Employees' Interest in Professional Advancement on LinkedIn Increases Susceptibility to Cyber-Social Engineering: An Empirical Test

Mohammed Alotaibi

Employees' Interest in Professional Advancement on LinkedIn Increases Susceptibility to Cyber-Social Engineering: An Empirical Test

Mohammed Khaled N. Alotaibi [0000-0003-3933-9194]

School of Computer Science and Statistics,

Trinity College Dublin, Dublin, Ireland
malotaib@tcd.ie

Abstract. Social networking sites (SNS) and platforms such as LinkedIn and Indeed are perceived as trustworthy, as they are portrayed as professional, unlike multipurpose platforms, such as Facebook. In career-oriented networking sites (CSNS), aside from self-presentation of credentials, the level of engagement with peers for professional advancement to purposefully amplify one's profile, such as by connecting with someone or, sometimes unwittingly, accepting messages, e.g., for recruitment, can make them a happy hunting ground for cyber-social engineers. This study examines the impact of two variables highlighted as leading motives behind the use of LinkedIn. It presents the findings of research into the ways employees in Saudi public organisations can be susceptible to cyberthreats while accessing the most popular career-oriented social networking site, LinkedIn, while at work.

Keywords: Cyber-Social engineering, LinkedIn, Susceptibility, Professional Advancement, Self-Presentation, Phishing

1 Introduction

This paper presents partial empirical findings of an ongoing project following an explanatory sequential design. It seeks to examine the association between employees' susceptibility to cyber-social engineering (CSE), particularly over career-oriented social networking sites (CSNS), while working in public organisations. The organisations studied offer advanced online e-government services to residents of Saudi Arabia; therefore, any internal or external weaknesses of employees that induce them to respond to malicious requests or messages could greatly jeopardize the system.

25% of the total time people spend on the internet is on SNS [1, 2]. Social engineering takes advantage of the fact that users on SNS platforms are often unaware of potential threats; they do not suspect communication from an unknown origin, or

even believe they might be susceptible to manipulation by cyber-social engineering [3]. This vulnerability leaves organisations open to attack [2]. According to a report by *Sophos*, LinkedIn is among the SN platforms most affected by increased spam and malware incidents [5-7].

Kim and Cha [8] suggested that there are four motivations behind the use of SNSs (Facebook, LinkedIn, Twitter):

1. Expressive information networking;
2. Entertainment, relief from boredom;
3. Professional advancement;
4. Escape through companionship.

They found that the motivations for using Facebook and LinkedIn differ. It is likely that CSE attackers will cultivate skillful influential messages to respond to these motivations, based on the context. For instance, users on LinkedIn use the site for professional advancement (sharing work-related curriculum vitae posts, networking with other professional contacts, obtaining peer support from others, etc.) and, secondly, for self-presentation (providing personal credentials, introducing or telling others about oneself). These motivations can be misused by a social engineer masquerading as an employer, a job-seeker or a colleague [9]. Several studies have looked at how users' personal information can be accessed through manipulative and persuasive tactics in the email environment [10-14].

However, SNSs have become a very attractive means of communication, and they reveal more of a user's character, as well as personal information and interactions (posts, shares, private messaging). It is easy to see how SNSs are becoming an attractive medium for CSE attacks (e.g., phishing links and impersonation) [15-17]. This type of internet crime has a financial impact on organizations infiltrated through an unsuspecting employee; in early 2016, the Internet Crime Complaint Center at the FBI reported that social engineering and associated cyber-crimes cost companies of all sizes across 108 countries more than $2bn between October 2013 and February 2016 [18].

CSE poses a serious threat to information and personal security, through its growing tendency to exploit and misuse social networks and virtual communities [19]. According to Mills [20], social networking sites are considered the new 'battleground' for cyber-attacks, since personal, employment, and other geographic and demographic information are exposed. He stresses that such sites "can be used as a means of social engineering against not only that person but any organization's information security with which this individual is affiliated" (Ibid.). For businesses that increasingly rely on remote collaboration, online channels of communication, online platforms and tools for virtual communication, CSE poses a serious threat to the security of their organizations' data centers. This is exacerbated by the growing trend towards BYOD, or 'bring your own device', which is linked by Krombholz et al. [21] with "policies and the use of online communities, communication and collaboration tools in private and business environments". Combining online tools in both private and business environments provides cyber attackers with many new opportunities for malicious operations.

Phishing attacks, or online scams, a common CSE technique, are easy to launch, since personal information can, at times, be publicly accessed from new media

platforms, such as social networking sites [22]. For instance, Sivasankaran, a security architect and member of a SecureWorks research team, is quoted in [23] as stressing the increase in CSE attacks through the utilization of the user's personal social media accounts. He adds that, "In early 2017, our research team observed phishing campaigns targeting several entities in the Middle East, with a focus on Saudi Arabian organizations". Similar attacks on Reuters are reported in [24].

These attacks are not new but are becoming more frequent and sophisticated in cyberspace throughout the world.

2 Susceptibility influenced by self-presentation and professional advancement

As noted earlier, the literature has shown that the use of career-related SNS platforms usually has two basic motivations; self-presentation and professional advancement [8]. Self-presentation is a form of information disclosure that involves providing personal credentials, and introducing or telling others about oneself [8], in the course of which the user reveals his/her professional identity [25]; consequently, individuals who are self-presentation-driven are more likely to be inclined to build relationships [26].

The goal of professional advancement is to develop a professional future; it is likely to involve sharing work-related career history posts, networking with professional contacts, and obtaining peer support from others.

Motives related to career advancement can be seen as an element that could be exploited by fake recruiter scams, for example, by a social engineer posing as an employer or job seeker, or using the cloned profile of a colleague [9]. As stated by [27], "job candidates are increasingly presenting themselves in online communities to impress employers"; therefore, any active individual who engages in a high degree of professional development and self-presentation behavior exposes herself or himself to cyber social engineering.

LinkedIn members have been found to be significantly more likely than Facebook users to allow public access to their professional and educational data [28], but there is little research specifically addressing these users' attitudes and dispositions toward potential cyber risk in the context of social networking sites generally and specifically over career-oriented SNS.

These considerations lead to two main hypotheses:

H1: Users who are motivated by career advancement on LinkedIn are more susceptible to CSE victimization than those who are less motivated in this way.

H2: Users who are more motivated to present themselves and their credentials on LinkedIn are more likely than others to be susceptible to CSE attacks.

3 Methodology

To explore the association between employees' susceptibility to cyber-social engineering and their inclination for self-presentation and professional advancement, with consideration also given to demographic factors, a survey was distributed to over 460 employees. The employees were selected by purposeful sampling of those who:

- work for a major government organisation, and
- use LinkedIn, and
- use another SNS

Data were collected from employees at an organisation which has access to data provided from the Saudi National Information Centre (NIC) as this portrays the magnitude of the organisation's sensitivity in terms of state security.

After cleaning, 394 responses were considered for data analysis. Males comprise three quarters of the sample (74.9%). The majority of the respondents were aged 29-39 (66.8%), but other age groups were also represented in the sample, with at least 19 people in each. Almost 87% of respondents were Saudis. Most participants were lower-level employees, but mid-level managers and top executives are also represented (20.8% and 4.3%, respectively). Only 0.5% (2 people) of the surveyed sample reported not using any SNS and only 3.3% (13 people) did not use any career-oriented SNS, Table 1 summarizes the distribution of respondents.

The majority of respondents used social networking websites at least sometimes, with LinkedIn being by the far the most popular social networking platform. More than 90% of respondents reported that they used this career-oriented website; in the section of the survey concerning susceptibility to CSE risks, respondents were asked about their experience with LinkedIn. ANOVA and Kruskal-Wallis analyses were conducted to test for significant differences among groups of respondents, using SPSS. Logistic regression was conducted using odds ratio (OR) to interpret relationships and test the hypotheses.

Table 1. Summary of Demographic Data of Survey Respondents (n=394)

Demographics		Count (N)	%
Gender	Female	99	25.1%
	Male	295	74.9%
Age	18 - 28	28	7.1%
	29 - 39	263	66.8%
	40 - 50	44	11.2%
	51 - 61	19	4.8%
	62 and over	40	10.2%
Nationality	Saudi Arabia	342	86.8%
	Non-Saudi (Expatriate)	52	13.2%

Government Organisation Sector Type	Social Development Sector (ORGSDS2)	278	70.6%
	Labour Sector (ORGLS1)	116	29.4%
Work Level in Organisation	Administrative Officer / Assistant (Employee)	295	74.9%
	Department management/Section supervisor or designee	85	21.6%
	Top-level management or designee	14	3.6%

3.1 Measuring Susceptibility

Previous studies in the literature have measured susceptibility by inviting users to click on spear-phishing links. This study, however, will refrain from using experimental scenarios on SNS because of the difficulties of conducting experimental attacks on a large number of participants, as well as for ethical reasons. Therefore, susceptibility measurement used a simple YES/NO question: this constitutes an indirect, non-invasive approach, addressing the binary YES/NO variable in accordance with [29, 30]. This approach was supported by expert academic reviewers in the fields of computer science, organizational psychology and human factors who were consulted on the project.

Participants were asked a binary-type self-report question; "In all the time since you have been using LinkedIn, have you ever had something bad happen (at your work or in your personal life) that you can trace back to your usage of LinkedIn?" Answers were coded (0=No, 1=Yes), and participants were given the option to elaborate further, in an open-ended follow-up question: "If you have answered yes to the question, could you briefly explain what happened and how you knew what you did on LinkedIn was the reason?" This question was reviewed by experts in the field of survey design and industrial and organizational psychology.

3.2 Measuring Self-Presentation and Professional Advancement

Self-presentation is defined as a form of information disclosure [25]. As such, individuals who are self-presentation-driven are keen to initiate interactions and build relationships. Self-presentation involves providing personal credentials and introducing or telling others about oneself.

Because users provide credentials only once, when they create an account, two scales were created to measure and determine the correlation of self-presentation with susceptibility to CSE as discussed in the literature; one was based on profile features requested by the platform, e.g., phone number, work experience, while the other was based on user-initiated activities such as making contacts and sharing files. The first scale is binary, as shown in Table 2; the other is a frequency scale to measure professional advancement, shown in Table 3. Internal consistency was measured for both scales, reporting Cronbach's alpha of .843 and .899 respectively.

The binary scale measures how much information employees put online in relation to their self-presentation, since the more information they put online, the more information cyber social engineers can glean to create a compelling fake profile or other intervention.

Professional development motivates use of LinkedIn in several ways: it is seen as helpful for developing a professional future, sharing work-related curriculum vitae posts, networking with professional contacts, and for obtaining peer support from others. Participants were asked to rate on a scale of 1-5 (never, rarely, sometimes, often, always) how often they used LinkedIn for these purposes.

Table 2. Self-presentation on LinkedIn (Binary questions)

Have you put your work experience history on?
Have you put your Educational history on?
Have you put your licenses on?
Have you put your certificates on?
Have you put your work email address on?
Have you put your work telephone number on?
Have you created an About me Page?
Have you put where you currently work?
Have you put your job title?
Have you put a profile picture?
Have you set your profile to public so anyone can view it?
Have you revealed or updated your current location?
Is your company logo on your profile?

Table 3. Professional Advancement on LinkedIn (Frequency Scale)

Have you connected with professionals that could help you with your professional advancement?
Have you followed other companies that you believe could increase your professional advancement?
Have you shared your work-related CV to companies which you believe could help you with your professional advancement?
Have you shared your work-related CV with professionals with whom you feel can help with your professional advancement?
Have you accepted connections from people whom you don't know but can see that they have many connections themselves?
Have you accepted network connections from people who are connected to your connections?
Have you accepted a connection request on LinkedIn because you recognized the photo?
Have you messaged your connections for support in career or work-related matters?
Have you shared documents, audio or video with connections in order to assist you with a problem?
Have you accepted documents, audio or videos from connections in relation to receiving support from them?

4 Data Analysis Findings

4.1 Susceptibility to cyber-social engineering *(dependent variable)*

24.1% of all respondents responded that they had suffered a bad experience that they could trace to LinkedIn. According to the chi-square test results, males had more negative experiences on LinkedIn than females (28.1% of males compared to 12.1% of females, p=0.023), while Saudis reported more such experiences than non-Saudis (26.0% vs 11.5%, p=0.023). The results also indicate that the higher the work level of the employee in the organization – the less likely respondents were to report negative experiences (28.5% of lower-level employees, 11.8% of mid-level employees and only 7.1% of top-level managers).

No statistically significant association was found between age and susceptibility to CSE victimization; sample estimates suggest that employees aged 51+ were less susceptible to online attacks in CSNS, but the sample size is insufficient to claim that this effect is significant. 44 respondents explained what happened. Even though the consequences of cyberattacks differed widely (viruses, hard drive crashes, creation of fake accounts using the respondent's personal information, stealing of payment details, etc.), most sources of cyberthreat fall into one of a few categories: phishing links sent in messages (46%); phishing emails with links (13%); fake job invitations to get personal/payment information from applicants (13%); using personal information to create fake profiles (7%); paying for fake products and services online (9%); requests to upload documents containing personal information (5%) or to download files which cause problems when opened (5%).

4.2 Self-Presentation *(independent variable)*

The binary scale of self-presentation consists of 13 yes/no items that measure how much information respondents have put online. The more information that is exposed online, the more potential there is for creating a compelling a fake profile or other undesirable cyber-intervention.

A self-presentation score (Table 5) was obtained by calculating the proportion of items put online (minimum = 0, maximum = 100) and a series of ANOVA and Kruskal-Wallis tests was conducted to test for the significance of differences among groups of respondents, based on gender, age, nationality and work level. The average self-presentation score is 44.8%. At the 5% significance level, no demographic differences were found, but at the 10% level, self-presentation is significantly higher (ANOVA p=0.079, Kruskal-Wallis p=0.053) for non-Saudis (M=51.0, SD=23.3) than for Saudis (M=43.9, SD=27.9). Some differences in individual items were significant at the 5% level: non-Saudis, for example, put their certificates and work telephone number on their LinkedIn page more often than Saudis see table 4.

Table 4. Self-presentation information placed online by nationality

Items	Total	Nationality		Chi-square test of association p-value
		Saudi Arabia	Non-Saudi (Expatriate)	
company (or organisation) logo	80.2%	79.8%	82.7%	0.629
put licences on	70.1%	68.4%	80.8%	0.070
put work telephone number on	62.9%	60.8%	76.9%	0.025
put certificates on	58.6%	56.7%	71.2%	0.049
set profile to public so anyone can view it	47.7%	46.8%	53.8%	0.342
created an "About me" page	38.6%	37.4%	46.2%	0.228
put educational history on	37.6%	36.5%	44.2%	0.287
put where currently worked	35.0%	34.2%	40.4%	0.385
put a profile picture	33.8%	34.8%	26.9%	0.263
revealed or updated current location	32.5%	31.9%	36.5%	0.503
put work experience history on	28.9%	28.4%	32.7%	0.521
put work email address on	28.7%	27.8%	34.6%	0.310
put job title	27.9%	26.6%	36.5%	0.137

4.3 Professional Advancement *(independent variable)*:

A professional advancement score was computed as the average of the 10 items and a series of ANOVA and Kruskal-Wallis tests was conducted to test for significant differences among groups of respondents, based on gender, age, nationality, and work level. This analysis indicated that non-Saudis were significantly more actively involved (ANOVA $p=0.017$, Kruskal-Wallis $p=0.019$) in professional development communication on LinkedIn ($M=2.25$, $SD=1.00$) compared to Saudis ($M=2.61$, $SD=1.03$). Non-Saudis were more likely than Saudis to connect with potentially helpful professionals, follow other companies, share their CV to other companies, and both share and accept various files.

4.4 Testing the Hypotheses

Bivariate logistic regressions of susceptibility on self-presentation and professional advancement were performed and the scores are presented in Table 5. The association between self-presentation and susceptibility to bad situations on LinkedIn is insignificant ($p=0.198$). However, an increase in the score characterizing behaviour associated with professional advancement (higher score meaning higher interest in professional advancement) increases the probability of having experienced cybersecurity problems over LinkedIn ($OR=1.048$, $p<0.001$).

The single action related to professional advancement that was most strongly associated with cybersecurity problems traceable to the use of LinkedIn was accepting connections from people who they did not know but who had many connections themselves ($OR=1.439$, $p<0.001$). Therefore, employees should be warned that being

linked with many other people is not a sign of the contact's trustworthiness. The statistical relationship between this action and susceptibility to cyber-social engineering is shown in Table 6. Table 7 summarises the levels of support for hypotheses 1 and 2.

Table 5. Parameter estimates of bivariate logistic regression models (dependent variable: *susceptibility*)

Variables	B	S.E.	Wald	Sig.	Exp (B)[1]
Self-Presentation score	-0.530	0.411	1.661	0.198	0.589
Constant	-0.907	0.216	17.621	0.000	0.404
Professional Advancement Score	0.047	0.012	15.720	0.000	1.048
Constant	-2.302	0.327	49.432	0.000	0.100

Table 6. Parameter estimates of the stepwise multivariate logistic regression model (dependent variable: *susceptibility*)

Item	B	S.E.	Wald	Sig.	Exp(B)
Accepted connections from people whom you don't know but can see that they have many connections themselves	0.364	0.085	18.346	0.000	1.439
Constant	-2.052	0.255	64.650	0.000	0.129

Table 7. Summary of hypothesis-testing results related to the effects of self-presentation and professional advancement on LinkedIn

Hypothesis		**Was evidence supporting the hypothesis found?**
H1:	Users who are motivated by career advancement on LinkedIn are more susceptible to CSE victimization than those who are less motivated in this way.	Yes, at 1% significance level
H2:	Users who are more motivated to present themselves and their credentials on LinkedIn are more likely than others to be susceptible to CSE attacks.	No

[1] Exponentiated coefficients of the logit model (Exp(B)) from the last column of regression tables) correspond to odds ratios, i.e, the number of times the odds of the bad outcome increase if the explanatory variable increases by 1 unit. Odds Ratio equals the exponentiated coefficient of the logistic regression and shows the number of times the odds of having been victimized on LinkedIn increase if the independent variable increases by 1. OR>1 indicates that the higher the value of the independent variable, the higher the risk of victimization.

4.5 Limitations and Recommendations for Future work

The findings of this study emanate from an ongoing project that attempts to examine an extended model pertaining to employees' susceptibility to cyber-social engineering over professional networking platforms in the workplace. One limitation of the current study is that deploying a self-reporting binary question may not precisely expose real-world negative experiences and that employees may be reluctant to admit being victims of cyber-social engineering. However, conducting a scenario-based experiment can be difficult over social media platforms, particularly for legal reasons.

An overall limitation is present at this point, since future work will present findings of how personality characteristics, cognitive and dispositional factors play a role in the risks faced by employees and, consequently, their organisations. There will also be a qualitative phase to dig deeper and unearth how and to what extent these factors, including employees' desire for professional advancement, are a threat to their safe use of career-oriented social networking sites.

5 Conclusion

Cyber-social engineering has proven to be an ongoing issue, whereby cyber engineers adapt their techniques of deceptive messages, based on unsuspecting individuals' needs and behaviours. The current study has shown that top management, as the structural power in the organisation, are less susceptible to CSE attacks on LinkedIn, they do not have a significant association with professional advancement and self-presentation when examining susceptibility to CSE attack. Aspirations for career advancement are shown to be the main reason for people's readiness to share information on LinkedIn. A possible explanation is that professional advancement involves actively contacting various people on LinkedIn and disclosing sensitive information that may be valuable to actual or fake recruiters or potential business partners.

The study also shows that non-Saudis are more likely to share information than Saudis. In addition, non-Saudis show increased levels of activity in professional advancements, which makes them more susceptible to CSE attacks than Saudi employees. The current study has found that nationality is the only demographic characteristic that plays a mediating factor when examining employee's professional advancement and its susceptibility to CSE over LinkedIn. Arguably, this could be due to Saudis having greater job security than non-Saudis, who are generally employed on fixed-term contracts and consequently have an eye open for the next opportunity. Motivation for professional advancement, however, leading to a greater readiness to divulge personal information, appears to be a common factor in making susceptibility greater among lower-level employees than in management, and among expatriate employees than among Saudis.

However, a further qualitative investigation is required to substantiate this interpretation.

References

1. GlobalWebIndex (2016) *GWI Social 2016 - Summary Report.*, *GlobalWebIndex's quarterly report on the latest trends in social networking.* . Available at: https://www.slideshare.net/globalwebindex/globalwebindex-social-q1-summary-report (Accessed: 3 February 2019).
2. Warner-Søderholm, G. et al. (2018) 'Who trusts social media?', *Computers in Human Behavior*, 81, pp. 303–315. doi: 10.1016/j.chb.2017.12.026.
3. George, B. (2016) *Opportunities and Risks in Online Gaming Environments*. University of Plymouth. Available at: http://hdl.handle.net/10026.1/8083 (Accessed: 1 December 2018).
4. Wilcox, H., Bhattacharya, M. and Islam, R. (2014) 'Social Engineering through Social Media: An Investigation on Enterprise Security', *Communications in Computer and Information Science*, 490, pp. 123–134. Available at: http://csusap.csu.edu.au/~mbhattac/pub/ATIS-2014-HW-MB-RI.pdf (Accessed: 30 November 2017).
5. Chi, M. and Wanner, R. (2011) 'Reducing the Risks of Social Media to Your Organization Security Policy and Social Media Use GIAC (GSEC) Gold Certification Security Policy and Social Media Use', *SANS institute*. Available at: https://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749 (Accessed: 4 September 2018).
6. Sophos (2010) *Malware and spam rise 70% on social networks, security report reveals*. Available at: https://www.sophos.com/en-us/press-office/press-releases/2010/02/security-report-2010.aspx (Accessed: 4 September 2018).
7. ITFORCE.IE (2016) *Social Media - one of the biggest threats to an organisations security - IT Force*, *ITFORCE*. Available at: https://www.itforce.ie/blog/social-media-one-of-the-biggest-threats-to-a-organisations-security (Accessed: 30 January 2019).
8. Kim, M. and 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). doi: 10.5210/fm.v22i11.8066.
9. Misra, S. and Goswami, S. (2017) 'Network Routing Fundamentals, Applications, and Emerging Technologies', in *Mobile Agents in Networking and Distributed Computing*, pp. 127–160. doi: 10.1002/9781118135617.ch6.
10. Goel, S., Williams, K. and Dincelli, E. (2017) 'Got Phished? Internet Security and Human Vulnerability', *Journal of the Association for Information Systems*, 18(1), pp. 22–44. doi: 10.17705/1jais.00447.
11. Halevi, T., Memon, N. and Nov, O. (2015) 'Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks', *SSRN Electronic Journal*. doi: 10.2139/ssrn.2544742.
12. Blythe, M., Petrie, H. and Clark, J. A. (2011) *F for Fake: Four Studies on How We Fall for Phish*. Available at: https://www-users.cs.york.ac.uk/~jac/PublishedPapers/FIsForFake.pdf (Accessed: 26 November 2018).
13. Junger, M., Montoya, L. and Overink, F. J. (2017) 'Priming and warnings are not effective to prevent social engineering attacks', *Computers in Human Behavior*. Elsevier Ltd, 66, pp. 75–87. doi: 10.1016/j.chb.2016.09.012.
14. Kleitman, S., Law Id, M. K. H. and Kay, J. (2018) 'It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling'. doi: 10.1371/journal.pone.0205089.
15. Chitrey, A. et al. (2012) 'Institute of Advanced Engineering and Science A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model',

International Journal of Information & Network Security (IJINS), 1(2), pp. 45–53. doi: 10.11591/ijins.v1i2.426.

16. 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: 29 September 2017).
17. Nagy, J. and Pecho, P. (2009) 'Social Networks Security', in *2009 Third International Conference on Emerging Security Information, Systems and Technologies*. IEEE, pp. 321–325. doi: 10.1109/SECURWARE.2009.56.
18. Scannell, K. (2016) *Cyber crime: How companies are hit by email scams*. Available at: https://www.ft.com/content/19ade924-d0a5-11e5-831d-09f7778e7377 (Accessed: 27 November 2017).
19. Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019-2036.
20. Mills, D. (2009) 'Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites', in *2009 Information Security Curriculum Development Conference on - InfoSecCD '09*, p. 139. doi: 10.1145/1940976.1941003.
21. Krombholz, K. et al. (2015) 'Advanced social engineering attacks', *Journal of Information Security and Applications*, 22, pp. 113–122. doi: 10.1016/j.jisa.2014.09.005.
22. Choo, K. R., Smith, R. and McCusker, R. (2007) 'Future directions in technology-enabled crime', *Australian Institute of Criminology 2007*, (78), pp. 53–54. Available at: http://www.aic.gov.au/media_library/publications/rpp/78/rpp078.pdf (Accessed: 27 November 2017).
23. Freer, E. (2017) *SecureWorks talks ransomware, cyber fraud and social engineering | Intelligent CIO Middle East*. Available at: http://www.intelligentcio.com/me/2017/11/01/secureworks-talks-ransomware-cyber-fraud-and-social-engineering-at-gitex/ (Accessed: 27 November 2017).
24. Paul, K. and Auchard, E. (2017) *Saudi agency says country targeted in cyber spying campaign | Reuters*, *Reuters*. Available at: https://www.reuters.com/article/us-saudi-cyber/saudi-agency-says-country-targeted-in-cyber-spying-campaign-idUSKBN1DK27M (Accessed: 7 February 2019).
25. Bronstein, J. (2013). 'Being private in public: Information disclosure behaviour of Israeli bloggers', *Information Research*, 18(4).
26. Schwämmlein, E. and Wodzicki, K. (2012) 'What to tell about me? Self-presentation in online communities', *Journal of Computer-Mediated Communication*, 17(4), pp. 387–407. doi: 10.1111/j.1083-6101.2012.01582.x.
27. Dekay, S. (2009) 'Are business-oriented social networking web sites useful resources for locating passive jobseekers? Results of a recent study', *Business Communication Quarterly*. doi: 10.1177/1080569908330378.
28. Zhitomirsky-Geffet, M., & Bratspiess, Y. (2016). Professional information disclosure on social networks: The case of Facebook and LinkedIn in Israel. *Journal of the Association for Information Science and Technology*, *67*(3), 493-504.
29. Nuno, A. and St. John, F. A. V. (2014) 'How to ask sensitive questions in conservation: A review of specialized questioning techniques', Biological Conservation. doi: 10.1016/j.biocon.2014.09.047.
30. Chaudhuri, A. and Christofides, T. C. (2013) 'A Plea for Indirect Questioning: Stigmatizing Issues of Social Relevance', in Indirect Questioning in Sample Surveys. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–7. doi: 10.1007/978-3-642-36276-7_1.