Computers & Security 125 (2023) 103038

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign

Simon Vrhovec*, Igor Bernik, Blaž Markelj

University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

ARTICLE INFO

Article history:
Received 19 April 2022
Revised 22 August 2022
Accepted 27 November 2022
Available online 1 December 2022

Keywords:
Social engineering
Cyber security
Computer security
Information security
Awareness intervention
Protection motivation theory
Theory of planned behavior
Privacy concern
Perceived performance of authorities

ABSTRACT

The human factor remains one of the key challenges in cybersecurity despite effective technical countermeasures in place. This study aims to determine what motivates individuals to seek information about social engineering by investigating the determinants of behavioral intention to follow the materials of a social engineering awareness campaign in Slovenia. A quantitative survey of individuals in Slovenia ($N = 542$) aged 15 or older was administered with participants recruited through University of Maribor students. Data were collected on constructs related to the protection motivation theory (PMT) and the theory of planned behavior (TPB) as well as privacy concerns and perceived performance of authorities. The survey instrument was validated with a confirmatory factor analysis. Covariance-based structural equation modeling (CB-SEM) was used to determine relationships between constructs and analysis of differences between students and employed individuals. Results indicate perceived threat, subjective norm, attitude toward behavior and authorities performance are all significant predictors of behavioral intention. The associations between perceived threat and behavioral intention, and privacy concern and attitude towards behavior was not significant among employed individuals. Among students, trust in authorities was not a significant predictor of authorities performance. This study has several implications. The results of this study suggest that fear appeals may be effective in motivating individuals to seek information about social engineering attacks thus improving the effectiveness of awareness campaigns. They also offer some insights into how to improve messaging towards the target populations. Messaging emphasizing perceived threat may directly increase information seeking intention while messaging emphasizing coping with social engineering may do so indirectly through attitude towards behavior. This study also indicates that messaging should be tailored to the target population (e.g., messaging emphasizing perceived threat may be much less effective for employed individuals than students).

1. Introduction

Cyberattacks targeting organizations and individuals online are wide-spread. Although effective technical countermeasures are in place, the human factor remains one of the key challenges of cybersecurity today (Branley-Bell et al., 2021; Choi et al., 2018). Social engineering attacks, such as phishing and scams, are prevalent (Mansoori and Welch, 2020; da Silva et al., 2020). They are considered as dangerous to a variety of internet users and a world-wide problem for different sectors as well as the general population (Jansen and van Schaik, 2019). Social engineering and cyberattacks in general may pose an even greater challenge for organizations that allow their employees to work from home and support the work-family balance (Žnidaršič and Bernick, 2021). Many cybersecurity experts and scholars consider cybersecurity awareness education and training as one of the most significant measures to counter online threats (Back and Guerette, 2021; Mihelič et al., 2019). Research on interventions however shows mixed results regarding their effectiveness (Back and Guerette, 2021; Gordon et al., 2019; Ikhalia et al., 2019; Kim et al., 2020; Tschakert and Ngamsuriyaroj, 2019; Weaver et al., 2021). Nevertheless, few alternatives to deal with social engineering threats exist fueling the need to improve their effectiveness. There are four key types of cybersecurity interventions: *education* (developing knowledge about online threats and how to mitigate them), *training* (developing information security skills), *awareness-raising* (warning about online threats and providing countermeasures) and *design* (nudges that gently push users to perform the right

* Corresponding author.
E-mail address: simon.vrhovec@um.si (S. Vrhovec).

https://doi.org/10.1016/j.cose.2022.103038

behavior) (Jansen and van Schaik, 2019). Since research investigating why people seek information about social engineering protection seems to be particularly scarce (Lemay et al., 2020; Williams and Joinson, 2020), we focus on a general public social engineering awareness campaign to study the determinants of the success of such interventions from the perspective of the target population.

Several theories have been applied to the broader context of cybersecurity. The two most established theories are the *protection motivation theory* (PMT) and the *theory of planned behavior* (TPB) (Kuppusamy et al., 2020). Both theories were applied to a range of specific information security behaviors (Williams and Joinson, 2020), such as information security policy compliance (Herath and Rao, 2009) and adoption of anti-malware technology (Boss et al., 2015), as well as related topics, such as how information security training affects threat and coping appraisal which are the essence of PMT (Abraham and Chengalur-Smith, 2019).

PMT and related theories (e.g., *technology threat avoidance theory* – TTAT) have been applied to the context of interventions in various areas, such as preventative health behavior (Ghaffari et al., 2020; Havaei et al., 2021; Heydari et al., 2021; Hoseini et al., 2021; Mohammadi et al., 2020; Okuhara et al., 2020; Sadeghi et al., 2020; Wong et al., 2021), computer security (Bax et al., 2021; Jiow et al., 2021) and privacy-preserving behavior online (Strycharz et al., 2021). Similarly, TPB has been applied to study interventions in areas, such as preventative health behavior (Berkley-Patton et al., 2019; Norman et al., 2019; Rhodes et al., 2021; 2020; Sinclair et al., 2019; Siuki et al., 2019; White et al., 2018; Zhao et al., 2019) and work safety (Jafaralilou et al., 2019). PMT and TPB have been also applied to the context of social engineering albeit such research seems to be particularly scarce (Williams and Joinson, 2020). For example, PMT has been employed to examine the motivation of users to learn about phishing (Lemay et al., 2020; Williams and Joinson, 2020), TTAT to study how social network users can persuade each other to engage in raising their awareness about social engineering malware threats (Ikhalia et al., 2019), and TPB to explain why employees click on phishing links (Jalali et al., 2020). PMT and TPB research on awareness raising interventions is therefore dominated by the healthcare domain with some research in the computer security and privacy areas.

In general, both theories have been often applied concurrently, e.g., to explain behavior related to the COVID-19 epidemic (Hanson et al., 2021; Margraf et al., 2020; Masser et al., 2020; Prasetyo et al., 2020; Rodríguez-Priego and Porcu, 2021; Sharma et al., 2021; Weston et al., 2020; Youn et al., 2021), tourism-related behavior (Al-Gasawneh and Al-Adamat, 2020; Seow et al., 2021), purchasing intentions (Boobalan and Nachimuthu, 2020; Pang et al., 2021), compliance with emergency notifications (Rogers et al., 2020), mobile health apps (Zhang et al., 2019), pollution-related behavior (Wang et al., 2019), risky driving (Yang et al., 2019) and climate adaptation (Schwaller et al., 2020). In the cybersecurity context, the simultaneous application of both theories was used to investigate employees' security compliance (Aigbefo et al., 2020; Aurigemma and Mattson, 2019; Herath and Rao, 2009; Hina et al., 2019; Khan and AlShare, 2019; Rajab and Eydgahi, 2019), behavior during phishing attacks (Shahbaznezhad et al., 2020) and password security (Grimes and Marquardson, 2019). Although there were several attempts at combining both theories, only a few focused on social engineering and none on interventions aiming to prevent it.

In this paper, we will address the above presented gaps in our understanding of what motivates people to seek information about social engineering. This paper makes three key contributions to the literature. First, this is one of the first studies examining the determinants of behavioral intention to follow a social engineering awareness campaign therefore contributing to the literature on cybersecurity interventions. Second, this study contributes to the literature on protection motivation and cognitive decision making by applying a tightly integrated PMT and TPB as theoretical lens and enriching the theory with new factors related to privacy concerns and perceived performance of authorities. Third, this study examines how behavioral intention to follow a social engineering awareness campaign differs between students and employed individuals thus contributing a new perspective to the literature on cybersecurity interventions.

2. Research model

In this study, we propose and empirically test a research model presented in Fig. 1. The model aims to explain the behavioral intention of respondents, namely, their intention to seek information on social engineering as a way to protect themselves against it. To achieve this, it synthesizes PMT and TPB into a unified framework by taking some ideas from the decomposed TPB (Taylor and Todd, 1995) and previous syntheses of PMT and TPB (e.g., Boobalan and Nachimuthu (2020), Grimes and Marquardson (2019), Herath and Rao (2009)). Additionally, it builds on current research on perceived performance of authorities (e.g., Crow et al. (2017)), and privacy concern (e.g., Belkhamza and Niasin (2017), Fujs et al. (2019), Sharma et al. (2021)).

PMT aims to explain how people respond to fear appeals, such as cybersecurity messaging (Johnston et al., 2019). Fear appeals first trigger threat appraisal followed by coping appraisal (Mousavi et al., 2020). Fear and perceived threat play varying roles in different variations of PMT and related theories (Vrhovec and Mihelič, 2021). The first two versions of PMT do not include fear and consider perceived threat as a second-order construct formed by perceived susceptibility and perceived severity (Maddux and Rogers, 1983). The third version of PMT includes fear as a partial mediator between perceived susceptibility and vulnerability, and protection motivation (Boss et al., 2015; Floyd et al., 2000). Although the extended parallel process model (EPPM) theory places fear similarly at first sight, it does not associate fear with protection motivation but rather with reactance (i.e., coping with fear instead of coping with the threat) (Witte, 1994). Recent research suggests that perceived threat may be a better predictor of protection motivation than fear as people use cognitive strategies instead of emotions when dealing with threats (Johnston et al., 2019; Vrhovec and Mihelič, 2021). Perceived threat is considered as a first-order construct in TTAT and recent PMT studies (Liang and Xue, 2010; Vrhovec and Mihelič, 2021). Studies that would include both perceived threat and fear in their research models are rare. Most PMT studies include fear as a (partial) mediator but not perceived threat as a first order construct (e.g., Bax et al. (2021)) while TTAT studies typically do not include fear (e.g., Ikhalia et al. (2019)). Nevertheless, studies show that perceived threat is positively associated with both behavioral intention and fear (Vrhovec and Mihelič, 2021). Based on existing PMT, EPPM and TTAT research, we therefore suggest the following hypotheses:

- *H1a*: Perceived severity is positively associated with perceived threat.
- *H1b*: Perceived vulnerability is positively associated with perceived threat.
- *H2a*: Perceived threat is positively associated with behavioral intention.
- *H2b*: Perceived threat is positively associated with fear.

TPB is one of the most influential explanations of human behavior (Jalali et al., 2020). It predicts that perceived behavioral control, subjective norm, and attitude towards behavior predict actual behavior (Rajab and Eydgahi, 2019). In the context of cybersecurity,

Das Modell zielt darauf ab, die Verhaltensabsicht der Befragten zu erklären, nämlich ihre Absicht, Informationen über Social Engineering zu suchen, um sich dagegen zu schützen.

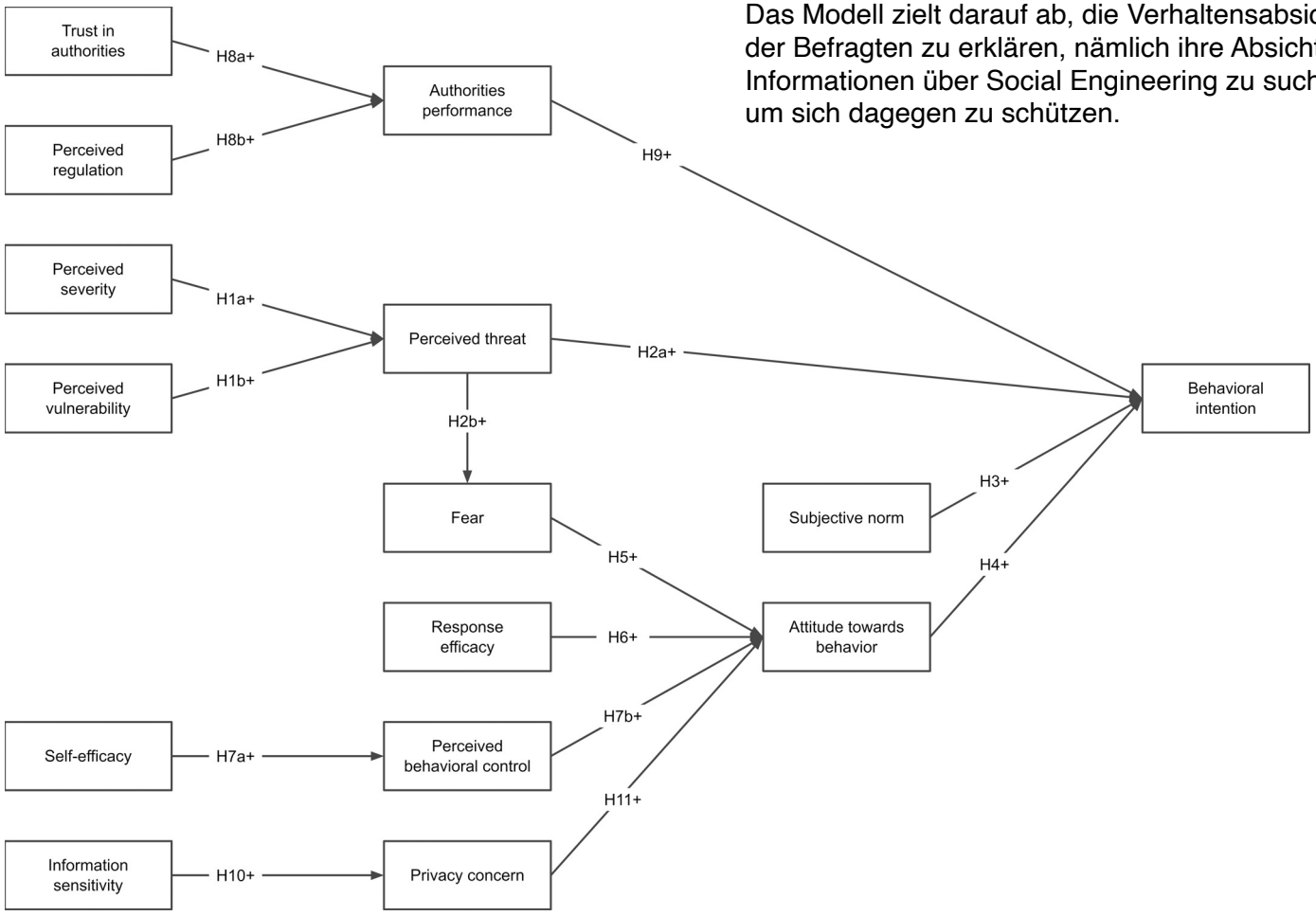

Fig. 1. Integrated framework for information seeking intentions.

several studies showed that secure behavior is associated with attitude (Aigbefo et al., 2020; Aurigemma and Mattson, 2019; Grimes and Marquardson, 2019; Hina et al., 2019) and subjective norm (Aigbefo et al., 2020; Aurigemma and Mattson, 2019; Grimes and Marquardson, 2019; Herath and Rao, 2009; Hina et al., 2019; Khan and AlShare, 2019; Shahbaznezhad et al., 2020). We therefore develop the following hypotheses based on TPB:

H3: Subjective norm is positively associated with behavioral intention.

H4: Attitude towards behavior is positively associated with behavioral intention.

Studies combining PMT and TPB showed that security breach concern affects attitude towards information security policy (Herath and Rao, 2009). We however integrate TPB more directly with PMT. Concerns are context-specific manifestations of fear (Mousavi et al., 2020; Vrhovec and Mihelič, 2021; Xu et al., 2011). Instead of its manifestations, we assume that fear may be directly associated with attitude towards behavior in this study. Thus, we propose the following hypothesis:

H5: Fear is positively associated with attitude towards behavior.

Coping appraisal according to PMT includes response efficacy and self-efficacy (Floyd et al., 2000; Mousavi et al., 2020; Vrhovec and Mihelič, 2021). Previous syntheses of PMT and TPB indicate that it is likely that individuals who believe that their actions are effective (i.e., response efficacy) will have a more positive attitude towards behavior (Boobalan and Nachimuthu, 2020; Grimes and Marquardson, 2019; Herath and Rao, 2009; Masser et al., 2020; Pang et al., 2021; Youn et al., 2021; Zhang et al., 2019). Thus, we propose the following hypothesis:

H6: Response efficacy is positively associated with attitude towards behavior.

According to TPB, perceived behavioral control is a belief about the presence of factors that may facilitate or impede a certain behavior (Herath and Rao, 2009). The *decomposed theory of planned behavior* (DTPB) (Taylor and Todd, 1995) associated perceived behavioral control with self-efficacy and resource facilitating conditions. Later studies integrating TPB and PMT in the cybersecurity domain however mostly excluded perceived behavioral control from their research models. A few studies in other domains alternatively excluded self-efficacy instead of perceived behavioral control (e.g., Boobalan and Nachimuthu (2020), Rogers et al. (2020)). The reasons for excluding perceived behavioral control and self-efficacy vary between studies and often seem somewhat vague. For example, Herath and Rao (2009) included self-efficacy and resource availability as a replacement for perceived behavioral control based on guidance from DTPB. Similarly, Sharma et al. (2021) included self-efficacy as the most relevant factor for perceived behavioral control in the context of adopting COVID-19 contact tracing apps. Next, Hina et al. (2019) excluded perceived behavioral control because of its similarity with self-efficacy. Some studies in other domains provided similar reasoning (e.g., Pang et al. (2021)). Grimes and Marquardson (2019) went further and simply equalized perceived behavioral control with

self-efficacy like certain studies in other domains (e.g., Prasetyo et al. (2020), Wang et al. (2019), Zhang et al. (2019)). In some cases, the reasoning for excluding perceived behavioral control or self-efficacy is not provided at all in the cybersecurity (e.g., Shahbaznezhad et al. (2020)) as well as other domains (e.g., Boobalan and Nachimuthu (2020), Masser et al. (2020), Rodríguez-Priego and Porcu (2021), Rogers et al. (2020), Yang et al. (2019)). Finally, studies in the cybersecurity domain also excluded both constructs (e.g., Aigbefo et al. (2020)) or did not attempt to integrate tightly PMT and TPB while keeping all constructs in their research models (e.g., Aurigemma and Mattson (2019), Rajab and Eydgahi (2019)). As a side effect, the latter studies provided some empirical evidence supporting the distinction between self-efficacy and perceived behavioral control as separate constructs.

In this study, we build on the original idea from DTPB (Taylor and Todd, 1995) associating self-efficacy with perceived behavioral control. DTPB and some later studies place perceived behavioral control as a mediator between self-efficacy and behavioral intent (Taylor and Todd, 1995; Youn et al., 2021). If an individual believes that he or she has the ability to perform a certain behavior, he or she is also likely to have more positive feelings (i.e., attitude) towards it (Herath and Rao, 2009). The literature suggests that both self-efficacy (Grimes and Marquardson, 2019; Herath and Rao, 2009; Pang et al., 2021; Zhang et al., 2019) and perceived behavioral control (Boobalan and Nachimuthu, 2020) may be associated with attitude towards behavior. Therefore, we place perceived behavioral control in a novel way as a mediator between self-efficacy and attitude towards behavior, and pose the following hypotheses:

H7a: Self-efficacy is positively associated with perceived behavioral control.

H7b: Perceived behavioral control is positively associated with attitude towards behavior.

Authorities performance relates to the ability of state authorities to achieve effective results when dealing with social engineering (Crow et al., 2017). Research suggests that several factors influence the public perception of authorities performance, such as crime rates and general public climate towards them (Crow et al., 2017). We assume that trusting beliefs towards state authorities (i.e., the perception of individuals that state authorities possess characteristics that would benefit them (McKnight et al., 2002)) reflect the general climate towards authorities. The perceived protection of privacy provided by privacy regulation has been associated with privacy concern Fujs et al. (2019). Similarly, regulation may be perceived as providing a framework that addresses the overall social engineering crime rates. Both trust in authorities and perceived regulation may thus be associated with perceived performance of authorities which may be in turn associated with individuals' intention to seek information provided by them. Based on the presented assumptions, we introduce these theoretical concepts to the cybersecurity domain and develop the following hypotheses:

H8a: Trust in authorities is positively associated with authorities performance.

H8b: Perceived regulation is positively associated with authorities performance.

H9: Authorities performance is positively associated with behavioral intention.

Privacy literature mostly revolves around privacy calculus and privacy paradox (Belanger and Crossler, 2019). These theories indicate that, although individuals are concerned about their privacy, they do not always engage in privacy-protecting behavior and empirical studies have produced varying results (Belanger and Crossler, 2019; Fujs et al., 2019; Rowe et al., 2020; Williams and Joinson, 2020). Social engineering attacks can take advantage of publicly available information related to the victims. Perceived information sensitivity has been proven to affect concerns about privacy (Fujs et al., 2019). It is however unclear whether individuals who may be less privacy-savvy (i.e., are less concerned about their privacy) are more or less likely to seek information about social engineering. Attitude towards behavior has been identified as a potential mediator between privacy concern and behavioral intention (Arpaci et al., 2015; Belkhamza and Niasin, 2017; Heirman et al., 2013; Mahrous, 2011; Sharma et al., 2021). We develop the last set of hypotheses based on these considerations:

H10: Information sensitivity is positively associated with privacy concern.

H11: Privacy concern is positively associated with attitude towards behavior.

3. Materials and methods

3.1. Research design

This study employed a cross-sectional research design to determine what motivates individuals to seek information about social engineering. A survey was conducted to investigate the determinants of behavioral intention to follow the materials of an on-going social engineering awareness campaign in Slovenia. The awareness campaign in the focus of this study is a continuous effort by the Slovenian national computer security incident response team (SI-CERT) aiming to raise the awareness of the general population by providing information on social engineering (e.g., how to recognize social engineering, how to protect against it, how to respond when incidents happen). Awareness campaign materials can be reached through various communication channels, such as Facebook, YouTube, the official campaign mailing list, and the official campaign website. In this study, we consider "following awareness campaign materials" as a way of seeking information on social engineering similarly to how Williams and Joinson (2020) consider "keeping up to date with phishing techniques" as seeking information on phishing.

3.2. Ethical considerations

This study did not require an approval from the Institutional Review Board according to the legislation of the Republic of Slovenia and internal acts of the University of Maribor.

3.3. Measures

Theoretical constructs were defined and operationalized as presented in Table 1. Most questionnaire items were taken from previously validated research and adapted to the context of the study. We developed a couple of new items for existing theoretical constructs. All theoretical constructs were modeled as first-order reflective constructs. Two items for *perceived severity* were adapted from Fujs et al. (2019) and one item from Moody et al. (2018). Two items for *perceived vulnerability* were taken from Fujs et al. (2019) and Jansen and van Schaik (2018), and a third item was developed for this study. Two items for *perceived threat* were adapted from Fujs et al. (2019) and one item from Liang and Xue (2010). Two items for *fear* were taken from Osman et al. (1994) and Jansen and van Schaik (2018) while a third item was developed for this study. One item for *subjective norm* was adapted from Venkatesh et al. (2003) and two items from Park and Smith (2007). Items for *attitude towards behavior* were adapted from Moody et al. (2018); Venkatesh et al. (2003) and Park and Smith (2007). Two items for *perceived behavioral control* were adapted from Park and Smith (2007) and one item

Table 1
Definitions of theoretical constructs.

Theoretical construct	Operational definition
Perceived severity [PS]	The perceived extent of consequences of a successful social engineering attack.
Perceived vulnerability [PV]	The perceived probability of a successful social engineering attack.
Perceived threat [PT]	The perceived extent of threats to the individual posed by social engineering attacks.
Fear [F]	The level of the individual's fear of social engineering.
Subjective norm [SN]	The perception of social approval from important others regarding following awareness campaign materials.
Attitude towards behavior [AtB]	An individual's positive versus negative evaluations of following awareness campaign materials.
Perceived behavioral control [PBC]	The perception of the ease or difficulty of following awareness campaign materials.
Self-efficacy [SE]	The individual's self-efficacy when implementing social engineering countermeasures (i.e., following awareness campaign materials).
Response efficacy [RE]	The perceived efficacy of social engineering countermeasures (i.e., following awareness campaign materials).
Trust in authorities [TiA]	The degree of trust (trusting beliefs (McKnight et al., 2002)) in state authorities.
Perceived regulation [PR]	The perceived overall appropriateness of the regulative framework for fighting social engineering.
Authorities performance [AP]	The perceived overall performance of state authorities when dealing with social engineering.
Information sensitivity [IS]	The perceived sensitivity of an individual's online information.
Privacy concern [PC]	The extent of concerns regarding privacy online.
Behavioral intention [BI]	The level of individual's motivation to follow awareness campaign materials in the near future.

from Venkatesh et al. (2003). Two items for *self-efficacy* were adapted from Johnston and Warkentin (2010) and one item from Anderson and Agarwal (2010). One item for *response efficacy* was adapted from Moody et al. (2018) and two items from Jansen and van Schaik (2018). Two items for *trust in authorities* were adapted from McKnight et al. (2002) and one item from Jansen and van Schaik (2018). Items for *perceived regulation* were adapted from Fujs et al. (2019), and items for *authorities performance* from Crow et al. (2017). Items for *information sensitivity* and *privacy concern* were adapted from Fujs et al. (2019). Finally, items for *behavioral intention* were adapted from Park and Smith (2007). All questionnaire items were measured by using a 5-point Likert scale from 1 "strongly disagree" to 5 "strongly agree". The survey was distributed in Slovenian which was the primary language of all respondents in our study.

To ensure that respondents understood the items and provided meaningful responses, the survey questionnaire included relevant details as close to the items as possible. First, the questionnaire provided the Police and the designated national computer security incident response team (SI-CERT) as examples of state authorities in prompts next to *trust in authorities* and *authorities performance* items. Second, the questionnaire included a brief description of social engineering and information on the most problematic kinds of social engineering in the year preceding the study according to SI-CERT (i.e., fake extortion, sextortion, love scams) before questions about social engineering. Third, respondents were presented with a description of the awareness campaign before answering questions about it. The description was strongly based on the official description of the awareness campaign and included information on who is leading the effort (i.e., SI-CERT), its aims (e.g., raising awareness by providing information on how to recognize social engineering, how to protect against it, how to respond when incidents happen), and how to follow awareness campaign materials (e.g., on Facebook, YouTube, the official campaign mailing list, the official campaign website).

3.4. Sample and data collection

The sample included 542 individuals in Slovenia who were at least 15 years old. The survey was conducted between January and June 2020. Respondents were recruited through University of Maribor students, implying a convenience sample. Students were asked to distribute the survey questionnaire to their family and friends. The students were not compensated for distributing the survey questionnaire. The respondents also did not receive any compensation for taking the survey. All batches of questionnaires were checked for any signs of misconduct on the part of the students (e.g., asking questions related to respondents upon returning the questionnaires, checking if the same pen was used, style of writing, face similarity of answers, logical errors). No signs of misconduct were noticed. A total of 553 questionnaires were returned. Responses with over 50 percent missing values for theoretical constructs included in the analysis and/or indicating respondent non-engagement (i.e., standard deviation equal to 0) were excluded. After excluding poorly completed responses, we were left with 542 useful responses which were used in further analyses.

Table 2
Sample characteristics.

	Frequency	Percent
Gender		
Male	224	41.3
Female	313	57.7
N/A	5	0.9
Age		
15–24	273	50.4
25–34	103	19.0
35–44	63	11.6
45–54	63	11.6
55–64	26	4.8
65–74	8	1.5
75+	2	0.4
N/A	4	0.7
Employment status		
Student	266	49.1
Employed	239	44.1
Unemployed	11	2.0
Retired	19	3.5
N/A	7	1.3
Formal education		
High school or less	345	63.7
Bachelor's degree	139	25.6
Master's degree	48	8.9
Doctoral degree	5	0.9
N/A	5	0.9

The survey was anonymous as no identifying information of any kind was gathered from the participants. Table 2 shows the sample characteristics. Age of the respondents ranged from 15 to 78 years old ($M = 30.6, SD = 13.2$). The sample appears to be biased towards younger respondents and students. Also, the unemployed and retired individuals seem to be underrepresented in our sample. These issues are likely a consequence of the convenience sampling method employed. Students seem to have on average more friends than close family members that they could ask to take the questionnaire. The study was partially conducted during the first wave of the COVID-19 pandemic which may have contributed to a

Table 3
Fit indices of the measurement model.

Measure	Threshold	Estimate	Interpretation
χ^2		1343.219	
df		840	
χ^2/df	≤ 5	1.599	Excellent
CFI	≥ 0.90	0.962	Excellent
SRMR	≤ 0.08	0.039	Excellent
RMSEA	≤ 0.08	0.033	Excellent

Notes: CFI – comparative fit index; *SRMR* – standardized root mean square residual; *RMSEA* – root mean square error of approximation.

lower share of older respondents as students might have avoided contacting them in order not to infect them.

3.5. Data analysis

Covariance-based structural equation modeling (CB-SEM) was employed to analyze the data since all measured theoretical constructs were reflective. CB-SEM enables the analysis of complex research models when these include latent variables (i.e., theoretical constructs) with multiple indicators which allow for indirect measurement through characteristics attributed to them. A key advantage of CB-SEM is that it integrates the measurements of latent variables and associations between them into a concurrent evaluation.

Data was analyzed with IBM SPSS Statistics and IBM SPSS Amos version 27. Missing values (0.8 percent) were imputed with medians prior to the analysis. Model fit of all measurement and structural models was determined with fit indices χ^2/df, comparative fit index (*CFI*), standardized root mean square residual (*SRMR*), and root mean square error of approximation (*RMSEA*). Standard thresholds were used to interpret how well the data fit the models ensuring that the results of CB-SEM analysis are meaningful.

To validate the survey instrument, a confirmatory factor analysis (CFA) was conducted. Convergent validity was determined by evaluating average variance extracted (AVE) and factor loadings of items on their corresponding latent variables. Discriminant validity was evaluated with a heterotrait-monotrait ratio of correlations (HTMT) analysis. Reliability was determined with composite reliability (CR).

A full sample structural model mirroring the research model was first constructed to test the hypotheses. Our sample is not representative as students in the age group 15–24 years are overrepresented. To deal with this issue, we split the sample according to the employment status of respondents into the *student* ($N_s = 266$) and *employed* ($N_e = 239$) subsamples. This enabled us to study more in-depth these two subsamples and determine whether the overrepresentation of the student population is a major issue thus partially addressing the issues with non-representatives of our sample. A structural model for multigroup analysis was developed to test the hypotheses for each subsample.

4. Results

4.1. Measurement model

A measurement model was developed to validate the survey instrument. The model fit presented in Table 3 indicates that the data fits the model well.

Table 4 presents *CR*, *AVE* and HTMT analysis which are relevant for determining the validity and reliability of the survey instrument. First, *CR* ranged from 0.751 to 0.934 thus exceeding the commonly accepted threshold 0.70. This demonstrates adequate reliability of all constructs. Next, *AVE* ranged from 0.503 to 0.826. Values above the 0.50 threshold are generally considered as adequate therefore indicating adequate convergent validity. Additionally, all factor loadings (see Table 5) were above the 0.50 threshold showing further support for adequate convergent validity. Finally, HTMT ratios of correlations were all below the conservative 0.85 threshold thus indicating adequate discriminant validity of the survey instrument.

4.2. Structural model

The full sample structural model was developed to test the hypothesized direct effects. Model fit of the full sample structural model presented in Table 6 suggests that it fits the data well. A structural model was then built for the multigroup analysis. As shown in Table 7, this model also fit the data well.

Standardized results of both structural models are presented in Fig. 2. The constructs in both models explain a meaningful share of variance of all predicted constructs (i.e., *authorities performance, perceived threat, fear, perceived behavioral control, privacy concern, attitude towards behavior*, and *behavioral intention*).

The results of the full sample structural model support hypotheses H1a, H1b, H2a, H2b, H3, H4, H5, H6, H7a, H7b, H8a, H8b and H10 ($p < 0.001$), H9 ($p = 0.002$) and H11 ($p = 0.011$). The results of the multigroup analysis indicate some differences between students and employed individuals. The structural model for the student subsample indicates support for hypotheses H1a, H1b, H2a, H2b, H3, H4, H5, H7a, H7b, H8b and H10 ($p < 0.001$), H6 ($p = 0.004$), H9 ($p = 0.037$) and H11 ($p = 0.006$). It however fails short to show support for hypothesis H8a ($p = 0.051$). The structural model for the employed subsample suggests support for hypotheses H1a, H1b, H2b, H3, H4, H5, H6, H7a, H7b, H8a, H8b and H10 ($p < 0.001$), and H9 ($p = 0.046$). The results however do not indicate support for hypotheses H2a ($p = 0.056$) and H11 ($p = 0.174$). The summary of hypotheses testing is presented in Table 8.

5. Discussion

This study aimed to determine what motivates individuals to seek information about social engineering by investigating the determinants of behavioral intention to follow a social engineering awareness campaign in Slovenia. It makes several contributions to the literature on cybersecurity interventions, protection motivation and human behavior. These are presented alongside practical implications in the following subsections.

5.1. Theoretical implications

The empirical findings of this study make several contributions to the theory. First, this study contributes to the literature on cybersecurity interventions by examining a rich set of determinants of behavioral intention to follow a social engineering awareness campaign. Existing research on information seeking in the context of cybersecurity is particularly scarce as, to the best of our knowledge, only three studies focus on this topic (Lemay et al., 2020; Williams and Joinson, 2020; Zhang and Borden, 2020). Two of these studies investigated information seeking behavior in the context of phishing (Lemay et al., 2020; Williams and Joinson, 2020), and the third one information seeking about a data breach (Zhang and Borden, 2020). The former studies indicate that PMT at least generally holds in the context of phishing (Lemay et al., 2020; Williams and Joinson, 2020). These studies are however exploratory and indicative of the directions that future work could take (e.g., reporting correlations (Williams and Joinson, 2020), small R^2 (Lemay et al., 2020)). The latter study suggests that perceived severity influences information seeking behavior which

Table 4
Validity and reliability of the survey instrument. Composite reliability (*CR*), average variance extracted (*AVE*), and heterotrait-monotrait ratio of correlations (HTMT) analysis.

Construct	*CR*	*AVE*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1: PBC	0.794	0.563														
2: IS	0.857	0.670	0.036													
3: PC	0.783	0.549	0.025	0.509												
4: TiA	0.897	0.747	0.261	0.138	0.056											
5: AP	0.823	0.608	0.065	0.105	0.073	0.420										
6: PR	0.751	0.503	0.071	0.106	0.008	0.377	0.632									
7: PV	0.821	0.606	0.172	0.179	0.176	0.065	0.179	0.233								
8: PS	0.827	0.619	0.010	0.246	0.285	0.032	0.067	0.122	0.495							
9: PT	0.889	0.728	0.102	0.209	0.251	0.012	0.109	0.088	0.495	0.570						
10: F	0.875	0.701	0.100	0.195	0.304	0.066	0.094	0.041	0.441	0.452	0.778					
11: SE	0.838	0.635	0.696	0.063	0.004	0.204	0.084	0.057	0.051	0.056	0.051	0.016				
12: RE	0.755	0.508	0.431	0.145	0.147	0.247	0.176	0.161	0.009	0.188	0.088	0.182	0.409			
13: SN	0.854	0.665	0.201	0.143	0.188	0.147	0.123	0.162	0.267	0.209	0.351	0.357	0.233	0.206		
14: AtB	0.897	0.743	0.395	0.154	0.208	0.168	0.176	0.109	0.068	0.205	0.201	0.282	0.292	0.449	0.362	
15: BI	0.934	0.826	0.221	0.127	0.179	0.164	0.226	0.154	0.243	0.194	0.367	0.377	0.253	0.264	0.567	0.452

Notes: PBC – perceived behavioral control; IS – information sensitivity; PC – privacy concern; TiA – trust in authorities; AP – authorities performance; PR – perceived regulation; PV – perceived vulnerability; PS – perceived severity; PT – perceived threat; F – fear; SE – self-efficacy; RE – response efficacy; SN – subjective norm; AtB – attitude towards behavior; BI – behavioral intention.

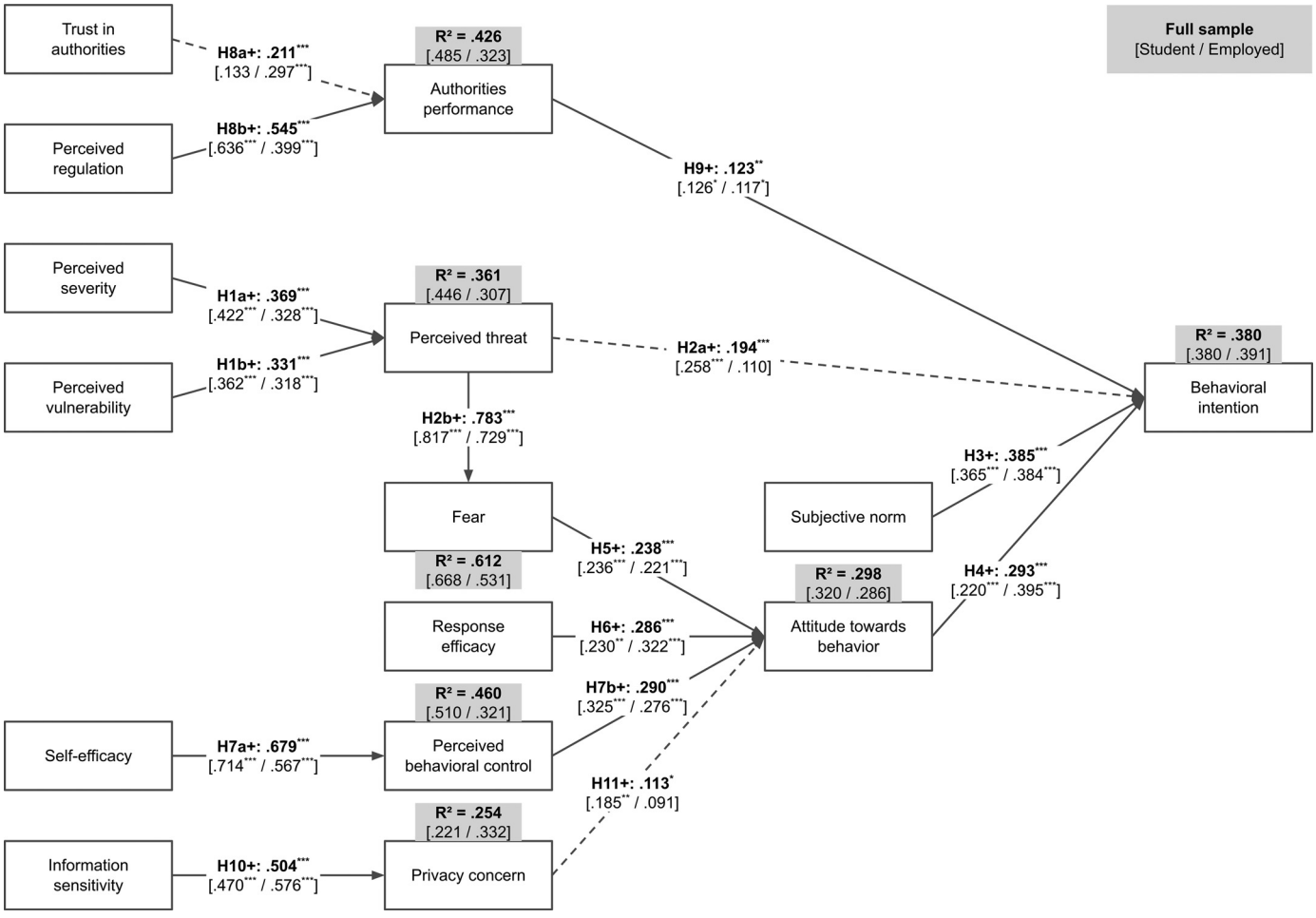

Fig. 2. Structural model. Results for the full sample and the student and employed subsamples. *Notes*: $^{*}p < 0.050$, $^{**}p < 0.010$, $^{***}p < 0.001$; Dashed association lines represent differences in significance between the student and employed subsamples (i.e., a significant association for the student subsample and a non-significant association for the employed subsample or vice versa).

is also in line with PMT. Our study advances these findings by a much richer set of theoretical constructs and employing more advanced data analysis. This provides more insights into the motivation of individuals to seek information about phishing: 1) by investigating the role of additional PMT constructs (i.e., perceived threat, fear), 2) by investigating TPB constructs (i.e., subjective norm, attitude towards behavior, perceived behavioral control), 3) by integrating PMT and TPB, 4) by investigating constructs related to privacy concerns (i.e., information sensitivity, privacy concerns), and 5) by investigating constructs related to the performance of state authorities (i.e., trust in authorities, perceived regulations, authorities performance). This study shows that perceived threat,

Table 5
Questionnaire items.

Construct	Loading	Item	Source
Perceived severity	0.820	PS1. My personal data acquired with social engineering could be misused for criminal purposes.	Fujs et al. (2019)
	0.887	PS2. My personal data collected with social engineering could be misused against me.	Fujs et al. (2019)
	0.630	PS3. Stealing of my personal data with social engineering would be a serious problem for me.	Moody et al. (2018)
Perceived vulnerability	0.795	PV1. I am very vulnerable to social engineering.	Fujs et al. (2019)
	0.821	PV2. I can easily become a victim of social engineering.	New
	0.715	PV3. It is likely that I will become a victim of social engineering in the near future.	Jansen and van Schaik (2018)
Perceived threat	0.884	PT1. I feel threatened by social engineering.	Fujs et al. (2019)
	0.856	PT2. Social engineering threatens me.	Fujs et al. (2019)
	0.818	PT3. Social engineering is a danger to me.	Liang and Xue (2010)
Fear	0.893	F1. I am afraid of social engineering.	Osman et al. (1994)
	0.804	F2. Social engineering is very frightening.	New
	0.811	F3. I am afraid of being victimized by social engineering.	Jansen and van Schaik (2018)
Subjective norm	0.832	SN1. People who are important to me think that I should follow awareness campaign materials.	Venkatesh et al. (2003)
	0.930	SN2. Most people whose opinion I value consider that I should follow awareness campaign materials.	Park and Smith (2007)
	0.660	SN3. It is expected of me that I follow awareness campaign materials.	Park and Smith (2007)
Attitude towards behavior	0.838	AtB1. Following awareness campaign materials is a very good idea.	Venkatesh et al. (2003)
	0.882	AtB2. Following awareness campaign materials would be very wise.	Moody et al. (2018)
	0.865	AtB3. Following awareness campaign materials is very beneficial.	Park and Smith (2007)
Perceived behavioral control	0.675	PBC1. If I want to, I can follow awareness campaign materials.	Park and Smith (2007)
	0.775	PBC2. I know how to follow awareness campaign materials.	Park and Smith (2007)
	0.796	PBC3. I have the resources necessary to follow awareness campaign materials.	Venkatesh et al. (2003)
Self-efficacy	0.744	SE1. It is easy to follow awareness campaign materials.	Johnston and Warkentin (2010)
	0.885	SE2. I would feel comfortable following awareness campaign materials.	Anderson and Agarwal (2010)
	0.753	SE3. I am able to follow awareness campaign materials without much effort.	Johnston and Warkentin (2010)
Response efficacy	0.719	RE1. Following awareness campaign materials lowers the success of social engineering.	Moody et al. (2018)
	0.764	RE2. Following awareness campaign materials helps in preventing social engineering.	Jansen and van Schaik (2018)
	0.650	RE3. If I follow awareness campaign materials, I am less likely to be victimized by social engineering.	Jansen and van Schaik (2018)
Trust in authorities	0.737	TiA1. I believe that the state authorities would act in my best interest.	McKnight et al. (2002)
	0.933	TiA2. I would characterize state authorities as honest.	McKnight et al. (2002)
	0.908	TiA3. I trust state authorities.	Jansen and van Schaik (2018)
Perceived regulation	0.769	PR1. Our legislation provides for appropriate measures for fighting social engineering.	Fujs et al. (2019)
	0.663	PR2. The international legislation provides for appropriate measures for fighting social engineering.	Fujs et al. (2019)
	0.691	PR3. The government does enough to fight social engineering.	Fujs et al. (2019)
Authorities performance	0.777	AP1. State authorities are successfully dealing with social engineering.	Crow et al. (2017)
	0.773	AP2. State authorities are successfully working with internet users to address social engineering.	Crow et al. (2017)
	0.789	AP3. State authorities are successfully preventing social engineering.	Crow et al. (2017)
Information sensitivity	0.689	IS1. I consider the content of my e-mails as very sensitive.	Fujs et al. (2019)
	0.894	IS2. I consider data on which websites I visit as very sensitive.	Fujs et al. (2019)
	0.857	IS3. I consider data on what I do online as very sensitive.	Fujs et al. (2019)
Privacy concern	0.715	PC1. It highly bothers me when websites ask me about my personal data.	Fujs et al. (2019)
	0.648	PC2. I always think twice before submitting my personal data online.	Fujs et al. (2019)
	0.846	PC3. I am very concerned that websites collect too much personal data about me.	Fujs et al. (2019)
Behavioral intention	0.910	BI1. I intend to follow awareness campaign materials in the near future.	Park and Smith (2007)
	0.895	BI2. I have it in my mind to follow awareness campaign materials in the near future.	Park and Smith (2007)
	0.921	BI3. I will follow awareness campaign materials in the near future.	Park and Smith (2007)

subjective norm, attitude towards behavior and authorities performance are associated with behavioral intention. This improves our understanding of how perceived severity (Williams and Joinson, 2020; Zhang and Borden, 2020) and perceived vulnerability (Williams and Joinson, 2020) relate to behavioral intentions. It also offers an alternative for the role of emotions, such as fear, as predictors of attitudes towards behavior instead of behavioral intentions (e.g., Lemay et al. (2020)).

Second, the novel integration of PMT and TPB, and a rich set of studied additional constructs provide new insights on cognitive decision making and protection motivation in general. This study confirmed that response efficacy relates to attitude towards behavior which is consistent with existing literature (Boobalan and Nachimuthu, 2020; Grimes and Marquardson, 2019; Herath and Rao, 2009). It is also confirming the findings found in the literature regarding the relation between self-efficacy and per-

Table 6
Fit indices of the structural model.

Measure	Threshold	Estimate	Interpretation
χ^2		1521.067	
df		902	
χ^2/df	≤ 5	1.686	Excellent
CFI	≥ 0.90	0.953	Excellent
SRMR	≤ 0.08	0.058	Excellent
RMSEA	≤ 0.08	0.036	Excellent

Notes: CFI – comparative fit index; *SRMR* – standardized root mean square residual; *RMSEA* – root mean square error of approximation.

Table 7
Fit indices of the structural model for multi-group analysis (student and employed subsamples).

Measure	Threshold	Estimate	Interpretation
χ^2		2712.111	
df		1804	
χ^2/df	≤ 5	1.503	Excellent
CFI	≥ 0.90	0.926	Acceptable
SRMR	≤ 0.08	0.068	Excellent
RMSEA	≤ 0.08	0.032	Excellent

Notes: CFI – comparative fit index; *SRMR* – standardized root mean square residual; *RMSEA* – root mean square error of approximation.

ceived behavioral control (Taylor and Todd, 1995), and perceived behavioral control and attitude towards behavior (Boobalan and Nachimuthu, 2020). However, this is the first study to consider and empirically confirm perceived behavioral control as a mediator between self-efficacy and attitude towards behavior. Since self-efficacy precedes perceived behavioral control from a theoretical viewpoint (Herath and Rao, 2009) and there is empirical support for its mediating role, perceived behavioral control should be included as a mediator between self-efficacy and attitude towards behavior in models integrating TPB and PMT.

There is some evidence for the relation between threat appraisal and attitude towards behavior in the literature through concerns related to a threat (Herath and Rao, 2009) although the relation between perceived severity and vulnerability, and attitude seems quite vague with poor empirical support (Grimes and Marquardson, 2019; Herath and Rao, 2009). This study fills in this gap by going one step back from *concern* (i.e., manifestation of fear) to *fear*. It shows that fear (like concern) is strongly associated with attitude towards behavior. However, our study explains better how fear is related to threat appraisal constructs (i.e., perceived severity, perceived vulnerability, perceived threat) than the current literature.

This study also contributes to the protection motivation literature by indicating that authorities performance may affect protection motivation. In our study, the studied countermeasure is following a social engineering awareness campaign. To further validate this finding, future studies may examine the role of authorities performance in different settings and countermeasures (Aurigemma and Mattson, 2019).

Few studies in the literature investigate the relation between privacy concern and attitude towards behavior. Research on purchasing behavior has mixed results indicating a weak association between privacy concerns and attitude towards purchasing behavior (Belkhamza and Niasin, 2017; Mahrous, 2011). Research on information disclosure however indicates a strong negative relation between privacy concerns and attitude towards information disclosure (Heirman et al., 2013). This study is somewhere in between as there is a strong association between privacy concern and attitude towards behavior for the student population while we found no significant association for employed individuals. Since all three studies found in the literature have relatively young samples (Belkhamza and Niasin, 2017; Heirman et al., 2013; Mahrous, 2011), the differences between populations in our study might be due to the study focus. Further investigations would however be needed to determine whether age (or employment status) moderates the association between privacy concern and attitude towards behavior in other settings as well.

Third, our study contributes to the literature on cybersecurity interventions by being one of the first to investigate how behavioral intention to follow a social engineering awareness campaign differs between students and employed individuals. The results suggest three noticeable differences between students and employed individuals. The first is related to the association between perceived threat and behavioral intention. It suggests that threat appraisal of employed individuals may not be associated with protection motivation thus eroding a core PMT component. This could be a consequence of their lower sensitivity to fear appeals although future studies would need to explore this suggestion.

The second difference is the above mentioned association between privacy concern and attitude towards behavior. These results suggest that the privacy paradox only applies to employed individuals but not students. Since existing studies show mixed results for the student population in other contexts (Belkhamza and Niasin, 2017; Heirman et al., 2013; Mahrous, 2011), further studies would

Table 8
Hypotheses testing summary.

Hypothesis	Evidence	Conclusion
H1a. Perceived severity is positively associated with perceived threat.	Significant associations in all models	Supported
H1b. Perceived vulnerability is positively associated with perceived threat.	Significant associations in all models	Supported
H2a. Perceived threat is positively associated with behavioral intention.	Significant associations in the full sample and the student subsample	Partially supported
H2b. Perceived threat is positively associated with fear.	Significant associations in all models	Supported
H3. Subjective norm is positively associated with behavioral intention.	Significant associations in all models	Supported
H4. Attitude towards behavior is positively associated with behavioral intention.	Significant associations in all models	Supported
H5. Fear is positively associated with attitude towards behavior.	Significant associations in all models	Supported
H6. Response efficacy is positively associated with attitude towards behavior.	Significant associations in all models	Supported
H7a. Self-efficacy is positively associated with perceived behavioral control.	Significant associations in all models	Supported
H7b. Perceived behavioral control is positively associated with attitude towards behavior.	Significant associations in all models	Supported
H8a. Trust in authorities is positively associated with authorities performance.	Significant associations in the full sample and the employed subsample	Partially supported
H8b. Perceived regulation is positively associated with authorities performance.	Significant associations in all models	Supported
H9. Authorities performance is positively associated with behavioral intention.	Significant associations in all models	Supported
H10. Information sensitivity is positively associated with privacy concern.	Significant associations in all models	Supported
H11. Privacy concern is positively associated with attitude towards behavior.	Significant associations in the full sample and the student subsample	Partially supported

be needed to determine whether the privacy paradox applies to the student population as well in other settings.

The third difference considers the association between trust in authorities and authorities performance. The results indicate that employed individuals perceive state authorities to be more effective if they trust them more. Students however do not seem to relate these two constructs. This difference could be attributed to the differences in experience with work environments of the two populations. Students may be idealizing that someone's performance is independent of how much they trust them. Since few studies have investigated this relation, future studies may be needed to clarify the underlying reasons for this difference.

Although the sample was split due to methodological issues, these results indicate a moderating role of employment status. A recent study found some evidence for the moderating role of age in the context of buying clothes online/offline during the COVID-19 pandemic (Youn et al., 2021) therefore the moderating role of age in our study cannot be excluded either. Future studies with more representative samples may be needed to determine whether employment status and/or age moderate the three differing associations.

5.2. Practical implications

The empirical findings of this study provide three key implications for practice. First, the results of this study confirm that information seeking behavior can be influenced by fear appeals confirming findings found in existing literature (Zhang and Borden, 2020). Social engineering campaigns may therefore consider including a fear appeal in their promotional materials and during their promotional activities. Different communication channels may prove effective in delivering adequate fear appeals. For example, online news have been shown to be able to successfully deliver significant fear appeals (Zhang and Borden, 2020).

Second, this study offers valuable insights on how to develop effective messaging. Fear appeals focusing on the social engineering threat may be effective in directly increasing the information seeking motivation. Messaging regarding coping with social engineering (i.e., focusing on response efficacy, self-efficacy and perceived behavioral control) may however have a more indirect effect through attitude towards an awareness campaign. Interestingly, attitude towards behavior may be also influenced by messaging related to the social engineering threat through aroused fear.

Third, the results of this study suggest that adapting the messaging regarding the awareness campaign to the specifics of different target populations may increase their effectiveness. For example, emphasizing the social engineering threat may be more effective for the student population than employed individuals. Also, messaging targeting privacy concerns of the student population may be effective in raising their attitude towards an awareness campaign while such messaging may be ineffective for employed individuals.

5.3. Limitations and future work

This study has a number of limitations. First, a key limitation is related to sampling and method of data collection. The sample is overrepresented by students and respondents younger than 25 years. While this could potentially bring some unwanted errors in the results, we tried to determine any differences between students and employed individuals. The comparison between the student and employed subsamples indicates that the results are comparable for most associations except for three (namely, associations between perceived threat and behavioral intention, between privacy concern and attitude towards behavior, and between trust in authorities and authorities performance). Although these results suggest that overrepresentation of students was not a major issue, a more representative sample would be needed to confirm our findings for the general population. Next, few respondents were aged 65 or more in our sample. Since the older generations seem to be more resistant to social engineering (Back and Guerette, 2021), future studies focusing on the older population would be needed to determine whether and how this affects their information seeking intentions. Further, the study was conducted in a single cultural context. Future studies may therefore compare multiple cultural contexts to determine investigate how they affect the motivation to follow social engineering awareness campaigns. Additionally, our study focused on the general population as individuals. Future studies would be needed to determine whether the findings are applicable to organizational settings. Finally, this study does not consider the moderating role of aroused fear (Vrhovec and Mihelič, 2021). Future research endeavors may be directed towards determining how the level of aroused fear affect the relations between the studied constructs.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Simon Vrhovec: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Visualization, Writing – original draft, Writing – review & editing. **Igor Bernik:** Investigation, Validation, Writing – review & editing. **Blaž Markelj:** Investigation, Validation, Writing – review & editing.

Data availability

Data will be made available on request.

Acknowledgments

We would like to express our sincere gratitude to the respondents who took their time to participate in our survey. Next, we would also like to thank the students who helped with data collection, and Luka Jelovčan for data screening and entry. Finally, we would like to thank the associate editor for handling our paper and the anonymous reviewers for their insightful and constructive comments.

This study is part of a research project *Safety and security of cyberspace users – Criminological, victimological and preventative aspects* (J5-9345, 2018–2020) funded by the Slovenian Research Agency, and carried out by the University of Maribor. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

References

Abraham, S., Chengalur-Smith, I., 2019. Evaluating the effectiveness of learner controlled information security training. Comput. Secur. 87, 101586. doi:10.1016/j.cose.2019.101586.

Aigbefo, Q.A., Blount, Y., Marrone, M., 2020. The influence of hardiness and habit on security behaviour intention. Behav. Inf. Technol. 1–20. doi:10.1080/0144929X.2020.1856928.

Al-Gasawneh, J.A., Al-Adamat, A.M., 2020. The relationship between perceived destination image, social media interaction and travel intentions relating to neom city. Acad. Strateg. Manag. J. 19 (2), 1–12.

Anderson, C.L., Agarwal, R., 2010. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Q. 34 (3), 613–643.

Arpaci, I., Kilicer, K., Bardakci, S., 2015. Effects of security and privacy concerns on educational use of cloud services. Comput. Hum. Behav. 45, 93–98. doi:10.1016/j.chb.2014.11.075.

Aurigemma, S., Mattson, T., 2019. Generally speaking, context matters: making the case for a change from universal to particular ISP research. J. Assoc. Inf. Syst. 20 (12), 1700–1742. doi:10.17705/1jais.00583.
Back, S., Guerette, R.T., 2021. Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks. J. Contemp. Crim. Justice doi:10.1177/10439862211001628. 104398622110016
Bax, S., McGill, T., Hobbs, V., 2021. Maladaptive behaviour in response to email phishing threats: the roles of rewards and response costs. Comput. Secur. 106, 102278. doi:10.1016/j.cose.2021.102278.
Belanger, F., Crossler, R.E., 2019. Dealing with digital traces: understanding protective behaviors on mobile devices. J. Strateg. Inf. Syst. 28 (1), 34–49. doi:10.1016/j.jsis.2018.11.002.
Belkhamza, Z., Niasin, M.A.F., 2017. The effect of privacy concerns on smartphone app purchase in malaysia: extending the theory of planned behavior. Int. J. Interact. Mob. Technol. (iJIM) 11 (5), 178. doi:10.3991/ijim.v11i5.6961.
Berkley-Patton, J.Y., Thompson, C.B., Moore, E., Hawes, S., Berman, M., Allsworth, J., Williams, E., Wainright, C., Bradley-Ewing, A., Bauer, A.G., Catley, D., Goggin, K., 2019. Feasibility and outcomes of an HIV testing intervention in african american churches. AIDS Behav. 23 (1), 76–90. doi:10.1007/s10461-018-2240-0.
Boobalan, K., Nachimuthu, G.S., 2020. Organic consumerism: a comparison between India and the USA. J. Retail. Consum. Serv. 53, 101988. doi:10.1016/j.jretconser.2019.101988.
Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. 39 (4), 837–864. doi:10.25300/MISQ/2015/39.4.5.
Branley-Bell, D., Coventry, L., Sillence, E., 2021. Promoting cybersecurity culture change in healthcare. In: The 14th PErvasive Technologies Related to Assistive Environments Conference. ACM, pp. 544–549. doi:10.1145/3453892.3461622.
Choi, S., Martins, J.T., Bernik, I., 2018. Information security: listening to the perspective of organisational insiders. J. Inf. Sci. 44 (6), 752–767. doi:10.1177/0165551517748288.
Crow, M.S., Snyder, J.A., Crichlow, V.J., Smykla, J.O., 2017. Community perceptions of police body-worn cameras. Crim. Justice Behav. 44 (4), 589–610. doi:10.1177/0093854816688037.
Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. J. Appl. Soc. Psychol. 30 (2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x.
Fujs, D., Mihelič, A., Vrhovec, S., 2019. Social network self-protection model: what motivates users to self-protect? J. Cyber Secur. Mobil. 8 (4), 467–492. doi:10.13052/jcsm2245-1439.844.
Ghaffari, M., Tezval, J., Rakhshanderou, S., Hevey, D., Harooni, J., Armoon, B., 2020. Skin cancer preventive behaviours among rural Illam farmers, western Iran: applying protection motivation theory. Rural Soc. 29 (2), 89–99. doi:10.1080/10371656.2020.1782108.
Gordon, W.J., Wright, A., Glynn, R.J., Kadakia, J., Mazzone, C., Leinbach, E., Landman, A., 2019. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J. Am. Med. Inform. Assoc. 26 (6), 547–552. doi:10.1093/jamia/ocz005.
Grimes, M., Marquardson, J., 2019. Quality matters: evoking subjective norms and coping appraisals by system design to increase security intentions. Decis. Support Syst. 119, 23–34. doi:10.1016/j.dss.2019.02.010.
Hanson, C.L., Crandall, A., Barnes, M.D., Novilla, M.L., 2021. Protection motivation during COVID-19: across-sectional study of family health, media, and economic influences. Health Educ. Behav. doi:10.1177/10901981211000318. 109019812110003
Havaei, M., Saeieh, S.E., Salehi, L., 2021. Sexual and reproductive health self-care: a theory-based intervention. Health Educ. 121 (1), 111–124. doi:10.1108/HE-04-2020-0024.
Heirman, W., Walrave, M., Ponnet, K., 2013. Predicting adolescents' disclosure of personal information in exchange for commercial incentives: an application of an extended theory of planned behavior. Cyberpsychol., Behav., Social Netw. 16 (2), 81–87. doi:10.1089/cyber.2012.0041.
Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125. doi:10.1057/ejis.2009.6.
Heydari, E., Dehdari, T., Solhi, M., 2021. Can adopting skin cancer preventive behaviors among seafarers be increased via a theory-based mobile phone-based text message intervention? A randomized clinical trial. BMC Public Health 21 (1), 134. doi:10.1186/s12889-020-09893-x.
Hina, S., Panneer Selvam, D.D.D., Lowry, P.B., 2019. Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. Comput. Secur. 87, 101594. doi:10.1016/j.cose.2019.101594.
Hoseini, Z.S., Ghouchani, H.T., Hakak, H.M., Lashkardoost, H., Mehri, A., Khankolabi, M., Salari, E., 2021. Effect of education on promoting healthy lifestyle behaviors that prevent breast cancer in middle-aged women: application of protection motivation theory. Korean J. Fam. Med. 42 (2), 166–171. doi:10.4082/kjfm.19.0164.
Ikhalia, E., Serrano, A., Bell, D., Louvieris, P., 2019. Online social network security awareness: mass interpersonal persuasion using a facebook app. Inf. Technol. People 32 (5), 1276–1300. doi:10.1108/ITP-06-2018-0278.
Jafaralilou, H., Zareban, I., Hajaghazadeh, M., Matin, H., Didarloo, A., 2019. The impact of theory-based educational intervention on improving helmet use behavior among workers of cement factory, Iran. J. Egypt. Public Health Assoc. 94 (1), 1. doi:10.1186/s42506-018-0001-6.
Jalali, M.S., Bruckes, M., Westmattelmann, D., Schewe, G., 2020. Why employees (still) click on phishing links: an investigation in hospitals. J. Med. Internet Res. 22 (1), e16775. doi:10.2196/16775.
Jansen, J., van Schaik, P., 2018. Testing a model of precautionary online behaviour: the case of online banking. Comput. Hum. Behav. 87, 371–383. doi:10.1016/j.chb.2018.05.010.
Jansen, J., van Schaik, P., 2019. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. Int. J. Hum. Comput. Stud. 123, 40–55. doi:10.1016/j.ijhcs.2018.10.004.
Jiow, H.J., Mwagwabi, F., Low-Lim, A., 2021. Effectiveness of protection motivation theory based: password hygiene training programme for youth media literacy education. J. Media Lit. Educ. 13 (1), 67–78. doi:10.23860/JMLE-2021-13-1-6.
Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34 (3), 549. doi:10.2307/25750691.
Johnston, A.C., Warkentin, M., Dennis, A.R., Siponen, M., 2019. Speak their language: designing effective messages to improve employees' information security decision making. Decis. Sci. 50 (2), 245–284. doi:10.1111/deci.12328.
Khan, H.U., AlShare, K.A., 2019. Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. J. Organ. Comput. Electron. Commer. 29 (1), 4–23. doi:10.1080/10919392.2019.1552743.
Kim, B., Lee, D.-Y., Kim, B., 2020. Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. Behav. Inf. Technol. 39 (11), 1156–1175. doi:10.1080/0144929X.2019.1653992.
Kuppusamy, P., Samy, G.N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., Perumal, S., 2020. Systematic literature review of information security compliance behaviour theories. J. Phys. 1551 (1), 012005. doi:10.1088/1742-6596/1551/1/012005.
Lemay, D.J., Basnet, R.B., Doleck, T., 2020. Examining the relationship between threat and coping appraisal in phishing detection among college students. J. Internet Serv. Inf. Secur. 10 (1), 38–49. doi:10.22667/JISIS.2020.02.29.038.
Liang, H., Xue, Y., 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. 11 (7), 394–413.
Maddux, J.E., Rogers, R.W., 1983. Protection motivation theory and self-efficacy: a revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19 (5), 469–479.
Mahrous, A.A., 2011. Antecedents of privacy concerns and their online actual purchase consequences: a cross-country comparison. Int. J. Electron. Mark. Retail. 4 (4), 248. doi:10.1504/IJEMR.2011.045610.
Mansoori, M., Welch, I., 2020. How do they find us? A study of geolocation tracking techniques of malicious web sites. Comput. Secur. 97, 101948. doi:10.1016/j.cose.2020.101948.
Margraf, J., Brailovskaia, J., Schneider, S., 2020. Behavioral measures to fight COVID-19: an 8-country study of perceived usefulness, adherence and their predictors. PLoS One 15 (12), e0243523. doi:10.1371/journal.pone.0243523.
Masser, B.M., Hyde, M.K., Ferguson, E., 2020. Exploring predictors of Australian community members' blood donation intentions and blood donation-related behavior during the COVID-19 pandemic. Transfusion 60 (12), 2907–2917. doi:10.1111/trf.16067.
McKnight, D.H., Choudhury, V., Kacmar, C., 2002. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. J. Strateg. Inf. Syst. 11 (3–4), 297–323. doi:10.1016/S0963-8687(02)00020-3.
Mihelič, A., Jevšček, M., Vrhovec, S., Bernik, I., 2019. Testing the human backdoor: organizational response to a phishing campaign. J. Univers. Comput. Sci. 25 (11), 1458–1477. doi:10.3217/jucs-025-11-1458.
Mohammadi, M., Mehri, A., Hashemian, M., Abadi, Z.S., Mohammadi, S., 2020. Investigating the effect of educational intervention based on protection motivation theory on osteoporosis preventive nutritional behaviors in women of reproductive age referring to healthcare centers in sabzevar, iran. Bangladesh J. Med. Sci. 19 (2), 254–261. doi:10.3329/bjms.v19i2.45004.
Moody, G.D., Siponen, M., Pahnila, S., 2018. Toward a unified model of information security policy compliance. MIS Q. 42 (1), 285–311. doi:10.25300/MISQ/2018/13853.
Mousavi, R., Chen, R., Kim, D.J., Chen, K., 2020. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decis. Support Syst. 135, 113323. doi:10.1016/j.dss.2020.113323.
Norman, P., Webb, T.L., Millings, A., 2019. Using the theory of planned behaviour and implementation intentions to reduce binge drinking in new university students. Psychol. Health 34 (4), 478–496. doi:10.1080/08870446.2018.1544369.
Okuhara, T., Okada, H., Kiuchi, T., 2020. Examining persuasive message type to encourage staying at home during the COVID-19 pandemic and social lockdown: arandomized controlled study in Japan. Patient Educ. Couns. 103 (12), 2588–2593. doi:10.1016/j.pec.2020.08.016.
Osman, A., Barrios, F.X., Osman, J.R., Schneekloth, R., Troutman, J.A., 1994. The pain anxiety symptoms scale: psychometric properties in a community sample. J. Behav. Med. 17 (5), 511–522. doi:10.1007/BF01857923.
Pang, S.M., Tan, B.C., Lau, T.C., 2021. Antecedents of consumers' purchase intention towards organic food: integration of theory of planned behavior and protection motivation theory. Sustainability 13 (9), 5218. doi:10.3390/su13095218.
Park, H.S., Smith, S.W., 2007. Distinctiveness and influence of subjective norms, personal descriptive and injunctive norms, and societal descriptive and injunctive norms on behavioral intent: a case of two behaviors critical to organ donation. Hum. Commun. Res. 33, 194–218. doi:10.1111/j.1468-2958.2007.00296.x.
Prasetyo, Y.T., Castillo, A.M., Salonga, L.J., Sia, J.A., Seneta, J.A., 2020. Factors affecting perceived effectiveness of COVID-19 prevention measures among filipinos during enhanced community quarantine in luzon, Philippines: integrating protec-

tion motivation theory and extended theory of planned behavior. Int. J. Infect. Dis. 99, 312–323. doi:10.1016/j.ijid.2020.07.074.
Rajab, M., Eydgahi, A., 2019. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Comput. Secur. 80, 211–223. doi:10.1016/j.cose.2018.09.016.
Rhodes, R.E., Boudreau, P., Josefsson, K.W., Ivarsson, A., 2021. Mediators of physical activity behaviour change interventions among adults: a systematic review and meta-analysis. Health Psychol. Rev. 15 (2), 272–286. doi:10.1080/17437199.2019.1706614.
Rhodes, R.E., Quinlan, A., Naylor, P.-J., Warburton, D.E.R., Blanchard, C.M., 2020. Predicting personal physical activity of parents during participation in a family intervention targeting their children. J. Behav. Med. 43 (2), 209–224. doi:10.1007/s10865-019-00116-2.
Rodríguez-Priego, N., Porcu, L., 2021. Challenges in times of a pandemic: what drives and hinders the adoption of location-based applications? Econ. Res. 1–21. doi:10.1080/1331677X.2021.1902364.
Rogers, C.J., Forster, M., Bahr, K., Benjamin, S.M., 2020. A cross-sectional study using health behavior theory to predict rapid compliance with campus emergency notifications among college students. Disaster Med. Public Health Prep. 1–10. doi:10.1017/dmp.2019.153.
Rowe, F., Ngwenyama, O., Richet, J.-L., 2020. Contact-tracing apps and alienation in the age of COVID-19. Eur. J. Inf. Syst. 1–18. doi:10.1080/0960085X.2020.1803155.
Sadeghi, R., Mazloomy Mahmoodabad, S.S., Fallahzadeh, H., Rezaeian, M., Bidaki, R., Khanjani, N., 2020. Hookah is the enemy of health campaign: a campaign for prevention of hookah smoking among youth. Health Promot. Int. 35 (5), 1125–1136. doi:10.1093/heapro/daz109.
Schwaller, N.L., Kelmenson, S., BenDor, T.K., Spurlock, D., 2020. From abstract futures to concrete experiences: how does political ideology interact with threat perception to affect climate adaptation decisions? Environ. Sci. Policy 112, 440–452. doi:10.1016/j.envsci.2020.07.001.
Seow, A.N., Choong, Y.O., Moorthy, K., Choong, C.K., 2021. Predicting medical tourism behavioural intention using social cognition models. Tourism Rev. 76 (2), 374–391. doi:10.1108/TR-06-2019-0267.
Shahbaznezhad, H., Kolini, F., Rashidirad, M., 2020. Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter? J. Comput. Inf. Syst. 1–12. doi:10.1080/08874417.2020.1812134.
Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., Dwivedi, Y.K., 2021. Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps. IEEE Trans. Eng. Manag. 1–17. doi:10.1109/TEM.2020.3019033.
da Silva, C.M.R., Feitosa, E.L., Garcia, V.C., 2020. Heuristic-based strategy for phishing prediction: asurvey of URL-based approach. Comput. Secur. 88, 101613. doi:10.1016/j.cose.2019.101613.
Sinclair, P.M., Kable, A., Levett-Jones, T., Holder, C., Oldmeadow, C.J., 2019. The CKD-DETECT study: an RCT aimed at improving intention to initiate a kidney health check in Australian practice nurses. J. Clin. Nurs. 28 (15–16), 2745–2759. doi:10.1111/jocn.14882.
Siuki, H.A., Peyman, N., Vahedian-Shahroodi, M., Gholian-Aval, M., Tehrani, H., 2019. Health education intervention on HIV/AIDS prevention behaviors among health volunteers in healthcare centers: an applying the theory of planned behavior. J. Soc. Serv. Res. 45 (4), 582–588. doi:10.1080/01488376.2018.1481177.
Strycharz, J., Smit, E., Helberger, N., van Noort, G., 2021. No to cookies: empowering impact of technical and legal knowledge on rejecting tracking cookies. Comput. Hum. Behav. 120, 106750. doi:10.1016/j.chb.2021.106750.
Taylor, S., Todd, P.A., 1995. Understanding information technology usage: a test of competing models. Inf. Syst. Res. 6 (2), 144–176. doi:10.1287/isre.6.2.144.
Tschakert, K.F., Ngamsuriyaroj, S., 2019. Effectiveness of and user preferences for security awareness training methodologies. Heliyon 5 (6), e02010. doi:10.1016/j.heliyon.2019.e02010.
Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D., 2003. User acceptance of information technology: toward a unified view. MIS Q. 27 (3), 425–478. doi:10.2307/30036540.
Vrhovec, S., Mihelič, A., 2021. Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. Comput. Secur. 106, 102309. doi:10.1016/j.cose.2021.102309.
Wang, Y., Liang, J., Yang, J., Ma, X., Li, X., Wu, J., Yang, G., Ren, G., Feng, Y., 2019. Analysis of the environmental behavior of farmers for non-point source pollution control and management: an integration of the theory of planned behavior and the protection motivation theory. J. Environ. Manag. 237, 15–23. doi:10.1016/j.jenvman.2019.02.070.
Weaver, B.W., Braly, A.M., Lane, D.M., 2021. Training users to identify phishing emails. J. Educ. Comput. Res. doi:10.1177/0735633121992516. 073563312199251
Weston, D., Ip, A., Amlôt, R., 2020. Examining the application of behaviour change theories in the context of infectious disease outbreaks and emergency response: a review of reviews. BMC Public Health 20 (1), 1483. doi:10.1186/s12889-020-09519-2.
White, K.M., Zhao, X., Starfelt Sutton, L.C., Young, R.M., Hamilton, K., Hawkes, A.L., Leske, S., 2018. Effectiveness of a theory-based sun-safe randomised behavioural change trial among Australian adolescents. Psycho-Oncology 28 (3), pon.4967. doi:10.1002/pon.4967.
Williams, E.J., Joinson, A.N., 2020. Developing a measure of information seeking about phishing. J. Cybersecur. 6 (1), 1–16. doi:10.1093/cybsec/tyaa001.
Witte, K., 1994. Fear control and danger control: a test of the extended parallel process model (EPPM). Commun. Monogr. 61 (2), 113–134. doi:10.1080/03637759409376328.
Wong, G.J., Lau, J., Tan, K.-K., 2021. The effect of a simple phone call intervention on FIT-positive individuals: an exploratory study. Int. J. Colorectal Dis. 36 (1), 187–190. doi:10.1007/s00384-020-03742-4.
Xu, H., Dinev, T., Smith, J., Hart, P., 2011. Information privacy concerns: linking individual perceptions with institutional privacy assurances. J. Assoc. Inf. Syst. 12 (12), 798–824. doi:10.17705/1jais.00281.
Yang, L., Zhang, X., Zhu, X., Luo, Y., Luo, Y., 2019. Research on risky driving behavior of novice drivers. Sustainability 11 (20), 5556. doi:10.3390/su11205556.
Youn, S.-y., Lee, J.E., Ha-Brookshire, J., 2021. Fashion consumers' channel switching behavior during the COVID-19: protection motivation theory in the extended planned behavior framework. Cloth. Text. Res. J. 39 (2), 139–156. doi:10.1177/0887302X20986521.
Zhang, X., Liu, S., Wang, L., Zhang, Y., Wang, J., 2019. Mobile health service adoption in China. Online Inf. Rev. 44 (1), 1–23. doi:10.1108/OIR-11-2016-0339.
Zhang, X.A., Borden, J., 2020. How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. J. Risk Res. 23 (10), 1336–1352. doi:10.1080/13669877.2019.1646315.
Zhao, X., White, K.M., McD Young, R., 2019. A TPB-based smoking intervention among Chinese high school students. Subst. Use Misuse 54 (3), 459–472. doi:10.1080/10826084.2018.1508298.
Žnidaršič, J., Bernick, M., 2021. Impact of work-family balance results on employee work engagement within the organization: the case of Slovenia. PLoS One 16, e0245078. doi:10.1371/journal.pone.0245078.

Simon Vrhovec received the Ph.D. degree in computer and information science from the University of Ljubljana, Ljubljana, Slovenia, in 2015. He is currently an Associate Professor at the University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia. His main research interests include human factors in cybersecurity, software security engineering, agile methods, and change management. He has been in the steering committee of the European Interdisciplinary Cybersecurity Conference (EICC), since 2019, and co-chaired the Central European Cybersecurity Conference (CECC), in 2018 and 2019. He is an Editorial Board Member of the Journal of Cyber Security and Mobility (JCSANDM), Frontiers in Computer Science, EUREKA: Social and Humanities, and International Journal of Cyber Forensics and Advanced Threat Investigations (CFATI). He serves or has served as a Guest Editor for IEEE Security & Privacy, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), and Journal of Universal Computer Science (J.UCS) (simon.vrhovec@um.si).

Igor Bernik (male) is Professor of Security Sciences, Vice Dean for Quality Assurance and Development and Acting Vice Dean for Research at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. He received the Ph.D. in Management of Information Systems from the University of Maribor. His research fields are information systems, cybernetics, cybersecurity, and the growing requirement for cybersecurity awareness. He is an author and co-author of several scientific articles published in recognized international journals and conferences as well as the author of a book entitled Cybercrime and Cyberwarfare published by Wiley in 2014 (igor.bernik@um.si).

Blaž Markelj received the Ph.D. degree in Security Science from the University of Maribor, Slovenia in 2014. He is currently an Associate Professor and Head of the Information Security Department at the University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia. His main research interests include information security, threats assessment in cybersecurity, mobile device cybersecurity, combining law and cybersecurity, regulations in cybersecurity. He has been in the steering committee of the European Interdisciplinary Cybersecurity Conference (EICC) since 2019 and the chair of National Conference of Cyber Security "Information Security: Thrust in Humans and Technology" since 2019. He is co-author of several scientific articles and author of books written in Slovenian language. He has conducted several scientific and professional presentation and lectures regarding cyber security to people in public sector and economy. (blaz.markelj@um.si)