Albladi, Samar and Weir, George R S (2016) Vulnerability to social engineering in social networks : a proposed user-centric framework. In: 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). IEEE, Piscataway, NJ, pp. 95-100. ISBN 9781509060962 , http://dx.doi.org/10.1109/ICCCF.2016.7740435

Vulnerability to Social Engineering in Social Networks: A Proposed User-Centric Framework

Samar Albladi and George R S Weir

Department of Computer and Information Sciences

University of Strathclyde

Glasgow, UK

***Abstract*— Social networking sites have billions of users who communicate and share their personal information every day. Social engineering is considered one of the biggest threats to information security nowadays. Social engineering is an attacker technique to manipulate and deceive users in order to access or gain privileged information. Such attacks are continuously developed to deceive a high number of potential victims. The number of social engineering attacks has risen dramatically in the past few years, causing unpleasant damage both to organizations and individuals. Yet little research has discussed social engineering in the virtual environments of social networks. One approach to counter these exploits is through research that aims to understand why people fall victim to such attacks. Previous social engineering and deception research have not satisfactory identified the factors that influence the users' ability to detect attacks. Characteristics that influence users' vulnerability must be investigated to address this issue and help to build a profile for vulnerable users in order to focus on increasing the training programs and education for those users. In this context, the present study proposes a user-centric framework to understand the user's susceptibility, relevant factors and dimensions.**

***Keywords*—** Social Engineering, Social Network, Information Security, Phishing, Deception.

I. INTRODUCTION

Social network users tend to reveal their private information online with ease as they rely on the companies running the networking sites to protect their privacy from criminals and offenders. Users tend to believe that popular companies like Facebook and Twitter will not allow anyone to exploit their users. However, instead of using technical means to exploit the user, social engineers use deception techniques to persuade users to accept an attack. Those attackers usually endeavour to look like an authorised user. Attackers choose their victims carefully to increase the likely success of the attack and to facilitate their next attack. However, no security threat can occur unless there is a vulnerability that can be exploited by the attacker [1].

Research aiming to understand the actions and behaviours that lead to vulnerability exploitations is important to eliminate the success of security exploits. Previous research on social engineering vulnerabilities has focused on factors that make users more vulnerable to social engineering-based attacks, such as personality traits, demographics, and online habits separately, and has never tried to examine their effect together in the same framework in the context of social networking. The present research proposes a user-centric framework in order to build a coherent understanding of user vulnerability to social engineering-based attacks in the social network context.

II. CHARACTERISTICS OF THE VULNERABLE USER

A. Behaviour variables

The definition of user vulnerability to social engineering (SE) is the set of user characteristics that make the user (rather than other individuals) a target for cybercriminals. In the social network (SN) context, users demonstrate their trust by engaging in the network. User behaviour in social networking is considered a determinant of network trust. Social networking users can be classified based upon user characteristics into high and low vulnerable users. One of these characteristics is level of engagement. SN users vary in terms of their engagement between high-active users to low-active users. Cybercriminals are more likely to attack high-active users as they consider them more influential [2]. For example, high-active users may help to guarantee the success of the attack for two reasons. First, high active users have more friends who can be lured easily if the attacker successfully impersonates the victim, who will be considered a credible user [3]. Second, if the victim accepts the friendship request from the attacker, the victim's friends may be deceived by a reverse social engineering technique [4]. Less-active users are users who have fewer engagement features, such as fewer friends, and less frequent use. Such users are not the best targets for the attacker because the attack message may not be seen at all, since the user does not use the SN frequently. Even if the victim falls for the attack, the outcome may not be appealing for the attacker (since there is less information available and fewer friends).

In general, cybercriminals are always looking to take advantage of the victim's account to spread the lure and deceive more victims. Therefore, high-active users are more vulnerable to attack by cybercriminals than less-active users. A study by Vishwanat [2] investigated how Facebook habits can determine the user's vulnerability to social media phishing

attacks, concluding that social engineering victimisation can be predicted by social media users' frequency of use, lack of control over usage-related behaviour and trying to maintain online relationships. However, the study reported in [2] does not explain why Facebook habits lead to user vulnerability to social media phishing attacks. One explanation for this relationship is that Facebook habits may influence users' perceptions, such as risk perception and trust perception, which in turn influence user vulnerability to social media phishing attacks.

B. Perceptual variables

Workman, Bommer and Straub's protection motivation theory [5] suggested that perceived severity of and perceived vulnerability from IS security threats are significant factors in users' security behaviour motivation. Protection motivation theory, as proposed by [6], considered appeals based on fear as a critical assessment factor that causes a change in users' behaviour. According to this theory, when a user faces a threat, four cognitive variables will help them to evaluate the threat: *perceived vulnerability* (estimation of negative outcome), *perceived severity* (how severe the consequences will be if no action is taken), *response-efficacy* (evaluation of individual protection probability if effective behaviour has been performed), and *self-efficacy* (evaluation of individual ability to do effective behaviour). Yet, Downs, Holbrook and Craner [7] found that perceived severity of the consequences of being phished has no relation to users' behaviour and vulnerability to email phishing. However, the study measurement scale concentrated on the perceived severity of the negative consequences of computer malice in general, and did not focus on phishing attacks.

C. Other variables influencing risky behaviour online

Workman [8] presented a grounded theory investigation that revealed how people's responses differ when faced with different persuasion techniques. Some people are persuaded by trust and friendly rapport, while fear tactics influence others. In a later work [9], Workman conducted a field study to examine the effects of two persuasion principles (authority and commitment) in user's behaviour in an international organisation in the USA by sending them a phishing email. The study result indicates that threat assessment, commitment, trust, and obedience to authority were strong factors in the success of social engineering tactics.

Furthermore, some studies have stated that particular personality traits may cause higher phishing vulnerability but have not shown, for example, if there is a correlation between gender and personality traits that cause the victim to be more susceptible to social engineering, although some personality traits may make women more vulnerable while other traits cause men to be more vulnerable. The study by Uebelacker [10] has proposed a framework to explain the influence of the Big Five Personality Traits (i.e., extraversion, neuroticism, agreeableness, conscientiousness and openness) on susceptibility to Cialdini's principles of influence [10a] that are used by social engineers. However, this theory-based framework has yet to be evaluated through empirical studies [10]. Some experimental studies have examined the correlation between the Big Five Personality Traits and email phishing responses [11], [12]. However, Halevi, Lewis and Memon's study [11] found that neuroticism is the factor most correlated to responding to phishing email, while Alseadoon, Othman and Chan [12] found that openness, extraversion and agreeableness are the three personality traits that increase the likelihood of user responses to phishing emails.

Also, there are some contradictory factors, such as gender, age, and education [13], that are repeatedly tested in phishing research. Moreover, some study results claim that younger targets are more vulnerable to deception. However, most of these studies report on limited samples comprised of university students, which make the results difficult to generalise [11], [12], [14].

Some studies have concentrated on the emotional triggers, such as fear, hedonism, and anxiety that gives users the motivation to respond to different phishing email types. One emotional factor that has not been fully tested is trust. In reality, trust is a critical factor in personal interaction and friendship development. People naturally trust others until their actions prove they are not trustworthy. Trust in social networking sites can be classified into two types: medium trust and members trust [15]. Previous studies argue that trusting the social networking site as well as trusting the members of that site leads to greater information sharing [15]. Trust often leads to a reduction in perceived risk of disclosure, which in turn might lead to an increase in the possibility of falling victim to a social engineering attack. The study by Krasnova, Veltri, and Günther [16] revealed that trust in the SNS provider has an impact on users' self-disclosure in individualistic cultures more than in collectivistic cultures. Therefore, cultural values might have an influence on trusting social networking sites and may be one factor that makes some cultures more vulnerable to social engineering than others.

Research in several fields shows that variation in cultural values often leads to different online attitudes, for example, users' self-disclosure in online communities [17], online deception behaviour [18], and social networking sites motivation and usage [19]. Yet, there is little research on the role of culture in vulnerability to social engineering in SNSs.

One report [20] has revealed that culture has an effect on users' vulnerability to email phishing. Some cultural values incline people to be more trustful, helpful and generous. So, such people, being inclined to help more easily and more frequently, are more likely to fall for exploits that play on emotions [20]. This makes it clear that cultural differences may influence users' motivation and behaviour in social networking sites. Another study [21] investigated whether culture has an influence on employees' resistance to phishing in different nations (USA, Sweden, and India). The result showed a difference in employees' behaviours and decision-making in these nations and proved that culture plays a critical role.

III. Framework Attributes

Following extensive literature research on user-related factors that may influence the user's judgment of online attacks, Table 1 shows the attributes that have been chosen to develop a user-centric framework (with their source authors). To construct the framework based on previous studies and theories, the following steps were implemented.

A. Attributes grouped under themes

Attributes have been categorised and grouped under themes according to the attribute's nature in order to facilitate the framework building.

B. Removing overlapping concepts

After grouping the attributes in themes, it was obvious that some attributes are similar and can be merged together to form one attribute. For example, country-specific factors and religion can be represented together by culture.

TABLE 1: CHOSEN ATTRIBUTES

Attribute	Author	Attribute	Author
SN frequency of use	[2]	Culture	[20]
SN usage behaviour control		Country specific factors	
Friendship establishment in SN		Interests	
		Beliefs	
Individual's trust	[22]	Religion	
Risk behaviour		Personal characteristics	
Computer experience at work			
Helpfulness		Intention to resist	[21]
Gender		Security awareness	
Age		IS policy awareness	
Fear		IS training	
Computer self-efficacy		Self-efficacy	
		Computer experience	
Commitment	[8]	Age	
Trust		Gender	
Obedience		Culture	
Reactance			
Age		Personality traits	[11]
Gender		Gender	
Education		Facebook engagement	
Previous victimization		Perceived vulnerability	
		Internet pessimism	
Gender	[14]	Computer expertise	
Age			
Education major		Personality traits	[12]
		Trust	
Gender	[13]	Submissiveness	
Age		Email experience	
Anti-phishing education		Email richness	

Computer expertise, computer experience and email experience are related factors and can be represented by education and knowledge. Moreover, SN habituation variables like frequency of use, number of friends, activity engagement can be grouped under level of involvement. This classification process converts 51 attributes into 13 factors (Figure 1).

A. Framework Construction

The framework is developed to give a full overview of user-centric characteristics that may influence the user's threat detection ability. Figure 1 shows that the themes group the attributes into 4 categories:

User characteristics			
Socio-psychological variables	**Perceptual variables**	**Habitual variables**	**Socio-Emotional variables**
a. Personality traits b. User's demographics: age, gender, education c. Culture	a. Perceived risk of social network activity b. Past experience with social network c. Perceived severity of negative consequences d. Perceived likelihood of negative consequences e. Privacy awareness f. Security awareness g. Self-efficacy	a.Level of engagement: users can be classified as high or less active users based on many variables, for instance, number of friends, number of subscribed groups, status level and frequency of use.	a. Trusting social network provider b. Trusting social network members c. Motivation to use/perceived value
Vunerability Level: High or Low			

FIGURE 1: USER-CENTRIC FRAMEWORK

1. Socio-psychological variables:

Socio-psychological factors are considered one of the main determinants of social engineering victimisation. The following are the most common factors:

a. *Personality traits*: Previous research has investigated the relationship between personality traits and demographic factors such as age, and gender. However, little research has concentrated on the role of those traits on phishing. Personality trait is an important factor that influences and is affected by other factors.
b. *User demographics*: demographic attributes have been studied extensively in previous research [13], [23]. Variables such as age, gender, and education have been considered determinant variables in information security research. There is no difference in users' susceptibility in terms of technical expertise. Users who have a technical job are also vulnerable to social engineering attacks because the sophisticated methods crafted by clever social engineers are hard to detect [24]. Therefore, the present study considers the importance of each demographic variable as an independent variable.
c. *Culture*: Culture is identified as playing a critical role in users' ability to detect deception. Some research in email phishing has taken the first steps toward measuring the impact of culture on users' susceptibility to email phishing [12], [20], but the role of culture in social engineering victimization in social networks needs more research.

2. Perceptual variables

Perceptual variables include all the factors that require the user to engage in interpretation activities or awareness of its boundaries and dimensions, such as the following:

a. *Perceived risk of social network*: can be defined by the user's level of uncertainty whether an online action is worthwhile or not. Perceived risk has many dimensions that will be explored in a future study.
b. *Past experience with social network*: Past online experience is an important measure to anticipate users' computer knowledge generally and security knowledge

specifically [7]. Also, it is important to measure users' past experience with social engineering threats to see whether this helps to increase the users' threat awareness.

c. *Perceived severity of negative consequences*: According to protection motivation theory, when people expect negative consequences, they tend to be more careful and try to implement protective actions [25]. Individuals' perception of threat is a critical factor against social engineering because if the user is unaware of the severity of the threat and the negative consequences that may result in a social network, users will feel safe online and may eventually be easily deceived.
d. *Perceived likelihood of threat*: Becker, Maiman, Care, and Jan [26] proposed a health belief model to predict patient compliance with health and medical advice and found that personal estimate of vulnerability was one of the most productive dimensions. Therefore, the present study assumes that perceived likelihood of being a victim online can encourage safe practice and reduce vulnerability to social engineering-based attack.
e. *Privacy awareness*: Users' actions and activities in order to protect their personal information online.
f. *Security awareness*: Users' actions and attitude to protecting themselves from online security threats.
g. *Self-efficacy*: can be defined by the individual's confidence in his/her ability to protect himself/herself against any undesirable online incidents. Previous research suggested that self-efficacy plays a critical role in users' risky behaviour online as individuals with high self-efficacy are less likely to make risky choices online [27].

3. Socio-Emotional variables

a. *Trusting social network provider*: In reality, trust is considered a critical factor to people's interaction or friendship development. People naturally trust others until their actions prove they are not trustworthy. Trust in the social network context can be classified into two types: medium trust and member trust [15]. Previous studies argue that trusting the social network provider as well as trusting the members of that network lead to greater information sharing [15].
b. *Trusting social network members*: Users who trust social network members usually believe that other social network users are not harmful and that they are trustworthy.
c. *Motivation to use*: Motivation is a substantial cause that makes people engage in specific actions. According to Hong, "a deeper understanding of end-user motivations, beliefs, and mental models is essential for the security community to build effective countermeasures" [28]. Social engineering attackers can utilize these motivations to manipulate and deceive users. For example, those who use social networks for a hedonistic purpose can be offered a free online game to try to encourage them to accept the deceit. Moreover, some researchers have examined the influence of SNS network users' motivation on behaviour such as frequency of use, usage time, and function of use [29], [30]. Since [2] confirms that such motivation has an effect on social engineering victimization, our study assumes that motivation to use social networks in addition to other factors can influence the user vulnerability to social engineering based attacks.

4. *Habitual variables*

a. *Level of engagement*: Users can be classified as more or less active users in a social network based on many variables, for instance, number of friends, number of subscribed groups, number of status updates and frequency of use.

IV. Comparison with similar frameworks

Predicting user susceptibility to social engineering victimization has been an area of focus for many years and a variety of frameworks have been proposed with a view to determining the factors that have the most influence on users' decisions, as a basis for preventing users from falling for social engineering based attacks. The present study analyses those frameworks, in relation to the selected attributes, as a step toward a robust user-centric framework.

A. Framework Review

1. **Phishing susceptibility framework (PSF):** this framework has four dimensions: personal (including culture, age, and gender), experiential (including general, technology, and professional experience), personality traits, and phishing susceptibility (likely to respond, and time to respond). Each of these dimensions plays a significant role in individual susceptibility to phishing attacks [31].
2. **SEPF:** This framework concentrates on the relation between a specific personality traits and susceptibility to Cialdini's principles of influence which are used by most social engineers to deceive victims [10].
3. **Phishing victims' profile (PVP):** The study that presented this framework [23], concluded that user demographic (included age, gender, and education) and personality traits are critical to predicting victim susceptibility to phishing attacks. The study also indicated that Internet usage behaviour has a moderate influence in social engineering victimization.
4. ***Tetri multidimensional approach (TMA)*:** Tetri and Vuorinen [32] developed a framework on the basis of a multi-dimensional approach that relies on three dimensions: persuasion, fabrication, and data gathering. The framework focusses on the users' interpretation of the attack in relation to information

security policy and education more than relying on the socio-psychological attributes of the user.

5. **Alseadoon model (SM):** Alseadoon, Othman, and Chan [12] proposed a framework based on the deception detection model to measure the users' characteristics that influence their email phishing detection behaviour. The model includes limited and focused attributes such as personality traits, trust, submissiveness, email richness and experience.

B. Framework Comparisons

The reviewed frameworks indicate the need for a multidimensional perspective. There are many important factors to consider when examining user susceptibility to social engineering. In contrast to the listed frameworks, our proposed framework affords a more extensive and holistic user-centric model that offers a starting point for future research to understand user susceptibility to social engineering. Table 2 shows a summary of the attributes that have been identified as a basis for comparing frameworks. A tick (√) shows that the attribute is included in the framework. Note that all listed attributes are included in our proposed User-Centric Framework.

TABLE 2: SIMILAR FRAMEWORKS COMPARISONS

Attributes		PSF	SEPF	PVP	TMA	SM
Socio-psychological	Personality traits	√	√	√		√
	Age	√		√		
	Gender	√		√		
	Education	√		√	√	
	Computer knowledge	√				√
	Culture	√				√
Habitual	Level of involvement in social network			√		
Socio-Emotional	Motivation to use social network					
	Trusting social network provider					
	Trusting social network members					√
Perceptual	Self-efficacy					
	Perceived risk of social network					
	Perceived severity of negative consequences					
	Perceived likelihood of negative consequences					
	Past experience	√				√
	Privacy awareness					
	Security awareness				√	

V. CONCLUSION

Studying users' behaviour and perception of social engineering-based exploits is vital to understanding the weak points in users' ability to detect and defeat these attacks. The proposed user-centric framework is based on the integration of insights from existing research literature and relevant theories after conducting an extensive study of the extant literature regarding user characteristics frameworks and related theories. Our future research will attempt to validate the proposed framework.

REFERENCES

[1] D. K. Mulligan and F. B. Schneider, "Doctrine for Cybersecurity," *Daedalus*, vol. 140, no. 4, pp. 70–92, 2011.

[2] A. Vishwanath, "Habitual facebook use and its impact on getting deceived on social media," *J. Comput. Commun.*, vol. 20, no. 1, pp. 83–98, 2015.

[3] A. Algarni, Y. Xu, and T. Chan, "Social Engineering in Social Networking Sites : The Art of Impersonation," *Proc. 11th Int. Conf. Serv. Comput. IEE Comput. Soc.*, pp. 797–804, 2014.

[4] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6739 LNCS, no. March 2010, pp. 55–74, 2011.

[5] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008.

[6] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *J. Psychol.*, vol. 91, pp. 93–114, 1975.

[7] J. S. Downs, M. B. Holbrook, and L. F. Cranor, "Behavioral response to phishing risk," *Proc. anti-phishing Work. groups 2nd Annu. eCrime Res. summit - eCrime '07*, pp. 37–44, 2007.

[8] M. Workman, "Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security," *J. Am. Soc. Inf. Sci. Technol.*, vol. 59, no. 4, pp. 662–674, 2008.

[9] M. Workman, "A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions." Information and Organization 19.4 (2009): 218-232.

[10] S. Uebelacker and S. Quiel, "The Social Engineering Personality Framework," 2014 Work. Socio-Technical Asp. Secur. Trust, pp. 24–30, 2014.

[10a] R. B. Cialdini, "Influence: Science and practice," Boston: Allyn & Bacon, 2001

[11] T. Halevi, J. Lewis, and N. Memon, "Phishing, Personality Traits and Facebook," arXiv Prepr. arXiv1301.7643., 2013.

[12] I. Alseadoon, M. F. I. Othman, and T. Chan, "What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?," in Advanced Computer and Communication Engineering Technology, Springer International Publishing, 2015, pp. 949–962.

[13] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?," Proc. 28th Int. Conf. Hum. factors Comput. Syst. - CHI '10, p. 373, 2010.

[14] T. N. Jagatic, N. a. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Commun. ACM, vol. 50, no. 10, pp. 94–100, 2007.

[15] C. Dwyer, S. R. Hiltz, C. Dwyer, and S. R. Hiltz, "Trust and Privacy Concern Within Social Networking Sites : A Comparison of Facebook and MySpace A comparison of Facebook and MySpace," 2007.

[16] H. Krasnova, N. F. Veltri, and O. Günther, "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," Bus. Inf. Syst. Eng., vol. 4, no. 3, pp. 127–135, 2012.

[17] C. Zhao, D. L. Street, and P. Hinds, "How and To Whom People Share : The Role of Culture in Self-Disclosure in Online Communities," Proc. ACM 2012 Conf. Comput. Support. Coop. Work, pp. 67–76, 2012.

[18] C. C. Lewis and J. F. George, “Cross-cultural deception in social networking sites and face-to-face communication,” Comput. Human Behav., vol. 24, no. 6, pp. 2945–2964, 2008.

[19] K. S. Al Omoush, S. G. Yaseen, and M. Atwah Alma’Aitah, “The impact of Arab cultural values on online social networking: The case of Facebook,” Comput. Human Behav., vol. 28, no. 6, pp. 2387–2399, 2012.

[20] M. Al-Hamar, R. Dawson, and L. Guan, “A culture of trust threatens security and privacy in Qatar,” Proc. - 10th IEEE Int. Conf. Comput. Inf. Technol. CIT-2010, 7th IEEE Int. Conf. Embed. Softw. Syst. ICESS-2010, ScalCom-2010, no. Cit, pp. 991–995, 2010.

[21] W. R. Flores, H. Holm, M. Nohlberg, and M. Ekstedt, “Investigating personal determinants of phishing and the effect of national culture,” Inf. Comput. Secur., vol. 23, no. 2, pp. 178–199, 2015.

[22] W. Flores, H. Holm, G. Svensson, and G. Ericsson, “Using phishing experiments and scenario-based surveys to understand security behaviours in practice,” Inf. Manag. Comput. Secur., vol. 22, no. 4, pp. 393–406, 2014.

[23] A. Darwish, A. El Zarka, and F. Aloul, “Towards understanding phishing victims’ profile,” 2012 Int. Conf. Comput. Syst. Ind. Informatics, ICCSII 2012, pp. 13–17, 2012.

[24] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, “Lessons from a real world evaluation of anti-phishing training,” eCrime Res. Summit, eCrime 2008, 2008.

[25] J. Inouye, Risk Percept. Theor. Strateg. Next Steps Exec. Summ., p. 2, 2014.

[26] M. H. Becker, L. A. Maiman, S. M. Care, and N. Jan, “Sociobehavioral Determinants of Compliance with Health and Medical Care Recommendations Stable URL : http://www.jstor.org/stable/3763271 Accessed : 02-03-2016 11 : 51 UTC Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of,” vol. 13, no. 1, pp. 10–24, 1975.

[27] G. R. Milne, L. I. Labrecque, and C. Cromer, “Toward an understanding of the online consumer’s risky behavior and protection practices,” J. Consum. Aff., vol. 43, no. 3, pp. 449–473, 2009.

[28] J. Hong, “The state of phishing,” Comput. Fraud Secur., vol. 2010, no. 6, pp. 5–8, 2010.

[29] H. Chen, “Relationship between Motivation and Behavior of SNS User,” J. Softw., vol. 7, no. 6, pp. 1265–1272, 2012.

[30] J.-L. Wang, L. A. Jackson, H.-Z. Wang, and J. Gaskin, “Predicting Social Networking Site (SNS) use: Personality, attitudes, motivation and Internet self-efficacy,” Pers. Individ. Dif., vol. 80, pp. 119–124, 2015.

[31] J. L. Parrish Jr., J. L. Bailey, and J. F. Courtney, “A Personality Based Model for Determining Susceptibility to Phishing Attacks,” Southwest Decis. Sci. Inst. Annu. Meet., no. July 2015, pp. 285–296, 2009.

[32] P. Tetri and J. Vuorinen, “Dissecting social engineering,” Behav. Inf. Technol., vol. 32, no. 10, pp. 1014–1023, 2013.