Contents lists available at ScienceDirect

Computers & Security

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

Susceptibility to phishing on social network sites: A personality information processing model

Edwin Donald Frauenstein*, Stephen Flowerday

Department of Information Systems, Rhodes University, South Africa

ARTICLE INFO

Article history:
Received 5 March 2019
Revised 26 April 2020
Accepted 28 April 2020
Available online 1 May 2020

Keywords:
Phishing
Big Five
Personality traits
Information processing
Heuristic processing
Systematic processing
Heuristic-systematic processing model
Structural equation modeling

ABSTRACT

Today, the traditional approach used to conduct phishing attacks through email and spoofed websites has evolved to include social network sites (SNSs). This is because phishers are able to use similar methods to entice social network users to click on malicious links masquerading as fake news, controversial videos and other opportunities thought to be attractive or beneficial to the victim. SNSs are a phisher's "market" as they offer phishers a wide range of targets and take advantage of opportunities that exploit the behavioural vulnerabilities of their users. As such, it is important to further investigate aspects affecting behaviour when users are presented with phishing. Based on the literature studied, this research presents a theoretical model to address phishing susceptibility on SNSs. Using data collected from 215 respondents, the study examined the mediating role that information processing plays with regard to user susceptibility to social network phishing based on their personality traits, thereby identifying user characteristics that may be more susceptible than others to phishing on SNSs. The results from the structural equation modeling (SEM) analysis revealed that conscientious users were found to have a negative influence on heuristic processing, and are thus less susceptible to phishing on SNSs. The study also confirmed that heuristic processing increases susceptibility to phishing, thus supporting prior studies in this area. This research contributes to the information security discipline as it is one of the first to examine the effect of the relationship between the Big Five personality model and the heuristic-systematic model of information processing.

1. Introduction

For several years, the Anti-Phishing Working Group (APWG) has defined phishing as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (APWG 2019). Lastdrager (2014) defines phishing as an "act of deception whereby impersonation is used to obtain information from a target". It is apparent that in the definitions, users are deceived in some way to give out information to the attacker. However, these definitions do not elaborate on the channel or environment in which phishing may be executed, or the attack vector, nor is any mention made of the use of persuasion to make phishing effective. Phishing is regarded as a type of Internet fraud typically carried out by sending victims an email ostensibly from a legitimate organisation or individual. Phishing emails often include hyperlinks that lead victims to spoofed websites; however, they can also include attachments, which users may unknowingly download and install spyware that data-mines the victim's computer for usernames, passwords and credit card information (Harrison et al., 2015).

The term "phishing" was coined as early as 1996 when attempts were made to steal passwords from the accounts of America Online (AOL) users (Ollmann, 2002). Several decades later, annual reports released by various information security organisations continue to emphasise the impact phishing has on numerous industries and their customers today (APWG, 2019). Almost daily, large successful organisations make headlines by falling victim to some form of phishing, resulting in substantial monetary losses. In November 2017, Facebook announced that of its 2.1 billion monthly active users, approximately 270 million user accounts could be duplicate or fraudulent (Titcomb, 2017). Earlier the same year, Facebook and Google were defrauded of more than $100 000 through a phishing scheme that impersonated a large Asian-based manufacturer (United States Department of Justice, 2017). Phishing is reported to be the fifth most common primary cause of security incidents, is ranked as the main cause of data breaches, and has the highest success rate of any threat vector (Verizon, 2019). In the third quarter of 2019, phishing attacks rose to heights not previ-

* Corresponding author.
E-mail addresses: edwin.frauenstein@gmail.coma (E.D. Frauenstein), s.flowerday@ru.ac.zab (S. Flowerday).

https://doi.org/10.1016/j.cose.2020.101862

ously seen since late 2016 (APWG, 2019). Sophisticated phishing attacks have continued to target mobile banking users and to deceive them into submitting bank-related information after having received a phishing email or a SMS containing a link on their mobile phones (Choudhary and Jain, 2018). This has allowed phishers to fraudulently perform a "SIM-swap", thereby giving them access to text messages directed to the victim's cell phone number (Samunderu, 2014). The phishers are then able to add beneficiaries to the victim's online Internet banking profile because the phisher will have access to confirm the two-factor authentication (2FA) code typically sent to the victim's mobile device. Furthermore, phishers are creating secure websites, thus foiling efforts to educate users into relying on HTTPS as a means of adjudicating whether a website is safe or not (APWG, 2019).

Phishers took advantage of the public's fear and uncertainty over the coronavirus (COVID-19) global pandemic. Since the start of January 2020, COVID-19 related email phishing attacks saw a steady increase followed by a sudden surge of 667% by the end of February, according to security firm Barracuda Networks (Muncaster, 2020). COVID-19-themed phishing attacks were in the form of scams (54%), brand impersonation (34%), blackmail (11%) and business email (1%). In April 2020, Google blocked more than 18 million COVID-19-related emails consisting of malware and phishing and 240 million COVID-related daily spam messages (Musil, 2020).

Approaches to mitigating phishing have focused mainly on two control measures: technological controls and user education. Mass phishing attacks have to a large extent gone the route of becoming spam, thus relying on the server-side filter technologies to prevent them from reaching users (Ollmann, 2002). However, for decades, the information security literature has emphasised that relying on technology alone is insufficient to counter phishing threats today, because such attacks focus to a large extent on exploiting human vulnerabilities rather than technical vulnerabilities. For this reason, many information security scholars mention the phrase "humans are the weakest link" (Yan et al., 2018). This has resulted in efforts to make users aware of phishing by improving security awareness, training and education programs (Volkamer et al., 2018). However, while it has been shown that security education training campaigns have indeed had an impact on user awareness of security threats, this has not produced the desired results as users who consider themselves to be aware of security threats have not demonstrated actual awareness (Caldwell, 2016). Furthermore, when faced with phishing, users may be preoccupied with other activities and thus not motivated to consider the security aspects associated with the threat (Moreno-Fernández et al., 2017). As such, to save time and effort, users may resort to various "cognitive shortcuts" when attempting to make decisions about the authenticity of a message (Vishwanath et al., 2011). This brings to the fore information processing as a variable which is considered in the current study.

Today, the range of communication technologies available has expanded, especially in the mobile device market, to include instant messenger (IM) and social applications. Phishing is versatile as it is not only carried out in emails and on fake websites, but also in other environments such as in text messages and on social networking sites (SNSs) (Aleroud and Zhou, 2017; Vishwanath, 2015a). While users appear to be aware of phishing emails impersonating financial institutions (Frauenstein, 2018), many may be unaware of modern social network threats and associated methods (Fire et al., 2014, Sophos, 2011). Krombholz et al. (2015) point out that users' awareness of SE on SNSs is still comparatively low compared to emails. There is currently no universally accepted term for phishing conducted on SNSs. As such, phishing on SNSs is sometimes referred to as social phishing (Jagatic et al., 2007), social media phishing (Vishwanath, 2015a) or social network phishing (Frauenstein and Flowerday, 2016). Phishing conducted on SNSs reaches a far wider audience than the traditional email phishing, consequently affecting both businesses and consumers (Wilcox and Bhattacharya, 2015). The core SE principles employed in traditional phishing emails have also expanded to social network environments (Frauenstein and Flowerday, 2016; Tsikerdekis and Zeadally, 2014). According to Vishwanath (2015a, 2015b), social network phishing attacks are multi-staged whereas email phishing is single-staged, although both share common techniques. Like phishing emails on SNSs phishers exploit the technical features offered, creating fake accounts and distributing malicious content (Fire et al., 2014). Phishers may take advantage of controversial or significant events that garner public interest or trigger emotions by creating clickbait posts on SNSs that "attract attention and encourage visitors to click on a link to a particular web page" (Chen et al., 2015). Attackers have been using SNSs to launch attacks on organisations by using various methods, including phishing, clickjacking, financial abuse, identity theft, impersonation, and physical crime. In addition to this, social network users are exposed to other risks such as cyberbullying, sexting, embarrassing photos, public sharing of locations, and the spread of dangerous pranks and games (Algarni et al., 2017; Branley and Covey, 2018; Reznik, 2013). Facebook users in particular are at more risk to focused attacks such as spear phishing and click jacking (Adewole et al., 2017; Algarni et al., 2017).

In South Africa, the rapidly growing Facebook group #ImStaying was established to create unity in a country that had experienced political and economic instability. Members post uplifting messages to inspire hope in others. However, anecdotal evidence suggests that groups such as these could be lucrative targets for cyber criminals who may conduct malicious SE attacks and steal personal or confidential information (McKane, 2019). This might be because social network users who join particular social network groups typically share common interests and exhibit similar behaviours. In the case of #ImStaying, as these members are generally like-minded and positively disposed, they may be open to giving out their personal information such as their mobile number on these groups to help others in need, which in turn can be used by social engineers to conduct further attacks. Millions of different email addresses can be collected by phishers simply by using the usernames of members of SNSs (Polakis et al., 2010).

Despite these risks, SNSs lack effective techniques for predicting, detecting or controlling SE attacks (Algarni et al., 2014). In addition, there generally appears to be inadequate or outdated laws to deal with the Internet identity theft and online impersonation prevalent on SNSs (Reznik, 2013). Social network users, on their part, exhibit unsafe behaviours that range from failing to implement privacy controls, clicking on links originating from seemingly trustworthy sources, and not giving enough attention or thought to the content of messages. Research has shown that the activities performed on SNSs reveal specific personality characteristics (Waheed et al., 2017) and in these contexts, attacks that exploit certain personality types in victims have been found to be successful (Parish et al., 2009). Specific types of users may be more vulnerable than others to particular forms of persuasion techniques employed by phishers (Lawson et al., 2018; Pattinson et al., 2011). On SNSs, user interaction with content is mainly click-based and information is presented spontaneously with little cognitive effort required on the part of the user. This adds another dimension to research in information security, as users may overlook suspicious messages by resorting to a heuristic approach instead of a systematic approach to processing information. This may be attributed to the design of the underlying software of the SNS itself, in that it relaxes users and thus could make them less aware of the potential risks of being deceived (Tsikerdekis and Zeadally, 2014).

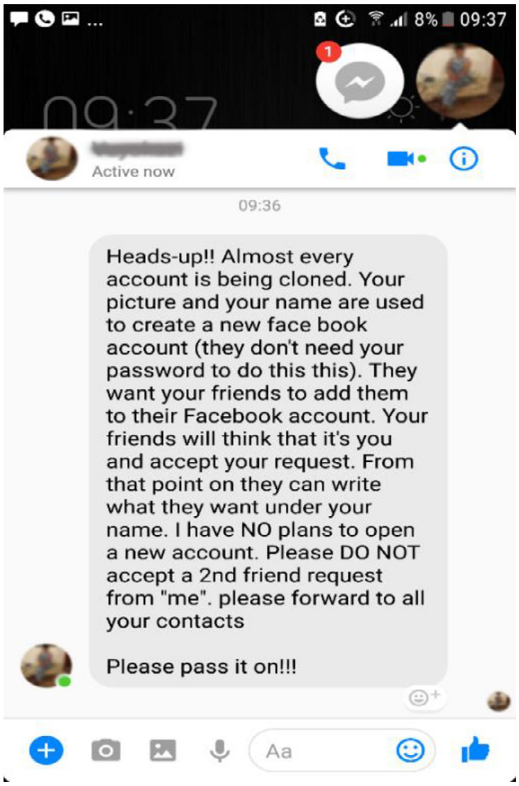
This section highlighted the inadequacy of current methods for addressing phishing, especially in the case of SNSs. Phishing programmes and the literature focus on training users to identify phishing emails and spoofed websites, but little attention has been given to social network phishing and other influential factors and their effects on user information processing (Vishwanath, 2015b). Furthermore, there is a lack of research on the individual differences that lead to susceptibility to online scams (Williams et al., 2017). This study shows that the techniques used in phishing emails can also be employed on SNSs, thus calling attention to the need for future phishing attack definitions and for taxonomies to be redefined. Importantly, this study proposes a theoretical model that can help identify the types of user who are more likely to be susceptible to phishing on SNSs and is an essential step towards improving online security.

2. Theoretical background

Phishing victimisation is a behavioural problem and, as such, researchers have focused mainly on understanding the factors that influence user behaviour (Wright and Marett, 2010). Various studies report that users' intentions to behave securely may differ from their actual security behaviour (Guo et al., 2011). Furthermore, it is difficult to predict user behaviour even when users have knowledge and awareness of security threats (Halevi et al., 2013), as some users willingly give up sensitive information despite their awareness of these threats (Workman, 2008a). Users who perceive themselves to be competent in using computers are just as likely to be phished as those who are not (Vishwanath et al., 2011). It has also been shown that users' attitudes to risk do not correlate with them being more or less vulnerable to phishing (Halevi et al., 2013). In this regard, Yan et al. (2018) maintain that identifying ordinary users as the weakest link is too general, and that specific users should be determined through quantitative assessment. Moreover, Williams et al. (2017) recommend that further research be conducted on the influential factors that affect user behaviour. As such, this study follows this recommendation by identifying particular users susceptible to social network phishing by their personality traits, as this is one of the factors that have recently been found to influence user behaviour (Shropshire et al., 2015). Moreover, based on personality traits, this identified the processing "mode" users would choose when confronted with phishing on SNSs.

2.1. Persuasion on social network sites

The strength of phishing lies in its use of SE techniques to manipulate the victim to carry out actions that are unsafe or to divulge confidential information (Mitnick and Simon, 2002). This can be effectively achieved by impersonating trustworthy or reputable sources such as a financial institution, government agency or the victim's own employer organisation. Phishers also make use of visual cues by replicating corporate logos and slogans of organisations to increase the users' trust in the message (Moreno-Fernández et al., 2017). The content and arguments in the body of the message can also effectively trigger human emotions (e.g. fear or excitement) and influence cognitive abilities, a ploy that is reinforced by the use of persuasion principles. Behavioural vulnerabilities can be exploited through persuasion such as gullibility and optimistic bias (Bullée et al., 2015). Phishers also take advantage of current and popular events, beliefs, prize offers, religion and politics to obtain a response from the victim. These techniques can influence information processing by the victim, who may not give sufficient attention to validating the authenticity of the message (Vishwanath et al., 2011).



Heads-up!! Almost every account is being cloned. Your picture and your name are used to create a new face book account (they don't need your password to do this this). They want your friends to add them to their Facebook account. Your friends will think that it's you and accept your request. From that point on they can write what they want under your name. I have NO plans to open a new account. Please DO NOT accept a 2nd friend request from "me". please forward to all your contacts

Please pass it on!!!

Fig. 1. Reciprocity principle applied in Facebook Messenger

Cialdini (2007) identified six key principles of persuasion, namely, reciprocity, commitment or consistency, social proof or conformity, authority, liking, and scarcity. While these techniques have been used in phishing emails, they can also be employed on SNSs (Algarni et al., 2014). This section demonstrates how effective these principles can be in persuading users to perform certain actions on SNSs. The images used in each of the persuasion principles are real-world cases personally obtained by the researcher.

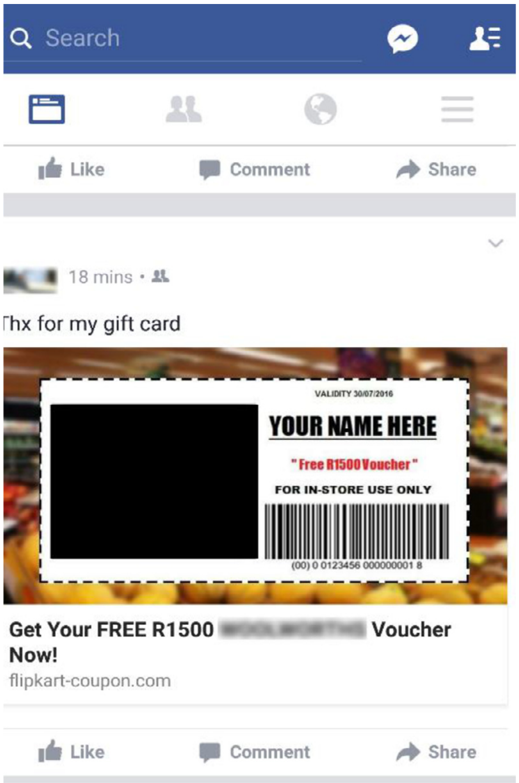
2.1.1. Reciprocity

A message is made to appear helpful and thus the user feels obligated to do something in return; for example to share a message warning others that there is a possibility that their Facebook account could be hacked. Fig. 1 gives an example of how this technique is used in Facebook messenger.

Fig. 1 is not considered an example of social network phishing but rather of the hoax messages found on Facebook. However, such hoax messages could effectively lead to phishing if the user is requested to click on a link with a message stating, "Click on the link to see if your profile has been hacked too". Users might comply with the instruction especially if the message originates from a trusted friend. Facebook responses such as complimenting, commenting on, or liking another user's posts can contribute towards developing a relationship between users, thus encouraging them to accept each other's requests (Algarni et al., 2014).

2.1.2. Commitment or consistency

The commitment principle refers to the likelihood of dedicating oneself to a cause or idea after having made a promise or agreement to do something (Cialdini, 2007). Typically, once people have made a choice to commit to something, they will encounter personal and interpersonal pressures to behave consistently with that commitment. According to Cialdini (2007), such pressures will cause people to respond in ways that justify their original decision to commit. Further, people will be more confident in their decision



Search

Like Comment Share

[redacted] 18 mins •

Thx for my gift card

VALIDITY 30/07/2016

[redacted]

YOUR NAME HERE

"Free R1500 Voucher"

FOR IN-STORE USE ONLY

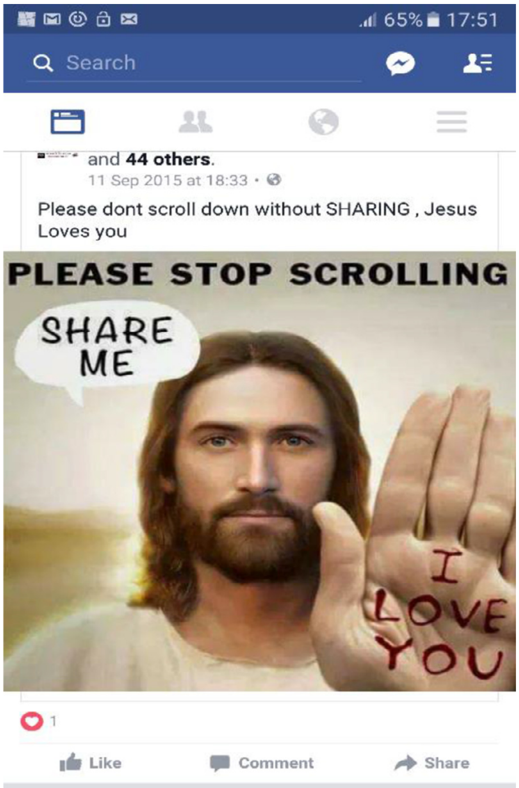
(00) 0 0123456 000000001 8

Get Your FREE R1500 [redacted] Voucher Now!

flipkart-coupon.com

Like Comment Share

Fig. 2. Authority principle applied in Facebook



65% 17:51

Search

[redacted] and **44 others**.

11 Sep 2015 at 18:33 ·

Please dont scroll down without SHARING , Jesus Loves you

PLEASE STOP SCROLLING

SHARE ME

I LOVE YOU

1

Like Comment Share

Fig. 3. Social proof principle applied in Facebook Messenger

to commit especially if they make it known publicly (Ferreira et al., 2015). In this regard, SNSs could be perceived by users as a suitable platform for making their commitment to something known.

2.1.3. Authority

The authority principle is the most used persuasion technique in phishing (Akbar, 2014). Messages designed to appear as if they originate from an authoritative or trustworthy entity (e.g. a bank, or from the recipient's employer or a friend) may persuade users to feel obligated to obey or respond to requests. This is because social learning encourages people not to question authority and therefore they are conditioned or may feel obligated to respond (Ferreira et al., 2015). On SNSs, this technique may be effective if the attacker has created an attractive profile or page with fabricated information intended to make it appear legitimate. The fake profile may also have many followers, mutual friends, recent updates and interesting photos, thus increasing the user's trust. Alternatively, the attacker could impersonate a public figure, clone a profile or pretend to be someone that the victim may trust (Stajano and Wilson, 2011). An earlier study by Jagatic et al. (2007) found that subjects were more likely to respond when the phishing email appeared to have been sent by a friend.

In Fig. 2, a well-recognised multinational retail company, is impersonated on Facebook with a claim to offer free shopping vouchers. Persuasion is further enhanced by creating urgency as the fake shopping voucher is only valid for a limited period.

2.1.4. Social proof or conformity

The tendency to imitate the behaviour of members of a group is known as social proof. People will comply with a request if they see others have also complied (Cialdini, 2007). For example, a message is shared on Facebook by the user's friends and the user in turn shares the post with others in his or her social network.

In Fig. 3, the message preys on users' Christian beliefs, as the message includes an image of Jesus and requests the user to "share me". In view of the sentiments expressed in the message, it may go against subjective norms if users choose to ignore such requests. The use of the *reciprocity* technique is also evident in this example.

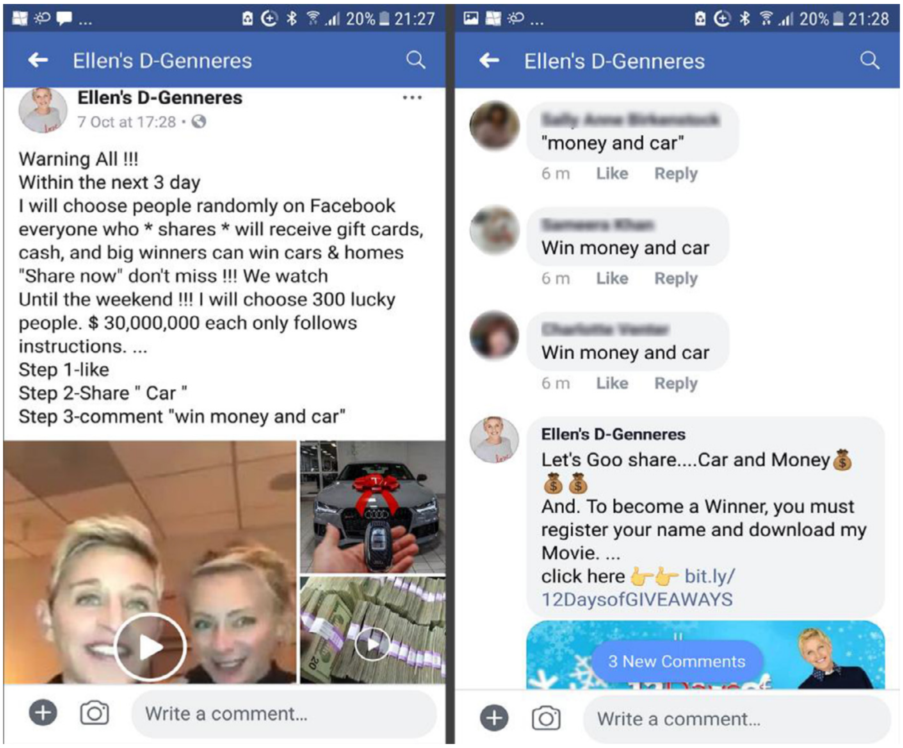
2.1.5. Scarcity

A message that incorporates "scarcity" may create a sense of urgency by putting the user under pressure to act. The user may respond in order to avoid missing out on an opportunity, a product, a service, or information, especially if it has limited availability (Bullée et al., 2015). Urgency can be enhanced by adding a consequence or a timeframe to the message (e.g. a special discount or a prize valid for a certain period), as seen in Fig. 2.

In Fig. 4, persuasion is further enhanced by impersonating the internationally known American comedian Ellen DeGeneres, thus taking advantage of the principle of *authority*. Evidently, users responded quickly to the request after which they received further instructions to register their name and to download a movie. In order to become a winner, users were required to click on the shortened URL link concealing the site that the user was directed to. It is apparent that the incorrect spelling of Ellen's name did not affect the trust of the respondents.

2.1.6. Liking

People may be persuaded to obey others if they display certain favourable or familiar characteristics (Ferreira et al., 2015). SNSs provide an environment that encourages "liking", as there are built-in features that allow the user to indicate their support for posts by means of a reaction such as "liking" or emotion indicators. People typically like or prefer to be associated with people who are similar to them in terms of personal interests, attitudes, beliefs, opinions, backgrounds, personality types and so on (Bullée et al., 2015). For example, a Facebook user may receive an invitation to accept a friend request but before accepting the request, he or she may seek information on the sender in relation to the number of


Ellen's D-Genneres

Ellen's D-Genneres
7 Oct at 17:28 ·

Warning All !!!
Within the next 3 day
I will choose people randomly on Facebook everyone who * shares * will receive gift cards, cash, and big winners can win cars & homes "Share now" don't miss !!! We watch
Until the weekend !!! I will choose 300 lucky people. $ 30,000,000 each only follows instructions. ...
Step 1-like
Step 2-Share " Car "
Step 3-comment "win money and car"

Write a comment...

Ellen's D-Genneres

[redacted]
"money and car"
6 m Like Reply

[redacted]
Win money and car
6 m Like Reply

[redacted]
Win money and car
6 m Like Reply

Ellen's D-Genneres
Let's Goo share....Car and Money💰💰💰
And. To become a Winner, you must register your name and download my Movie. ...
click here 👉👉 bit.ly/12DaysofGIVEAWAYS

3 New Comments

Write a comment...

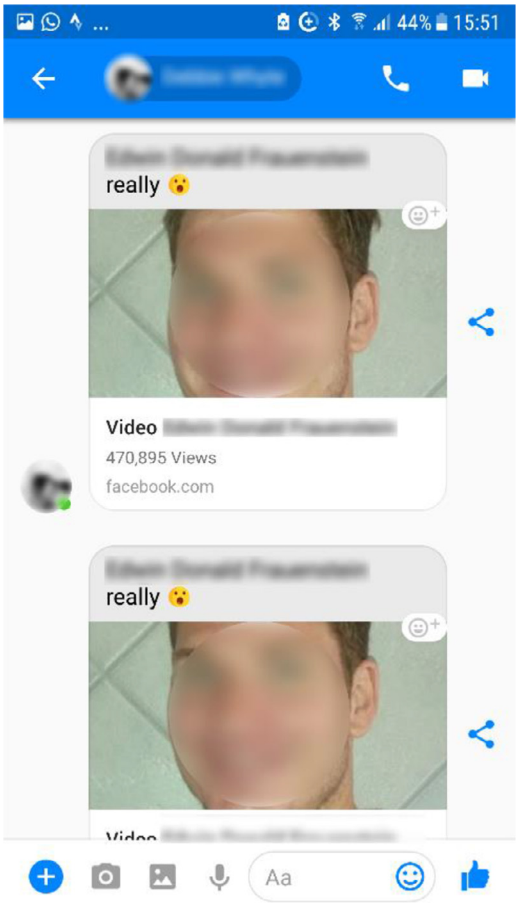
Fig. 4. Scarcity principle applied in Facebook Messenger.

friends they have in common, photo albums, occupation and where they live. If there are characteristics that the user likes, they may decide to accept the invitation or comply with a request. If the user agrees strongly with the sender on something important to them, the likelihood of responding increases.

Phishers take advantage of current affairs, controversial news and events reported in social media, thus preying on users' interests and *curiosity*. (Krombholz et al., 2015) note that "curiosity" is a technique overlooked by Cialdini (2007). However, curiosity has been equated with an openness to experience personality trait (McElroy et al., 2007). Fig. 5 shows how the curiosity technique can be employed on Facebook messenger.

Heartfield and Loukas (2015) classified this type of an attack as an instant message phishing. In Fig. 5, the effectiveness of this technique is enhanced by visual cues, as the message includes the statement "really" with a shocked emotion icon, as well as an exact image of the victim's profile picture. It also prompts the user's attention and creates urgency as it indicates that hundreds of thousands of users have already viewed the video. Although not considered to be part of Cialdini's persuasion taxonomy, this technique could use "fear" in order to create urgency (Workman, 2008b). Interestingly, user training interventions have made use of "fear appeals" as a means to counteract phishing attacks (Jansen and Van Schaik, 2018, Schuetz et al., 2016).

In these scenarios, if the persuasion principles are used in combination it may influence the way in which the user responds. For example, Lawson et al. (2017) found that a combination of authority and scarcity persuasion principles was most likely to arouse suspicion in relation to phishing emails. Furthermore, the context in which persuasive techniques are executed can also play a substantial role in the success of a SE attack (Bullée et al., 2015). As a result, identifying which persuasion techniques users in general are more likely to fall victim is difficult. Accordingly, as the phishing literature suggests, it is important to consider users' personality traits as another vulnerability factor (Parish et al., 2009).


[redacted]

[redacted]
really 😮

Video [redacted]
470,895 Views
facebook.com

[redacted]
really 😮

Video [redacted]

Aa

Fig. 5. Curiosity used to entice victims applied in Facebook Messenger

2.2. The Big Five personality traits

Personality traits describe individual differences in terms of characteristic thoughts, feelings and behaviours (Funder, 2001). Personalities are unique to each individual as they are predominantly determined by genetics, social and environmental influences, and experiences (McCrae and John, 1992). Personality characteristics are integral to the way humans think and behave, and therefore have an influence on whether or not an individual is likely, be it intentionally or unintentionally, to become involved in malicious activities or risky behaviour (Nurse et al., 2014). Personality is considered a leading factor in understanding why people behave as they do on the Internet (Amichai-Hamburger, 2002). Personality traits are also influenced by gender differences which subsequently affect Internet usage behaviour (Amichai-Hamburger and Ben-Artzi, 2000). Prior literature has also investigated personality traits and its influence on social network use (Amichai-Hamburger and Vinitzky, 2010, Correa et al., 2010, Moore and McElroy, 2012, Ryan and Xenos, 2011). Personality traits can also predict the security behaviour intentions of users towards protecting their computer devices (Gratian et al., 2018) and can also have a significant effect on perceived trust and risk, thus affecting decision making (Cho et al., 2016).

Research involving personality traits has been a topic of interest for a number of decades, with several rating instruments applied in many studies across various disciplines and contexts (Costa and McCrae, 1992; John and Srivastava, 1999). Scholars, particularly in the psychology domain, continue to explore a variety of focus areas within personality trait research. For example, anxiety and anger, which are among the neuroticism personality traits, are positively associated with risky driving behaviour (Yang et al., 2013). In the information security domain, studies that involve personality traits have gained the interest of scholars, as certain traits are considered important predictors of human behaviour (Albladi and Weir, 2017; Gratian et al., 2018). Of the many types of personality scales scholars can adopt, the Big Five has been noted as the most widely accepted as it shows consistency across time, culture and age groups and is considered more structured as the five traits do not overlap with each other (Erder and Pureur, 2016). The five-factor model (FFM), consisting of the "Big Five" personality traits, is the most widely used and extensively researched model of personality (John and Srivastava, 1999; McCrae and Costa Jr, 1999). It comprises the five empirically derived factors or dimensions of openness, conscientiousness, extraversion, agreeableness and neuroticism, which are usually represented by the acronym OCEAN or CANOE. Now known as the "Big Five", has resulted from numerous improvements, refinements and iterations which have led to a wide array of personality scales. On the other hand, prior literature has also examined the "Dark Triad" personality traits, consisting of psychopathy, machiavellianism and narcissism, and its influence on the behaviour of Facebook users (Lopes and Yu, 2017).

Combining the descriptions of the Big Five personality traits given by (Zhang, 2006; John and Srivastava, 1999; Rolland, 2002), each of the five personality traits are described as follows:

Openness to experience is the personality trait related to people who are open-minded and seek new experiences, have an active imagination, and focus on intellectual pursuits. They tend to be independent of judgement and have an appreciation for art, nature and different ideas and beliefs.

Conscientiousness refers to individuals who are honest, trustworthy, neat and hardworking. They have self-discipline, are goal-oriented, are prudent and tend to follow the rules, standards and procedures.

Extraversion is the personality trait attributed to individuals who tend to experience positive emotions such as excitement. They prefer to work with others and tend to be sociable, energetic, talkative, assertive, impulsive and dominant.

Agreeableness is attributed to individuals who are tolerant, compassionate, modest, polite, cooperative and trusting of others, as they believe that the people they interact with are generally well intentioned and honest. They also value and respect other people's beliefs and conventions.

Neuroticism is the opposite of emotional stability and is attributed to individuals who tend to experience negative emotions such as pessimism, embarrassment and guilt. Such people are generally sad or nervous, and sometimes hot-tempered, and tend to have low self-esteem.

Pertaining to Cialdini's principles of persuasion mentioned earlier, prior research investigated whether certain users, based on their personality type, may be more susceptible to specific persuasion techniques (Gkika et al., 2016). Others investigated personality traits and the influence persuasion strategies has on users detection of phishing emails (Butavicius et al., 2015; Lawson et al., 2018; Lawson et al., 2017; Oyibo et al., 2017; Uebelacker and Quiel, 2014). Researchers have also focused on exploring the influence of gender and personality traits on phishing susceptibility (Halevi et al., 2013; Mayhorn et al., 2015; Parish et al., 2009; Pattinson et al., 2011; Sumner et al., 2011). Halevi et al. (2013) examined the relationship between the Big Five personality traits and email phishing responses, as well as how these traits affect users' privacy behaviour on Facebook. Their study revealed that 17% of the respondents had been "phished" and found a correlation between gender and personality traits. For women, a very high correlation to neuroticism was found, while for men no correlation was found to any personality trait, although neuroticism and openness had an inverse correlation to extraversion. Halevi et al. (2013) found that the tendency to share information on Facebook correlated mainly with openness, while Halevi et al. (2015) found conscientiousness to be most at risk to spear phishing. Pattinson et al. (2011) investigated the behavioural responses of users when presented with phishing emails and found that those with the personality traits of extraversion and openness were better at detecting phishing emails. However, studies by Albladi and Weir (2017) and Lawson et al. (2017) presented opposing findings as they found that high extraversion increased susceptibility to phishing attacks. Furthermore, Alseadoon et al. (2015) found that openness, extraversion and agreeableness increase user tendency to comply with phishing email requests. These contradictions were noted by Albladi and Weir (2017), who found that conscientiousness, agreeableness and neuroticism significantly decrease the user's susceptibility to phishing on SNSs. They propose that other factors mediate the involvement of personality traits such as the individual's competence level, motivation to use the services of social networks, trust in social network members and providers, and users' experience of cybercrime (Albladi and Weir, 2017). Although "scepticism" is not regarded as a Big Five trait, in the cyberworld it would be preferable if users could adopt this trait, as a "trust no one" approach may encourage users to exercise more caution when receiving requests. In the current study, we explored whether information processing could be one of the mediating factors influenced by personality traits.

2.3. Information processing – heuristic vs systematic

As phishers constantly improve the authenticity of spoofed websites, the visual discrepancies between spoofed websites and their original counterparts are often difficult for users to detect. Prior studies have referred to existing theories and have designed models to understand the phenomenon of phishing (Algarni and Xu, 2013). Vishwanath et al. (2018) state that social-psychological research on phishing has identified a lack of cognitive processing as the main reason for individual victimisation. Persuasion is one of the key factors that influence information processing in online environments (Guadagno and Cialdini, 2005). The effectiveness of persuasive communication increases if the message is relevant to the target audience (Petty and Cacioppo, 1986). As this study also posits that social network users are vulnerable to phishing because they do not process persuasive messages with enough circumspection, theories and models related to information processing were considered. In this context, popular persuasion theories and models include the Elaboration Likelihood Model (ELM), the Heuristic-Systematic Model of information processing (HSM) and Social Judgement Theory (Cameron, 2009). Recently, the HSM has received favourable attention from information security researchers as a suitable theoretical framework for understanding victimisation by phishing (Harrison et al., 2016; Luo et al., 2013; Valecha et al., 2015; Vishwanath, 2015b; Vishwanath et al., 2018; Zhang et al., 2012).

An earlier study by Furnell (2007) presented participants with 20 messages and asked them to judge the authenticity of each message. Participants subsequently gave insights on the aspects that influenced their choices. According to Furnell (2007), most of the responses could be classified as follows: visual factors (i.e. logos, symbols such as copyright and trademarks, font styles), technical indications (i.e. URL in messages, using “https”), and language and content characteristics of the messages (language errors, presence/absence of recipient details, style of the message). Furnell (2007) notes that despite these useful insights, participants often arrived at “incorrect conclusions”. Although Furnell’s study did not investigate information processing, it highlights that in evaluating the message, users took a heuristic route, focusing more on visual characteristics than on the quality of the argument in the message. Ironically, phishers use visual characteristics to their advantage with the aim of enhancing users’ trust.

As pointed out earlier, persuasion is one of the means by which phishers successfully trick their victims. The HSM is a model that originated from persuasion research in social psychology (Eagly and Chaiken, 1993) and attempts to explain individual information processing and attitude formation in persuasive contexts. Dual-process models, such as the ELM and the HSM, are the most influential persuasion paradigms (Crano and Prislin, 2006). Both propose two significant approaches to persuasion: the central route (i.e. systematic) and the peripheral route (i.e. heuristic). Scholars have used the ELM, designed by Petty and Cacioppo (1986), to describe how cognitive processing influences deception (Vishwanath et al., 2011). The key difference between the two models is that the HSM recognises that the two distinct modes of thinking about information can cooccur, while the ELM suggests information processing occurs on a continuum.

According to Harris and Yates (2015), users evaluate phishing based on two main criteria: the *visual* quality of the message and the quality of the message *argument,* of which the latter requires more effort to make a decision. Visual quality is concerned with aspects related to source address, company logos, grammar, context and the instruction given in the message (Wang, Chen, & Rao, 2012). Compared to systematic processing, Eagly and Chaiken (1993) explain *heuristic processing* as “a limited mode of information processing that requires less cognitive effort and fewer cognitive resources” (p. 327). Heuristic processing is focused on simple decision prompts, often termed “rules of thumb”, and follows when people lack motivation or cognitive resources. This mode of processing occurs at a shallow or surface level, allowing the receiver to form judgements based on certain factors or indicators such as trustworthiness, appeal and the length of the message (Cameron, 2009) – all of which are vital SE techniques used by phishers. Luo et al. (2013) add that heuristic processing takes advantage of the factors mentioned above for the user to conduct a swift validity assessment.

In contrast, Luo et al. (2013) state that *systematic processing* takes place when users thoughtfully analyse the content of the message and perform further investigations to validate its authenticity. Workman (2008a) states that phishing messages are typically designed to decrease systematic processing. Ideally, systematic processing would be the preferred method when users are engaged on SNSs. However, this type of processing requires more effort, time and cognitive resources. Systematic processing not only depends on one’s capacity to think critically but also on other factors such as one’s existing knowledge, self-efficacy in obtaining relevant information and the perceived usefulness and credibility of available information (Griffin et al., 2002). Moreover, users may be involved with other information-seeking activities, using different software applications, which distracts them. In this regard, Ivaturi et al. (2014) suggest that users may not be in the correct frame of mind when presented with security attacks, thus leaving them vulnerable. Moreover, as SNSs include both asynchronous (i.e. personal messages sent within the SNS) and synchronous (i.e. embedded chat functions within the SNS) modes of communication (Kuss and Griffiths, 2011), this too can distract users.

Taking this into consideration, users may limit systematic processing unless they are motivated to do so (Chen et al., 1999). If users consider determining the validity of a phishing message on an SNS as being too time-consuming, difficult or unimportant, this may influence them to resort to heuristic processing. Human emotions may also interfere with the users’ judgement of message content (Workman, 2007). Moreover, personality traits can also influence these decisions. Cho et al. (2016) found that the personality traits of agreeableness and neuroticism can affect decision making, as these traits have a significant influence on whether these users perceive information as either trusted or distrusted. Ideally, if users were to systematically process the information they receive, checking it for validity and paying attention to visual cues, there would be fewer phishing victims.

2.4. Theoretical model and hypotheses

In the previous section, the literature discussed the relationships between personality traits and their effect on phishing susceptibility, and in doing so revealed contradictory findings. Moreover, a paucity of research was found that investigated the relationship between personality traits and information processing. Vishwanath (2015b) states that decades of empirical research have failed to show any relationships between the Big Five personality traits and information processing. However, prior research has not investigated these aspects in a social network and phishing context. As a result, the formulation of hypotheses for the present study was affected by the following limitations: 1) contradictory findings in the literature on the effects personality traits have on phishing susceptibility and 2) prior literature has examined personality traits and information processing separately from each other. It is the second of these limitations to which the present study makes a contribution. As a result, hypothesis formulation relied mainly on prior literature that described the characteristics of personality traits, and on literature, albeit contradictory, that examined their influence on users when presented with phishing (outlined in Section 2.2). Based on this explanation this study hypothesises the following:

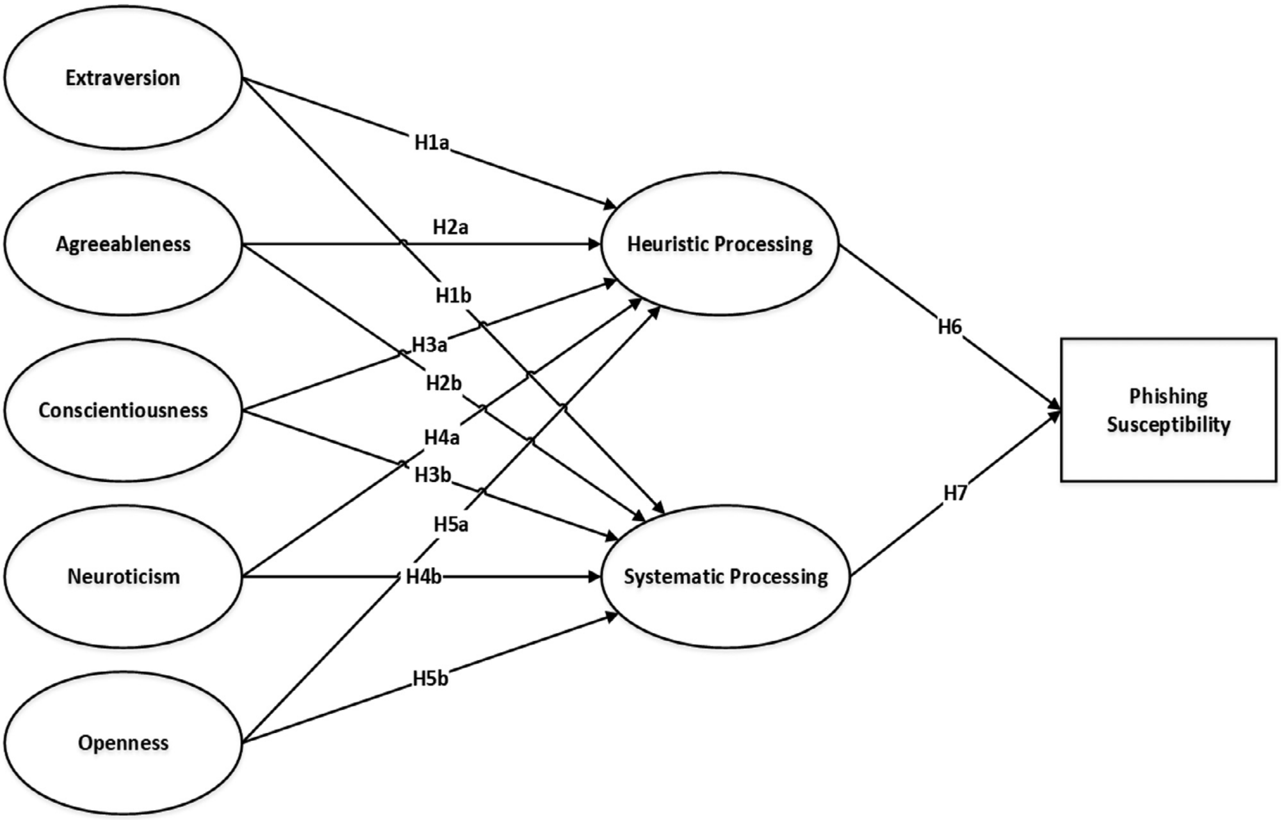


Fig. 6. The proposed model

- **H1a:** Extraversion has a positive influence on heuristic processing.
- **H1b:** Extraversion has a negative influence on systematic processing.
- **H2a:** Agreeableness has a positive influence on heuristic processing.
- **H2b:** Agreeableness has a positive influence on systematic processing.
- **H3a:** Conscientiousness has a negative influence on heuristic processing.
- **H3b:** Conscientiousness has a positive influence on systematic processing.
- **H4a:** Neuroticism has a negative influence on heuristic processing.
- **H4b:** Neuroticism has a positive influence on systematic processing.
- **H5a:** Openness has a positive influence on heuristic processing.
- **H5b:** Openness has a negative influence on systematic processing.
- **H6:** Heuristic processing will increase the likelihood of susceptibility to social network phishing.
- **H7:** Systematic processing will decrease the likelihood of susceptibility to social network phishing.

In summary, the proposed theoretical model in Fig. 6 consists of three major components, personality traits, information processing, and phishing susceptibility, with hypothesised associations. The personality traits comprise five latent variables (Big Five) proposed to each have an influence on information processing. Information processing is comprised of heuristic and systematic processing and proposed to have an effect on the likelihood of an individual falling victim to phishing on SNSs.

3. Methodology

3.1. Sample and data collection

Our sampling frame was a convenience sample drawn from final-year undergraduate students enrolled in various courses at a South African university located across three different sites in the Eastern Cape province. The total population consisted of 587 final year engineering students. As this study aimed to achieve a 95% confidence level, a minimum of 234 users were required (Kothari, 2004). The choice of students was based on the following reasons. Firstly, students are actively engaged on SNSs (Dixit and Prakash, 2018). Secondly, the choice of final year students, instead of any particular level of student, was based on the notion that they may bring security risks to the organisations that they anticipate working for in the following year. Finally, university students are more susceptible to email phishing attacks (Bailey et al., 2008).

SurveyMonkey®, an online survey tool, was used to collect primary data. Approval was granted by the university where the target sample was located. We managed to collect data from 285 respondents, of which seventy cases had incomplete responses and were removed from the analysis. 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). Sheng et al. (2010) found participants in this age group were more likely to fall victim to phishing than people of other ages.

3.2. Common method variance

As a self-reported questionnaire was the sole method used to collect data from the participants in a single-sitting, there is the prospect that the tested relationships among the constructs might be inaccurate caused by the effect of common method variance (CMV) (Podsakoff and Organ, 1986). CMV is “attributable to the measurement method rather than to the constructs the measures represent” (Podsakoff et al., 2003). As such, CMV can potentially lead to incorrect conclusions concerning the reliability and validity of the item scales measures. Two main approaches can help overcome CMV- procedural and statistical. The procedural or preventative approach (an ex-ante technique) is the most preferred and is applied early in the research design stage. The statistical approach (an ex-post technique) is conducted in the empirical stage to detect or possibly eliminate CMV (Chang et al., 2010, Podsakoff et al., 2003). Following the guidelines of Podsakoff et al. (2003), we employed the following *procedural* strategies in this study to minimise CMV. An initial version of the survey was pilot-tested to establish whether the research instrument could be considered reliable. Respondents were instructed to provide feedback relating to any misinterpretations about what the questions expected of them. To ensure that the survey was clear and unambiguous, we included synonyms in parenthesis where necessary, for some of the personality scale items. For example, “can be tense (i.e. nervous, anxious)”. To encourage honest responses, the respondents were informed of the purpose of the study, participation was voluntary, that there are no right or wrong answers, and that they could withdraw from the survey at any time. Data was collected anonymously and no identifiable personal information was requested from the respondents. For the *statistical* approach to detect if CMV exists, we performed two tests. First, we conducted the Harman’s single-factor test by including all the variables in a principal component factor analysis (Podsakoff et al., 2003). If the total variance for a single factor is less than 50%, it suggests CMV to be of no concern. Our results show that the largest variance explained by a single factor was 10.76% indicating that none of the emergent factors could explain the majority of the covariance. Second, Bagozzi et al. (1991) suggested that CMV can have an effect on the discriminant validity of the constructs. As such we examined the correlation matrix (in Table 2) to determine whether any of the correlations between any pair of constructs exceeded 0.9 – this procedure was also performed by Pavlou et al. (2007). As the correlations were below 0.9, this suggests that CMV is unlikely to be a significant issue (Bagozzi et al., 1991).

3.3. Variable descriptions and measures

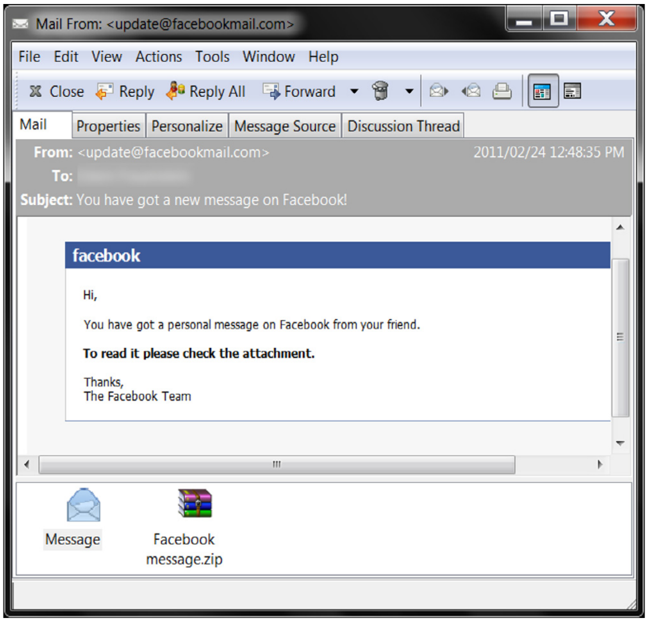
The measures and individual items for personality traits and information processing were adopted from prior studies as they had been proven to be statistically reliable. The variables are discussed in further detail.

3.3.1. Personality traits

The public domain instrument known as the Big Five Inventory (BFI) scale test by John and Srivastava (1999) was used to determine the personality traits. This instrument (see Appendix A) consists of 44 items scored on a five-point Likert scale (1 = Disagree strongly to 5 = Agree strongly). The test determines into which of the five personality traits a person’s personality predominantly fits. The personality test has been shown to have solid psychometric properties when compared to other even more comprehensive personality tests (John and Srivastava, 1999).

3.3.2. Information processing

In the survey instrument, this section consisted of six stimuli/images of a social network phishing-related message (i.e., persuasive message) found on Facebook and personally obtained by the researcher. As mentioned earlier, persuasion is increased if the message is relevant to the audience (Petty and Cacioppo, 1986). As the respondents were students and accustomed to engaging on SNSs using their mobile devices, the stimuli used were screenshots derived from the Facebook smartphone apps. None of the screenshots contained spelling errors which the literature recommends as one of the cues that may assist in identifying phishing. As the primary focus of the study was not to determine which persuasion principle is most effective, not all persuasion principles were tested. As reported in Table 1, the screenshots illustrated that a particular action was required from the user (e.g. to click on play). The purpose of including a variety of different phishing cases was to address the respondents’ potential bias as they might give more attention to some messages than others based on their interests or prior encounters. Heuristic processing was measured by adopting a four-item scale (see Appendix B) used in prior research (Griffin et al., 2002; Vishwanath, 2015b). Systematic processing was measured using a three-item scale (see Appendix B) adapted from prior research (Griffin et al., 2002; Vishwanath et al., 2011). Both the heuristic and systematic items were scored on a five-point Likert scale (1 = Disagree strongly to 5 = Agree strongly). The above-mentioned 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 behaviour.



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

Fig. 7. Phishing email purportedly originating from Facebook

3.3.3. Phishing susceptibility

Fig. 7 depicts a screenshot of a phishing email personally received by the researcher, which was subsequently used in the survey to test phishing susceptibility.

Evidently, the email depicted in Fig. 7 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. The purpose of this variable was to test susceptibility to phishing directly and for this purpose a multiple-choice item scale was used (see Appendix C). In the analysis, we employed Generalised Structural Equation Model (GSEM), taking into account the binary dependent variable which we created on testing phishing susceptibility (coded as 0 = Not susceptible; 1 = Susceptible). The items: "Reply to the email" and "check

Table 1
The constructs and their descriptive statistics.

Construct	Description of stimuli	Instruction to user	Persuasion Principle(s)	Items	Mean	S.D.	Factor Loading	CR
InfoP1	Opportunity to win a free store voucher worth R1500. The voucher contains an expiry date.	Click/Share	Authority and scarcity	1	3.26	1.40	.879	0.73
				2	3.87	1.26	.800	
				3	3	1.57	.626	
				4	2.75	1.50	.738	
				5	3.34	1.43	.591	
				6	3.29	1.60	.544	
				7	3.30	1.50	.649	
InfoP2	Owner is giving an opportunity for others to win a 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	1	3.16	1.52	.883	0.70
				2	3.78	1.37	.807	
				3	3.29	1.56	.519	
				4	2.60	1.51	.724	
				5	3.35	1.44	.446*	
				6	3.37	1.57	.349*	
				7	3.20	1.50	.518	
InfoP3	RIP: Breaking News of famous local athlete Caster Semenya died in a car accident. Video claiming to show footage of the accident.	Click link	Curiosity	1	3.18	1.48	.920	0.60
				2	3.68	1.37	.780	
				3	2.66	1.53	.680	
				4	2.52	1.43	.828	
				5	3.22	1.30	.523	
				6	3.14	1.54	.511	
				7	3.04	1.54	.643	
InfoP4	Opportunity to have financial freedom. Image shows a proof of payment received.	Comment with personal info (i.e. contact number)	Scarcity and social proof	1	3.30	1.61	.812	0.74
				2	3.36	1.56	.686	
				3	2.73	1.62	.412*	
				4	2.88	1.60	.616	
				5	3.13	1.59	.513	
				6	3.01	1.65	.366*	
				7	2.91	1.62	.500	
InfoP5	Video claiming a drunk woman appearing to be raped – 15 216 215 views	Click play	Curiosity	1	3.20	1.59	.838	0.70
				2	3.22	1.60	.675	
				3	2.24	1.48	.569	
				4	2.84	1.66	.835	
				5	3.04	1.58	.500	
				6	2.65	1.67	.345*	
				7	2.67	1.57	.510	
InfoP6	Shocking video of a 16-year-old girl allegedly being raped at Makeni.	Click play	Curiosity	1	3.24	1.59	.890	0.73
				2	3.27	1.57	.678	
				3	2.38	1.52	.538	
				4	2.67	1.56	.807	
				5	3.00	1.57	.424*	
				6	2.83	1.57	.391*	
				7	2.86	1.58	.408*	
Personality Trait	Extraversion			1	3.76	1.18	.522	0.70
				6	3.56	1.17	.828	
				11	4.15	0.94	.566	
				16	3.74	0.94	.751	
				21	2.66	1.39	.660	
				26	4.10	0.96	.716	
				31	2.43	1.31	.743	
				36	3.56	1.28	.681	
Personality Trait	Agreeableness			2	3.53	1.24	.882	0.57
				7	4.48	1.02	.793	
				12	4.31	0.91	.835	
				17	4.35	0.99	.697	
				22	3.84	1.11	.806	
				27	3.04	1.34	.796	
				32	4.39	0.89	.671	
				37	3.95	1.38	.749	
				42	4.25	0.91	.632	
Personality Trait	Conscientiousness			3	3.95	1.01	.727	0.70
				8	2.95	1.30	.659	
				13	4.31	0.91	.597	
				18	3.59	1.29	.562	
				23	3.33	1.39	.629	
				28	4.17	0.99	.754	
				33	4.15	0.79	.677	
				38	3.84	1.07	.740	
				43	2.83	1.43	.796	
Personality Trait	Neuroticism			4	2.02	1.20	.865	0.73
				9	2.04	1.15	.673	
				14	3.41	1.26	.656	
				19	3.44	1.43	.674	
				24	2.27	1.34	.674	

(continued on next page)

Table 1 (*continued*)

		29	2.82	1.47	.735	
		34	2.12	1.14	.707	
		39	3.08	1.46	.556	
Personality Trait	Openness	5	4.09	0.96	.599	0.72
		10	4.43	0.78	.749	
		15	3.79	0.99	.650	
		20	4.34	0.82	.619	
		25	3.51	1.02	.662	
		30	3.91	1.10	.739	
		35	2.04	1.08	.875	
		40	3.96	1.00	.479**	
		41	2.59	1.25	.779	
		44	3.38	1.35	.733	

* Items < 0.5 factor loading were dropped;
** item rounded off to 0.5.

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 considered to be a missing observation as it does not inform the exact position of the respondent's choice.

4. Data analysis

Structural Equation Modeling (SEM), also referred to as path analysis, is known for representing causal relations in multivariate data in the behavioural and social sciences disciplines (McDonald and Ho, 2002). SEM provides a way to test the relationships among observed and latent variables holistically and allows for theory testing even when experiments are not possible (Savalei and Bentler, 2006). The statistical software package, STATA® 14, was used in this study to conduct data analysis. Likert scales were predominantly used and are typically regarded as observed variables represented graphically by squares or rectangles (Schreiber et al., 2006), while unobserved variables are termed latent factors or constructs and are depicted graphically by circles or ovals (Schreiber et al., 2006).

SEM consists of two main parts, the *measurement* model and *structural* model (Civelek, 2018); Hair Jr, Hult, Ringle, & Sarstedt, 2017). McDonald and Ho (2002 state that the latter is a composite of the measurement and path models.

4.1. Measurement model assessment

The measurement model is a conventional confirmatory factor model that represents a set of observable variables as multiple indicators of a smaller set of latent variables (McDonald and Ho, 2002). In simpler terms, the measurement model pertains to how observed variables relate to unobserved variables. In SEM, the measurement model corresponds to confirmatory factor analysis (Civelek, 2018). Owing to the alpha limitations, it is technically more appropriate for researchers to apply composite reliability (CR) values because this takes into consideration the different outer loadings of the indicator variables (Jr et al., 2017)). Much like Cronbach's alpha, CR values exceeding 0.7 as shown in Table 1, are deemed acceptable for reliability (Chin, 1998). Convergent and discriminant validity are both considered subcategories of construct validity. Firstly, the convergent validity of the items was examined by the factor loadings and composite reliability (CR). Factor loading exceeding 0.5 demonstrated acceptable convergent validity (Civelek, 2018). Items loading less than 0.5 were dropped from the model. Secondly, for discriminant validity we used the Fornell-Larcker criterion by examining the square roots of the average variance extracted (AVE) against the correlation coefficients of the latent variables (Fornell and Larcker, 1981). For adequate discriminant validity, the norm is that the square root of each construct's AVE should be greater than its highest correlation with any other construct (Jr et al., 2017)). Table 2 shows the correlation matrices and their discriminant validities.

4.2. Structural model assessment

As noted earlier, the structural model is based on the measurement model (Civelek, 2018). The goal of path analysis, and more generally of SEM, is to determine how well the proposed model, which is a set of specified causal and non-causal relationships among variables, accounts for the observed relationships among these variables. To evaluate the proposed model constructs, the structural model incorporated path analysis, which not only indicated the magnitude of the relationships between the constructs but also whether these relationships are statistically significant. Chin et al. (2003) state that researchers should not only indicate whether the relationship between variables is significant or not, but also report the effect size between these variables. This view is shared by Bowman (2017), who adds that all data analyses should report relevant effect size statistics because although *p*-values may explain statistical significance from the null, they are unable to offer insight into the magnitude of the actual size of an effect. The effect size (f^2) informs whether constructs have a substantive impact on one another. In simple terms, effect size assesses the strength of the relationship between the latent variables and therefore helps researchers to assess the overall contribution of a research study (Sullivan and Feinn, 2012). The guidelines for assessing 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 (Sullivan and Feinn, 2012). Effect size values of less than 0.02 indicate that there is no effect. Table 3 reports on the path estimates, *t*-statistics, effect sizes and overall statistical significance.

The path diagram illustrated in Fig. 8 shows the hypothesised associations and the corresponding beta (ß) values and *p*-values. Model fit determines the extent to which the proposed model fits the sample data (Schermelleh-Engel et al., 2003). Barrett (Barrett, 2007) controversially advocates for an outright ban on approximate fit indexes and posits that the chi-square (χ^2) exact fit test is the only applicable test of model fit for SEM. The χ^2 test statistic is the only goodness-of-fit measure that has an associated significance test, while all other measures are descriptive (Schermelleh-Engel et al., 2003). A non-significant χ^2 result at >.05 threshold is desired to achieve a good fit between the variance and covariance matrix (Barrett, 2007). The χ^2 test achieved an acceptable fit: χ^2= 24.39, df = 16 and p = 0.08. In addition to the χ^2 test, (Kline, 2016) recommends reporting the following approximate fit indices: the Root Mean Square Error of Ap-

Table 2
Discriminant validity of constructs.

Constructs	1	2	3	4	5	6	7	8
1. Extraversion	**0.526**							
2. Agreeableness	0.177	**0.437**						
3. Conscientiousness	0.120	0.050	**0.536**					
4. Neuroticism	0.006	0.016	0.043	**0.479***				
5. Openness	0.218	0.130	0.165	0.027	**0.534**			
6. Heuristic Processing	0.010	0.038	0.009	0.057	0.027	**0.652**		
7. Systematic Processing	0.035	0.071	0.021	0.028	0.080	0.191	**0.708**	
8. Phishing Susceptibility	0.000	0.013	0.001	0.002	0.001	0.081	0.015	**1.0**

Note: the square root of the AVEs are represented in bold, as appearing down the diagonal
* Indicates item rounded off to 0.5

Table 3
Path estimates and hypothesis outcomes.

Tested	Path	ß	SE	*t*-Value	*p*-Value	Effect Size (f^2)	Outcome (based on *p*-Value)	Outcome (based on f^2)
H1a	Extraversion→Heuristic	0.013	0.079	0.160	0.873	0.000	Not supported	No effect
H1b	Extraversion→Systematic	0.003	0.078	0.040	0.968	0.000	Not supported	No effect
H2a	Agreeableness→Heuristic	0.152**	0.074	2.057	0.041	0.020	Supported	Small effect
H2b	Agreeableness→Systematic	0.173**	0.073	2.360	0.019	0.027	Supported	Small effect
H3a	Conscientiousness→Heuristic	-0.155**	0.077	-2.022	0.044	0.020	Supported	Small effect
H3b	Conscientiousness→Systematic	0.063	0.076	0.824	0.411	0.003	Not supported	No effect
H4a	Neuroticism→Heuristic	0.163**	0.070	2.330	0.021	0.026	Supported	Small effect
H4b	Neuroticism→Systematic	0.131*	0.069	1.893	0.060	0.017	Supported	No effect
H5a	Openness→Heuristic	0.140*	0.081	1.740	0.083	0.014	Supported	No effect
H5b	Openness→Systematic	0.172**	0.080	2.158	0.032	0.022	Supported	Small effect
H6	Heuristic→Phishing Susceptibility	0.287***	0.073	3.914	0.000	0.072	Supported	Small effect
H7	Systematic→Phishing Susceptibility	-0.005	0.073	-0.063	0.949	0.000	Not supported	No effect

Note:
* $p < 0.1$;
** $p < .05$
*** ; $p < 0.001$.

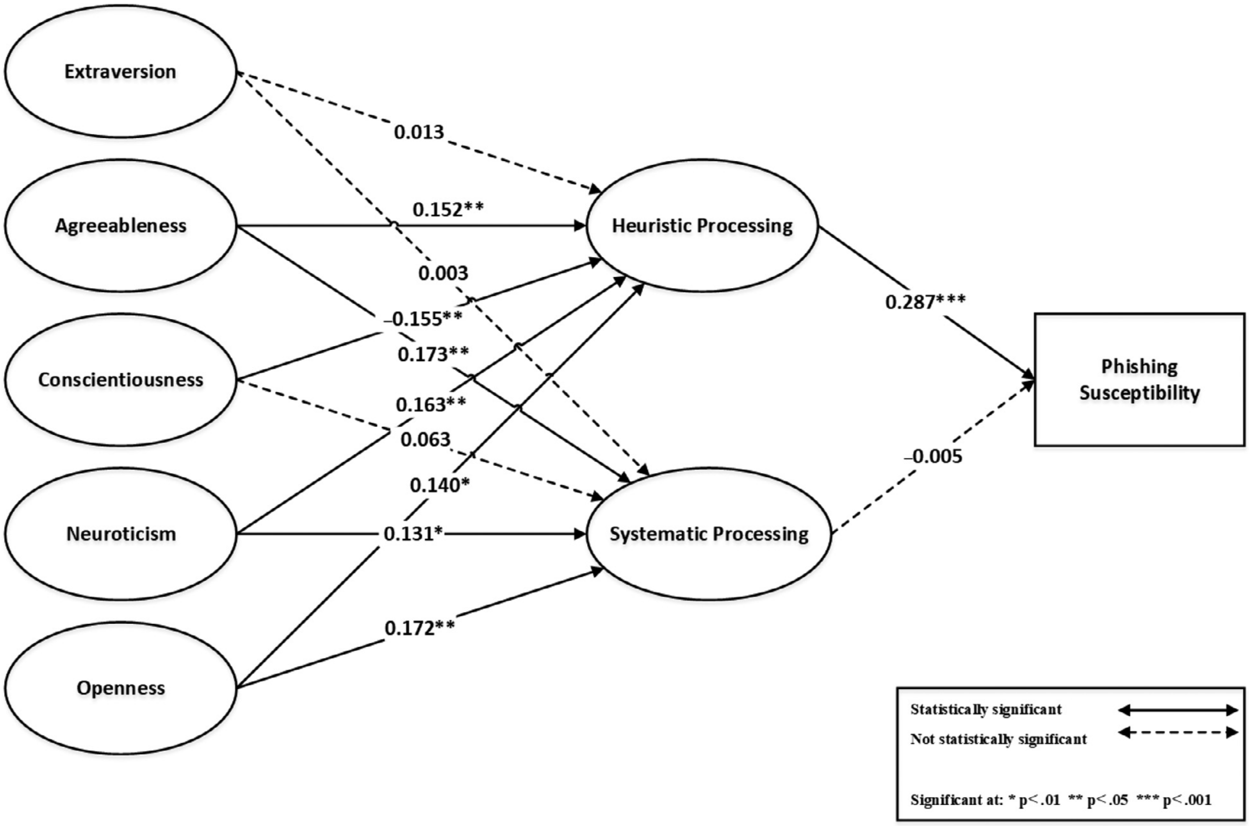


Fig. 8. The structural model

Table 4
Goodness of Fit indices.

Fit Indices	Model Value	Acceptable standard
CFI	0.911	≥ 0.9
SRMR	0.052	< 0.08
RMSEA	0.049	≤ 0.08

proximation (RMSEA), the Standardized Root Mean Square Residual (SRMR) and the Comparative Fit Index (CFI). For each of the aforementioned approximate fit indicators, Hu and Bentler (1999), Schermelleh-Engel et al. (2003) and Hooper et al. (2008) provided a set of acceptable "rules of thumb" thresholds. These thresholds were considered in interpreting the various fit indices for the model.

The RMSEA determines to what extent the model, with unknown but optimally chosen parameter estimates, would fit the populations' covariance matrix (Hooper et al., 2008). A RMSEA value of zero indicates the best result (Kline, 2016). However, a cut-off value close to .06 or a strict upper limit of .07 appears to be the acceptable norm (Hooper et al., 2008). The SRMR is an absolute fit index and is computed as the square-root of the difference between the residuals of the sample covariance matrix and the hypothesized model. Similar to the RMSEA, an SRMR value of zero indicates perfect fit (Hooper et al., 2008) and a value as high as .08 are deemed acceptable fit (Hu and Bentler, 1999). The CFI, an incremental fit index, assumes that all latent variables are independent of the model and compares the sample covariance matrix with the null model (Hooper et al., 2008). A CFI value exceeding 0.9 is required in order to ensure that "misspecified" models are not accepted (Hu and Bentler, 1999). Table 4 presents a summary of the approximate fit indexes with its associated threshold values.

5. Results

This section presents the results of the various statistical tests that were discussed in the previous section. Most results in Table 1 show an acceptable level of composite reliability as all the constructs exceeded 0.7, except for the constructs InfoP3 and agreeableness.

In Table 2, we examined the correlations between all the pairs of constructs in order to establish the discriminant validity of the constructs. The correlations between all of these pairs were below the recommended threshold value of 0.9 (Safa et al., 2016) suggesting that all constructs are distinct from each other.

Table 3 presents the results of the hypothesis tests and associated relationships between the five personality traits, heuristic and systematic processing and phishing susceptibility. Each path is a hypothesised correlation between variables representing the causal and consequent constructs of a theoretical proposition (Lowry and Gaskin, 2014).

The results of the hypothesis tests presented in Table 3 show that some of the personality traits have significant relationships in regard to heuristic and systematic information processing. Following the hypothesis tests and outcomes presented in Table 3, the structural model was created. Fig. 8, depicted as a path diagram, presents the theoretical model demonstrating the predictors of phishing susceptibility on SNSs in terms of personality traits and information processing. The model shows the correlation coefficients and significance of the relationships between the variables.

For further insights, direct phishing susceptibility was examined by excluding the influences of personality traits and information processing in the analysis. The data revealed that respondents would fall victim to a phishing email originating from Facebook, as 40.09% of the respondents chose the option "check the attachment because I am interested to know what my friend has to say" while 9.68% would delete the email. Only 20.78% did not trust the phishing email.

The values of the approximate fit indices demonstrated in Table 4 support the conclusion that the estimated model provides an acceptable fit with the data. Implying inferences can be made from the study findings which is discussed next.

6. Discussion

The present study revealed that apart from extraversion and conscientiousness (partly), personality traits do indeed have significant relationships with both heuristic and systematic processing, which may lead to phishing susceptibility on SNSs.

It was unexpected that extraversion would be the sole construct to have no statistically significant influence on both heuristic (ß = 0.013, p = 0.873) and systematic processing (ß = 0.003, p = 0.968). As such, our results did not support hypotheses 1a and 1b. Owing to the characteristics that describe the extraversion trait, it was anticipated that respondents who possess this trait would be excited and would act impulsively towards the stimuli, thereby resorting to heuristic processing. This is confirmed by Lawson et al. (2017), who found extraversion to be highly predictive of susceptibility to phishing emails. Moreover, it was anticipated that these users would be less likely to apply the cognitive resources aligned with systematic processing. Our results could be because the extraversion trait is found to be sensitive to the cultural background of individuals (Rolland, 2002).

As expected, agreeableness was found to be statistically significant and having a positive influence for both heuristic (ß = 0.152, p = 0.041, small effect) and systematic processing (ß = 0.173, p = 0.019, small effect), thereby supporting H2a and H2b. As the agreeableness trait describes individuals as tolerant, cooperative, tending to experience emotional concern for others' well-being and trusting of others, it was predicted that users might process the stimuli in either mode. While this may be deemed contradictory, it does support the large base of literature that shares these contradictory findings. For example, the study by Enos et al. (2006) revealed that people with high agreeableness were better at detecting deception, while conversely Modic and Lea (2012)found that highly agreeable people are more susceptible to phishing because they are more likely to trust in uncertain situations. Alkiş and Taşkaya Temizel (2015) found that agreeableness is the most susceptible personality trait to persuasion strategies and Cusack and Adedokun (2018) concluded that users high in agreeableness are likely to be more susceptible to SE attacks than others. Alseadoon et al. (2015) found agreeableness increased user tendency to comply with phishing email requests while Albladi and Weir (2017) found that agreeableness significantly decreased susceptibility to phishing.

Ryan and Xenos (2011) found that Facebook users are less conscientious than nonusers of the platform. In our study conscientiousness was found to be statistically significant for heuristic processing and had a negative influence (ß = -0.155, p = 0.044, small effect), thus supporting hypothesis 3a. As expected, this indicates that an individual with the conscientiousness trait would not process heuristically and thus be less likely to fall victim to social network phishing. This finding supports Albladi and Weir (2017) and Parish et al. (2009) findings. A study by Moutafi, Furnham, and Paltiel (Moutafi et al., 2004) found consistent evidence that intelligence is strongly negatively correlated with conscientiousness. Moutafi et al. (2004) argued that this is caused by fluid intelligence, which is the capacity to think logically and solve problems in novel situations independently of acquired knowledge. This explanation by Moutafi et al. (2004) may also explain why users would resort to heuristic processing. By contrast, conscientiousness was not found to be statistically significant for systematic processing (ß = 0.063, p = 0.411), although it had a positive influence. As such, hypothesis 3b is rejected.

Neuroticism was found to be statistically significant for both heuristic and systematic processing. However, it was predicted that neuroticism would be negatively correlated with heuristic processing (ß = 0.163, p = 0.021, small effect), although this was not the case in our findings. Thus hypothesis 4a was rejected. As mentioned by Parish et al. (2009), neuroticism has been associated with computer anxiety and as such this may indirectly help protect individuals with the personality trait of neuroticism against cybercrime. Our findings revealed that neuroticism is significantly positively related to systematic processing (ß = 0.131, p = 0.060, no effect), thus supporting hypothesis 4b. This finding supports the studies by Sumner et al. (2011) and Li et al. (2019), who found that users high in neuroticism were more concerned for their privacy. It also supports Albladi and Weir (2017) finding that neuroticism significantly decreased susceptibility to phishing.

Openness was found to be statistically significant for both heuristic and systematic processing. Individuals with the personality trait of openness are intellectually curious and as such it was anticipated that, given the nature of the images depicted in the stimuli, it would have promoted them to process the stimuli heuristically. As expected, openness has a positive relationship with heuristic processing (ß = 0.140, p = 0.083, no effect) thus supporting hypothesis 5a. This supports studies by Halevi et al. (2013) and Alseadoon et al. (2015), who found that openness is closely related to high phishing susceptibility. Hypothesis 5b is thus rejected, as the relationship to systematic processing was expected to be negative (ß = 0.172, p = 0.032, small effect). This might substantiate the findings by Pattinson et al. (2011), who found individuals with the trait of openness were better at detecting phishing emails. In addition, the study by Kreitz et al. (2015) showed that in comparison to the other Big Five traits, individuals with the openness trait are more perceptive as they were able to detect unexpected stimuli in their environment.

As expected, heuristic processing had a significant positive effect on increasing susceptibility to phishing (ß = 0.287, p = 0.000, small effect), therefore supporting hypothesis 6 and the results by Vishwanath (2015b). However, the relationship of systematic processing to phishing susceptibility was found not to be statistically significant (ß = -0.005, p = 0.949, no effect) and as such hypothesis 7 was rejected. Although not statistically significant, the data revealed that systematic processing was negatively related to phishing susceptibility, thus decreasing the risk posed by phishing.

The overall findings revealed that there are indeed significant relationships between several personality traits and information processing and also that the mode of processing influences the outcome of susceptibility to phishing on SNSs. However, following the results of the hypothesis tests, the current study has revealed that predicting the mode of information processing a user would take, based on personality traits, had some unforeseen expectations. The results showed certain traits, such as agreeableness, neuroticism and openness, processed information in both modes thus supporting the dual nature of the HSM – both modes can occur simultaneously. Ironically, this aspect could explain the contradictory findings found in phishing literature related to the Big Five personality traits. Furthermore, our findings suggests that apart from personality traits, information processing could also be influenced by the context or persuasion technique (Vishwanath et al., 2011). This is further explained by McAndrew (2018), who states that behaviours associated with a particular personality trait can be influenced by specific situations and environments. This is also highlighted by Johnson (1997), who points out that personality traits do not mean that someone's reactions are absolutely consistent; people may react consistently to similar situations but they may also respond differently in the same situations. Similarly, Cusack and Adedokun (2018) are of the view that traits are also influenced by moderating variables such as emotional state, the environment and motivations. As mentioned earlier the Big Five personality scale, classified by five distinct classes, has been shown to be reliable and consistent across many studies. In contrast, Cusack and Adedokun (2018) state that the Big Five taxonomy defines personalities along a continuum rather than in categories or types, thus allowing for different types of behaviour under different circumstances. As such, the current study showed a "snapshot" view of the students' perceptions and behaviour at that particular time. Thus, if this survey were to be conducted again in a different environment, it is possible that the results could be slightly different. As a result, this promotes opportunities for other researchers to conduct similar studies or to improve on this study by considering different variables and environments.

7. Limitations and future research

While our study offers some insights for behavioural researchers, there were several limitations that open possibilities for future research. The convenience sampling method used and the small sample size minimises the generalisability of the findings as the sample, consisting solely of students, was not representative of the general public. Furthermore, the stimuli used in the instrument to test information processing originated on the researcher's Facebook profile. This creates bias as the stimuli originated from acquaintances connected to the researcher and not to the respondents. To make the experiment more accurate to reflect its intended environment, researchers could create a Facebook profile (i.e. a dummy account), and survey participants could add this profile by responding to a friend request. Respondents could then comment on how they would respond to stimuli appearing on their timeline which originates from the researcher's dummy profile. However, this would have to be carefully designed in adherence to ethical guidelines and practices.

The study assumed that respondents would address the section on information processing in the survey using the same amount of time and attention to detail as they would in an online social network environment. As the instrument was a survey, the measures used were indirect and consequently could not measure response time, which could be particularly important with regard to information processing. Although the survey instrument consisted of several persuasive stimuli, respondents only had to deal with one post at a time. In the SNS environment, users would be exposed to a larger set of posts at one time appearing on their timeline. Furthermore, the instrument has an option "I ignored the message content", however this did not take into account users "cognitively" ignoring stimuli. As a result, it is possible that users could dismiss posts, thus making no decision, without applying any mode of processing that may pass through their timeline.

This study did not aim to identify which specific persuasion strategy is more susceptible to phishing, as has been done previously in other studies. As a result, the current instrument design did not test responses for each of the six persuasion principles. However, as noted by Lawson et al. (2017), phishers tend to use a combination of persuasion types and thus, in such cases, the instrument in its current form cannot determine which specific persuasion principle a user is more likely to fall victim to. Furthermore, measuring certain principles such as "liking" makes it difficult to draw conclusions as individuals each have their own set of preferences. Also, it was not possible to assess the effect of personality traits on information processing in respect of the persuasion principles of "commitment" and "reciprocity", as this would require prior knowledge of the respondents' past choices and commitments. These specific principles were also identified by Butavicius et al. (2015) as being less suited to their laboratory study.

The study has implications for organisations as they could develop a similar instrument to identify their employees at risk to phishing. Organisations could use the personality test together with an assessment tool that examines employees' preferences; for example, to determine their interest in free prizes, movie genres, employment opportunities, financial stability and the like. These preferences could identify potential behavioural vulnerabilities that phishers could use to persuade victims on both email and SNSs. Following the identification of vulnerable employees, organisations could classify these users accordingly and design security awareness programmes orientated to addressing employees' personal sets of vulnerabilities with consideration to their personality traits.

The current study also has implications for researchers. Research in personality traits and information processing and their influence on phishing susceptibility has the potential to grow further. The model could be extended to include other variables such as perceived risk, self-efficacy, knowledge, social norms, culture and the like, which could potentially offer further insights into phishing susceptibility. Moreover, there is a lack of studies investigating the influence of personality traits on habit. This was pointed out by Wood (2017), who stated that "habit" is largely missing from modern social and personality psychology. A study by Vishwanath (2015b) concluded that habits and information processing jointly influence phishing susceptibility. Similarly, Frauenstein and Flowerday (2016) posited that the habitual behaviours exhibited by social network users could influence them to not process phishing messages on SNSs with sufficient consideration, thus becoming vulnerable to social network phishing.

8. Conclusion

The threat of phishing continues to pose a problem for both organisations and consumers. Protection against phishing threats has limitations when relying solely on technical controls. Phishers will take advantage of new events, catastrophes and global headlines when designing persuasive messages, thus making it difficult to predict what user education should address. People may serve as a protective measure but only if they "recognise" the threat. However, owing to the individual behavioural vulnerabilities that characterise each user, any security awareness efforts may be ineffective when users are faced with phishing. Thus, any steps taken to protect users should also include understanding the individual characteristics that may consequently influence user behaviour and make them vulnerable. In addition, the popularity of SNSs create new opportunities for phishers to exploit the behavioural vulnerabilities of its users. Prior literature has indicated that the personality traits of an individual influence susceptibility to phishing and that the mode of information processing can influence susceptibility to phishing. The current study makes a contribution by bringing together these two distinct areas of research to better understand their relationship to phishing susceptibility on SNSs.

This study proposed a theoretical model that can help identify the types of user who are more likely to be susceptible to phishing on SNSs and is an essential step towards improving online security. Prior literature has highlighted that there are inconsistent findings with regard to personality type and its direct relationship on phishing susceptibility. Similarly, our study revealed that the Big Five traits of agreeableness, neuroticism and openness had a positive influence to both heuristic and systematic processing. Conscientiousness was found to have a negative influence on heuristic processing. It is therefore expected that if conscientious people are faced with phishing on SNSs, they are more likely to closely inspect it before resorting to heuristic processing. Extraversion was the only trait found to have no statistical significance on both modes of processing in the study. The study also confirmed that heuristic processing significantly increases susceptibility to phishing on SNSs, thus supporting prior studies in this area.

Declaration of Competing Interest

This article has not been published or accepted for publication and it is not under consideration at any other outlet. To our knowledge, we have no known conflicts of interest with this work.

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

Items measured (1= disagree strongly – 5 = agree strongly)

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), aesthetic 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. Information processing (Griffin et al., 2002; Vishwanath et al., 2011)

Items measured (1= disagree strongly – 5 = agree strongly)	
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 C. Phishing susceptibility (Facebook Phishing Email)

What action would you most likely take?
Reply to the email
Immediately delete the email
Check the attachment because I am interested to know what my friend has to say
Ignore the email
I do not trust this email
Unsure

CRediT authorship contribution statement

Edwin Donald Frauenstein: Conceptualization, Methodology, Investigation, Formal analysis, Writing - original draft. **Stephen Flowerday:** Conceptualization, Writing - review & editing, Supervision.

References

Adewole, K.S., Anuar, N.B., Kamsin, A., Varathan, K.D., Razak, S.A., 2017. Malicious accounts: Dark of the social networks. J. Netw. Comput. Appl. 79 (1), 41–67. doi:10.1016/j.jnca.2016.11.030.

Akbar, N., 2014. *Analysing persuasion principles in phishing emails* (MSc Computer Science). University of Twente Retrieved from https://essay.utwente.nl/66177/ .

Albladi, S.M., Weir, G.R.S., 2017. Personality traits and cyber-attack victimisation: Multiple mediation analysis. Paper presented at the Joint 13th CTTE and 10th CMI Conference on Internet of Things – Business Models, Users, and Networks doi:10.1109/CTTE.2017.8260932.

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

Algarni, A., Xu, Y., 2013. Social engineering in social networking sites: Phase-based and source-based models. Int. J. e-Educ. e-Bus. e-Manag. e-Learn. 3 (6), 456–462. doi:10.7763/ijeeee.2013.v3.278.

Algarni, A., Xu, Y., Chan, T., 2017. An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. Eur. J. Inf. Syst. 26 (6), 661–687. doi:10.1057/s41303-017-0057-y.

Algarni, A., Xu, Y., Chan, T., Tian, Y.-C., 2014. Social engineering in social networking sites: how good becomes evil. In: Paper presented at the Proceedings of The 18th Pacific Asia Conference on Information Systems (PACIS 2014). Chengdu. China: Association for Information Systems.

Alkiş, N., Taşkaya Temizel, T., 2015. The impact of individual differences on influence strategies. Person. Ind. Diff. 87, 147–152. doi:10.1016/j.paid.2015.07.037.

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 Proceedings of the 1st International Conference on Communication and Computer Engineering. Malaysia.

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

Amichai-Hamburger, Y., Ben-Artzi, E., 2000. The relationship between extraversion and neuroticism and the different uses of the Internet. Comput. Hum. Behav. 16 (4), 441–449. doi:10.1016/S0747-5632(00)00017-0.

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

APWG. (2019). *Phishing Activity Trends Report*, 3rd Quarter 2019, Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

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

Bailey, J.L., Mitchell, R.B., Jensen, B.K., 2008. Analysis of Student Vulnerabilities to Phishing. Paper presented at the 14th Americas Conference on Information Systems (AMCIS) http://aisel.aisnet.org/amcis2008/.

Barrett, P., 2007. Structural equation modeling: Adjudging model fit. Person. Ind. Diff. 42 (5), 815–824. doi:10.1016/j.paid.2006.09.018.

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

Branley, D.B., Covey, J., 2018. Risky behavior via social media: the role of reasoned and social reactive pathways. Comput. Hum. Behav. 78, 183–191. doi:10.1016/j.chb.2017.09.036.

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

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., 2015. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. Australasian Conference on Information Systems.

Caldwell, T., 2016. Making security awareness training work. Comput. Fraud Secur. 2016 (6), 8–14. doi:10.1016/S1361-3723(15)30046-4.

Cameron, K.A., 2009. A practitioner's guide to persuasion: An overview of 15 selected persuasion theories, models and frameworks. Patient Educ. Couns. 74 (3), 309–317. doi:10.1016/j.pec.2008.12.003.

Chang, S.-J., van Witteloostuijn, A., Eden, L., 2010. From the Editors: Common method variance in international business research. J. Int. Bus. Stud. 41 (2), 178–184. doi:10.1057/jibs.2009.88.

Chen, S., Duckworth, K., Chaiken, S., 1999. Motivated heuristic and systematic processing. Psychol. Inquiry 10 (1), 44–49. doi:10.1207/s15327965pli1001_6.

Chen, Y., Conroy, N.J., Rubin, V.L., 2015. Misleading online content: Recognizing clickbait as "false news". In: Paper presented at the Proceedings of the 2015 ACM on Workshop on Multimodal Deception Detection. Seattle, Washington, USA.

Chin, W.W., 1998. The partial least squares approach to structural equation modeling. In: Marcoulides, G.A. (Ed.), Modern Methods for Business Research. Lawrence Erlbaum Associates, Mahwah, NJ, pp. 295–336.

Chin, W.W., Marcolin, B.L., Newsted, P.R., 2003. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. Inf. Syst. Res. 14 (2), 189–217. doi:10.1287/isre.14.2.189.16018.

Cho, J.-H., Cam, H., Oltramari, A., 2016. Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA).

Choudhary, N., Jain, A.K., 2018. Comparative Analysis of Mobile Phishing Detection and Prevention Approaches. In: International Conference on Information and Communication Technology for Intelligent Systems. Springer, Cham, pp. 349–356. doi:10.1007/978-3-319-63673-3_43.

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

Civelek, M.E., 2018. Essentials of Structural Equation Modeling, 64. Zea E-Books Retrieved from http://digitalcommons.unl.edu/zeabook/64/ .

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

Costa, P., & McCrae, R. C. (1992). *The revised NEO personality inventory (NEO-PI-R)* (Vol. 2). Odessa, TX, USA: Psychological Assessment Resources.

Crano, W.D., Prislin, R., 2006. Attitudes and persuasion. Annu. Rev. Psychol. 57, 345–374. doi:10.1146/annurev.psych.57.102904.190034.

Cusack, B., Adedokun, K., 2018. The impact of personality traits on user's susceptibility to social engineering attacks. In: Proceedings of the 16th Australian Information Security Management Conference. Perth, Australia. Security Research Institute, Edith Cowan University.

Dixit, R.V., Prakash, G., 2018. Intentions to Use Social Networking Sites (SNS) Using Technology Acceptance Model (TAM): An Empirical Study. Paradigm 22 (1), 65–79. doi:10.1177/0971890718758201.

Eagly, A.H., Chaiken, S., 1993. The Psychology of Attitudes. Harcourt Brace Jovanovich College Publishers, Fort Worth, TX.

Enos, F., Benus, S., Cautin, R.L., Graciarena, M., Hirschberg, J., Shriberg, E., 2006. Personality factors in human deception detection: Comparing human to machine performance. The Ninth International Conference on Spoken Language Processing, INTERSPEECH-2006.

Erder, M., Pureur, P., 2016. Chapter 8 - Role of the Architect. In: Erder, M., Pureur, P. (Eds.), Continuous Architecture. Morgan Kaufmann, Boston, pp. 187–213.

Ferreira, A., Coventry, L., Lenzini, G., 2015. Principles of persuasion in social engineering and their use in phishing. In: Tryfonas, T., Askoxylakis, I. (Eds.), Human Aspects of Information Security, Privacy, and Trust. Springer, London, pp. 36–47.

Fire, M., Goldschmidt, R., Elovici, Y., 2014. Online social networks: Threats and solutions. IEEE Commun. Surv. Tutor. 16 (4). doi:10.1109/COMST.2014.2321628.

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

Frauenstein, E.D., 2018. An investigation into students responses to various phishing emails and other phishing-related behaviours. Paper presented at the 17th International Information Security South Africa Conference.

Frauenstein, E.D., Flowerday, S.V., 2016. Social network phishing: Becoming habituated to clicks and ignorant to threats? Paper presented at the 2016 Information Security for South Africa (ISSA) Conference.

Funder, D.C., 2001. Personality. Annu. Rev. Psychol. 52 (1), 197–221. doi:10.1146/annurev.psych.52.1.197.

Furnell, S., 2007. Phishing: can we spot the signs. Comput. Fraud Secur. 2007 (3), 10–15 10.1016/S1361-3723(07)70035-0.

Gkika, S., Skiada, M., Lekakos, G., Kourouthanassis, P.E., 2016. Investigating the role of personality traits and influence strategies on the persuasive effect of personalized recommendations. Paper presented at the EMPIRE@RecSys 2016.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. Comput. Secur. 73, 345–358. doi:10.1016/j.cose.2017.11.015.

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

Guadagno, R., Cialdini, R., 2005. Online persuasion and compliance: Social influence on the Internet and beyond. In: Amichai-Hamburger, Y. (Ed.), The Social Net: Human Behavior in Cyberspace. Oxford University Press, New York.

Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E., 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. J. Manag. Inf. Syst. 28 (2), 203–236. doi:10.2753/MIS0742-1222280208.

Jr, Hair, F., J., Hult, G., Ringle, C.M., Sarstedt, M., 2017. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), second ed. Sage Publications, Thousand Oaks, CA.

Halevi, T., Lewis, J., Memon, N., 2013. A pilot study of cyber security and privacy related behavior and personality traits. In: Paper presented at the Proceedings of the 22nd International Conference on World Wide Web Companion (WWW). Rio de Janeiro, Brazil.

Halevi, T., Memon, N., & Nov, O. (2015). *Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks*. doi:10.2139/ssrn.2544742

Harris, A.L., Yates, D., 2015. Phishing Attacks Over Time: A Longitudinal Study. Paper presented at the Twenty-first Americas Conference on Information Systems http://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/38.

Harrison, B., Vishwanath, A., Rao, R., 2016. A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), 5–8, pp. 5628–5634 January.

Harrison, B., Vishwanath, A., Ng, Y.J., Rao, R., 2015. Examining the impact of presence on individual phishing victimization. In: 2015 48th Hawaii International Conference on System Sciences, pp. 3483–3489.

Heartfield, R., Loukas, G., 2015. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Comput. Surv. 48 (3), 1–39. doi:10.1145/2835375.

Hooper, D., Coughlan, J., Mullen, M.R., 2008. Structural equation modeling: Guidelines for determining model fit. Electron. J. Bus. Res. Methods 6 (1), 53–60. doi:10.21427/D7CF7R.

Hu, L., Bentler, P.M., 1999. Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. Struct. Equat. Model. 6 (1), 1–55. doi:10.1080/10705519909540118.

Ivaturi, K., Janczewski, L., Chua, C., 2014. Effect of frame of mind on users' deception detection attitudes and behaviours. Paper presented at the International Conference on Information Resources Management (CONF-IRM).

Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F., 2007. Social phishing. Commun. ACM 50 (10), 94–100. doi:10.1145/1290958.1290968.

Jansen, J., Van Schaik, P., 2018. Persuading end users to act cautiously online: a fear appeals study on phishing. Inf. Comput. Secur. 26 (3), 264–276. doi:10.1108/ICS-03-2018-0038.

John, O.P., Srivastava, S., 1999. The Big Five trait taxonomy: History, measurement, and theoretical perspectives. In: Pervin, L.A., John, O.P. (Eds.), Handbook of Personality: Theory and Research. US: Guilford Press, New York, NY, pp. 102–138.

Johnson, J.A., 1997. Units of analysis for the description and explanation of personality. In: Hogan, R., Johnson, J.A., Briggs, S.R. (Eds.), Handbook of Personality Psychology. US: Academic Press, San Diego, CA, pp. 73–93.

Kline, R.B., 2016. Principles and Practice of Structural Equation Modeling, fourth ed. Guilford Press, New York, NY.

Kothari, C.R., 2004. Research methodology: Methods and Techniques. New Age International, New Delhi, India.

Kreitz, C., Schnuerch, R., Gibbons, H., Memmert, D., 2015. Some See It, Some Don't: Exploring the Relation between Inattentional Blindness and Personality Factors. PLoS One 10 (5). doi:10.1371/journal.pone.0128158.

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

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

Lastdrager, E.E., 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Sci. 3 (1), 9. doi:10.1186/s40163-014-0009-y.

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. In: Paper presented at the Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018). Florence, Italy.

Lawson, P., Zielinska, O., Pearson, C., Mayhorn, C.B., 2017. Interaction of personality and persuasion tactics in email phishing attacks. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 61, pp. 1331–1333. doi:10.1177/1541931213601815.

Li, Y., Huang, Z., Wu, Y.J., Wang, Z., 2019. Exploring how personality affects privacy control behavior on social networking sites. Front. Psychol. 10 (1771). doi:10.3389/fpsyg.2019.01771.

Lopes, B., Yu, H., 2017. Who do you troll and why: An investigation into the relationship between the Dark Triad Personalities and online trolling behaviours towards popular and less popular Facebook profiles. Comput. Hum. Behav. 77, 69–76. doi:10.1016/j.chb.2017.08.036.

Lowry, P.B., Gaskin, J., 2014. 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), 123–146. doi:10.1109/TPC.2014.2312452.

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

Mayhorn, C.B., Welka, A.K., Zielinska, O.A., Murphy-Hill, E., 2015. Assessing individual differences in a phishing detection task. In: Paper presented at the Proceedings 19th Triennial Congress of the IEA. Melbourne, Australia.

McAndrew, F.T., 2018. When do personality traits predict behavior? Personality can predict behavior, but only when we understand its limitations. Psychol. Today. [Online]. Retrieved from https://www.psychologytoday.com/us/blog/out-the-ooze/201810/when-do-personality-traits-predict-behavior .

McCrae, R.R., Costa Jr, P.T., 1999. A Five-Factor theory of personality. In: Pervin, L.A., John, O.P. (Eds.), Handbook of personality: Theory and Research. Guilford Press, New York, NY, pp. 139–153.

McCrae, R.R., John, O.P., 1992. An introduction to the five-factor model and its applications. J. Pers. 60 (2), 175–215. doi:10.1111/j.1467-6494.1992.tb00970.x.

McDonald, R.P., Ho, M.-H.R., 2002. Principles and practice in reporting structural equation analyses. Psychol. Methods 7 (1), 64–82. doi:10.1037/1082-989X.7.1.64.

McElroy, J.C., Hendrickson, A., Townsend, A.M., DeMarie, S.M., 2007. Dispositional factors in internet use: Personality versus cognitive style. MIS Quarterly 31 (4), 809–820. doi:10.2307/25148821.

McKane, J., 2019. #ImStaying is a playground for criminals. Mybroadband. [Online]. Retrieved from https://mybroadband.co.za/news/internet/327659-imstaying-is-a-playground-for-criminals.html?source=newsletter .

Mitnick, K.D., Simon, W.L., 2002. The Art of Deception: Controlling the Human Element of Security. Wiley, New York.

Modic, D., Lea, S.E.G., 2012. How neurotic are scam victims, really? The Big Five and Internet scams. In: In Proceedings of the *2011* Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology. Exeter, United Kingdom. Washington Singer Press doi:10.2139/ssrn.2448130.

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

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

Moutafi, J., Furnham, A., Paltiel, L., 2004. Why is Conscientiousness negatively correlated with intelligence. Person. Ind. Diff. 37 (5), 1013–1022. doi:10.1016/j.paid.2003.11.010.

Muncaster, P., 2020. #COVID19 Drives Phishing Emails Up 667% in Under a Month. Infosecurity Magazine. [Online]. Retrieved from https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/ .

Musil, S., 2020. Google blocking 18M malicious coronavirus emails every day. CNET. [Online]. Retrieved from https://www.cnet.com/news/google-seeing-18m-malicious-coronavirus-emails-each-day/ .

Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T., Whitty, M., 2014. Understanding insider threat: A framework for characterising attacks. In: Paper presented at Proceedings of the 2014 IEEE Security and Privacy Workshops.

Ollmann, G. (2002). *The phishing guide: Understanding & preventing phishing attacks*. Retrieved from www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf

Oyibo, K., Orji, R., Vassileva, J., 2017. Investigation of the influence of personality traits on Cialdini's persuasive strategies. In: Paper presented at the Proceedings of the Personalization in Persuasive Technology Workshop, Persuasive Technology 2017. Amsterdam, Netherlands.

Parish, J., Bailey, J., Courtney, J.F., 2009. A personality Based Model for Determining Susceptibility to Phishing Attacks. University of Arkansas, Little Rock, Arkansas.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., Butavicius, M., 2011. Why do some people manage phishing e-mails better than others. Inf. Manag. Comput. Secur. 20 (1), 18–28. doi:10.1108/09685221211219173.

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

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

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

Podsakoff, P.M., Organ, D.W., 1986. Self-reports in organizational research: Problems and prospects. J. Manag. 12 (4), 531–544. doi:10.1177/014920638601200408.

Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., Markatos, E.P., 2010. Using social networks to harvest email addresses. In: Paper presented at the Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. Chicago, Illinois, USA.

Reznik, M., 2013. Identity theft on social networking sites: Developing issues of Internet impersonation. Touro Law Review 29 (2), 455–483. Retrieved from https://digitalcommons.tourolaw.edu/lawreview/vol29/iss2/12 .

Rolland, J.P., 2002. The cross-cultural generalizability of the Five Factor Model of Personality. In: McCrae, R.R., Allik, J. (Eds.), The Five Factor Model of Personality across cultures. Kluwer Academic/Plenum, New York, NY, pp. 7–28.

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

Safa, N.S., Von Solms, R., Furnell, S., 2016. Information security policy compliance model in organizations. Comput. Secur. 56, 70–82. doi:10.1016/j.cose.2015.10.006.

Samunderu, T., 2014. SIM swap fraud : no way out?: financial law. Without Prejudice 14 (6), 32–33. Retrieved from https://journals.co.za/content/jb_prej/14/6/EJC157199 .

Savalei, V., Bentler, P., 2006. Structural equation modeling. In: Grover, R., Vriens, M. (Eds.), The handbook of marketing research: Uses, misuses, and future advances. Sage Publications, Thousand Oaks, CA Retrieved from http://sk.sagepub.com/reference/hdbk_mktgresearch doi:10.4135/9781412973380.

Schermelleh-Engel, K., Moosbrugger, H., Müller, H., 2003. Evaluating the fit of structural equation models: tests of significance and descriptive goodness-of-fit measures. Methods Psychol. Res. 8 (2), 23–74.

Schreiber, J.B., Nora, A., Stage, F.K., Barlow, E.A., King, J., 2006. Reporting structural equation modeling and confirmatory factor analysis results: a review. J. Educ. Res. 99 (6), 323–338. doi:10.3200/JOER.99.6.323-338.

Schuetz, S.W., Lowry, P.B., Thatcher, J.B., 2016. Defending against spear-phishing: Motivating users through fear appeal manipulations. Paper presented at the 20th Pacific Asia Conference on Information Systems (PACIS 2016).

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. In: Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Atlanta, Georgia, USA.

Shropshire, J., Warkentin, M., Sharma, S., 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Comput. Secur. 49, 177–191. doi:10.1016/j.cose.2015.01.002.

Sophos, 2011. Social Netw. Secur. Threats. Retrieved from https://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats/facebook.aspx .

Stajano, F., Wilson, P., 2011. Understanding scam victims: Seven principles for systems security. Commun. ACM 54 (3), 70–75. doi:10.1145/1897852.1897872.

Sullivan, G.M., Feinn, R., 2012. Using Effect Size—or Why the P Value Is Not Enough. J. Grad. Med. Educ. 4 (3), 279–282. doi:10.4300/jgme-d-12-00156.1.

Sumner, C., Byers, A., Shearing, M., 2011. Determining personality traits & privacy concerns from Facebook activity. Paper presented at the Black Hat Briefings.

Titcomb, J., 2017. Facebook admits up to 270m users are fake and duplicate accounts. Telegraph. [Online]. Retrieved from https://www.telegraph.co.uk/technology/2017/11/02/facebook-admits-270m-users-fake-duplicate-accounts/ .

Tsikerdekis, M., Zeadally, S., 2014. Online deception in social media. Commun. ACM 57 (9), 72–80. doi:10.1145/2629612.

Uebelacker, S., Quiel, S., 2014. The Social Engineering Personality Framework. In: Proceedings of the 2014 Workshop on Socio-Technical Aspects in Security and Trust. IEEE Computer Society.

United States Department of Justice. (2017). Lithuanian man arrested for theft of over $100 million in fraudulent email compromise scheme against multinational Internet companies [Press release]. Accessed from https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme

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).

Verizon. (2019). 2019 *Data Breach Investigations Report (DBIR)*. Retrieved from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Vishwanath, A., 2015a. Habitual Facebook use and its impact on getting deceived on social media. J. Computer-Mediat. Communi.cation 20 (1), 83–98. doi:10.1111/jcc4.12100.

Vishwanath, A., 2015b. Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. J. Computer-Mediat. Commun. 20 (5), 570–584. doi:10.1111/jcc4.12126.

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

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

Volkamer, M., Renaud, K., Reinheimer, B., Rack, P., Ghiglieri, M., Mayer, P., Kunz, A., Gerber, N., 2018. Developing and evaluating a five minute phishing awareness video. In: Furnell, S., Mouratidis, H., Pernul, G. (Eds.). In: Trust, Privacy and Security in Digital Business. TrustBus 2018. Lecture Notes in Computer Science, 11033. Cham, Switzerland: Springer., pp. 119–134.

Waheed, H., Anjum, M., Rehman, M., Khawaja, A., 2017. Investigation of user behavior on social networking sites. PLoS One 12 (2), e0169693. doi:10.1371/journal.pone.0169693.

Wilcox, H., Bhattacharya, M., 2015. Countering social engineering through social media: An enterprise security perspective.. In: Proceedings of the 7th International Conference on Computational Collective Intelligence Technologies and Applications (ICCCI 2015).

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

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

Workman, M., 2007. Gaining access with social engineering: An empirical study of the threat. Inf. Syst. Secur. 16 (6), 315–331. doi:10.1080/10658980701788165.

Workman, M., 2008a. A test of interventions for security threats from social engineering. Inf. Manag. Computer Secur. 16 (5), 463–483. doi:10.1108/09685220810920549.

Workman, M., 2008b. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. J. Am. Soc. Inf. Sci. Technol. 59 (4), 662–674. doi:10.1002/asi.20779.

Wright, R.T., Marett, K., 2010. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. J.f Manag. Inf. Syst. 27 (1), 273–303.

Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., Sprissler, E., 2018. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment. Comput. Hum. Behav. 84, 375–382. doi:10.1016/j.chb.2018.02.019.

Yang, J., Du, F., Qu, W., Gong, Z., Sun, X., 2013. Effects of personality on risky driving behavior and accident involvement for Chinese drivers. Traffic Inj. Prev. 14 (6), 565–571. doi:10.1080/15389588.2012.748903.

Zhang, L., 2006. Thinking styles and the big five personality traits revisited. Person. Ind. Diff. 40 (6), 1177–1187. doi:10.1016/j.paid.2005.10.011.

Zhang, W., Burd, S.D., Luo, X., Seazzu, A.F., 2012. How could I fall for that? Exploring phishing victimization with the Heuristic-Systematic Model. Paper presented at the 45th Hawaii International Conference on System Sciences.