Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 181 (2021) 59–66

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2020

The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering

Tanja Grassegger, Dietmar Nedbal*

University of Applied Sciences Upper Austria, Wehrgrabengasse 1-3, 4400 Steyr, Austria

Abstract

Social engineering is a form of attack trying to manipulate employees to make them disclose confidential information or perform actions that threatens the security of organizations. The goal of this paper is to study both individual and organizational factors that affect information security awareness of employees and how this leads to intention to resist social engineering attacks. The proposed research model is validated using survey data of 136 employees. The empirical results suggest that leadership and the tendency toward risky behavior are influencing information security awareness of employees. Information security awareness was confirmed as a central factor for information security, whereby the promotion of awareness for information security is indicated as an important aspect to protect a company from potential attacks. The impact of information security awareness on attitude, perceived behavior control and subjective norm in addition to the indirect effect on the intention to resist social engineering, underline the importance of this factor.

Keywords: social engineering; theory of planned behavior; information security; information security awareness

* Corresponding author. Tel.: +43 (0)50804-33415; fax: +34 (0)50804-33499.
E-mail address: dietmar.nedbal@fh-steyr.at

10.1016/j.procs.2021.01.103

1. Introduction

The growing importance of digital information presents not only opportunities but also security risks. The spread of social networking platforms enables attackers to collect personal data of employees via their online footprints. The information obtained in this manner can then be used to facilitate attacks on an organization [1]. As humans make decisions and bear responsibility, the human factor is making an important contribution to the aspect of information security [2]. Even the strongest technical protective measures are useless if an attacker can successfully influence employees [3]. Social engineering is a form of attack in which people are deliberately manipulated to divulge confidential information or to perform actions desired by the attacker that threaten the security of the person or the company [4]. Social engineering attacks include physical, social and technical aspects that are used in the various phases of an attack. Even if such an attack is initially unsuccessful, any insight into individual and organizational security processes can be used for future attacks. This phenomenon is called harvesting [5]. Social engineers use techniques such as (spear) phishing [6–8], pretexting [6,9], dumpster diving [7], shoulder surfing [7,9], reverse (social) engineering [6,7], waterholing [7], baiting [7], or staff impersonation [6,9] to gain access to personal data or secured systems. Employees with a lack of knowledge about such security risks are among the biggest risks in the company [10]. To ensure information security, measures are necessary to promote employees‘ information security awareness [3,11–13].

The object of this paper is therefore to identify individual and organizational factors that affect information security awareness and to examine the influence of information security awareness on the intention to resist social engineering attacks. Section 2 briefly examines related work and proposes hypotheses for this context, which leads to the research model. Section 3 presents the approach and results of the quantitative survey and the evaluation of the research model. Results of the survey are discussed in section 4 and section 5 provides concluding remarks.

2. Background and Hypotheses

An analysis of theories used in related work showed that the theory of reasoned action (TRA) and/or its extension the theory of planned behavior (TPB) is often used [2,14–17]. TPB is a commonly utilized intrapersonal theory to predict behavioral intention and actual behavior [18]. According to TPB, a person’s behavioral intention is determined by three independent factors: (i) the attitude towards the behavior, (ii) the subjective norm, and (iii) the level of perceived behavioral control [18]. In the context of information security policies, behavioral intention is a discretionary question of how a person will behave in terms of complying with information security policies. When viewed from the perspective of social engineering, the determinants influence the intent to resist social engineering attacks, and thus the actual resistance to attack. Gulenko used TPB as a theoretical foundation for the development of an application that raises awareness of security issues in Facebook [14]. Rocha Flores & Ekstedt [2] showed that transformational leadership, information security culture and awareness are determinants that shape the intention to resist social engineering. Saridakis et al. [15] explore the behavior of individual users on social networking sites becoming a victim of cybercrime. Siponen et al. [16] used a multi-theory based model to evaluate factors influencing the intention to comply with information security policies.

TPB was chosen as theoretical basis for the present work because of its applicability with regard to the research topic. As research focuses on information security awareness of employees, it is necessary to extend current research by identifying factors that affect a person’s behavioral intention to resist against social engineering attacks. Thus, the novelty of this research is therefore the development of an innovative model incorporating relevant individual and organizational factors that affect information security awareness and the intention to resist against social engineering attacks. Information security awareness (ISA) is defined as an employee’s individual perception of his/her general knowledge about information security and his/her cognizance of information security policies of his/her organization [2,19]. The construct intention is defined as an employee’s intention to resist social engineering [2]. In the following, several hypotheses are derived from literature. Table 1 provides an overview.

As an organizational factor that affects ISA, the influence of leadership is discussed in literature. In this context, leadership is defined as a leader’s actions to generate awareness and motivate employees to change their information security behaviours, so that all employees can easily and clearly understand the objectives of information security efforts in the organization [2]. Yuryna Connolly et al. conclude that it is important for employees and leaders to share

common values and feel personally responsible for the success of their organization [20]. Rocha Flores & Ekstedt show that the behavior of security executives has a positive influence on the employees [2]. Thus, hypothesis H1 proposes that leadership has a positive impact on the ISA of employees.

Another possibility to promote ISA and motivate employees to act beyond their own interest for the benefit of the group is the declaration of an information security policy. The aim of such a directive is that all employees can clearly and easily understand the purpose of information security measures in the company [2]. Yuryna Connolly et al. found that the establishment of information security policies affect employee actions indirectly through information security awareness [20]. This means that employees' awareness of organizational information security requirements, security threats and the consequences of illegal activities can in turn promote compliant behavior. This leads to hypothesis H2.

Table 1. Proposed Hypotheses

No.	Hypothesis
H1	Leadership has a positive impact on the information security awareness of employees.
H2	Security policies have a positive impact on the information security awareness of employees.
H3	SETA programs have a positive impact on the information security awareness of employees.
H4	The tendency towards high trust negatively affects the information security awareness of employees.
H5	The tendency to take fewer risks positively affects the information security awareness of employees.
H6	Information security awareness of employees has a positive influence on their attitude towards resistance against social engineering.
H7	Information security awareness of employees positively affects the perceived behavioral control.
H8	Information security awareness of employees positively influences the perceived subjective norm.
H9	Information security awareness of employees positively affects the intention to resist social engineering.
H10	The attitude of employees positively affects their intention to resist social engineering attacks.
H11	The perceived behavioral control of employees positively affects their intention to resist social engineering attacks.
H12	The employees' subjective norms positively affect their intention to resist social engineering attacks.

D'Arcy et al. argue that security education, training and awareness programs (“SETA programs”) are necessary to prevent the misuse of information systems [21]. Smith et al. explain that this defense technique not only makes users aware of the results or the attacks that have become known, but also helps them develop a deeper understanding of the underlying principles. By being able to recognize the attacks as such by means of certain characteristics, employees are more likely to identify the threat [13]. Related research also concludes that an effective way to prevent social engineering attacks is to educate employees [22–25]. These findings lead to the formulation of hypothesis H3.

As previously mentioned, individual factors also have an impact on the ISA of employees. Workman [26] discusses the approach of social engineering attacks, in which a potential victim is made to sympathize with the attacker and to trust him by building a relationship. Social engineers use a pattern of trust by exploiting the need for friendship, creating a sense of similarity with the potential victim, faking personal connections, or even pretending to be a famous person. Language and knowledge of situational facts build credibility and confidence to deceive potential victims [27]. Trust in an online environment can be seen as a willingness to rely on others to fulfill their promises and commitments, a belief that others use any personal information in an ethical manner, or a perception that any communication with another party is secure [25]. Yuryna Connolly et al. [20] also treat trust in the context of organizations’ information security. They argue that a high degree of social compatibility leads to a special bond between the employees, whereby they trust each other. Therefore, the hypothesis H4 was derived.

Trust is closely related to the concept of risk [28]. Therefore, the second individual factor that is being of interest for this research is the tendency of an employee’s behavior to take risks. The perceived risk is the factor that helps to predict the likelihood of a person accepting a risk in an uncertain situation [25]. While risk perception differs in individual situations, the attitude to perceived risk remains relatively stable. In the organizational context, employees take risks, such as communicating with strangers online or sharing personal information, which can increase the likelihood of a social engineering attack [15]. In terms of personality, it has been found that more conscientious,

sympathetic and open-minded individuals and those with a propensity to take fewer risks have higher information security awareness [29]. The hypothesis H5 is therefore proposed.

The influence of ISA is seen as a central factor of information security [29,30]. The goal of creating this awareness is to empower employees with information security risks and educate them about their roles and responsibilities. Based on the theory of planned behavior (TPB) [18], it is believed that awareness of information security not only affects employees' beliefs about outcomes, but also directly influences an employee's attitude to information security compliance [19]. Attitude in this context is defined as the degree to which the performance of the information security behavior is positively valued [2]. Additionally, it was shown that an increased ISA has a positive effect on the attitude, as it helps employees better understand the importance of information security measures [20]. In addition, with regard to the factor perceived behavioral control it is crucial for employees to be aware of the threats to information security in order to be able to identify common social engineering techniques and react to it [2]. Perceived behavioral control here is seen as the extent of control the person thinks he/she has of resisting social engineering. Gulenko [14] also states that ISA is a crucial factor in increasing the perceived behavioral control of employees. Further, the influence of subjective norms on the behavior of people is discussed in literature. People thus orient their behavior towards the behavior of their social circle [2]. According to this notion, a person will behave more consciously when the social environment changes [14]. Based on the aforementioned research, the hypotheses H6, H7, and H8 are considered.

Further, Yuryna Connolly et al. [20] discuss ISA as an important factor in encouraging compliant behavior. The results of their study show that employees are more likely to use safe practices when they understand that there is a reason for certain regulations. McCormac et al. show that the knowledge of potential threats and protective measures affects not only the attitude but also leads to compliant behavior [29]. As the collection of data on actual behaviors remains challenging, especially in the field of information security [2] and as, according to the theory of planned behavior, intention is an immediate antecedent of actual behavior [18], this study focuses on capturing employees' intention and considers hypothesis H9.

The central factor of TPB is the intention of an individual to perform a behavior [18]. The stronger the intention in the direction of the actual behavior, the more likely the behavior will actually be carried out. Variations in intention are explained by attitude, perceived behavioral control, and subjective norms. Rocha Flores & Ekstedt found support that these three intrinsic factors directly impact the intention to resist social engineering attacks [2]. Siponen et al. have also shown the positive influence of the three factors on the intention of employees to comply with information security policies [16]. Additional previous work (e.g. [14,22,27,30]) also supports the hypotheses H10, H11, and H12.

3. Empirical Study

Based on the proposed hypotheses, this chapter deals with the empirical study. The research design and the implementation of the survey are described. Then, the collected data is presented and the main results are analyzed.

3.1. Questionnaire design and data collection

The work collected from the literature review in the previous section was analyzed and items used in related studies on the constructs used were identified. The constructs were adapted from other literature and some questions were slightly reformulated to fit the very context of this study (i.e. leadership [2], information security training [21], SETA program [21], trust [25,26], risk [15,28], information security awareness [2,19], attitude [2], perceived behavioral control [2,15,26], subjective norm [2], intention [2,19]). A list of the items relevant for the present study and actual questionnaire design can be obtained from the authors per email. As a response to the questions, a 5-point Likert scale ("strongly agree", "somewhat agree", "neutral", "somewhat disagree", "strongly disagree") was chosen. In addition, the study asked questions regarding the demographics (i.e. gender, year of birth, company size, industry, and the professional background). This study is exploratory, since past research has not addressed all the previously mentioned individual and organizational factors that affect information security awareness of employees in a single study.

To check the questionnaire design for comprehensibility and syntactic correctness, a pretest was carried out with 9 test persons of different age and professional background. As part of the pretest, respondents were asked to provide comments on each question. Based on the comments and results of the pretest, the wording and the arrangement of the questions were slightly revised.

The data was collected using the online survey software QuestionPro in the period from 22.03.2019 to 17.04.2019. The questionnaire was disseminated via various online channels, including Xing and LinkedIn, through its own professional and private network and through the SurveyCircle study platform in German language. A total of 267 people took part in the survey. Then, data was checked for completeness and appropriateness of the content. Due to incomplete answers, 127 records were removed, and a further 4 records were excluded from the results, due to inappropriate answers. Finally, 136 complete and correct responses were used for data analysis.

3.2. Sample characteristics

The sample is divided into 49.3% women and 50.7% men. The majority of the sample is in the age group 25-34 (42%). The age groups 35-44 and 45-54 are each represented in the same proportion in the sample (18%). A similar value applies to the age group 15-24 (17%). The remaining 6 respondents are in the 55+ age group (4%).

Nearly half of the respondents work in companies with over 250 employees (46.7%). The other company size groups show a similar distribution with 17.8% for the group of 50-249 employees, 20.7% for group of 10-249 employees, and 14.8% for the group of companies with less than 10 employees. The sample is within the German-language region and comprises different sectors of activity (IT: 26.9%, production/industry: 26.9%, marketing/communication: 11.2%, service industry: 8.2%, healthcare: 6%, all others below 3%). In terms of job position, there is a good spread across the individual characteristics, with newcomers to the job market (25.7%), respondents having several years' professional experience (36.8%), to respondents working in the middle (11.8%) and top (20.6%) management, as well as self-employed (5.1%).

3.3. Model Evaluation

To analyze the structural model and to evaluate the hypotheses, the PLS-SEM approach was chosen. PLS-SEM is a causal modeling approach that aims to maximize the clarified variance of the dependent latent constructs [31,32]. Variance-based PLS-SEM was used as it is also suitable for a smaller sample size [31,33]. In the first step, the measurement model was evaluated and revised before the path coefficients for the structural model were calculated. Details for these steps are given in the following.

Table 2. Final number of items per construct, Factor loading limits, Cronbach's Alpha, Composite Reliability and Average Variance Extracted

Construct	No. Of items	Factor loadings: min	Factor loadings: max	Cronbach's Alpha (CA)	Composite Reliability (CR)	Average Variance Extracted (AVE)
Attitude (ATT)	3	0.752	0.896	0.794	0.876	0.704
Intention (INT)	6	0.608	0.869	0.872	0.904	0.614
Information Security Awareness (ISA)	5	0.689	0.807	0.810	0.866	0.565
Information Security Training (ISP)	5	0.777	0.837	0.864	0.902	0.647
Leadership (LEAD)	5	0.707	0.897	0.854	0.895	0.631
Perceived Behavioral Control (PERC)	5	0.676	0.818	0.791	0.850	0.533
Risk (RISK)	3	0.686	0.748	0.537	0.758	0.511
Information Security Training (SETA)	5	0.755	0.873	0.857	0.897	0.636
Subjective Norm (SUBN)	4	0.753	0.844	0.813	0.876	0.639
Trust (TRST)	2	0.808	0.865	0.576	0.824	0.701

A reflective measurement model was modelled using SmartPLS (v3.2.8), as the indicators (i.e. items) of the latent constructs are considered to be caused by that factor (i.e. construct) [34,35]. To evaluate the outer model, the convergence and factor loadings were considered first. The analysis of factor loadings at indicator level provides information on how well the indicators are suitable as a measure of the latent construct [33]. A value higher than or close to 0.7 is acceptable for indicator reliability [31]. From the results of the first evaluation several items were dropped since the values were below the threshold. In addition, cross loadings were considered and one additional item was dropped as it similarly loaded to another construct with a value of above 0.6. On the other side, the other

factors with values above 0.6 were kept for analysis, as they did not cross-load with other constructs. With this adaptations, convergence was achieved in eight iterations. An overview of the remaining number of items and the factor loading limits (i.e. minimum and maximum factor loading value of the items) can be found in Table 2.

Then, the reliability and validity of the constructs were evaluated. Table 2 also contains an overview of the results of Cronbach's Alpha (CA), Composite Reliability (CR) and Average Variance Extracted (AVE). CA indicates whether the latent variable indicators have convergent validity and therefore display reliability [36]. Since CA can underestimate the reliability of a scale, CR usually is used as alternative for testing convergent validity. In exploratory studies, values above 0.6 are considered satisfactory for CR [31]. AVE indicates the percent of variance captured by a construct [35]. In an adequate model, factors should explain at least half the variance of their respective indicators (i.e. AVE should be above 0.5) [36]. As shown in Table 2 the CA values for risk behavior (RISK) and trust (TRST) are just below the recommended limit of 0.6 for exploratory studies. However, since the values for both CR and AVE are above the threshold, the two constructs were taken into account in further data analysis.

The inner model was first evaluated by blindfolding through the analysis of the Stone-Geisser's Q^2 value. The Q^2 values were between 0.1 and 0.213 (i.e. all above 0), which confirms the predictive relevance of the structural model [36]. Then the model was checked by bootstrapping to evaluate the significance of the path coefficients. The procedure was performed with 5,000 subsamples and a significance level of 0.1. Critical t-values for a two-step test are 1.65 (significance level $p < 10\%$), 1.96 ($p < 5\%$), and 2.58 ($p < 1\%$). The effect size is used to determine the influence on an endogenous latent variable. A value above the cutoffs 0.35, 0.15 and 0.02 are seen to be "high", "moderate" and "low" respectively [33]. The path coefficients indicate the strength of the relationships between the latent variables. Paths that show no connection or context against the hypothetical direction do not support the postulated hypotheses. Such values lead to the rejection of the corresponding hypothesis.

The final evaluation of the structural model is visualized in Fig. 1. In addition to the path coefficients and the significance level the amount of variances explained (R^2) are presented. Based on significant path coefficients and the other results, the five hypotheses H5, H6, H7, H8, and H10 received strong support ($p < 0.01$), hypothesis H1 showed weak support ($p < 0.1$), and six hypotheses were rejected (H2, H3, H4, H9, H11, H12). Approximately 41.3% of variance was explained for intention to resist social engineering.

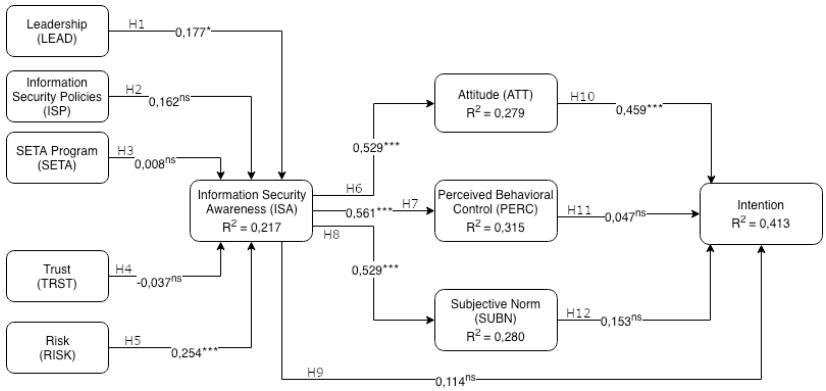

Fig. 1. Results of structural model testing (*…p < 0,1; **…p < 0,05; ***…p < 0,01; ns…not significant)

4. Discussion

Findings show that ISA is influenced by the tendency for risky behavior. Although previous studies have considered risk as a personal factor related to ISA, none of the studies show such a strong influence of this factor. Consistent with McCormac et al. [29] this results suggests that more conscientious, sympathetic and open-minded individuals and those with a propensity to take fewer risks have higher ISA. On the other hand it was not confirmed that the second individual factor "trust" has an impact on ISA.

From the three organizational factors influencing ISA, only a weak connection between leadership and ISA could be proven. In contrast to other research [20,21], results show only a small effect size with no significant path between

security policies and ISA. The same applies to SETA measures and ISA. Although other studies show that especially security policies and training has raised the awareness of information security, it was not supported by this study. Rocha Flores & Ekstedt have found a significant correlation between leadership and ISA [2]. Their study focused on the relationship between leadership and employee engagement in resisting social engineering attacks, but could only fully explain it through the information security culture. The less significant result in the present study could therefore be explained by the lack of consideration of the information security culture in the organization.

The proposed impact of ISA is consistently supported by this study, with the exception of the direct impact on the intention to resist attack. This confirms the results of other studies, such as Rocha Flores & Ekstedt's study [2] with similar factors, as well as the applicability of the theory of planned behavior in the context of the research topic. ISA could thus be identified as a decisive factor, which affects ATT, PERC and SUBN.

In addition, a strong connection between the attitude and the intention to resist social engineering attacks could be identified. This was also confirmed by the studies of Bulgurcu et al. [19], Yuryna Connolly et al. [20], D'Arcy et al. [21], and Rocha Flores & Ekstedt [2].

5. Conclusion

The study centers on the role of employees' ISA and its intention to resist social engineering attacks. From a theoretical perspective, results show the applicability of the theory of planned behavior in the context of social engineering. The results also show that it is important for organizations to understand that technical measures alone are not enough to ensure information security. From a managerial perspective, the promotion of ISA should be central to the development of information security protection measures. As shown, leadership and the tendency towards risky behavior can be considered as important factors influencing ISA. Therefore, an assessment of the tendency toward risky behavior, training and workshops related to awareness-raising activities is recommended for organizations. On the other hand, six hypotheses were rejected, such as, for example, that information security policies and SETA measures had no significant correlation to ISA. Likewise, there was no significant correlation between perceived behavioral control and the subjective norm with the intention of resisting social engineering attacks.

Like most empirical research, it is important to consider limitations of the presented study. The findings of this exploratory study are based on a relatively small sample. Therefore, conducting a survey with a larger sample and with specific target groups would be useful, for example, to allow comparison of countries, or industries or identify differences in employee positions. Another limitation is the use of intention instead of actual behavior. Although previous literature has shown support for using intention as a predictor of actual behavior, there is no guarantee that employees would behave as they have indicated. Therefore, additional studies that use a control group to manipulate certain factors and measure actual user behavior in an experimental design should be carried out.

References

[1] Albladi SM, Weir GRS. User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences 2018;8(1). https://doi.org/10.1186/s13673-018-0128-7.

[2] Rocha Flores W, Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security 2016;59:26–44. https://doi.org/10.1016/j.cose.2016.01.004.

[3] Stirnimann S. Der Mensch als Risikofaktor bei Wirtschaftskriminalität. Wiesbaden: Springer Fachmedien Wiesbaden; 2018.

[4] Hauser D. Social Engineering Awareness in Business and Academia. In: MWAIS 2016 Proceedings; 2016, p. 3.

[5] Bakhshi T. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In: 13th International Conference on Emerging Technologies (ICET); 2017.

[6] Ivaturi K, Janczewski L. A Taxonomy for Social Engineering attacks. CONF-IRM 2011 Proceedings 2011.

[7] Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. Journal of Information Security and Applications 2015;22:113–22. https://doi.org/10.1016/j.jisa.2014.09.005.

[8] Ohaya C. Managing Phishing Threats in an Organization. In: Proceedings of the 3rd Annual Conference on Information Security Curriculum Development. New York, NY, USA: ACM; 2006, p. 159–161.

[9] Alazri AS. The awareness of social engineering in information revolution: Techniques and challenges. In: 10th International Conference for Internet Technology and Secured Transactions (ICITST); 2015, p. 198–201.

[10] Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. Computers & Education 2009;52(1):92–100. https://doi.org/10.1016/j.compedu.2008.06.011.

[11] Mouton F, Leenen L, Malan MM, Venter HS. Towards an Ontological Model Defining the Social Engineering Domain. In: Kimppa K, Whitehouse D, Kuusela T, Phahlamohlaka J, editors. ICT and Society. Berlin, Heidelberg: Springer Berlin Heidelberg; 2014, p. 266–279.

[12] Mouton F, Leenen L, Venter HS. Social engineering attack examples, templates and scenarios. Computers & Security 2016;59:186–209. https://doi.org/10.1016/j.cose.2016.03.004.

[13] Smith A, Papadaki M, Furnell SM. Improving Awareness of Social Engineering Attacks. In: Dodge RC, Futcher L, editors. Information Assurance and Security Education and Training. Berlin, Heidelberg: Springer; 2013, p. 249–256.

[14] Gulenko I. Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. Information Management & Computer Security 2013;21(2):91–101. https://doi.org/10.1108/IMCS-09-2012-0053.

[15] Saridakis G, Benson V, Ezingeard J-N, Tennakoon H. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change 2016;102:320–30. https://doi.org/10.1016/j.techfore.2015.08.012.

[16] Siponen M, Adam Mahmood M, Pahnila S. Employees' adherence to information security policies: An exploratory field study. Information & Management 2014;51(2):217–24. https://doi.org/10.1016/j.im.2013.08.006.

[17] Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior 2008;24(6):2799–816. https://doi.org/10.1016/j.chb.2008.04.005.

[18] Ajzen I. The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes 1991;50:179–211.

[19] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 2010;34(3):523–48.

[20] Yuryna Connolly L, Lang M, Gathegi J, Tygar DJ. Organisational culture, procedural countermeasures, and employee security behaviour. Information and Computer Security 2017;25(2):118–36. https://doi.org/10.1108/ICS-03-2017-0013.

[21] D'Arcy J, Hovav A, Galletta D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 2009;20(1):79–98. https://doi.org/10.1287/isre.1070.0160.

[22] Kruger H, Drevin L, Steyn T. A vocabulary test to assess information security awareness. Information Management & Computer Security 2010;18(5):316–27. https://doi.org/10.1108/09685221011095236.

[23] Vishwanath A, Herath T, Chen R, Wang J, Rao HR. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems 2011;51(3):576–86. https://doi.org/10.1016/j.dss.2011.03.002.

[24] Wahyudiwan DDH, Sucahyo YG, Gandhi A. Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. In: ICSITech: Proceedings 2017 3rd International Conference on Science in Information Technology "Theory and application of IT for education, industry, and society in big data era" October 25-26, 2017, Bandung, Indonesia. New York: IEEE; 2018, p. 654–658.

[25] Wright RT, Marett K. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. Journal of Management Information Systems 2010;27(1):273–303. https://doi.org/10.2753/MIS0742-1222270111.

[26] Workman M. A test of interventions for security threats from social engineering. Information Management & Computer Security 2008;16(5):463–83. https://doi.org/10.1108/09685220810920549.

[27] Stajano F, Wilson P. Understanding scam victims. Communications of the ACM 2011;54(3):70–5. https://doi.org/10.1145/1897852.1897872.

[28] Öğütçü G, Testik ÖM, Chouseinoglou O. Analysis of personal information security behavior and awareness. Computers & Security 2016;56:83–93. https://doi.org/10.1016/j.cose.2015.10.002.

[29] McCormac A, Zwaans T, Parsons K, Calic D, Butavicius M, Pattinson M. Individual differences and Information Security Awareness. Computers in Human Behavior 2017;69:151–6. https://doi.org/10.1016/j.chb.2016.11.065.

[30] Mamonov S, Benbunan-Fich R. The impact of information security threat awareness on privacy-protective behaviors. Computers in Human Behavior 2018;83:32–44. https://doi.org/10.1016/j.chb.2018.01.028.

[31] Hair JF, Ringle CM, Sarstedt M. PLS-SEM: Indeed a silver bullet. The Journal of Marketing Theory and Practice 2011;19(2):139–52.

[32] Hair JF. A primer on partial least squares structural equations modeling (PLS-SEM). Los Angeles: Sage; 2014.

[33] Schloderer M, Ringle C, Sarstedt M. Einführung in die varianzbasierte Strukturgleichungsmodellierung. Grundlagen, Mo-dellevaluation und Interaktionseffekte am Beispiel von SmartPLS. In: Schwaiger M, Meyer A, editors. Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende. München: Vahlen; 2009, p. 573–602.

[34] Eberl M. Formative und reflektive Indikatoren im Forschungsprozess: Entscheidungsregeln und die Dominanz des reflektiven Modells.

[35] Gefen D, Straub D, Boudreau M-C. Structural Equation Modeling and Regression: Guidelines for Research Practice. Communications of the Association for Information Systems 2000;4.

[36] Garson D. Partial Least Squares: Regression & Structural Equation Models. Asheboro, North Carolina: Statistical Associates Publishing; 2016.