A Hypothesised Model to Examine Susceptibility to Cyber-Social Engineering Through LinkedIn in The Workplace

M. K. N. Alotaibi

School of Computer Science and Statistics, Trinity College Dublin, The University of Dublin, Ireland
e-mail: malotaib@tcd.ie

Abstract

To date, few studies have examined how users are susceptible to Cyber-social engineering (CSE) on social networking sites. Employees using LinkedIn have been found to have difficulties controlling the type of material they post and are therefore vulnerable to attack. A number of studies have presented frameworks to examine if personality traits are associated with vulnerability to cybercrimes, but these and various other human aspects of vulnerability to risks have not been thoroughly examined. This study extends these frameworks by examining the susceptibility of employees to CSE by combining personality traits, personal dispositions, attitudes to risk, habitual behaviours and technological self-efficacy, as well as the impact of their demographic, including structural power (position within the organisation). This study will focus on public sector personnel who are accessing a professional SNS and are working in government organisations and affiliates under the Ministry of Interior, Saudi Arabia. This study will adopt a mixed research method, namely sequential explanatory design.

Keywords

Cyber-social Engineering (CSE), Social Engineering (SE), Personality Traits, LinkedIn, Social Networking Sites (SNS), Victimisation, Susceptibility, Five Factor Model (FFM)

1 Introduction

Over time, social networking sites have become a major repository for all types of personal and demographic data, including groups individuals are affiliated with, whom they are connected with, their streaming updates and personal credentials (Ellison and Boyd, 2013). This has created a vulnerability which can allow criminals access to an organisation's data (Kirichenko, Radivilova and Carlsson, 2018) by using manipulative and persuasive techniques. LinkedIn is a popular professional network platform that has not yet been extensively studied. It is important to examine LinkedIn, since users' motivations in this particular platform differ from other platforms, such as Facebook, and this difference might affect their behaviour and susceptibility.

Users of job-related social networking platforms are motivated by self-presentation and professional advancement (Kim and Cha, 2017). Self-presentation is a form of information disclosure (Bronstein, 2013). As such, individuals who are self-presentation driven are keen to initiate interactions and build relationships

(Schwämmlein and Wodzicki, 2012). These motives of career advancement can be seen as an element that could be exploited by fake recruiter scams. LinkedIn members are found to be significantly more likely than Facebook users to allow public access to their professional and educational data (Zhitomirsky-Geffet and Bratspiess, 2009), but there is little research specifically addressing these users' attitudes and dispositions toward potential cyber risk.

LinkedIn has been portrayed as a site on which users do not need to be concerned about who views their personal information or photos, since the activity on this SNS is geared towards business activities (Cooper and Naatus, 2014). However, a cyber-social engineer could elicit and appropriate available information about the company posted on its LinkedIn profile, such as its addresses, logos and affiliated groups. Then, such an engineer could create a bogus profile, with which they could request a link to employees' SNS profiles, and such attempts are often successful (Silic and Back 2016; Jagatic et al., 2007). A recent counterintelligence study by the German Bundesamt für Verfassungsschutz (BfV), or Federal Office for the Protection of the Constitution, showed that LinkedIn was of interest to the Chinese intelligence services, which gathered employees' personal data. The BfV stated that "the intent is to compromise individuals' computers and their corporate or government access to ultimately penetrate organisations of interest" (TechCentral.ie, 2017).

At the time of writing, there are more than 567 million LinkedIn accounts (Wang and Barrilleaux, 2018). More than 117 million accounts were hacked by a phishing email campaign in 2012. It is reported that the LinkedIn hack ultimately resulted in users' information and credentials being placed on the dark web in 2016 (BBC 2012; Silic and Back 2016; Dellinger 2017). Several recent studies note that the increased numbers of CSE attacks are the result of a lack of training offered to users (Junger, Montoya and Overink, 2017; Terlizzi, deSouza and Cortez da Cunha, 2017). Silic and Back (2016) found that, while employees are periodically made aware of security issues and given training programs to address potential threats in IS environments, the training does not include the online realities of threats involved when using SNS at work. As it is hard to regulate and control SNS usage in the workplace (Vaast and Kaganer, 2013), it is hard to mitigate cyberspace scam victimisation. This is increasingly the case, especially with the growth of the mobile ecosystem and the related increase of IS security threats due to unintentional insider attitudes to potential cyber risk.

2 Review of Literature

CSE is defined as a creative tactic with the main purpose of deploying a network attack to deliver implicit malware or to persuade gullible, curious, greedy, or susceptible individuals to give out personal information, by using techniques such as phishing emails or online impersonation (CERT-UK, 2015), Albladi and Weir (2018) define susceptibility to CSE as "… a set of user attributes that incline…a user to be a victim of social engineering attacks" (p. 4). The attributes that influence the success of victimisation can be internal, such as human factors, personality traits or external, e.g., culture and organisation.

Few studies to date have looked at LinkedIn (Utz, 2016; Silic and Back, 2016b). However, it has been found that LinkedIn users are more likely than Facebook users to allow public access to their details (Zhitomirsky-Geffet and Bratspiess, 2009). Skeels and Grudin (2009) and Silic and Back (2016), when studying workplace users of Facebook and LinkedIn, found that employees often have difficulty controlling the content they post when switching between SNS platforms; in fact, this raises questions as to the adequacy of individuals' ability to control their information and/or efficacy to use the computer.

The information contained on LinkedIn, in particular, can pose a risk for organisations, considering that, in 2008, LinkedIn launched 'Company Profiles' (Samuelson, 2008), a feature that enables organisations to have their own independent profile after a pre-authentication process. Therefore, "social engineers can gather a vast amount of employee information a lot faster" (Scheelen et al., 2012, p. 44) from these profiles, such as job titles, names, email addresses, partnering organisations and upcoming projects. This information can be exploited easily to identify "different staff in different buildings and different departments…the easiest way to build a target list is the business social network, LinkedIn" (Allsopp, 2017, p.68). Such exploitation can be initiated through various weaknesses in internal personal disposition factors.

2.1 Personality Traits

A number of studies have examined the influence of personality traits on susceptibility to cyber-crime. Uebelacker and Quiel (2014) developed a social engineering personality framework (SEPF) to examine personality traits and their relation to persuasion tactics, using Cialdini's principles. However, this framework has never been empirically tested and its validation is questionable as the operationalisation of Cialdini's principles is unknown. The Five Factor Model (FFM) has been used in a study to compare susceptibility to traditional crimes and susceptibility to cyber deception (van de Weijer and Leukfeldt, 2017), however, their study collected data over 2 years, which does not necessarily reflect reality, as people's IS security awareness can improve over time and they did not consider other factors as predictors of personality traits.

Albladi and Weir (2017) investigated how FFM and trust, competence, previous experience, and motivation influence an individual's ability to identify cybercrime in Facebook. Their study used a phishing email experiment, followed by images of CSE tactics used on Facebook, to test students' ability to identify malicious examples. discrepancies in previous research findings when examining personality traits are present and some researchers found that these traits, except extraversion, were associated with reduced propensity to take risks and higher levels of information security awareness (ISA) (McCormac et al., 2017b; Hadlington, 2017; Butavicius et al., 2017). In addition, Salgado (2002) found that personality traits can predict workplace behaviours. The following hypotheses are to be tested in relation to personality traits:

H1: Employees who express high levels of conscientiousness are less susceptible to CSE attacks on LinkedIn than those who express low levels of conscientiousness.

H2: Employees who express high levels of extraversion are more susceptible to CSE attacks on LinkedIn than those who express low levels of extraversion.

H3: Employees who express high levels of agreeableness are more susceptible to CSE attacks on LinkedIn than those who express low levels of agreeableness.

H4: Employees who express high levels of openness to experience are more susceptible to CSE attacks on LinkedIn than those who express low levels of openness to experience.

H5: Employees who express high levels of neuroticism are less susceptible to CSE attacks on LinkedIn than those who express low levels of neuroticism.

Users' risk perception and habitual behaviour have been proven to play a crucial role in susceptibility to CSE (Vishwanath, 2014; Silic and Back, 2016a; Moody, Galletta and Dunn, 2017), but were not considered in when personality characterises investigated by Albladi and Weir's Mediating Factors Model of CSE on Facebook. Thus, it appears that direct examination of the susceptibility of user behaviours to CSE attacks in SNS platforms is at its early stage (Algarni, 2016; Albladi and Weir, 2016).

Saridakis et al. (2016) considered personal and behavioural dispositions, but their study did not look at how FFM could have a link to their findings. Also, the literature reveals that personality traits can correlate to other personality characteristics or personal dispositions, such as self-control and conscientiousness or extraversion.

To the best of the author's knowledge, there is no study which has addressed susceptibility to CSE victimisation by combining personal characteristics associated with other factors, such as personal dispositions, habitual behaviours and other demographic variables, such as age and gender. A study of the relationship between such factors and the perception of cyber risks can provide further explanation of vulnerability to a cybercrime.

2.2 Personal disposition to security and risks of CSE victimisation

Personal disposition includes risk perception, which is the level at which an individual can identify risks (Paek and Hove, 2017) in the context of cyber social engineering victimisation. Risk perception in this research refers to the likelihood an employee can recognise themselves to be at risk. Workman (2007) argues, "when people perceive that risk has diminished, they will behave in a less cautious manner" (p. 317). The literature suggests that employees' goal in LinkedIn is career advancement and self-presentation (Kim and Cha 2017; Vishwanath 2017); the desire to achieve a goal in

cyberspace can increase the propensity to take risks (Nguyen and Kim, 2017) and, thus, could potentially make users fall victim to employment fraud (Kelly, 2017; CSO, 2016) using CSE tactics.

Since risk propensity is mediated by risk perception (Weingart and Sitkin, 1995; Wang et al., 2013; van Schaik et al., 2017) it needs to be considered when examining susceptibility to deception. Also, risky behaviours can be due to users' low self-efficacy to protect their online information (Milne, Labrecque and Cromer, 2009; Di Giunta et al., 2013). Saridakis et al. (2016) found that, in the SNS context, self confidence in one's own ability and skills in computer use is linked to susceptibility to cyber victimisation; for this reason, IT self-efficacy, which is found to correlate with concerns of control over the privacy of users' information, is another dimension where further research is needed.

The following hypotheses are to be tested in relation to personal disposition:

H6: Employees who claim high levels of risk perception are less likely to become susceptible to CSE victimisation on LinkedIn than employees with low levels of risk perception.

H7: Employees with high levels of willingness to assume risk on LinkedIn are more likely to become susceptible to CSE victimisation on LinkedIn than employees with low levels of willingness to assume risk.

H8: Employees who perceive they have control over information (privacy risk) are less likely to become susceptible to CSE victimisation on LinkedIn than employees who perceive they have little control over information (privacy risk).

H9: Employees who claim a high level of IT Self-Efficacy are less likely to become susceptible to CSE victimisation on LinkedIn than employees who express a low level of Computer Self-Efficacy.

2.3 Habitual behaviour

Some studies have considered incorporating habitual variables in models of CSE victimisation risk in the context of SNSs. These variables include, for example, email habits (Vishwanath, Harrison and Ng, 2016), level of involvement (Albladi and Weir, 2018) and social media usage (Saridakis et al., 2016b). The findings of these studies all suggest that a high level of engagement on SNS and constant checking of emails, combined with low self-control, can increase the risk of cyber-attack victimisation in both contexts (email and SNS) (Vishwanath, 2015a; Saridakis et al., 2016; Albladi and Weir, 2018). Therefore:

H10: Employees with high levels of engagement on LinkedIn are more likely to become victims of CSE than those with lower levels of engagement on LinkedIn.

2.4 Demographic factors

The literature has shown that age and gender have relevance in influencing individuals' ability to identify CSE attacks (e.g., phishing emails) (Sheng et al., 2010; Jagatic et al., 2007; Kumaraguru et al., 2010). However, the empirical findings on how age and gender affect individuals' susceptibility to CSE are contradictory. Rocha Flores (2016), Al-Hamar et al. (2010) and Albladi and Weir (2018) found that countries' social differences of inherited cultural, language, religion and customs, especially their collectivist/individualist character, could impact individuals' susceptibility to CSE. Also, Williams et al. (2017) inferred that employees in a "position of relatively low power or status within the organisation, may [be] particularly susceptible to influence attempts" (p. 418)

The following hypotheses are proposed:

H11: Older employees are less likely to become susceptible to CSE risks on LinkedIn than younger employees.

H12: Female employees are more likely than male colleagues to have a cautious attitude towards risks of CSE on LinkedIn.

H13: Employees in a senior position in the organisation are more likely to have a cautious attitude towards risks of CSE on LinkedIn than employees in a junior position.

H14: The nationality of an employee can influence their susceptibility to CSE risks.

3 Proposed Model

The following diagram (see Figure 1) presents the factors that will be investigated in this study. These factors were revealed in the literature and serve to extend Saridakis' (2016) existing model of SNS Risk Victimisation. The model is based on the lifestyle/routine activity theory (LRAT) (Cohen and Felson, 1979) and the theories of planned behaviour and reasoned action (Ajzen 1991; Fishbein and Ajzen 1975; Ajzen 1985). The LRAT theory suggests that an attack is likely to take place based on the activity of a potential victim, the lack of a capable guardian, and the presence of a willing offender. In an online-setting, Leukfeldt and Yar (2016) and Hutchings and Hayes (2009) argue that the lack of ability to manage personal information can have negative consequences for users, which may be compounded by users frequently checking emails, visiting SNSs and/or online shopping. Lack of perception of cyber risks may arise from the absence of guardianship in safeguarding and protection from threat.

Cohen and Felson theorized that individuals' activity outside their homes can increase their likelihood of encountering a motivated-offender; therefore, through the lens of LRAT, level of engagement (activity on SNSs) will be examined. Ajzen and

Fishbein's theories of planned behaviour (TPB) and reasoned actions (TRA) posit that beliefs about 1) outcomes of behaviours, 2) necessary resources (i.e. skills), and 3) perceived beliefs are antecedents of intentions and behaviours. Additionally, a study by Terry and O'Leary (1995) found that self-efficacy should be included in the TPB; in fact, several studies successfully paired self-efficacy with TPB in various behavioural settings, such as predicting alcohol use (Armitage, Conner, Loach, and Willets, 1999) and food choices (Povey, Conner, Sparks, James, and Shepherd, 2000). These theories have been used to explain specific online behaviours and predict particular behavioural intention (Saridakis et al., 2016). For example, willingness to avoid or take risks is considered a behavioural trait involved in decision-making (Trimpop, 1994). TRA and TPB, therefore, are used as a lens to examine susceptibility hypotheses H6, H7, H8, H9, H10, incorporating the Five Factor Model (FFM), H1, H2, H3, H4, H5 and the demographic variables stated in H11, H12, H13, H14.

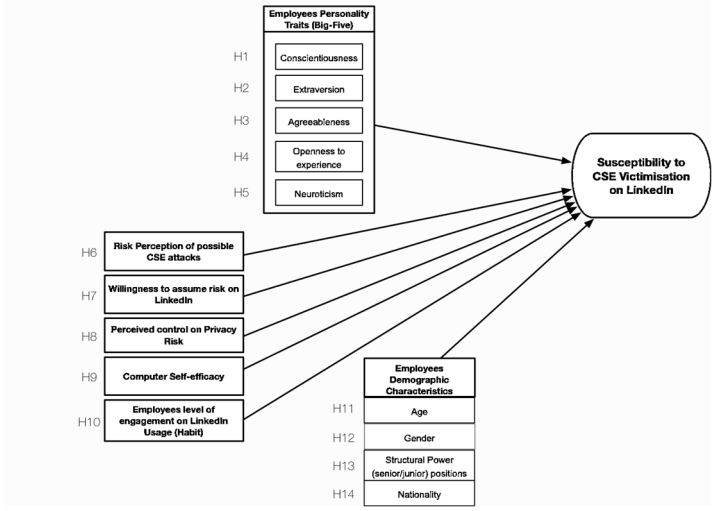

Figure 1: Cyber-Social Engineering - Proposed Model to be Examined

4 Proposed Methodology

Since previous studies examined susceptibility to CSE using quantitative methods, an explanatory mixed-methods design will be used for this study to dig deeper and understand the relationships through an expanded version of Saridakis' (2016) Model of SNS Risk Victimisation (Figure 1), looking at employees of government organisations using LinkedIn. Data will be collected from surveys disseminated to employees working at government agencies in Saudi Arabia which house sensitive data on citizens and expatriates, followed by interviewing experts and some of the same employees. The aim is to find out how and to what extent the hypotheses in the extended model can play a role in employees' susceptibility to CSE over career-oriented SNS (CSNS), such as LinkedIn.

The rationale for using such a method is to bridge the gap between the quantitative and qualitative approaches, as interpretation of findings obtained from just one methodology (quantitatively) is inadequate and limits the insights to be gained. By employing mixed methods, one can ensure that pre-assumptions are less likely from a researcher standpoint, ensuring variation in collected data for greater validity. Also, mixed methods can answer questions from a number of perspectives (Venkatesh et al. 2016).

5 Future Work

This study is part of a project that attempts to explain how and to what extent personal characteristics associated with other factors, such as personal dispositions, habitual behaviours and demographic variables, such as age and gender, can predict susceptibility to cyber-social engineering over professional social networking sites (SNS). This study is novel in that it examines the impact of individuals' position in the power structure in the organisation in relation to CSE susceptibility, as well as their cultural background, using nationality as a proxy measure. The challenge of this research remains in how likely it is that participants can be credible when answering the survey measurements adapted to evaluate these hypotheses, as well as determining the most suitable susceptibility measurement, since, in a social networking site context, unlike CSE in email environments, it can be difficult to deploy real CSE attack scenarios to hundreds of employees and it is also ethically suspect.

6 Conclusion

In the realm of cyber-social engineering, personality characteristics, human perception and behaviours, demographics and an employee's self-efficacy in aspects of information technology, have been predicted to have an impact on employee's safe use over cyberspace. LinkedIn has been perceived as a different context from leisure-oriented SNS platforms, such as Facebook, because users' motivations differ. These differences could cultivate both different intentions of employees when using LinkedIn and, in return, different CSE attacks to induce users to disclose personal information or accept a malicious message. Those who seek career advancement may be tempted to disclose credentials that give access to their organisations and contacts. This project seeks to unearth the characteristics that tend to make unwary employees vulnerable to such indiscretions in their use of professional SNS making them and their organization susceptible to a cyberattack.

7 References

Ajzen, I., 1985. From Intentions to Actions: A Theory of Planned Behavior. In *Action Control*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 11–39.

Ajzen, I., 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), pp.179–211.

Al-Hamar, M., Dawson, R. & Guan, L., 2010. A Culture of Trust Threatens Security and Privacy in Qatar. In 2010 *10th IEEE International Conference on Computer and Information Technology*. IEEE, pp. 991–995. Available at: http://ieeexplore.ieee.org/document/5578490/.

Albladi, S. & Weir, G.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, pp. 1–6.

Albladi, S.M. & Weir, G.R.S., 2018. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8(1), p.5.

Algarni, A.A., 2016. *The impact of source characteristics on users' susceptibility to social engineering victimization in social networks mixed method study based on Facebook*. PhD Thesis. Available at: https://eprints.qut.edu.au/95604/1/Abdullah Ayed M_Algarni_Thesis.pdf [Accessed September 29, 2017].

Allsopp, W., 2017. *Advanced Penetration Testing: Hacking the World's Most Secure Networks*. John Wiley and Sons

Bronstein, J., 2013. Being private in public: Information disclosure behaviour of Israeli bloggers. *Information Research*, 18(4).

Butavicius, M. A., Parsons, K., Pattinson, M. R., McCormac, A., Calic, D., & Lillie, M., 2017. Understanding Susceptibility to Phishing Emails: Assessing the Impact of Individual Differences and Culture. In Human Aspects of Information Security & Assurance.

CERT-UK, 2015. *An Introduction to Social Engineering*. Available at: https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf [Accessed August 29, 2018].

Cohen, L.E. & Felson, M., 1979. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), p.588.

CSO, 2016. *The rise of LinkedIn fraud* | CSO Online. CSO from IDG. Available at: https://www.csoonline.com/article/3036072/social-networking/the-rise-of-linkedin- fraud.html [Accessed February 1, 2019].

Dellinger, A., 2017. LinkedIn Phishing Scam: Compromised Accounts Attack User Messages. *International Business Times*. Available at: https://www.ibtimes.com/linkedin-phishing- scam-compromised-accounts-attack-user-messages-2589093 [Accessed September 14, 2018].

Ellison, N.B. & Boyd, D.M., 2013. Sociality Through Social Network Sites in Dutton, W. H. (ed.), *The Oxford handbook of internet studies*. Oxford University Press.

Fishbein, M. & Ajzen, I., 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Di Giunta, L., Alessandri, G., Gerbino, M., Kanacri, P. L., Zuffiano, A., & Caprara, G. V. (2013)., 2013. The determinants of scholastic achievement: The contribution of personality traits, self-esteem, and academic self-efficacy. *Learning and Individual Differences*, 27, pp.102–108.

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), p.e00346. Available at: http://dx.doi.org/10.1016/j.heliyon.2017.e00346.

Hutchings, A. & Hayes, H., 2009. Routine Activity Theory and Phishing Victimisation. *Current Issues in Criminal Justice*, 20(3), p.20.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F., 2007. Social phishing. *Communications of the ACM*, 50(10), pp.94–100.

Kelly, L. (independent.ie., 2017. Irish engineer claims fake recruiter "catfished" him out of job after contacting him on LinkedIn - Independent.ie. *independent.ie*. Available at: https://www.independent.ie/business/in-the-workplace/irish-engineer-claims-fake- recruiter-catfished-him-out-of-job-after-contacting-him-on-linkedin-35799579.html [Accessed November 26, 2018].

Kim, M. & Cha, J., 2017. A comparison of Facebook, Twitter, and LinkedIn: Examining motivations and network externalities for the use of social networking sites. *First Monday*, 22(11).

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*.

Leukfeldt, E.R. & Yar, M., 2016. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), pp.263–280.

Lyudmyla, K., Tamara, R. & Anders, C., 2018. *Detecting cyber threats through social network analysis: short survey*. Available at: https://arxiv.org/pdf/1805.06680.pdf [Accessed September 3, 2018].

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M., 2017. Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, pp.151–156.

Milne, G.R., Labrecque, L.I. & Cromer, C., 2009. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3), pp.449–473.

Moody, G.D., Galletta, D.F. & Dunn, B.K., 2017. Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, 26(6), pp.564–584.

Nguyen, Q.N. & Kim, D.J., 2017. *Enforcing Information Security Protection : Risk Propensity and Self-Efficacy Perspectives*. Available at: http://hdl.handle.net/10125/41763 [Accessed February 1, 2019].

Paek, H.-J. & Hove, T., 2017. Risk Perceptions and Risk Characteristics. Oxf. Res. Encycl. Commun, 1-14.

Salgado, J.F., 2002. The Big Five Personality Dimensions and Counterproductive Behaviors. International Journal of Selection and Assessment.

Samuelson, M., 2008. Now Companies too have profiles on LinkedIn! | *Official LinkedIn Blog*. LinkedIn. Available at: https://blog.linkedin.com/2008/03/20/company-profile [Accessed January 31, 2019].

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. 2016. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change, 102, pp.320–330.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P., 2017. Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75, pp.547–559.

Scheelen, Y. et al., 2012. The devil is in the details: Social Engineering by means of Social Media. Universieit Van Amsterdam.

Schwämmlein, E. & Wodzicki, K., 2012. What to tell about me? Self-presentation in online communities. *Journal of Computer-Mediated Communication*, 17(4), pp.387–407.

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. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 373-382. ACM

Silic, M. & Back, A., 2016b. The dark side of social networking sites: understanding phishing risks. *Computers in Human Behavior*, 60, pp.35–43.

Skeels, M.M. & Grudin, J., 2009. When social networks cross boundaries. In *Proceedings of the ACM 2009 international conference on Supporting group work* (pp. 95-104). ACM.

Terry, D.J. & O'Leary, J.E., 1995. The theory of planned behaviour: The effects of perceived behavioural control and self-efficacy. *British Journal of Social Psychology*, 34(2), pp.199–220.

Trimpop, R., 1994. *The psychology of risk taking behavior*, North-Holland.

Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE.

Utz, S., 2016. Is LinkedIn making you more successful? The informational benefits derived from public social media. *New Media and Society*, 18(11), pp.2685–2702.

Vaast, E. & Kaganer, E., 2013. Social media affordances and governance in the workplace: An examination of organizational policies. *Journal of computer-mediated communication*, *19*(1),

Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, 17(5), 328-376.

Vishwanath, A., 2015. Diffusion of deception in social media: Social contagion effects and its antecedents. *Information Systems Frontiers*, 17(6), pp.1353–1367.

Vishwanath, A., 2017. Getting phished on social media. Decision Support Systems, 103, pp.70–81.

Vishwanath, A., 2015b. Habitual Facebook Use and its Impact on Getting Deceived on Social Media. Journal of Computer-Mediated Communication, 20(1), pp.83–98.

Vishwanath, A., Harrison, B. & Ng, Y.J., 2016. Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. Communication Research, p.009365021562748.

Wang, D. & Barrilleaux, B., 2018. Spreading the Love in the LinkedIn Feed with Creator-Side Optimization | LinkedIn Engineering. LinkedIn Engineering.

Wang, T., Kannan, K.N. & Ulmer, J.R., 2013. The Association Between the Disclosure and the Realization of Information Security Risk Factors. Information Systems Research, 24(2), pp.201–218.

van de Weijer, S.G.A. & Leukfeldt, E.R., 2017. Big Five Personality Traits of Cybercrime Victims. Cyberpsychology, Behavior, and Social Networking, 20(7), pp.407–412.

Weingart, L.R. & Sitkin, S.B., 1995. DETERMINANTS OF RISKY DECISION-MAKING BEHAVIOR : A TEST OF THE MEDIATING ROLE OF RISK PERCEPTIONS AND PROPENSITY. Academy of Management Journal, 38(6), pp.1573–1592.

Williams, E.J., Beardmore, A. & Joinson, A.N., 2017. Individual differences in susceptibility to online influence: A theoretical review. Computers in Human Behavior, 72, pp.412–421.

Workman, M., 2007. Gaining access with social engineering: An empirical study of the threat. Information Systems Security, 16(6), pp.315–331.

Zhitomirsky-Geffet, M. & Bratspiess, Y., 2009. Professional Information Disclosure on Social Networks: The Case of Facebook and LinkedIn in Israel. Journal of the journal of the journal of the journal of the association for information science and technology, pp.2353–2361.