Social Network Phishing: Becoming Habituated to Clicks and Ignorant to Threats?

Edwin D. Frauenstein[1] and Stephen V. Flowerday[2]
Department of Information Systems
University of Fort Hare
East London, South Africa
edwin.frauenstein@gmail.com[1], sflowerday@ufh.ac.za[2]

***Abstract* — With the rise in number of reported phishing cases in statistical reports and online news, it is apparent that the threat of phishing is not retreating. Phishers continuously seek new methods to deceive individuals into sharing their confidential information. As a result, today the traditional form of conducting phishing solely through email and spoofed websites has evolved. Social network phishing is a serious threat as it reaches a far wider audience, consequently affecting both business and private individuals. This paper argues that due to the constant updates of information users are engaged in on social networking sites, users may become habituated to clicking and sharing links, liking posts, copying and pasting messages, and uploading and downloading media content, thus resulting in information overload. This behavioral priming leads users to becoming more susceptible to social engineering attacks on social networks as they do not cognitively process messages with a security lens. This paper introduces social network phishing and briefly discusses activities users engage in on social networks sites, thus highlighting the formation of "bad" habits. Further, existing information processing models applicable to this context are discussed.**

Keywords—social network phishing; social media phishing; phishing; social engineering; habits; information processing;heuristic processing; systematic processing

I. INTRODUCTION

With approximately two billion Internet users worldwide using social networking sites (SNSs) today [1], it is rare not to find individuals active on at least one social network (SN). The introduction of Web 2.0 technologies has given rise to widely popular SNSs such as Facebook, Twitter, LinkedIn, MySpace, Pinterest, Google Plus+, Tumblr, Snapchat, Instagram and Flickr. Facebook is the most popular SN and according to Facebook Corporation, it is used worldwide by approximately 1.55 billion monthly active users, increasing by 14% each year [1]. As of September 2015, an estimated 1.01 billion people log onto Facebook daily. Every minute on Facebook, 510 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded. Facebook Messenger, accessed mostly through smartphones, is used by 800 million users. Other SNSs have staggering figures too: WhatsApp is used by approximately 1 billon users; 400 million use LinkedIn; 307 million Twitter users, and Instagram with 200 million [1]. These figures constantly rise and will soon be out-of-date.

Despite users having different levels of computer experience, backgrounds, cultures, race and gender, it is apparent that SNSs are not restricted to any particular type of user. Given the statistics, it should not be unexpected that SNs present an opportunistic market for information security threat agents such as phishers.

One of the easiest ways of acquiring individuals' information is through the popular SN Facebook. By having mutual friends, people can access a user's profile. If the user concealed their information through privacy settings, an option would be to send them a friend request. Alternatively, for more specific information such as educational background and work history, other SNSs such as LinkedIn can be searched. If this fails, search for names using a search engine or lure them to open malicious links. This is the connected world we live in today. Information is not as private as one may perceive and this particular means of acquiring information and befriending strangers can be performed by any person, including phishers.

With the popularity of SNSs increasing and its extension to smartphone applications (apps), users may be subjecting themselves to a wider degree of security threat agents than anticipated. The traditional method of conducting phishing mainly through emails and spoofed websites has progressed to social platforms whereby it can infiltrate into organisation networks [2]. Since SNSs are widely popular, have an extensive number of users with diverse backgrounds, and encourage sharing of personal information, phishers use this as an ideal opportunity to gain confidential information, often made openly available by members of these sites. This information could then be used to conduct more targeted forms of phishing attacks (i.e. spear phishing, whaling and mishing) both on and off SNSs. Furthermore, phishers target users' poor privacy habits or exploit their online behaviour by enticing them to click on links that is of interest to them.

The objective of the paper is to highlight social network phishing and related threats, SN habits, information processing models and its implications thereof to users.

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

II. Social Engineering, Phishing and Social Network Phishing

A. Social Engineering Explained

Phishing is effective because it uses social engineering (SE) techniques to influence people into performing certain actions that will benefit the phisher. Reference [3] defines SE as using "[i]nfluence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation". To persuade users, phishers make use of SE techniques that focus on prompting human emotions [4] such as greed, fear, heroism and desire to be liked. In general, people desire to obey authority such as a bank official or policeman. As such, scams use authoritative words or imitate organisations and authoritative persons in order to initiate a response. Another technique, typically used in traditional marketing, is making an opportunity seem scarce, or making the victim feel they have made a commitment by responding to the scam offer. Table 1 below by [5] presents a taxonomy of SE persuasion techniques with a comparison of persuasion principles by three key authors in this area.

TABLE I. Principles of Persuasion in Social Engineering [5]

Principles of Influence [6]	Psychological Triggers [7]	Principles of Scams [8]
Authority	Authority	Social Compliance
Social Proof	Diffusion Responsibility	Herd
Linking and Similarity	Deceptive Relationship	Deception
Commitment and Consistency	Integrity and Consistency	Dishonesty
Scarcity	Overloading	Time
Reciprocation	Reciprocation	Need & Greed
	Strong Affect	Distraction

From the table above, it is evident that there are common techniques overlapping in each of the principles used by social engineers (e.g. authority, reciprocation). This is necessary to persuade users into performing actions instructed by the social engineer. Some of these techniques and principles are applied in other forms of SE attacks such as baiting, pretexting, ransomware and phishing.

B. Phishing Explained

Definitions of phishing constantly change, especially since phishers seek new practices to carry out their attacks. The Anti-Phishing Working Group define phishing as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" [9]. Reference [10] define it as "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion." Using phishing definitions from 2458 publications, [11] defines phishing as "a scalable act of deception whereby impersonation is used to obtain information from a target." As noticed from all the definitions, the specific channel(s) used by phishers to exploit attacks is not mentioned. This is not unexpected given that today phishers continue to use a variety of methods to conduct a phishing attack and these methods constantly change too. As a result, this presents challenges to educate users effectively to identify new techniques that aim to scam them [4]. More especially since phishing is designed to focus on exploiting human weaknesses, in particular cognitive biases, instead of technology vulnerabilities [12].

For many years, phishers typically use email messages and spoofed websites designed to appear as if they originate from a recognised and trusted source/authority (e.g. financial institution). By imitating as a legitimate source, phishers gain the victim's trust who then carry out the actions instructed by the phisher. The phisher would gain confidential information which can be used by the phisher or sold to other illegal entities. Confidential information is usually login information such as usernames and passwords. However, more sensitive information is also sought after such as identification/social security numbers and credit card details.

Phishing is regarded as a socio-technical attack. The "social" aspect uses SE techniques, as seen in Table 1, to convince users into performing actions which in turn benefits the phisher. Timing is also an important factor as phishers will take advantage of events such as religious festivities, holidays and tax season. This establishes urgency on the part of the victim as they may believe it is an opportunity that is available for a limited time period only. As depicted in Table 1, this preys on SE techniques of scarcity, overloading, distraction, need and greed.

Typically, the phisher directs an email to the victim expressing a fabricated event in the message. The message can take the approach of alerting the victim of an imminent threat or danger. For example, the victim may be warned that his/her bank account may be "hacked" as the organisation being imitated has been experiencing fraudulent activity such as a security breach. Alternatively, the message may convince the victim that they have won a substantial reward or prize. In both cases this is regarded as the "bait", and would require the user to open an attachment or click on a hyperlink for verification purposes. If the user clicks on the hyperlink, they are subsequently directed to the spoofed website that appears identical in design to the genuine website of the institution being imitated. This is seen as the "hook". They then unsuspectingly log-in to the spoofed website with their personal account information. This is known as the "catch". For this to be effective, it must convince the victim and establish trust. This can be accomplished by the strength of the message arguments and the authority of where the email purportedly originates from such as a recognised or reputable organisation. In this regard, institutional logos or branding are used within the email thereby convincing victims of its authenticity. To further convince the user to comply with the request, the phisher might add an element of fear in the message. For example, the email may state that should the victim decide to ignore the request, it may result in their account or membership being suspended or terminated in a certain time frame. This preys on SE techniques of authority, distraction and time. The addition of fear may increase the likelihood of the victim following through with the phisher's

request. From these instructions provided in the email, the user "thinks" they have a choice to decide on which action to take; however, ultimately there are no correct choices as the instructions supplied are false to begin with. From this discussion, much importance is placed on email design to carry out phishing attacks successfully.

C. Social Network Phishing Explained

Phishers make use of SNSs to carry out attacks on their victims. Currently, there is no common accepted definition for social network phishing as the terms "social media phishing", "social phishing" and "social networking phishing" are used interchangeably in literature. The common element is that SE techniques are used to conduct attacks in SN environments. Security experts of the company Proofpoint, determined in the past year that the number of phishing attempts on popular SNSs have increased by 150% [13]. According to [14], 22% of phishing scams on the web target Facebook (see Fig.1), and phishing sites imitating SN websites consist of more than 35% of all cases whereby Kaspersky anti-virus software was triggered.

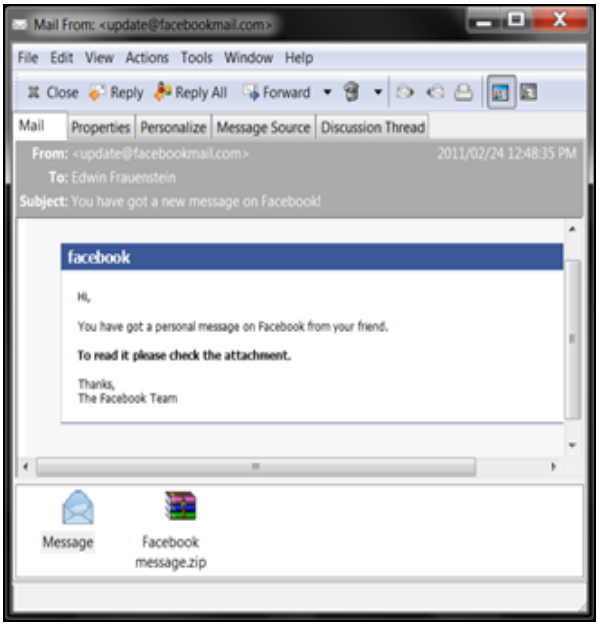

Fig. 1. Phishing email purportedly originating from Facebook

Users of SNSs like Facebook or Twitter have a greater risk of being targeted for SE attacks because of the vast amount personal information people openly share about themselves [15]. Furthermore, it is easy for phishers to impersonate a friend of the victim to gain their trust. This can lead to more targeted forms of attacks such as spear phishing and clickjacking, which are discussed in the next section.

III. Social Network Phishing Techniques

This section reveals that SNSs are a playground to conduct various forms of phishing attacks. The SE techniques used frequently in phishing emails is also employed in a SN environment. Since Facebook is the most used SN, one can expect it to be the prime target for phishing attacks. Scams on Facebook include cross-site scripting, clickjacking, survey scams and identity theft [16]. Ways in which these scams can be carried out can be in the form of fake comments, fake media content, or fake promotion discounts (see Fig. 2).

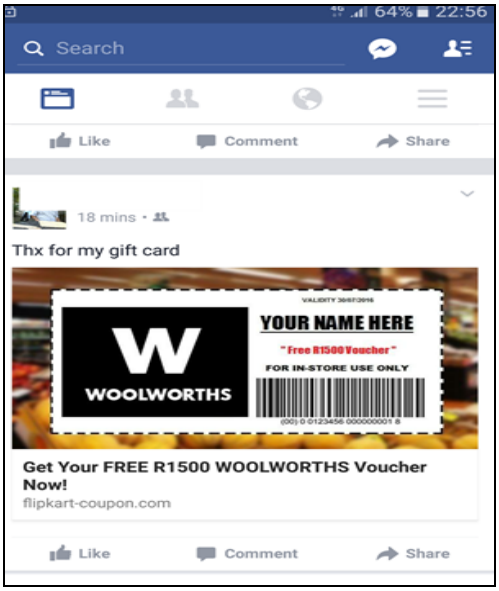

Fig. 2. Fake free shopping voucher found on Facebook

Scams such as the one depicted in Fig. 2 prey on SE techniques of authority, scarcity, need and greed. Trust can be further enhanced if these fake vouchers are shared by trusted friends.

A. Spoofing

Much like standard phishing, SN users are enticed to click on a link which subsequently directs them to a fake webpage to log-in. Victims may have been enticed through a message originating from a hijacked friend's account, malware infected links or attachments, or a phishing email with a link to log-in to a spoofed SN webpage. Preying on the authority SE technique, imagine the strength of phishing if the phisher impersonates a celebrity. The fake profile would then include a network of bogus friends associated with that particular fake account. This is used to persuade the victim into believing that the account is genuine because a profile consisting of few friends may be suspicious to the victim.

B. Identity Theft (Cloning)

Cloning is when a phisher creates a SN account imitating the victim's account and is not regarded as hacking because the victim's account was not compromised. Cloning is common on Facebook and is made easier for the phisher if the victim has made their profile information and images publicly visible. Through the cloned account, the phisher submits friend requests attached with a convincing message to the victim's friends. For example, "My account has been hacked, please delete my other account you have and communicate with me using this one only. If you don't delete it, you may be hacked too!" Once accepted, the phisher begins sending messages to the friends connected to the victim instructing the

recipient to click on a link, consequently acquiring personal information from them. Similar to phishing emails, various SE techniques will be employed in the fabricated message to convince the user to click on the link.

Business orientated SNSs such as LinkedIn offer phishers the opportunity to collect data on companies and their employees. They can then use that information to launch spear phishing attacks, targeting employees specific to that organisation [16]. On LinkedIn, phishers could pose as prospective job recruiters, requesting documentation from the victim such as a curriculum vitae. This would contain a range of personal information the phisher could then use to conduct identity theft. Moreover, the phisher may request the victim to provide them with a copy of their identity document which can be used to conduct other crimes. The victim would willingly give out this information as it is not unusual to receive such requests from recruiters.

C. *Malware-based*

Malware-based phishing refers to a spread of phishing messages by using malware. For example, the victim installs a rogue Facebook app which automatically sends messages to all their Facebook friends. Such messages often contain links allowing the recipients also to install the rogue Facebook app on their computers or smartphone devices. Other deceptive techniques include promising Facebook users that by installing a particular app, which is malware, will allow them to see a list of people who visit their Facebook profile page. Another example: Enticing users with the option of installing the Facebook Color Changer app that will allow the user to change the colour of their Facebook account from the standard blue to a colour of their choice [17].

Other forms of malware-based phishing include content-injection which is malicious content. The malicious content can often be in the form of bogus posts (e.g. Facebook or LinkedIn posts, tweets) published by users whose accounts were affected with rogue apps. In many cases, victims are unable to see the bogus posts posted by the malware apps on their behalf. The bogus posts, for example, may contain a photo of the user and the statement: "I am injured and in the hospital. If you would like to help me, please sign up by clicking on the following link." When the victim clicks on the link, they will be requested to provide their personal data, which may be used by the phisher to commit identity theft and other scams. A post may contain malicious content and hoax text that requests the user to share the post. For example, a distributed hoax message stating that Facebook founder Mark Zuckerberg is giving away $45 million to ordinary users and to be selected as one of the thousand lucky entrants, the message must be copied and pasted to one's wall along with five friends tagged in the post [18]. Again, this preys on SE techniques of scarcity, need and greed and so on.

Given the variations of how scams are conducted on SNSs, it is difficult to expect users to be updated with phishers' new techniques on exploiting technology and the methods in which they carry out their attacks on SNSs.

IV. Brief Background on Phishing Literature

A brief literature survey of "phishing" reveals that the most cited articles were published more than a decade ago. Even so, most researchers in the area of phishing continue to cite these published works. Although much research is available, the problem of addressing phishing still remains and as such continues to be an area of interest amongst scholars.

Early phishing research focused on technological controls with the testing and measurement of anti-phishing detection tools such as web browser toolbars [19], email detection filters [20], and URL detection [21,22,23,24]. Technological controls certainly perform a vital role in detecting the majority of phishing emails as they are automatically detected and filtered, preventing it from reaching the user. Other technological tools, such as web browser warnings, indicate to the user potentially malicious webpages.

Despite the technological tools available to assist users to identify phishing appropriately, they did not meet expectations. Research turned towards investigating user responses in how users interpret web browser warnings [25,26,27,28].

Information security literature highlights that humans are vulnerable to social engineering attacks and that security is a "people problem" [29]. As a result, research efforts were directed towards educating the human element to change their current behaviour [30, 31]. Educational approaches used were online games [32] and embedded email training systems [33]. Furthermore, research aimed at improving users' security awareness in phishing [34].

Recently, to understand this problem more, research focused on exploring differences in gender and personality traits with regard to phishing susceptibility. Openness, conscientiousness, extraversion, agreeableness, and neuroticism are considered the Big Five personality traits [35]. Other research applied a scenario-based design to study both the relationships between demographics and phishing susceptibility, and the effectiveness of several anti-phishing educational materials [36]. The relationship between the Big Five personality traits and email phishing response and how these traits affect users' privacy behaviour on Facebook was examined [4]. Additionally, [37] assessed the basic demographics of personality characteristics, dispositional trust, impulsivity, and web/computer based behaviour, beliefs, and previously experienced phishing consequences. Their study examined two behavioural/consequence factors: experiencing a monetary loss without reimbursement, and a belief that one may receive a legitimate request to confirm account information via email. A conceptual phishing susceptibility framework that utilises the Big Five personality traits and links the level of social engineering security-exploit susceptibility to an individual's personality traits was proposed by [38], and [39] investigated users' behaviour response when presented with phishing emails. They found personality traits of extraversion and openness were better at detecting phishing emails.

One of the earliest phishing experiments in the context of SNSs was by [40]. They discussed how phishing attacks can

be more effective by exploiting personal information found from SNSs. In a study by [41], they analysed data recorded from different parts of the world which compared the phishing emails used by phishers to lure victims in 2008 and 2014 respectively. They found that phishers have recently shifted their focus towards targeting online social media such as Facebook and YouTube to spread their phishing links. There is a lack of research dedicated to the susceptibility of social engineering victimization in SNSs, or to understanding which demographic factors correlate with falling for social engineering tricks in the context of SNSs [42]. As a result, a study by [42] attempts to predict a person's vulnerability to SE based on demographic factors (i.e. age, gender and educational level), relationship status, and personality type.

This section revealed that phishing research began addressing technological aspects, moved towards educating users, and finally examining the relationship of certain personality traits with phishing susceptibility on SNSs. The subsequent sections discuss emerging areas of interest in phishing research, namely habits and information processing.

V. Social Network Activities That May Lead Towards Habit Formation

This section begins by discussing some popular activities SN users are engaged in and how its usage of such may develop into habits. As a result, it may affect them not to pay particular attention to suspicious information such as phishing scams. Furthermore, these habits may influence their behaviour to such an extent, that it may influence them on other online applications.

In public, it is not abnormal to see majority of people glued to their smartphones, most of whom are most likely using social apps to update their status or post pictures. This behaviour may be reinforced as it is repeated frequently. How one behaves in the physical world may not be much different compared to online SN environments. For example, industry professionals exchanging business cards with others is not uncommon practice – even if one has had no prior history with that person. Thus, receiving "invites" through a professional SN such as LinkedIn, members may behave similarly in this environment too by accepting invitations from strangers as the user has been conditioned to operate in this manner. Phishers may use this as an opportunity to gather personal information from the user.

Interconnectivity between smartphone apps gives users the freedom to broadcast their activities or messages across to other SNSs. For example, the Strava™ app, a social running and cycling app, allows users to publish their run to Facebook by simply clicking on the embedded Facebook icon. Other runners, who can be strangers, can follow one's run and view the map of the route. In another example, LinkedIn updates can also broadcast as tweets on Twitter. For the latter, a Twitter audience could be anyone provided they follow the user. If phishers have access to this specific information, they can perform spear phishing attacks on their targets.

Members of SNSs can also be notified via email of any activities linked to their preferences, e.g. tagged in a friend's post. Thus, receiving an email appearing to originate from the SNS (as depicted in Fig. 1) may not appear suspicious to the user. As most users have a SN account, many websites, including e-commerce websites, allow users the option to log-in with their SN credentials (i.e. username and password). Thus, if a SN account has been hijacked, it may provide a means for phishers to conduct other forms of cybercrime using those credentials.

SNSs have common "social" functions that users have grown accustomed to. For example, most SNS, including social apps, have features such as inserting profile pictures, a status, mood, commenting on and liking posts. Most of these features exist in Facebook, LinkedIn and further instant messenger applications such as Whatsapp. "Following" users and pages is a standard function across most SNSs such as Facebook, LinkedIn, Twitter and others. It may not be concerning to members to be followed back or to receive a friend request from a stranger. As a result, receiving an email, purportedly originating from a SNS to accept a friend request may increase the chances for users to not be suspicious. As pointed out by [14], users are more likely to click on links in suspicious emails if it originates from a Facebook friend rather than from a bank.

YouTube is a popular media platform to watch online video content ranging from amateur footage that users have uploaded to various channels dedicated to particular areas of interest. These videos can be shared to other SNSs such as Facebook. To view the video, users have to click on the play icon, something which most users would be accustomed to. The latter poses a problem if phishers are sharing spoofed media content to other SNSs to lure users into viewing the video – especially if it is of interest to the user.

SN users also appear to post insensitive messages without thinking of its consequences. Users may think because they are not dealing directly with people, they are in a protective 'bubble'. Recently, the South African public has been outraged by racial comments made by Penny Sparrow referring to Black people as "monkeys" [43]. Shortly thereafter, other prominent figures such as former Standard Bank investment strategist Chris Hart and radio personality Gareth Cliff were also accused of arguably "tweeting" racial utterances. In all cases, the organisations for which these individuals worked were pressured into taking action against them. This emphasises that users' behaviour on SNSs can put organisations' reputation at risk. As a result, organisations have seen the need to introduce social media policies [2].

From the SN activities described in this section, users may develop SN habits which can influence their ability to detect potential phishing attacks.

VI. Discussion

Anti-phishing educational interventions typically focus on educating users on email messages and spoofed websites. Users are made aware to examine the message content for poor grammatical and spelling errors, not to click on hyperlinks within emails, not to open attachments from unknown sources and so on. However, phishers can take advantage of each of these education aspects on SNSs. For example, with the diverse language cultures of users in SNSs,

some users may not be able to identify grammatical errors in phishing emails. On the other hand, research uncovered that in some cases the grammatical errors, known as scammer grammar, may be crafted intentionally by the scammers [44] on the assumption that less educated users may be more susceptible to fall for scam offers.

SN users are inundated with links on their Facebook, Twitter and LinkedIn profiles and have grown accustomed that these shortcuts will lead them directly to content within the webpage or externally to other sources. Phishers are using URL shorteners not only for reducing space but also to hide their identity [45]. It is difficult for Twitter users to know whether the URLs they have received are legitimate [46]. Since Twitter limits any messages (i.e. tweets) posted to 140 characters, link shortening services, such as bit.ly, are used to shorten longer Internet addresses. Despite Twitter recently announcing that usernames, quoted tweets, photos and other media attachments will not count against the 140 character limit, these link shortening services are still currently being used. This presents educational concerns because consequently users will be unable to identify the website name of where these shortened links lead to, thus making it even more difficult to establish whether they are potentially dangerous. Phishers also use this opportunity to create shortened URLs to redirect users to malicious sites [16]. Furthermore, smartphone browsers display limited security information due to its small screen size. As a result, users who have been educated in phishing to look for the secure https:// protocol in the URL bar may not be able to see this directly on their smartphone. Furthermore, users may be engaged with other information seeking activities using other software applications thus distracting them. From these distractions, users may not be in the right frame of mind when presented with security attacks, thus leaving them vulnerable [47]. Users may also be overloaded with emails. Reference [48] found an increased likelihood of falling victim to phishing by the volume users receive.

VII. HABITS

What if user SN behaviour has become automated, to a certain degree, by going through the motions of scrolling through posts by friends, liking and sharing posts, clicking on various links and pages and not processing this information with more consideration to detail? It was found that users who habitually engage on Facebook are significantly more likely to fall prey to a social media phishing attack [49].

It was reported that one of the main reasons for social media usage is for self-distraction and boredom relief [50]. Receiving continual support in the form of comments and "likes" reinforces users' behaviours and as such will be repeated by them [50]. Habitual clicking may lead to the user building a schema which leads them to instant gratification. As a result, it may become difficult for users to break this habit. It may be possible that these habits affect users to process information found on SNSs in a more systematic manner. This is elaborated more in Section VIII.

According to [51], almost no Information Systems research has investigated the potential importance of subconscious (automatic) behaviours known as habits. Users' "habitual pattern of email use is an issue that has yet to be examined within the phishing-based deception context" [49]. Overtime, when enacted repeatedly, behaviours become action-scripts that are applied without conscious reflection about its antecedents, consequences, or even its enactment [52]. In the context of Information Systems (IS) usage, [51] define "habit" as "the extent to which people tend to perform behaviours automatically because of learning." These authors suggest that continued usage of Information Systems is not only a consequence of intention, but also of habit. As pointed out earlier, SNSs are exceedingly popular and as such, users are engaged for many hours on these sites. However, habit is not the same as behaviour [51]. It should be understood as a type of mindset that enhances the perceptual readiness for habit related cues, and prevents an individual from being distracted and from adopting other, less efficient courses of action. A stable context promotes habit formation in that it only requires a minimum of the individual's attention in reacting adequately to certain situations. In the context of phishing, this stable context could be engaging in SNSs or checking email. Once a habit is established, behaviour is performed automatically to such a degree that it requires little or no conscious attention and minimal mental effort. Thus, if users continuously open links on Facebook and Twitter without any fear of consequence, it may cross other environment too, for example email or banking websites.

VIII. INFORMATION PROCESSING MODELS

According to [53], social-psychological research on phishing has implicated ineffective cognitive processing as the key reason for individual victimization. As such, it is important to consider models related to this problem. Therefore, this section focuses on persuasion theories applicable to the phishing context.

The heuristic-systematic model (HSM) is a model of information processing that originated from persuasion research in social psychology [54]. The model attempts to explain individual information processing and attitude formation in persuasive contexts. The HSM and elaboration likelihood model (ELM) are closely related models and are recognised as dual process models because they both propose two major approaches to persuasion, namely: the central route and the peripheral route. The key difference between the two models is that HSM explicitly recognises dual processing (i.e. parallel or jointly), while ELM suggests information processing occurs on a continuum. Researcher [55] found that the ELM offers an encouraging framework for understanding the ways in which social engineers gather sensitive information or get unwitting victims to comply with their request.

Since its introduction, dual-process models remain today's most influential persuasion paradigms [56]. Compared to systematic processing, [54] define heuristic processing as "a limited mode of information processing that requires less cognitive effort and fewer cognitive resources." Heuristic processing draws upon simple decision cues, often termed ''rules of thumb", and occurs when individuals lack motivation or cognitive resources. This processing occurs at a

superficial level, allowing the receiver to form judgments based on cues such as credibility, attractiveness, and message length [57] – all of which are key SE techniques. Additionally, heuristic processing takes advantage of the factors embedded within or surrounding a message (heuristic cues) such as its source, format, length and subject in order for the user to perform a validity assessment quickly [12]. Phishing emails exploit these factors the most. If receivers are able and properly motivated, they will elaborate, or systematically analyse, persuasive messages. If the message is well reasoned and logical, it will persuade them [56]. Further, systematic processing takes place when users carefully analyse the message's content and may also conduct further research to validate the message [12].

According to [12], persuasion research studies how received messages can change users' attitudes. The model suggests that people either use heuristics and short-cuts in decision-making, or they systematically process the merits and demerits of a given argument. The HSM and the theory of planned behaviour was linked by [58] through a model of risk information seeking and processing model (RISP). They proposed that the method of information processing users apply to risk information from media and other sources affects their beliefs, evaluations and attitudes.

According to [59], systematic processing is more likely when careful thought is likely to generate judgment confidence. Further, if the message is particularly relevant to the person on a personal level such as their goals or interests.

Ideally, systematic processing would be the preferred method of choice when users are presented with phishing. However, this type of processing requires more effort, time and cognitive resources. As such, users may limit systematic processing unless they are motivated to do so by following motivational factors by [12]: perceived risks, perceived importance of decision outcome, skills level, time and other pressures and the presence/absence of heuristic cues.

Users may process information concerning risks intensively, superficially, or not at all [58]. Unfortunately, users typically trust phishing messages on superficial cues like design and author. If users consider determining the validity of a phishing message or messages received via a SNS as being too time consuming, difficult or unimportant, this may influence users to resort to heuristic processing. As such, this will put them at risk to phishing attacks. Ideally, if users were motivated to systematically process information they receive, checking it for validity, there would presumably be less victims of phishing.

IX. Summary

This paper introduced social network phishing and discussed its similarities with traditional email phishing. It is evident that phishers continue to make use of SE effectively to persuade their victims into performing certain actions, including on SNSs. The paper further discussed a brief literature background of phishing research and how it has progressed from technological controls to psychological theories. It also discussed how SNS users are becoming habituated to behaving in a certain manner which may influence them not to pay closer attention to certain deceptive methods employed on SNSs. This behaviour may influence usage on other platforms such as email. The paper also highlighted habits and information processing models as areas in phishing research that require more attention by researchers. It is only recently that models have been developed which take into consideration habits and information processing. Future research aims to develop a user susceptibility model which considers investigating the linkages between SE techniques, habits and information processing.

References

[1] Statista, "Statistics and facts about Social Networks," 2015. http://www.statista.com/topics/1164/social-networks/

[2] H. Wilcox and M. Bhattacharya, "Countering Social Engineering through Social Media: An Enterprise Security Perspective," 7th International Conference on Computational Collective Intelligence Technologies and Applications (ICCCI 2015), LNAI, Springer, vol. 9330, 2008, pp. 54-64.

[3] K.D. Mitnick and W.L. Simon, The art of deception: Controlling the human element of security. New York, NY: Wiley. 2002.

[4] T. Halevi, J. Lewis, and N. Memon, "A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits," WWW 2013 Companion, Rio de Janeiro, Brazil. ACM. 2013.

[5] A. Ferreira, L. Coventry, and G. Lenzini, "Principles of persuasion in social engineering and their use in phishing," In: Human Aspects of Information Security, Privacy, and Trust. Lecture Notes in Computer Science, 9190 . Springer, Cham, 2015. pp. 36-47.

[6] R. B. Cialdini, Influence: The Psychology of Persuasion. Harper Business, 2007.

[7] D. Gragg, "A Multi-Level Defense Against Social Engineering", SANS Institute - InfoSec Reading Room, Tech. Rep, 2003.

[8] F. Stajano and P. Wilson, "Understanding Scam Victims: Seven Principles for Systems Security", Commun. ACM, vol. 54, no. 3, pp. 70-75, Mar. 2011.

[9] APWG, Phishing Activity Trends Report, 4th Quarter 2014, https://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf

[10] M. Jakobsson and S. Myers, Phishing and countermeasures: understanding the increasing problem of electronic identity theft. 2006

[11] E.E.H. Lastdrager, "Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature," Crime Science,3, 2014.

[12] X. Luo, W. Zhang, S. Burd, and A. Seazzu, "Investigating phishing victimization with the Heuristic-Systematic Model: A theoretical framework and an exploration," Computers and Security, Vol.38, October, 2013, pp. 28-38.

[13] H. King, Top 5 social media scams to avoid, CNN Money, http://money.cnn.com/2016/04/22/technology/facebook-twitter-phishing-scams/

[14] A. Stern, "Social Networkers Beware: Facebook is a Major Phishing Portal," Kaspersky Lab, 23 June 2014, https://blog.kaspersky.com/1-in-5-phishing-attacks-targets-facebook/5180/

[15] J. Allen, L. Gomez, M. Green, P. Ricciardi, C. Sanabria, and S. Kim, "Social Network Security Issues: Social Engineering and Phishing Attacks," Proceedings of Student-Faculty Research Day, CSIS, Pace University, 2012.

[16] Sophos, "Social Networking Security Threats," 2011. https://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats/facebook.aspx.

[17] S. Khandelwal, "Warning – Facebook Color Changer App Is Just A Scam, Infects 10000 Users," 2014. The Hacker News, http://thehackernews.com/2014/08/warning-facebook-color-changer-app-is_9.html

[18] K. Wagstaff, "Hoax Alert! No, Zuckerberg Isn't Giving Millions to Facebook Users," NBC News, 28 December 2015,

http://www.nbcnews.com/tech/social-media/hoax-alert-no-zuckerberg-isnt-giving-millions-facebook-users-n476551

[19] Y. Zhang, J.I. Hong, and L.F. Cranor, "Cantina: a content-based approach to detecting phishing web sites," In: 16th international conference on World Wide Web, ACM. 2007, pp. 639-648.

[20] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," Proceedings of the 16th international conference on World Wide Web. ACM. 2007.

[21] S. Garera, N. Provos, M. Chew, and A.D. Rubin, "A framework for detection and measurement of phishing attacks," Proceedings of the 2007 ACM workshop on Recurring malcode. Alexandria, VA: ACM. 2007, pp.1-8.

[22] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A Comparison of Machine Learning Techniques for Phishing Detection," APWG eCrime Researchers Summit, Pittsburgh, PA, USA. 2007, pp. 60-69.

[23] L. Wenyin, G. Huang, L. Xiaoyue, Z. Min, and X. Deng, "Detection of Phishing Webpages based on Visual Similarity," WWW 2005, ACM

[24] Y. Zhang, S. Egelman, L.F. Cranor, and J. Hong, "Phinding phish: Evaluating anti-phishing tools", 2006.

[25] R. Dhamija, J.D. Tygar, and M. Hearst, "Why phishing works," In: SIGCHI conference on Human Factors in computing systems," Montreal,Canada: ACM. 2006, pp. 581-590.

[26] M. Wu, R.C. Miller, and S.L. Garfinkel, "Do security toolbars actually prevent phishing attacks?," Proceedings of the SIGCHI conference on Human Factors in computing systems: ACM. 2006.

[27] J.S. Downs, M.B. Holbrook, and L.F. Cranor, "Decision strategies and susceptibility to phishing," Proceedings of the second symposium on Usable privacy and security. Pittsburgh, Pennsylvania: ACM. 2006, pp. 79-90.

[28] S. Egelman, L.F. Cranor, and J. Hong, "You've been warned: An empirical study of the effectiveness of web browser phishing warnings," Twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy: ACM. 2008, pp. 1065-1074.

[29] R. West, C.B. Mayhorn, J. Hardee, and J. Mendel, "The Weakest Link: A Psychological Perspective on Why," Social and Human Elements of Information Security: Emerging Trends, 2009, pp. 43-60

[30] M.B. Burns, A. Durcikova, and J.L. Jenkins, "What kind of interventions can help users from falling for phishing attempts: a research proposal for examining stage-appropriate interventions," 46th Annual Hawaii International Conference on System Sciences, 2013, pp. 4023-4032.

[31] I. Kirlappos and M.A. Sasse, "Security education against phishing: A modest proposal for a major re-think," 2009.

[32] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J. Hong, and E. Nunge, "Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish," Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh, Pennsylvania: ACM. 2007.

[33] P. Kumaraguru, Y. Rhee, A. Acquisti, L.F. Cranor, J. Hong, and E. Nunge, "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System," CHI 2007. San Jose, California: ACM. 2007, pp. 905-914.

[34] C.R. Dodge, C. Carver, and A.J. Ferguson, "Phishing for user security awareness," Computers & Security, 26, 2007, pp. 73–80.

[35] S. Gosling, P. Rentfrow, and W. Swann Jr. "A very brief measure of the Big-Five personality domains," Journal of Research in Personality, 2003, pp. 504-528.

[36] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, and J. Downs, "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions," Proceedings of the 28th international conference on Human factors in computing systems. Atlanta, Georgia, USA: ACM. 2010.

[37] C.B. Mayhorn, A.K. Welk, O.A. Zielinska, and E. Murphy-Hill, "Assessing Individual Differences in a Phishing Detection Task," Proceedings 19th Triennial Congress of the IEA, Melbourne. 2015.

[38] J. Parish, J. Bailey, and J.F. Courtney, "A Personality Based Model for Determining Susceptibility to Phishing Attacks," Southwest Decision Sciences Institute, 2009.

[39] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, " Why do some people manage phishing e-mails better than others?," Information Management & Computer Security, Vol. 20 Iss 1 2012. pp. 18-28.

[40] T.N. Jagatic, N.A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," Communications of the ACM. 50 (10). 2007, pp. 94-100.

[41] S. Gupta and P. Kumaraguru, "Emerging Phishing Trends and Effectiveness of the Anti-Phishing Landing Page," 2014.

[42] A. Algarni, Y. Xu, Yue, T. Chan, and T. Yu-Chu, "Social engineering in social networking sites: how good becomes evil," In Proceedings of the 18th Pacific Asia Conference on Information Systems. 2014.

[43] J. Flanagan, "Estate agent forced to go into hiding after Facebook post deriding black people as 'monkeys' for dropping litter on beaches causes a storm in South Africa," 2015, http://www.dailymail.co.uk/news/article-3383844/Estate-agent-forced-hiding-Facebook-post-deriding-black-people-monkeys-dropping-litter-beaches-causes-storm-South-Africa.html.

[44] B. Nikiforova and D.W. Gregory, "Globalization of trust and internet confidence emails," Journal of Financial Crime, vol. 20 Iss: 4, 2013, pp. 393-405.

[45] S. Chhabra, A. Aggarwal, F. Benevenuto, and P. Kumaraguru, "Phi.sh/$oCiaL: The Phishing Landscape through Short URLs," CEAS '11, Perth, Australia:ACM. 2011.

[46] C. Everett, "Social media: opportunity or risk?," Computer Fraud & Security, vol 2010, Issue 6, June 2010, pp. 8-10.

[47] K. Ivaturi, L, Janczewski, and C. Chua, "Effect of Frame of Mind on Users' Deception Detection Attitudes and Behaviours," 2014, CONF-IRM.

[48] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H.R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," Decision Support Systems, 51, 2011, pp. 576–586.

[49] A. Vishwanath, "Habitual Facebook Use and its Impact on Getting Deceived on Social Media," Journal of Computer-Mediated Communication, 20. 2015, pp. 83–98.

[50] T. Priestley, "Is Social Media Just Another Bad Habit To Break?" Forbes, August 2015, http://www.forbes.com/sites/theopriestley/2015/08/13/is-social-media-just-another-bad-habit-to-break/#2c533f9e6f99

[51] M. Limayem, S.G. Hirt and C.M.K. Cheung, "How Habits Limit The Predictive Power of Intention: The Case Of Information Systems Continuance," MIS Quarterly, vol. 31 (4), 2007, pp. 705-737.

[52] R. LaRose and M.S. Eastin, "Social cognitive theory of Internet uses and gratifications: Toward a new model of media attendance," Journal of Broadcasting & Electronic Media, 48(3), 2004, pp. 358–377.

[53] A. Vishwanath, B. Harrison, and Y.J. Ng, (in-press). "Suspicion, Cognition, Automaticity Model (SCAM) of Phishing Susceptibility," Communication Research.

[54] A.H. Eagly and S. Chaiken. The psychology of attitudes. FortWorth,TX: Harcourt Brace and Jovanovich. 1993.

[55] M. Workman, "Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security," Journal of the American Society For Information Science And Technology, 59 (4), 2008, pp. 662–674.

[56] W.D. Crano and R. Prislin, "Attitudes and Persuasion. Annu. Rev. Psychol, 57, 2006, pp. 345–74.

[57] K.A. Cameron, "A practitioner's guide to persuasion: An overview of 15 selected persuasion theories, models and frameworks," Patient Education and Counseling, 74, 2009, pp. 309–317.

[58] R. J. Griffin, K. Neuwirth, J. Giese, and S. Dunwoody, "Linking the Heuristic-Systematic Model and Depth of Processing," Communication Research, vol. 29 No. 6, 2002, pp. 705-732.

[59] ChangingMinds, "Heuristic-Systematic Persuasion Model," http://changingminds.org/explanations/theories/heuristic-systematic_persuasion.htm