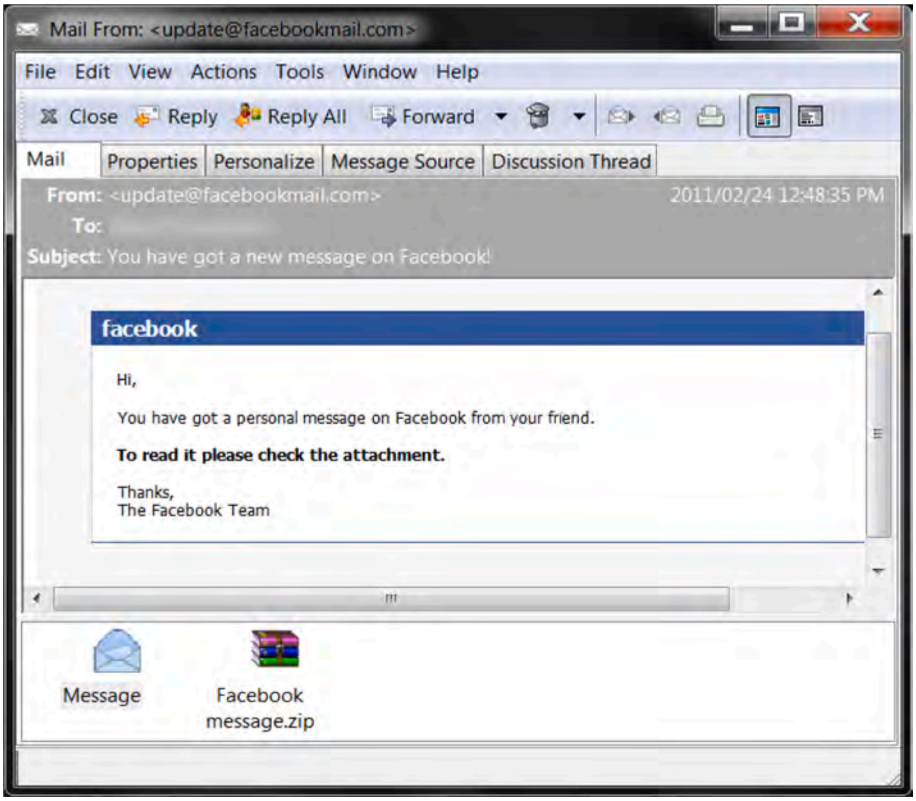
Information Processing – Stimulus (S6)



[FROM THE ARCHIVES] WARNING: GRAPHIC VISUALS. A hail of bullets is fired and he... See more

Appendix J – Phishing Susceptibility

Phishing email used to test phishing susceptibility


Mail From: <update@facebookmail.com>
File Edit View Actions Tools Window Help
Close Reply Reply All Forward
Mail
Properties
Personalize
Message Source
Discussion Thread
Message
Facebook message.zip

From: <update@facebookmail.com> 2011/02/24 12:48:35 PM

To: [redacted]

Subject: You have got a new message on Facebook!

facebook

Hi,

You have got a personal message on Facebook from your friend.

To read it please check the attachment.

Thanks,
The Facebook Team

References

[1] S. Grabner-Kräuter, Web 2.0 Social networks: the role of trust, J. Bus. Ethics 90 (4) (2009) 505–522, https://doi.org/10.1007/s10551-010-0603-1.

[2] Statista (2022a). Global social network user growth from 2018 to 2027 https://www.statista.com/statistics/270919/worldwide-social-network-user-growth/.

[3] Benenson, Z., Girard, A., Hintz, N., & Luder, A. (2014). *Susceptibility to URL-based Internet attacks: facebook vs. email.* Paper presented at the Sixth IEEE Workshop on SECurity and SOCial Networking, Budapest, Hungary.

[4] Statista (2022b). Most popular social networks worldwide as of January 2022, ranked by number of monthly active users. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

[5] T.L. James, P.B. Lowry, L. Wallace, M. Warkentin, The effect of belongingness on obsessive-compulsive disorder in the use of online social networks, J. Manage. Infor. Syst. 34 (2) (2017) 560–596, https://doi.org/10.1080/07421222.2017.1334496.

[6] C.M.K. Cheung, P.-Y. Chiu, M.K.O. Lee, Online social networks: why do students use Facebook? Comput. Hum. Behav. 27 (4) (2011) 1337–1343, https://doi.org/10.1016/j.chb.2010.07.028.

[7] APWG. (2022). Phishing activity trends report, 3rd quarter 2022. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf.

[8] Blythe, M., Petrie, H., & Clark, J.A. (2011). *F for fake: four studies on how we fall for phish.* Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada.

[9] A. Vishwanath, Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack, J. Comput.-Med. Commun. 20 (5) (2015) 570–584, https://doi.org/10.1111/jcc4.12126.

[10] Y. Chen, F.M. Zahedi, A. Abbasi, D. Dobolyi, Trust calibration of automated security IT artifacts: a multi-domain study of phishing-website detection tools, Infor. Manage. 58 (1) (2021), 103394, https://doi.org/10.1016/j.im.2020.103394.

[11] Netwrix. (2020). 2020 Cyber threats report. https://www.netwrix.com/download/collaterals/2020_Cyber_Threats_Report.pdf.

[12] E.D. Frauenstein, S. Flowerday, Susceptibility to phishing on social network sites: a personality information processing model, Comput. Secur. 94 (2020), 101862, https://doi.org/10.1016/j.cose.2020.101862.

[13] K. Krombholz, H. Hobel, M. Huber, E. Weippl, Advanced social engineering attacks, J. Infor. Secur. Appl. 22 (C) (2015) 113–122, https://doi.org/10.1016/j.jisa.2014.09.005.

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

[15] Alutaybi, A., Arden-Close, E., McAlaney, J., Stefanidis, A., Phalp, K., & Ali, R. (2019). *How can social networks design trigger fear of missing out?* Paper presented at the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy.

[16] C. Sushama, M. Sunil Kumar, P Neelima, Privacy and security issues in the future: a social media, Mater. Today: Proc. (2021), https://doi.org/10.1016/j.matpr.2020.11.105.

[17] M. Fire, R. Goldschmidt, Y. Elovici, Online social networks: threats and solutions, IEEE Commun. Surveys Tutor. 16 (4) (2014), https://doi.org/10.1109/COMST.2014.2321628.

[18] Kahimise, J., & Shava, F.B. (2020). An analysis of social networking threats. Paper presented at the 15th International Conference on Cyber Warfare and Security, Norfolk, Virginia, USA.

[19] Ophoff, J., & Robinson, M. (2014). *Exploring end-user smartphone security awareness within a South African context.* Paper presented at the 13th Information Security for South Africa conference (ISSA 2014), Johannesburg, South Africa.

[20] Statista (2021). Facebook access penetration 2021, by device. https://www.statista.com/statistics/377808/distribution-of-facebook-users-by-device/.

[21] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, M. Butavicius, Why do some people manage phishing e-mails better than others? Infor. Manage. Comput. Secur. 20 (1) (2012) 18–28, https://doi.org/10.1108/09685221211219173.

[22] Turel, O., & Serenko, A. (2011). *Developing a (bad) habit: antecedents and adverse consequences of social networking website use habit.* Paper presented at the 17th Americas Conference on Information Systems (AMCIS 2011). Detroit, Michigan, USA.

[23] B. Verplanken, H. Aarts, Habit, attitude, and planned behaviour: is habit an empty construct or an interesting case of goal-directed automaticity? Eur. Rev. Soc. Psychol. 10 (1) (1999) 101–134, https://doi.org/10.1080/14792779943000035.

[24] A. Vishwanath, Getting phished on social media, Decis. Support Syst. 103 (C) (2017) 70–81, https://doi.org/10.1016/j.dss.2017.09.004.

[25] Krasnova, H., Kolesnikova, E., & Günther, O. (2009). *"It won't happen to me!" Self-disclosure in online social networks.* Paper presented at the 15th Americas Conference on Information Systems (AMCIS 2009), Atlanta, Georgia.

[26] S.J. Kim, J.T. Hancock, Optimistic bias and Facebook use: self–other discrepancies about potential risks and benefits of facebook use, Cyberpsychol., Behav. Soc. Network. 18 (4) (2015) 214–220, https://doi.org/10.1089/cyber.2014.0656.

[27] Warkentin, M., Xu, Z., & Mutchler, L. (2013). *I'm safer than you: the role of optimism bias in personal IT risk assessments.* Paper presented at the 2013 Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13, Niagara Falls, NY.

[28] Wang, N., Xu, H., & Grossklags, J. (2011). *Third-party apps on Facebook: privacy and the illusion of control.* Paper presented at the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology, Cambridge, Massachusetts.

[29] J. Colliander, This is fake news": investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media, Comput. Hum. Behav. 97 (2019) 202–215, https://doi.org/10.1016/j.chb.2019.03.032.

[30] A. Vishwanath, T. Herath, R. Chen, J. Wang, H.R. Rao, Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model, Decis. Support Syst. 51 (3) (2011) 576–586, https://doi.org/10.1016/j.dss.2011.03.002.

[31] A. Aleroud, L. Zhou, Phishing environments, techniques, and countermeasures, Comput. Secur. 68 (C) (2017) 160–196, https://doi.org/10.1016/j.cose.2017.04.006.

[32] S. Mansfield-Devine, The ever-changing face of phishing, Comput. Fraud Secur 2018 (11) (2018) 17–19, https://doi.org/10.1016/S1361-3723(18)30111-8.

[33] T.R. Levine, Truth-Default Theory (TDT): a theory of human deception and deception detection, J. Lang. Soc. Psychol. 33 (4) (2014) 378–392, https://doi.org/10.1177/0261927x14535916.

[34] B. Schneier, Stop trying to fix the user, IEEE Secur. Priv. 14 (5) (2016) 96, https://doi.org/10.1109/MSP.2016.101. –96.

[35] A.C. Johnston, M. Warkentin, M. McBride, L. Carter, Dispositional and situational factors: influences on information security policy violations, Eur. J. Infor. Sys. 25 (3) (2016) 231–251, https://doi.org/10.1057/ejis.2015.15.

[36] P. Briggs, D. Jeske, L. Coventry, Behavior change interventions for cybersecurity, in: L. Little, E. Sillence, A. Joinson (Eds.), Behavior Change Research and Theory, Academic Press, San Diego, 2017, pp. 115–136.

[37] I. Kirlappos, M.A. Sasse, Security education against phishing: a modest proposal for a major re-think, IEEE Secur. Privacy 10 (2) (2012) 24–32, https://doi.org/10.1109/MSP.2011.179.

[38] S. Goel, K.J. Williams, J. Huang, M. Warkentin, Can financial incentives help with the struggle for security policy compliance? Infor. Manage. 58 (4) (2021), 103447 https://doi.org/10.1016/j.im.2021.103447.

[39] J.D. Wall, M. Warkentin, Perceived argument quality's effect on threat and coping appraisals in fear appeals: an experiment and exploration of realism check heuristics, Infor. Manage. 56 (8) (2019), 103157, https://doi.org/10.1016/j.im.2019.03.002.

[40] Facebook. (2021). What steps can I take to protect myself from phishing on Facebook? https://www.facebook.com/help/166863010078512.

[41] Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., & Ebner, N. (2017). *Dissecting spear phishing emails for older* vs *young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing.* Paper presented at the CHI Conference on Human Factors in Computing Systems, Denver, Colorado, USA.

[42] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q. 34 (3) (2010) 523–548, https://doi.org/10.2307/25750690.

[43] J.-W. Bullée, L. Montoya, W. Pieters, M. Junger, P.H. Hartel, The persuasion and security awareness experiment: reducing the success of social engineering attacks, J. Exp. Criminol. 11 (1) (2015) 97–115, https://doi.org/10.1007/s11292-014-9222-7.

[44] W.D. Kearney, H.A. Kruger, Theorising on risk homeostasis in the context of information security behaviour, Infor. Comput. Secur. 24 (5) (2016) 496–513, https://doi.org/10.1108/ICS-04-2016-0029.

[45] E.J. Williams, J. Hinds, A.N. Joinson, Exploring susceptibility to phishing in the workplace, Int. J. Hum. Comput. Stud. 120 (2018) 1–13, https://doi.org/10.1016/j.ijhcs.2018.06.004.

[46] S.M. Albladi, G.R.S. Weir, User characteristics that influence judgment of social engineering attacks in social networks, Human-centric Comput. Infor. Sci. 8 (1) (2018), https://doi.org/10.1186/s13673-018-0128-7.

[47] Alseadoon, I., Othman, M.F.I., & Chan, T. (2015). *What is the influence of users' characteristics on their ability to detect phishing emails?* Paper presented at the 1st International Conference on Communication and Computer Engineering, Malaysia.

[48] S. Goel, K. Williams, E. Dincelli, Got phished? Internet security and human vulnerability, J. Assoc. Infor. Syst. 18 (2017) 22–44, https://doi.org/10.17705/1jais.00447.

[49] Kaptein, M., Markopoulos, P., De Ruyter, B., & Aarts, E. (2009). *Can you be persuaded? Individual differences in susceptibility to persuasion.* Paper presented at the 13th International Conference on Human-Computer Interaction (INTERACT 2009), Uppsala, Sweden.

[50] Mayhorn, C.B., Welka, A.K., Zielinska, O.A., & Murphy-Hill, E. (2015). *Assessing individual differences in a phishing detection task.* Paper presented at the 19th Triennial Congress of the IEA, Melbourne, Australia.

[51] G.D. Moody, D.F. Galletta, B.K. Dunn, Which phish get caught? An exploratory study of individuals′ susceptibility to phishing, Eur. J. Infor. Sys. 26 (6) (2017) 564–584, https://doi.org/10.1057/s41303-017-0058-x.

[52] A. Vishwanath, B. Harrison, Y.J. Ng, Suspicion, cognition, and automaticity model of phishing susceptibility, Communic. Res. 45 (8) (2018) 1146–1166, https://doi.org/10.1177/0093650215627483.

[53] M. Workman, Gaining access with social engineering: an empirical study of the threat, Infor. Syst. Security 16 (6) (2007) 315–331, https://doi.org/10.1080/10658980701788165.

[54] M. Workman, Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security, J. Am. Soc. Infor. Sci. Technol. 59 (4) (2008) 662–674, https://doi.org/10.1002/asi.20779.

[55] R.T. Wright, K. Marett, The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived, J. Manage. Infor. Syst. 27 (1) (2010) 273–303, https://doi.org/10.2753/MIS0742-1222270111.

[56] Cho, J.-H., Cam, H., & Oltramari, A. (2016). *Effect of personality traits on trust and risk to phishing vulnerability: modeling and analysis.* Paper presented at the IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA 2016), San Diego, CA.

[57] Cusack, B., & Adedokun, K. (2018). *The impact of personality traits on user's susceptibility to social engineering attacks.* Paper presented at the 16th Australian Information Security Management Conference, Perth, Australia.

[58] Halevi, T., Lewis, J., & Memon, N. (2013). *A pilot study of cyber security and privacy related behavior and personality traits.* Paper presented at the 22nd international conference on World Wide Web companion (WWW), Rio de Janeiro, Brazil.

[59] Jin-Hee, C., Hasan, C., & Oltramari, A. (2016). *Effect of personality traits on trust and risk to phishing vulnerability: modeling and analysis.* Paper presented at the 6th IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA 2016), San Diego, USA.

[60] Y. Amichai-Hamburger, Internet and personality, Comput. Hum. Behav. 18 (1) (2002) 1–10, https://doi.org/10.1016/S0747-5632(01)00034-6.

[61] A. Quan-Haase, A.L. Young, Uses and gratifications of social media: a comparison of Facebook and Instant Messaging, Bull. Sci. Technol. Soc. 30 (5) (2010) 350–361, https://doi.org/10.1177/0270467610380009.

[62] A. Vishwanath, Habitual Facebook use and its impact on getting deceived on social media, J. Comput.-Med. Commun. 20 (1) (2015) 83–98, https://doi.org/10.1111/jcc4.12100.

[63] Harrison, B., Vishwanath, A., Ng, Y.J., & Rao, R. (2015). *Examining the impact of presence on individual phishing victimization.* Paper presented at the 48th Hawaii International Conference on System Sciences (HICSS 2015), Hawaii, USA.

[64] X. Luo, W. Zhang, S. Burd, A. Seazzu, Investigating phishing victimization with the Heuristic-Systematic Model: a theoretical framework and an exploration, Comput. Secur. 38 (2013) 28–38, https://doi.org/10.1016/j.cose.2012.12.003.

[65] Valecha, R., Chen, R., Herath, T., Vishwanath, A., Wang, J., & Rao, H.R. (2015). *An exploration of phishing information sharing: a heuristic-systematic approach.* Paper presented at the 2015 IEEE 9th International Symposium on Intelligent Signal Processing (WISP) Proceedings, Siena, Italy.

[66] Z. Xu, W. Zhang, Victimized by phishing: a heuristic-systematic perspective, J. Internet Bankin.Comm. 17 (3) (2012) 1–16.

[67] H.J. Parker, S.V. Flowerday, Contributing factors to increased susceptibility to social media phishing attacks, South Afr. J. Infor. Manage.(SAJIM) 22 (1) (2020) 1–10, https://doi.org/10.4102/sajim.v22i1.1176.

[68] Alotaibi, M. (2019). *A hypothesised model to examine susceptibility to cyber-social engineering through LinkedIn in the workplace.* Paper presented at the Human Aspects of Information Security & Assurance (HAISA 2019), Nicosia, Cyprus.

[69] P. Costa, R.C. McCrae, The Revised NEO Personality Inventory (NEO-PI-R), 2, Psychological Assessment Resources, Inc, Odessa, TX, USA, 1992. Vol.

[70] A. Binks, The art of phishing: past, present and future, Comput. Fraud Secur. 2019 (4) (2019) 9–11, https://doi.org/10.1016/S1361-3723(19)30040-5.

[71] PhishLabs (2019). 2019 Phishing trends and intelligence report. https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf.

[72] Frauenstein, E.D. (2018). *An investigation into students responses to various phishing emails and other phishing-related behaviours.* Paper presented at the 17th Information Security for South Africa conference (ISSA 2018), Pretoria, South Africa.

[73] F.K.-Y. Chou, A.P.-S. Chen, V.C.-L. Lo, Mindless response or mindful interpretation: examining the effect of message influence on phishing susceptibility, Sustainability 13 (4) (2021) 1651, https://doi.org/10.3390/su13041651.

[74] J. Fogel, E. Nehmad, Internet social network communities: risk taking, trust, and privacy concerns, Comput. Hum. Behav. 25 (1) (2009) 153–160, https://doi.org/10.1016/j.chb.2008.08.006.

[75] R.B. Cialdini, Influence: The Psychology of Persuasion, Harper Collins, New York, 2007.

[76] K. Parsons, M. Butavicius, P. Delfabbro, M. Lillie, Predicting susceptibility to social influence in phishing emails, Int. J. Hum. Comput. Stud. 128 (2019) 17–26, https://doi.org/10.1016/j.ijhcs.2019.02.007.

[77] Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). *Social engineering in social networking sites: how good becomes evil.* Paper presented at the 18th Pacific Asia Conference on Information Systems (PACIS 2014), Chengdu, China.

[78] X. Lin, P.R. Spence, K.A. Lachlan, Social media and credibility indicators: the effect of influence cues, Comput. Hum. Behav. 63 (2016) 264–271, https://doi.org/10.1016/j.chb.2016.05.002.

[79] J. Heinström, Five personality dimensions and their influence on information behaviour, Infor. Res. 9 (1) (2003). http://InformationR.net/ir/9-1/paper165.html.

[80] L. Zheng, T. Zheng, Innovation through social media in the public sector: information and interactions, Gov. Inf. Q. 31 (2014) S106–S117, https://doi.org/10.1016/j.giq.2014.01.011.

[81] Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P.G., & Cranor, L.F. (2011). *"I regretted the minute I pressed share": a qualitative study of regrets on Facebook*. Paper presented at the Proceedings of the 7th Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania.

[82] Y. Amichai-Hamburger, G. Vinitzky, Social network use and personality, Comput. Hum. Behav. 26 (6) (2010) 1289–1295, https://doi.org/10.1016/j.chb.2010.03.018.

[83] T. Correa, A.W. Hinsley, H.G. de Zúñiga, Who interacts on the Web?: the intersection of users' personality and social media use, Comput. Hum. Behav. 26 (2) (2010) 247–253, https://doi.org/10.1016/j.chb.2009.09.003.

[84] E. Mancinelli, G. Bassi, S. Salcuni, Predisposing and motivational factors related to social network sites use: systematic review, JMIR Formative Res. 3 (2) (2019), https://doi.org/10.2196/12248.

[85] K. Moore, J.C. McElroy, The influence of personality on Facebook usage, wall postings, and regret, Comput. Hum. Behav. 28 (1) (2012) 267–274, https://doi.org/10.1016/j.chb.2011.09.009.

[86] C. Ross, E.S. Orr, M. Sisic, J.M. Arseneault, M.G. Simmering, R.R. Orr, Personality and motivations associated with Facebook use, Comput. Hum. Behav. 25 (2) (2009) 578–586, https://doi.org/10.1016/j.chb.2008.12.024.

[87] T. Ryan, S. Xenos, Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage, Comput. Hum. Behav. 27 (5) (2011) 1658–1664, https://doi.org/10.1016/j.chb.2011.02.004.

[88] K. Wilson, S. Fornasier, K.M. White, Psychological predictors of young adults' use of social networking sites, Cyberpsychol., Behav. Soc. Network. 13 (2) (2010) 173–177, https://doi.org/10.1089/cyber.2009.0094.

[89] R.R. McCrae, P.T Costa Jr, A Five-Factor theory of personality. Handbook of personality: Theory and Research, 2nd ed., Guilford Press, New York, NY, US, 1999, pp. 139–153.

[90] A. Terracciano, P.T. Costa Jr., R.R McCrae, Personality plasticity after age 30, Pers. Soc. Psychol. Bull. 32 (8) (2006) 999–1009, https://doi.org/10.1177/0146167206288599.

[91] R.I. Damian, M. Spengler, A. Sutu, B.W. Roberts, Sixteen going on sixty-six: a longitudinal study of personality stability and change across 50 years, J. Pers. Soc. Psychol. 117 (3) (2019) 674–695, https://doi.org/10.1037/pspp0000210.

[92] O.P. John, S Srivastava, The Big Five Trait taxonomy: history, measurement, and theoretical perspectives, in: L.A. Pervin, O.P. John (Eds.), Handbook of personality: Theory and Research, 2nd ed., Guilford Press, New York, NY, 1999, pp. 102–138.

[93] P.T. Costa, R.R. McCrae, Four ways five factors are basic, Pers. Individ. Dif. 13 (6) (1992) 653–665, https://doi.org/10.1016/0191-8869(92)90236-I.

[94] L.-F. Zhang, Thinking styles and the big five personality traits revisited, Pers. Individ. Dif. 40 (6) (2006) 1177–1187, https://doi.org/10.1016/j.paid.2005.10.011.

[95] Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). *Breaching the human firewall: social engineering in phishing and spear-phishing emails*. Paper presented at the Australasian Conference on Information Systems, Adelaide, Australia.

[96] Lawson, P.A., Crowson, A.D., & Mayhorn, C.B. (2018). *Baiting the hook: exploring the interaction of personality and persuasion tactics in email phishing attacks*. Paper presented at the 20th Congress of the International Ergonomics Association (IEA 2018), Florence, Italy.

[97] P. Lawson, O. Zielinska, C. Pearson, C.B. Mayhorn, Interaction of personality and persuasion tactics in email phishing attacks, Proceed. Hum. Factors Ergon. Soc. Ann. Meet. 61 (1) (2017) 1331–1333, https://doi.org/10.1177/1541931213601815.

[98] Oyibo, K., Orji, R., & Vassileva, J. (2017). *Investigation of the influence of personality traits on Cialdini's persuasive strategies*. Paper presented at the Personalization in Persuasive Technology Workshop, Persuasive Technology 2017, Amsterdam, Netherlands.

[99] Uebelacker, S., & Quiel, S. (2014). *The Social Engineering Personality Framework*. Paper presented at the 2014 Workshop on Socio-Technical Aspects in Security and Trust, Vienna, Austria.

[100] M. Kajzer, J. D'Arcy, C.R. Crowell, A. Striegel, D. Van Bruggen, An exploratory investigation of message-person congruence in information security awareness campaigns, Comput. Secur. 43 (2014) 64–76, https://doi.org/10.1016/j.cose.2014.03.003.

[101] C. Montag, C. Sindermann, D. Lester, K.L. Davis, Linking individual differences in satisfaction with each of Maslow's needs to the Big Five personality traits and Panksepp's primary emotional systems, Heliyon 6 (7) (2020) e04325, https://doi.org/10.1016/j.heliyon.2020.e04325.

[102] B. Gardner, A review and analysis of the use of 'habit' in understanding, predicting and influencing health-related behaviour, Health Psychol. Rev. 9 (3) (2015) 277–295, https://doi.org/10.1080/17437199.2013.876238.

[103] H. Aarts, B. Verplanken, A. Van Knippenberg, Predicting behavior from actions in the past: repeated decision making or a matter of habit? J. Appl. Soc. Psychol. 28 (15) (1998) 1355–1374, https://doi.org/10.1111/j.1559-1816.1998.tb01681.x.

[104] M. Limayem, S.G. Hirt, C.M.K. Cheung, How habits limit the predictive power of intention: the case of information systems continuance, MIS Q. 31 (4) (2007) 705–737, https://doi.org/10.2307/25148817.

[105] Florencio, D., & Herley, C. (2007). *A large-scale study of web password habits*. Paper presented at the 16th international conference on World Wide Web, Banff, Alberta, Canada.

[106] B. Friendman, A Study of South African Computer users' Password Usage Habits and Attitude Towards Password Security, Masters of Science). Rhodes University, Grahamstown, South Africa, 2014.

[107] Stobert, E., & Biddle, R. (2016). *Expert Password Management*, Paper presented at 9th International Conference on Passwords, Cambridge, UK.

[108] R. LaRose, The psychology of interactive media habits, in: S.S. Sundar (Ed.), The Handbook of the Psychology of Communication Technology, Wiley Online Library, 2015.

[109] R. LaRose, J.-H. Kim, W. Peng, Social networking: addictive, compulsive, problematic or just another media habit? in: Z. Papacharissi (Ed.), A Networked self: Identity, community, and Culture On Social Network Sites Routledge, New York, NY, 2011, pp. 59–81.

[110] R. LaRose, C.A. Lin, M.S. Eastin, Unregulated internet usage: addiction, habit, or deficient self-regulation? Media Psychol. 5 (3) (2003) 225–253, https://doi.org/10.1207/S1532785XMEP0503_01.

[111] S. Mouakket, Factors influencing continuance intention to use social network sites: the Facebook case, Comput. Hum. Behav. 53 (2015) 102–110, https://doi.org/10.1016/j.chb.2015.06.045.

[112] Thadani, D., & Cheung, C. (2011). *Exploring the role of online social network dependency in habit formation*. Paper presented at the 32nd International Conference on Information Systems (ICIS), Shanghai, China.

[113] O. Turel, A. Serenko, The benefits and dangers of enjoyment with social networking websites, Eur. J. Infor. Sys. 21 (5) (2012) 512–528, https://doi.org/10.1057/ejis.2012.1.

[114] Dahlberg, T., & Oorni, A. (2007, 3-6 Jan. 2007). *Understanding changes in consumer payment habits: do mobile payments and electronic invoices attract consumers?* Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS 2007), Big Island, Hawaii.

[115] C. Liao, P. Palvia, H.-N. Lin, The roles of habit and web site quality in e-commerce, Int. J. Inf. Manage. 26 (6) (2006) 469–483, https://doi.org/10.1016/j.ijinfomgt.2006.09.001.

[116] V. Venkatesh, J. Thong, X. Xu, Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology, MIS Q. 36 (1) (2012) 157–178, https://doi.org/10.2307/41410412.

[117] A. Vance, M. Siponen, S. Pahnila, Motivating IS security compliance: insights from habit and protection motivation theory, Infor. Manage. 49 (3) (2012) 190–198, https://doi.org/10.1016/j.im.2012.04.002.

[118] Alqarni, Z., Algarni, A., & Xu, Y. (2016). *Toward Predicting Susceptibility to Phishing Victimization on Facebook*. Paper presented at the IEEE International Conference on Services Computing (SCC 2016). San Francisco, CA, USA.

[119] Frauenstein, E.D., & Flowerday, S. (2016). *Social network phishing: becoming habituated to clicks and ignorant to threats?* Paper presented at the 15th Information Security for South Africa conference (ISSA 2016), Johannesburg, South Africa.

[120] Volkman, E. (2020). Why social media is increasingly abused for phishing attacks. https://info.phishlabs.com/blog/how-social-media-is-abused-for-phishing-attacks.

[121] Herath, T., & D'Arcy, J. (2015). *Social networking behaviors: role of personality, perceived risk, and social influences*. Paper presented at the International Conference on Information Resources Management (Conf-IRM 2015), Ottawa, Ontario, Canada.

[122] W. Jager, Breaking 'bad habits': A dynamical Perspective On Habit Formation and Change, University of Groningen, Netherlands, 2003. Paper presented at the Human Decision Making and Environmental PerceptionUnderstanding and Assisting Human Decision Making in Real-life Settings.

[123] H.C. Triandis, Values, attitudes, and interpersonal behavior, Nebr. Symp. Motiv. 27 (1980) 195–259.

[124] W. Wood, D. Rünger, Psychology of habit, Annu. Rev. Psychol. 67 (2016) 289–314, https://doi.org/10.1146/annurev-psych-122414-033417.

[125] W. Wood, D. Neal, A new look at habits and the habit-goal interface, Psychol. Rev. 114 (2007) 843–863, https://doi.org/10.1037/0033-295X.114.4.843.

[126] S. Mehdizadeh, Self-presentation 2.0: narcissism and self-esteem on Facebook, Cyberpsychol., Behav. Soc. Network. 13 (4) (2010) 357–364, https://doi.org/10.1089/cyber.2009.0257.

[127] S. Kabadayi, K. Price, Consumer – brand engagement on Facebook: liking and commenting behaviors, J. Res. Interact. Market. 8 (3) (2014) 203–223, https://doi.org/10.1108/JRIM-12-2013-0081.

[128] C.T. Carr, D.Y. Wohn, R.A. Hayes, As social support: relational closeness, automaticity, and interpreting social support from paralinguistic digital affordances in social media, Comput. Hum. Behav. 62 (2016) 385–393, https://doi.org/10.1016/j.chb.2016.03.087.

[129] Arntz, P. (2019). Explained: like-farming. https://blog.malwarebytes.com/101/2019/04/explained-like-farming/.

[130] S. Yang, B. Wang, Y. Lu, Exploring the dual outcomes of mobile social networking service enjoyment: the roles of social self-efficacy and habit, Comput. Hum. Behav. 64 (2016) 486–496, https://doi.org/10.1016/j.chb.2016.07.010.

[131] J.M. Balcerowska, P. Bereznowski, A. Biernatowska, P.A. Atroszko, S. Pallesen, C. S. Andreassen, Is it meaningful to distinguish between Facebook addiction and social networking sites addiction? Psychometric analysis of Facebook addiction and social networking sites addiction scales, Curr. Psychol. (2020), https://doi.org/10.1007/s12144-020-00625-3.

[132] T.L. James, L. Wallace, M. Warkentin, B.C. Kim, S.E. Collignon, Exposing others' information on online social networks (OSNs): perceived shared risk, its

determinants, and its influence on OSN privacy control use, Infor. Manage. 54 (7) (2017) 851–865, https://doi.org/10.1016/j.im.2017.01.001.

[133] D.J. Kuss, M.D. Griffiths, Social networking sites and addiction: ten lessons learned, Int. J. Environ. Res. Public Health 14 (3) (2017) 311, https://doi.org/10.3390/ijerph14030311.

[134] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, S. Arthi, Why is phishing still successful? Comput. Fraud Secur. 2020 (9) (2020) 15–19, https://doi.org/10.1016/S1361-3723(20)30098-1.

[135] A.R. Lee, S.-M. Son, K.K. Kim, Information and communication technology overload and social networking service fatigue: a stress perspective, Comput. Hum. Behav. 55 (2016) 51–61, https://doi.org/10.1016/j.chb.2015.08.011.

[136] A. Thomas-Jones, You've been poked: bullying, harassment and everyday undercurrents, in: A. Thomas-Jones (Ed.), The Host in the Machine, Chandos Publishing, 2010, pp. 99–121.

[137] Smoliarova A.S., Gromova T.M., Pavlushkina N.A. (2018). Emotional stimuli in social media user behavior: emoji reactions on a news media Facebook page. In: Bodrunova S. (eds) Internet Science. INSCI 2018. Lecture Notes in Computer Science, vol 11193. Springer, Cham. https://doi.org/10.1007/978-3-030-01437-7_19.

[138] M.M. Moreno-Fernández, F. Blanco, P. Garaizar, H. Matute, Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud, Comput. Hum. Behav. 69 (2017) 421–436, https://doi.org/10.1016/j.chb.2016.12.044.

[139] Z. Jian, W. Zhang, L. Tian, W. Fan, Y. Zhong, Self-deception reduces cognitive load: the role of involuntary conscious memory impairment, Front. Psychol. 10 (2019) 1718, https://doi.org/10.3389/fpsyg.2019.01718. –1718.

[140] D.B. Buller, J.K. Burgoon, Interpersonal deception theory. Communication Theory, 1996, pp. 203–242, https://doi.org/10.1111/j.1468-2885.1996.tb00127.x.

[141] Pfeiffer, T., Kauer, M., & Röth, J. (2014). *"A bank would never write that!" A qualitative study on e-mail trust decisions*. Paper presented at the annual conference of the Gesellschaft für Informatik (GI), Stuttgart, Germany.

[142] Bayl-Smith, P., Sturman, D., & Wiggins, M. (2020). Cue utilization, phishing feature and phishing email detection. In (pp. 56–70).

[143] Lin, E., Greenberg, S., Trotter, E., Ma, D., & Aycock, J. (2011). *Does domain highlighting help people identify phishing sites?* Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada.

[144] M.J. Metzger, A.J. Flanagin, Credibility and trust of information in online environments: the use of cognitive heuristics, J. Pragmat. 59 (2013) 210–220, https://doi.org/10.1016/j.pragma.2013.07.012.

[145] D. Sterrett, D. Malato, J. Benz, L. Kantor, T. Tompson, T. Rosenstiel, K. Loker, Who shared it?: deciding what news to trust on social media, Digital Journal. 7 (6) (2019) 783–801, https://doi.org/10.1080/21670811.2019.1623702.

[146] S. Grazioli, Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet, Group Dec. Negot. 13 (2) (2004) 149–172, https://doi.org/10.1023/B:GRUP.0000021839.04093.5d.

[147] S. Chen, K. Duckworth, S. Chaiken, Motivated heuristic and systematic processing, Psychol. Inq. 10 (1) (1999) 44–49, https://doi.org/10.1207/s15327965pli1001_6.

[148] Harrison, B., Vishwanath, A., & Rao, R. (2016). *A user-centered approach to phishing susceptibility: the role of a suspicious personality in protecting against phishing.* Paper presented at the 49th Hawaii International Conference on System Sciences (HICSS 2016), Hawaii, USA.

[149] C.W. Trumbo, Information Processing and Risk Perception: an Adaptation of the Heuristic-Systematic Model, J. Commun. 52 (2) (2006) 367–382, https://doi.org/10.1111/j.1460-2466.2002.tb02550.x.

[150] A. Gardikiotis, W.D. Crano, Persuasion theories, in: J.D. Wright (Ed.), International Encyclopedia of the Social & Behavioral Sciences, Second Edition, Elsevier, Oxford, 2015, pp. 941–947.

[151] K. McCloskey, B.T. Johnson, You are what you repeatedly do: links between personality and habit, Pers. Individ. Dif. 181 (2021), https://doi.org/10.1016/j.paid.2021.111000.

[152] W. Wood, Habit in personality and social psychology, Pers. Soc. Psychol. Rev. 21 (4) (2017) 389–403, https://doi.org/10.1177/1088868317720362.

[153] A. Bandura, A social cognitive theory of personality, in: L.A. Pervin, & O. John (Eds.), Handbook of Personality, 2nd ed., Guilford Publications, New York, 1999, pp. 154–196.

[154] Y. Amichai-Hamburger, E. Ben-Artzi, Loneliness and internet use, Comput. Hum. Behav. 19 (1) (2003) 71–80, https://doi.org/10.1016/S0747-5632(02)00014-6.

[155] J.R. Acopio, L. Bance, Personality traits as predictors of Facebook use, Int. J. Psychol. Counsel. 8 (2016) 45–52, https://doi.org/10.5897/IJPC2015.0311.

[156] D. Blackwell, C. Leaman, R. Tramposch, C. Osborne, M. Liss, Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction, Pers. Individ. Dif. 116 (2017) 69–72, https://doi.org/10.1016/j.paid.2017.04.039.

[157] E. Vlachopoulou, C. Boutsouki, Facebook usage among teenagers – the effect of personality and peer group pressure; an exploratory study in Greece, Int. J. Internet Market. Adv. 8 (4) (2014) 285–299, https://doi.org/10.1504/ijima.2014.067661.

[158] Sumner, C., Byers, A., & Shearing, M. (2011). *Determining personality traits & privacy concerns from Facebook activity*. Paper presented at the Black Hat Briefings, Abu Dhabi, UAE.

[159] Wehrli, S. (2008). Personality on social network sites: an application of the five factor model. *Eth Zurich Sociology Working Papers*, 0.37-33.54.

[160] T.R. Choi, Y. Sung, J.-A. Lee, S.M. Choi, Get behind my selfies: the big five traits and social networking behaviors through selfies, Pers. Individ. Dif. 109 (2017) 98–101, https://doi.org/10.1016/j.paid.2016.12.057.

[161] Gou, L., Zhou, M.X., & Yang, H. (2014). *KnowMe and ShareMe: understanding automatically discovered personality traits from social media and user sharing preferences*. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Toronto, Ontario, Canada.

[162] D. Modic, S.E. Lea, How neurotic are scam victims, really? The Big Five and internet scams, Law Human. eJ. (2012), https://doi.org/10.2139/ssrn.2448130.

[163] K. van der Schyff, S. Flowerday, H. Kruger, N. Patel, Intensity of Facebook use: a personality-based perspective on dependency formation, Behav. Inf. Technol. (2020) 1–17, https://doi.org/10.1080/0144929X.2020.1800095.

[164] Parrish Jr, J.L., Bailey, J.L., & Courtney, J.F. (2009). A personality based model for determining susceptibility to phishing attacks. *Decision Sciences Institute*, 285–296.

[165] Y. Hwang, D.J. Kim, Customer self-service systems: the effects of perceived Web quality with service contents on enjoyment, anxiety, and e-trust, Decis. Support Syst. 43 (3) (2007) 746–760, https://doi.org/10.1016/j.dss.2006.12.008.

[166] A.R. Korukonda, Differences that do matter: a dialectic analysis of individual characteristics and personality dimensions contributing to computer anxiety, Comput. Hum. Behav. 23 (4) (2007) 1921–1942, https://doi.org/10.1016/j.chb.2006.02.003.

[167] R. Joiner, M. Brosnan, J. Duffield, J. Gavin, P. Maras, The relationship between Internet identification, Internet anxiety and Internet use, Comput. Hum. Behav. 23 (3) (2007) 1408–1420, https://doi.org/10.1016/j.chb.2005.03.002.

[168] V. Özbek, Ü. Alnıaçık, F. Koc, M.E. Akkılıç, E. Kaş, The impact of personality on technology acceptance: a study on smart phone users, Procedia - Soc. Behav. Sci. 150 (2014) 541–551, https://doi.org/10.1016/j.sbspro.2014.09.073.

[169] R.J. Swickert, J.B. Hittner, J.L. Harris, J.A. Herring, Relationships among Internet use, personality, and social support, Comput. Hum. Behav. 18 (4) (2002) 437–451, https://doi.org/10.1016/S0747-5632(01)00054-1.

[170] J.-E. Lönnqvist, J.V.A. Itkonen, Homogeneity of personal values and personality traits in Facebook social networks, J. Res. Pers. 60 (2016) 24–35, https://doi.org/10.1016/j.jrp.2015.11.001.

[171] T.W. Robbins, R.M. Costa, Habits, Curr. Biol. 27 (22) (2017) R1200–R1206, https://doi.org/10.1016/j.cub.2017.09.060.

[172] S. Park, Effects of heuristic-systematic information processing about the flu and the flu vaccination, Soc. Sci. 7 (6) (2018) 260–267, https://doi.org/10.11648/j.ss.20180706.13.

[173] R.B. Cialdini, M.R. Trost, Social influence: social norms, conformity and compliance, in: The Handbook of Social Psychology, 4th ed., 1-2, McGraw-Hill, New York, NY, 1998, pp. 151–192. *Vols.*.

[174] Dincelli, E., & Goel, S. (2017). *Can privacy and security be friends? A cultural framework to differentiate security and privacy behaviors on online social networks,* Paper presented at the 50th Hawaii International Conference on System Sciences (HICSS), Waikoloa Village, Hawaii.

[175] N.S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N.A. Ghani, T. Herawan, Information security conscious care behaviour formation in organizations, Comput. Secur. 53 (2015) 65–78, https://doi.org/10.1016/j.cose.2015.05.012.

[176] M.Z. Yao, R.E. Rice, K. Wallis, Predicting user concerns about online privacy, J. Am. Soc. Infor. Sci. Technol. 58 (5) (2007) 710–722, https://doi.org/10.1002/asi.20530.

[177] N.A.G. Arachchilage, S. Love, Security awareness of computer users: a phishing threat avoidance perspective, Comput. Hum. Behav. 38 (2014) 304–312, https://doi.org/10.1016/j.chb.2014.05.046.

[178] J.C.-Y. Sun, S.-J. Yu, S.S.J. Lin, S.-S. Tseng, The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference, Comput. Hum. Behav. 59 (2016) 249–257, https://doi.org/10.1016/j.chb.2016.02.004.

[179] J.M. Davis, B.M. Tuttle, A heuristic–systematic model of end-user information processing when encountering IS exceptions, Infor. Manage. 50 (2) (2013) 125–133, https://doi.org/10.1016/j.im.2012.09.004.

[180] J. Wang, Y. Li, H.R. Rao, Coping responses in phishing detection: an investigation of antecedents and consequences, Inf. Syst. Res. 28 (2) (2017) 378–396, https://doi.org/10.1287/isre.2016.0680.

[181] J. Cox, Information systems user security: a structured model of the knowing–doing gap, Comput. Hum. Behav. 28 (5) (2012) 1849–1858, https://doi.org/10.1016/j.chb.2012.05.003.

[182] P.A. Pavlou, D. Gefen, Building effective online marketplaces with institution-based trust, Inf. Syst. Res. 15 (1) (2004) 37–59, https://doi.org/10.1287/isre.1040.0015.

[183] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, H.R. Rao, Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service, Infor. Syst. J. 24 (1) (2014) 61–84, https://doi.org/10.1111/j.1365-2575.2012.00420.x.

[184] Parsons, K., McCormac, A., & Butavicius, M.A. (2011). *Human factors and information security: individual, culture and security environment executive summary*. Command Control Communications and Intelligence Division (C3ID) Defence Science and Technology Organization (DSTO), Edinburgh, Australia.

[185] R.W. Rogers, A protection motivation theory of fear appeals and attitude change, J. Psychol. 91 (1) (1975) 93–114, https://doi.org/10.1080/00223980.1975.9915803.

[186] G.J.S. Wilde, Risk homeostasis theory: an overview, Inj. Prev. 4 (2) (1998) 89–91, https://doi.org/10.1136/ip.4.2.89.

[187] Pattinson, M., Anderson, G. (2005). Risk Communication, Risk Perception and Information Security. In: Dowland, P., Furnell, S., Thuraisingham, B., Wang, X.S.

(eds) Security Management, Integrity, and Internal Control in Information Systems. IICIS 2004. IFIP International Federation for Information Processing, vol 193. Springer, Boston, MA. https://doi,org/10.1007/0-387-31167-X_11.

[188] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., & Downs, J. (2010). *Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions*. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA.

[189] T. Sharot, The optimism bias, Curr. Biol. 21 (23) (2011) R941–R945, https://doi.org/10.1016/j.cub.2011.10.030.

[190] H. de Bruijn, M. Janssen, Building cybersecurity awareness: the need for evidence-based framing strategies, Gov. Inf. Q. 34 (1) (2017) 1–7, https://doi.org/10.1016/j.giq.2017.02.007.

[191] R. West, The psychology of security, Commun. ACM 51 (4) (2008) 34–40, https://doi.org/10.1145/1330311.1330320.

[192] Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2013). *Social engineering in social networking sites: affect-based model.* Paper presented at the 8th International Conference for Internet Technology and Secured Transactions (ICITST 2013). London, UK.

[193] R.B. Kline, Principles and Practice of Structural Equation Modeling, 4th ed., Guilford Press, New York, NY, 2016.

[194] R. Weston, P.A. Gore, A brief guide to structural equation modeling, Couns. Psychol. 34 (5) (2006) 719–751, https://doi.org/10.1177/0011000006286345.

[195] R.V. Dixit, G. Prakash, Intentions to use social networking sites (SNS) using technology acceptance model (TAM): an empirical study, Paradigm 22 (1) (2018) 65–79, https://doi.org/10.1177/0971890718758201.

[196] C.R. Kothari, Research Methodology Methods and Techniques, 2nd rev. ed., New Age International, New Delhi, 2008.

[197] M.J. Boudreaux, D.J. Ozer, Five factor model of personality, assessment of, in: J. D. Wright (Ed.), International Encyclopedia of the Social & Behavioral Sciences, 2nd ed., Elsevier, 2015, pp. 230–235.

[198] K. van der Schyff, S. Flowerday, P.B. Lowry, Information privacy behavior in the use of Facebook apps: a personality-based vulnerability assessment, Heliyon 6 (8) (2020) e04714, https://doi.org/10.1016/j.heliyon.2020.e04714.

[199] B. Verplanken, S. Orbell, Reflections on past behavior: a self-report index of habit strength, J. Appl. Soc. Psychol. 33 (6) (2003) 1313–1330, https://doi.org/10.1111/j.1559-1816.2003.tb01951.x.

[200] A. Soror, Z.R. Steelman, O. Turel, Exhaustion and dependency: a habituation–sensitization perspective on the duality of habit in social media use, Infor. Technolo. People 35 (1) (2022) 67–95, https://doi.org/10.1108/ITP-11-2019-0603.

[201] R.E. Petty, J.T. Cacioppo, The elaboration likelihood model of persuasion central and peripheral routes to attitude change. Communication and Persuasion, Springer Verlag, New York, 1986, pp. 1–24.

[202] F. Hassandoust, H. Singh, J. Williams, The role of contextualization in individuals' vulnerability to phishing attempts, Australasian J. Infor. Syst. 24 (0) (2020), https://doi.org/10.3127/ajis.v24i0.2693.

[203] R.J. Griffin, K. Neuwirth, J. Giese, S. Dunwoody, Linking the heuristic-systematic model and depth of processing, Communic. Res. 29 (6) (2002) 705–732, https://doi.org/10.1177/009365002237833.

[204] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88 (5) (2003) 879–903, https://doi.org/10.1037/0021-9010.88.5.879.

[205] D.R. Compeau, C.A. Higgins, Computer self-efficacy: development of a measure and initial test, MIS Q. 19 (2) (1995) 189–211, https://doi.org/10.2307/249688.

[206] K.P. Hocevar, A.J. Flanagin, M.J. Metzger, Social media self-efficacy and information evaluation online, Comput. Hum. Behav. 39 (C) (2014) 254–262, https://doi.org/10.1016/j.chb.2014.07.020.

[207] G. Marakas, R. Johnson, P. Clay, The evolving nature of the computer self-efficacy construct: an empirical investigation of measurement construction, validity, reliability and stability over time, J. Assoc. Infor. Sys. 8 (1) (2007) 16–46, https://doi.org/10.17705/1jais.00112.

[208] P. van Schaik, J. Jansen, J. Onibokun, J. Camp, P. Kusev, Security and privacy in online social networking: risk perceptions and precautionary behaviour, Comput. Hum. Behav. 78 (2018) 283–297, https://doi.org/10.1016/j.chb.2017.10.007.

[209] J. Nilsson, Segmenting socially responsible mutual fund investors: the influence of financial return and social responsibility, Int. J. Bank Market. 27 (2009) 5–31, https://doi.org/10.1108/02652320910928218.

[210] J.F. Hair Jr, G. Hult, C.M. Ringle, M Sarstedt, A Primer On Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd Ed., Sage Publications, Thousand Oaks, CA, 2017.

[211] R.P. Bagozzi, Y. Yi, On the evaluation of structural equation models, J. Acad. Market. Sci. 16 (1) (1988) 74–94, https://doi.org/10.1007/BF02723327.

[212] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Market. Res. 18 (1) (1981) 39–50, https://doi.org/10.2307/3151312.

[213] R.P. Bagozzi, Y. Yi, L.W. Phillips, Assessing construct validity in organizational research, Adm. Sci. Q. 36 (3) (1991) 421–458, https://doi.org/10.2307/2393203.

[214] P.A. Pavlou, H. Liang, Y. Xue, Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective, MIS Q. 31 (1) (2007) 105–136, https://doi.org/10.2307/25148783.

[215] P.B. Lowry, J. Gaskin, Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it, IEEE Trans. Prof. Commun. 57 (2) (2014) 123–146, https://doi.org/10.1109/TPC.2014.2312452.

[216] Zhu, W. (2016). $p < 0.05$, < 0.01, < 0.001, < 0.0001, < 0.00001, < 0.000001, or < 0.0000001 …. *J. Sport Health Sci.,* 5(1), 77–79. https://doi.org/10.1016/j.jshs.2016.01.019.

[217] N.D. Bowman, The importance of effect size reporting in communication research reports, Commun. Res. Rep. 34 (3) (2017) 187–190, https://doi.org/10.1080/08824096.2017.1353338.

[218] G.M. Sullivan, R. Feinn, Using effect size—Or why the p value is not enough, J. Grad. Med. Educ. 4 (3) (2012) 279–282, https://doi.org/10.4300/jgme-d-12-00156.1.

[219] J. Cohen, Statistical Power Analysis For the Behavioral Sciences, 2nd ed., Routledge, New York, NY, 1988.

[220] R.M. Baron, D.A. Kenny, The moderator–mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations, J. Pers. Soc. Psychol. 51 (6) (1986) 1173–1182, https://doi.org/10.1037/0022-3514.51.6.1173.

[221] P. Barrett, Structural equation modelling: adjudging model fit, Pers. Individ. Dif. 42 (5) (2007) 815–824, https://doi.org/10.1016/j.paid.2006.09.018.

[222] D. Hooper, J. Coughlan, M.R. Mullen, Structural equation modelling: guidelines for determining model fit, Electr. J. Bus. Res. Methods 6 (1) (2008) 53–60, https://doi.org/10.21427/D7CF7R.

[223] L. Hu, P.M. Bentler, Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives, Struct. Eq. Model.: A Multidiscipl. J. 6 (1) (1999) 1–55, https://doi.org/10.1080/10705519909540118.

[224] E. Katz, M. Gurevitch, H. Haas, On the use of the mass media for important things, Am. Sociol. Rev. 38 (2) (1973) 164–181, https://doi.org/10.2307/2094393.

[225] T. Rajesh, D.B. Rangaiah, Facebook addiction and personality, Heliyon 6 (1) (2020) e03184, https://doi.org/10.1016/j.heliyon.2020.e03184.

[226] J.P. Rolland, The cross-cultural generalizability of the five factor model of personality, in: R.R. McCrae, J. Allik (Eds.), The Five Factor Model of Personality Across Cultures, Kluwer Academic/Plenum Publishers, New York, NY, US, 2002, pp. 7–28.

[227] J.-H. Tang, M.-C. Chen, C.-Y. Yang, T.-Y. Chung, Y.-A. Lee, Personality traits, interpersonal relationships, online social support, and Facebook addiction, Telemat. Informat. 33 (1) (2016) 102–108, https://doi.org/10.1016/j.tele.2015.06.003.

[228] D.J. Hughes, M. Rowe, M. Batey, A. Lee, A tale of two sites: twitter vs. Facebook and the personality predictors of social media usage, Comput. Hum. Behav. 28 (2) (2012) 561–569, https://doi.org/10.1016/j.chb.2011.11.001.

[229] S. Butt, J.G. Phillips, Personality and self-reported mobile phone use, Comput. Hum. Behav. 24 (2) (2008) 346–360, https://doi.org/10.1016/j.chb.2007.01.019.

[230] D.J. Kuss, M.D. Griffiths, Online social networking and addiction: a review of the psychological literature, Int. J. Environ. Res. Public Health 8 (9) (2011) 3528–3552, https://doi.org/10.3390/ijerph8093528.

[231] C.S. Andreassen, M.D. Griffiths, S.R. Gjertsen, E. Krossbakken, S. Kvam, S. Pallesen, The relationships between behavioral addictions and the five-factor model of personality, J. Behav. Addict. 2 (2) (2013) 90–99, https://doi.org/10.1556/jba.2.2013.003.

[232] Z. Hussain, B. Simonovic, E.J.N. Stupple, M. Austin, Using eye tracking to explore Facebook use and associations with Facebook addiction, mental well-being, and personality, Behav. Sci. (Basel) 9 (2) (2019), https://doi.org/10.3390/bs9020019.

[233] Dhamija, R., Tygar, J.D., & Hearst, M. (2006). *Why phishing works*. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Montreal, Quebec, Canada.

[234] Algarni, A., Xu, Y., & Chan, T. (2015). *Susceptibility to social engineering in social networking sites: the case of Facebook*. Paper presented at the International Conference on Information Systems (ICIS 2015), Fort Worth, TX.

[235] P. Lawson, C.J. Pearson, A. Crowson, C.B. Mayhorn, Email phishing and signal detection: how persuasion principles and personality influence response patterns and accuracy, Appl. Ergon. 86 (2020), 103084, https://doi.org/10.1016/j.apergo.2020.103084.

[236] A.J. Burns, M.E. Johnson, D.D. Caputo, Spear phishing in a barrel: insights from a targeted phishing campaign, J. Organiz. Comput. Electr. Commerce 29 (1) (2019) 24–39, https://doi.org/10.1080/10919392.2019.1552745.

[237] K.D. Mitnick, W.L. Simon. *The art of deception: Controlling the human element of security*, John Wiley & Sons, 2003.

[238] M.L. Jensen, M. Dinger, R.T. Wright, J.B. Thatcher, Training to mitigate phishing attacks using mindfulness techniques, J. Manage. Infor. Syst. 34 (2) (2017) 597–626, https://doi.org/10.1080/07421222.2017.1334499.

[239] D. Sturman, C. Valenzuela, O. Plate, T. Tanvir, J.C. Auton, P. Bayl-Smith, M. W. Wiggins, The role of cue utilization in the detection of phishing emails, Appl. Ergon. 106 (2022), 103887, https://doi.org/10.1016/j.apergo.2022.103887.

[240] P.E. Johnson, S. Grazioli, K. Jamal, R.G. Berryman, Detecting deception: adversarial problem solving in a low base-rate world, Cogn. Sci. 25 (3) (2001) 355–392, https://doi.org/10.1207/s15516709cog2503_2.

[241] M. Silic, A. Back, The dark side of social networking sites: understanding phishing risks, Comput. Hum. Behav. 60 (2016) 35–43, https://doi.org/10.1016/j.chb.2016.02.050.

[242] S.L. Pfleeger, M.A. Sasse, A. Furnham, From weakest link to security hero: transforming staff security behavior, J. Homeland Secur. Emerg. Manage. 11 (4) (2014) 489–510, https://doi.org/10.1515/jhsem-2014-0035.

[243] D. Jampen, G. Gür, T. Sutter, B. Tellenbach, Don't click: towards an effective anti-phishing training. A comparative literature review, Hum.-centric Comput. Infor. Sci. 10 (1) (2020) 1–41, https://doi.org/10.1186/s13673-020-00237-7.

[244] B. Verplanken, W. Wood, Interventions to Break and Create Consumer Habits, Journal of Public Policy & Marketing 25 (1) (2006) 90–103. https://doi.org/10.1509/jppm.25.1.90.

[245] A.T. Church, Personality traits across cultures, Curr. Opin. Psychol. 8 (2016) 22–30, https://doi.org/10.1016/j.copsyc.2015.09.014.

[246] C. Guo, M. Warkentin, X. Luo, A. Gurung, J.P. Shim, An imposed etic approach with Schwartz polar dimensions to explore cross-cultural use of social network services, Infor. Manage. 57 (8) (2020), 103261, https://doi.org/10.1016/j.im.2019.103261.

[247] F.L. Greitzer, W. Li, K.B. Laskey, J. Lee, J. Purl, Experimental investigation of technical and human factors related to phishing susceptibility, ACM Trans. Soc. Comput. 4 (2) (2021), https://doi.org/10.1145/3461672.

[248] Mohebzada, J.G., Zarka, A.E., Bhojani, A.H., & Darwish, A. (2012). *Phishing in a university community: two large scale phishing experiments.* Paper presented at the 2012 International Conference on Innovations in Information Technology (IIT 2012), Abu Dhabi, UAE.

[249] J.H. Nord, A. Koohang, K. Floyd, J. Paliszkiewicz, Impact of habits on information security policy compliance, Issues Infor. Syst. 21 (3) (2020) 217–226.

[250] W.R. Flores, H. Holm, G. Svensson, G. Ericsson, Using phishing experiments and scenario-based surveys to understand security behaviours in practice, Infor. Manage. Comput. Secur. 22 (4) (2014) 393–406, https://doi.org/10.1108/IMCS-11-2013-0083.

[251] S.D. Gosling, P.J. Rentfrow, W.B. Swann, A very brief measure of the Big-Five personality domains, J. Res. Pers. 37 (2003) 504–528, https://doi.org/10.1016/S0092-6566(03)00046-1.

[252] E.L. Spottswood, J.T. Hancock, Should I share that? Prompting social norms that influence privacy behaviors on a social networking site, J. Comput.-Med. Commun. 22 (2) (2017) 55–70, https://doi.org/10.1111/jcc4.12182.

[253] H. Saleem, A. Beaudry, A.-M. Croteau, Antecedents of computer self-efficacy: a study of the role of personality traits and gender, Comput. Hum. Behav. 27 (5) (2011) 1922–1936, https://doi.org/10.1016/j.chb.2011.04.017.

[254] J. Shropshire, M. Warkentin, S. Sharma, Personality, attitudes, and intentions: predicting initial adoption of information security behavior, Comput. Secur. 49 (2015) 177–191, https://doi.org/10.1016/j.cose.2015.01.002.

[255] E.J. Williams, A. Beardmore, A.N. Joinson, Individual differences in susceptibility to online influence: a theoretical review, Comput. Hum. Behav. 72 (2017) 412–421, https://doi.org/10.1016/j.chb.2017.03.002.

Edwin Donald Frauenstein is a Senior lecturer in the Department of Information Technology at the Walter Sisulu University in East London, South Africa. He holds a PhD in Information Systems from the Rhodes University in Grahamstown, South Africa. His-research interests lie in the domain of human factors and behavioral aspects related to information security. Edwin has presented papers in the field of behavioral information security both locally and internationally. He also serves as a peer reviewer for various international journal outlets.

Stephen Flowerday is a Professor at the University of Tulsa in the School of Cyber Studies, Tulsa, Oklahoma, USA. His-research interests lie in the field of cybersecurity, behavioral cybersecurity, and information security management. Over the last seventeen years, he has authored and co-authored more than 130 refereed publications. Stephen has received funding for his work from IBM, THRIP, NRF, SASUF, Erasmus+, GMRDC, and others.

Syden Mishi is an Associate Professor of Economics at Nelson Mandela University, where he serves as Head of department and leads a Research group for Behavioral and Experimental Economics. His-research focuses on analysis of individuals' risk, social and time preferences and organisational behavior. He is author to more than 30 peer-reviewed journal articles and has contributed book chapters. He is Guest Editor for a special issue in Emerald Publishing's *African Journal of Economic and Management Studies*. Syden has received the 2022 South African National Research Foundation (NRF) Research Excellence Award in the category of Early Career Researchers and has received. Syden is a rated researcher in South Africa, having received a first time C rating. His-work has been funded, among others, by NRF, Eastern Cape Socio-Economic Consultative Council a regional government think-tank and business chamber. He is member of the Province of Eastern Cape Economic Commission.

Merrill Warkentin is a William L. Giles Distinguished Professor at Mississippi State University, where he serves as the James J. Rouse Endowed Professor of Information Systems in the College of Business. He has been named an ACM Distinguished Scientist. His-research, primarily on the impacts of organizational, situational, and dispositional influences on individual behaviors in the contexts of information security, privacy, social media, and eGovernment has appeared in *MIS Quarterly, Journal of MIS, Journal of the AIS, Eur. J. Infor. Sys., Information Systems Journal, Decision Sciences, Infor. Manage.*, MIT Sloan Management Review, and others. He is the author of over 110 peer-reviewed journal articles and the author or editor of seven books. Merrill has served in editorial roles for *MIS Quarterly, Information Systems Research, Journal of the AIS, Decision Sciences, Eur. J. Infor. Sys., Infor. Manage.*, and others, and is currently an Associate Editor at *Infor. Manage.* and the Editor-in-Chief of the *Journal of Intellectual Capital*. His-work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. He has chaired and presented keynote addresses at numerous international conferences and universities.