Survey about social engineering and the Varni na internetu awareness campaign, 2020

SIMON VRHOVEC, University of Maribor, Slovenia

This paper reports on a study aiming to explore factors associated with behavioral intention to follow a social engineering awareness campaign. The objectives of this study were to determine how perceived severity, perceived vulnerability, perceived threat, fear, subjective norm, attitude towards behavior, perceived behavioral control, self-efficacy, response efficacy, trust in authorities, perceived regulation, authorities performance, information sensitivity and privacy concern are associated with individuals’ behavioral intention to follow a social engineering awareness campaign. The study employed a cross-sectional research design. A survey was conducted among individuals in Slovenia between January and June 2020. A total of 553 respondents completed the survey providing for N=542 useful responses after excluding poorly completed responses (27.9 percent response rate). The survey questionnaire was developed in English. A Slovenian translation of the survey questionnaire is available.

Additional Key Words and Phrases: social engineering, awareness campaign, intervention, cybersecurity, cyber threat, computer security, internet

1 INTRODUCTION

The survey questionnaire was designed to measure theoretical constructs included in the research model. All items were taken or adapted from existing literature to fit the study’s context. Table 1 presents the theoretical constructs included in the research model, their definition in this research, and sources from which construct items were taken or adapted.
## 2 METHOD

### 2.1 Survey instrument

To test the research model a survey questionnaire was developed. Adapted and new questionnaire items (i.e., perceived severity, perceived vulnerability, perceived threat, fear, subjective norm, attitude towards behavior, perceived behavioral control, self-efficacy, response efficacy, trust in authorities, perceived regulation, authorities performance, information sensitivity, and behavioral intention) were developed by following a predefined protocol.

The questionnaire was first developed in English and then translated into Slovenian by a translator. The Slovenian questionnaire has been pre-tested by 3 independent respondents who provided feedback on its clarity. Based on the received feedback, the Slovenian questionnaire was reviewed to remove any ambiguity. Items were reworded, added, and deleted in the pre-test. To ensure the consistency between the Slovenian and English questionnaire, the Slovenian questionnaire was translated back to English. No significant differences in the meaning between the original items in English and back-translations were noticed. The English questionnaire was however reviewed to update the items and to remove any ambiguity based on the back-translation.

Table 2 presents the survey questionnaire in English and Table 3 presents the Slovenian translation of the survey questionnaire. All items were measured using a 5-point Likert scale as presented in Table 4.

### Table 1. Theoretical constructs in the survey questionnaire.

| Theoretical construct          | Definition in this research                                                                 | Sources |
|-------------------------------|---------------------------------------------------------------------------------------------|---------|
| Perceived severity            | The perceived extent of consequences of a successful social engineering attack.             | [3, 8]  |
| Perceived vulnerability       | The perceived probability of a successful social engineering attack.                         | [3, 4]  |
| Perceived threat              | The perceived extent of threats to the individual posed by social engineering attacks.      | [3, 6]  |
| Fear                          | The level of the individual’s fear of social engineering.                                    | [4, 9]  |
| Subjective norm               | The perception of social approval from important others regarding following awareness campaign materials. | [10, 11] |
| Attitude towards behavior     | An individual’s positive versus negative evaluations of following awareness campaign materials. | [8, 10, 11] |
| Perceived behavioral control  | The perception of the ease or difficulty of following awareness campaign materials.          | [10, 11] |
| Self-efficacy                 | The individual’s self-efficacy when implementing social engineering countermeasures (i.e., following awareness campaign materials). | [1, 5]  |
| Response efficacy             | The perceived efficacy of social engineering countermeasures (i.e., following awareness campaign materials). | [4, 8]  |
| Trust in authorities          | The degree of trust (trusting beliefs) in state authorities.                                  | [4, 7]  |
| Perceived regulation          | The perceived appropriateness of the regulative framework for fighting social engineering. | [3]     |
| Authorities performance       | The perceived performance of state authorities when dealing with social engineering.         | [2]     |
| Information sensitivity       | The perceived sensitivity of an individual’s online information.                             | [3]     |
| Privacy concern               | The extent of concerns regarding privacy online.                                             | [3]     |
| Behavioral intention          | The level of individual’s motivation to follow awareness campaign materials in the near future. | [10]    |
**Table 2. Survey questionnaire items (English original).**

| Construct                  | Prompt/Item                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Perceived severity (PS)    | Mark your agreement with the statements about social engineering:  
| PS1. My personal data acquired with social engineering could be misused for criminal purposes.  
| PS2. My personal data collected with social engineering could be misused against me.  
| PS3. Stealing of my personal data with social engineering would be a serious problem for me. |
| Perceived vulnerability (PV)| Mark your agreement with the statements about social engineering:  
| PV1. I am very vulnerable to social engineering.  
| PV2. I can easily become a victim of social engineering.  
| PV3. It is likely that I will become a victim of social engineering in the near future. |
| Perceived threat (PT)      | Mark your agreement with the statements about social engineering:  
| PT1. I feel threatened by social engineering.  
| PT2. Social engineering threatens me.  
| PT3. Social engineering is a danger to me. |
| Fear (F)                   | Mark your agreement with the statements about social engineering:  
| F1. I am afraid of social engineering.  
| F2. Social engineering is very frightening.  
| F3. I am afraid of being victimized by social engineering. |
| Subjective norm (SN)       | Mark your agreement with the statements about following the Varni na internetu awareness campaign:  
| SN1. People who are important to me think that I should follow awareness campaign materials.  
| SN2. Most people whose opinion I value consider that I should follow awareness campaign materials.  
| SN3. It is expected of me that I follow awareness campaign materials. |
| Attitude towards behavior (AtB)| Mark your agreement with the statements about following the Varni na internetu awareness campaign:  
| AtB1. Following awareness campaign materials is a very good idea.  
| AtB2. Following awareness campaign materials would be very wise.  
| AtB3. Following awareness campaign materials is very beneficial. |
| Perceived behavioral control (PBC)| Mark your agreement with the statements about following the Varni na internetu awareness campaign:  
| PBC1. If I want to, I can follow awareness campaign materials.  
| PBC2. I know how to follow awareness campaign materials.  
| PBC3. I have the resources necessary to follow awareness campaign materials. |
| Self-efficacy (SE)         | Mark your agreement with the statements about following the Varni na internetu awareness campaign:  
| SE1. It is easy to follow awareness campaign materials.  
| SE2. I would feel comfortable following awareness campaign materials.  
| SE3. I am able to follow awareness campaign materials without much effort. |
| Response efficacy (RE)     | Mark your agreement with the statements about following the Varni na internetu awareness campaign:  
| RE1. Following awareness campaign materials lowers the success of social engineering.  
| RE2. Following awareness campaign materials helps in preventing social engineering.  
| RE3. If I follow awareness campaign materials, I am less likely to be victimized by social engineering. |
| Trust in authorities (TiA) | Mark your agreement with the statements about state authorities (e.g., police, national cybersecurity response center SI-CERT):  
| TiA1. I believe that the state authorities would act in my best interest.  
| TiA2. I would characterize state authorities as honest.  
| TiA3. I trust state authorities. |
| Perceived regulation (PR)  | Mark your agreement with the statements about the adequacy of the legislation for fighting social engineering:  
| PR1. Our legislation provides for appropriate measures for fighting social engineering.  
| PR2. The international legislation provides for appropriate measures for fighting social engineering.  
| PR3. The government does enough to fight social engineering. |
| Authorities performance (AP)| Mark your agreement with the statements about the activities of state authorities (e.g., police, national cybersecurity response center SI-CERT) for fighting social engineering:  
| AP1. State authorities are successfully dealing with social engineering.  
| AP2. State authorities are successfully working with internet users to address social engineering.  
| AP3. State authorities are successfully preventing social engineering. |
| Information sensitivity (IS)| Mark your agreement with the statements about your activity online:  
| IS1. I consider the content of my e-mails as very sensitive.  
| IS2. I consider data on which websites I visit as very sensitive.  
| IS3. I consider data on what I do online as very sensitive. |
| Privacy concern (PC)       | Mark your agreement with the statements about your personal data online:  
| PC1. It highly bothers me when websites ask me about my personal data.  
| PC2. I always think twice before submitting my personal data online.  
| PC3. I am very concerned that websites collect too much personal data about me. |
| Behavioral intention (BI)  | Mark your agreement with the statements about following the Varni na internetu awareness campaign:  
| BI1. I intend to follow awareness campaign materials in the near future.  
| BI2. I have it in my mind to follow awareness campaign materials in the near future.  
| BI3. I will follow awareness campaign materials in the near future. |
| Construct | Prompt/Item |
|-----------|-------------|
| Perceived severity (PS) | Označite svoje strinjanje z izjavami o družbenem inženiringu: <br>PS1. Moji osebni podatki, pridobljeni z družbenim inženiringom, bi bili lahko zlorabljeni v kriminalne namene. <br>PS2. Moji osebni podatki, pridobljeni z družbenim inženiringom, bi bili lahko zlorabljeni zoper mene. <br>PS3. Kraja mojih osebnih podatkov z družbenim inženiringom bi bila zame resna težava. |
| Perceived vulnerability (PV) | Označite svoje strinjanje z izjavami o družbenem inženiringu: <br>PV1. Zelo sem ranljiv za družbeni inženiring. <br>PV2. Zahtjevam informacije o družbenem inženiringu v bližini prihodnosti. <br>PV3. Verjetno bom postal žrtva družbenega inženiringa v bližini prihodnosti. |
| Perceived threat (PT) | Označite svoje strinjanje z izjavami o družbenem inženiringu: <br>PT1. Zaradi družbenega inženiringa se počutim ogroženega. <br>PT2. Družbeni inženiring mi predstavlja nevarnost. <br>PT3. Družbeni inženiring mi predstavlja nevarnost. |
| Fear (F) | Označite svoje strinjanje z izjavami o družbenem inženiringu: <br>F1. Bojim se družbenega inženiringa. <br>F2. Družbeni inženiring je zelo zastrašujoč. <br>F3. Bojim se družbenega inženiringa. |
| Subjective norm (SN) | Označite svoje strinjanje z izjavami o spremljanju vsebin programa ozaveščanja Varni na internetu: <br>SN1. Ljudje, ki so mi pomembni, mislijo, da bi moral spremljati vsebine programa ozaveščanja. <br>SN2. Večina ljudi, katerih cenim, meni, da bi moral spremljati vsebine programa ozaveščanja. <br>SN3. Od mene se pričakuje, da spremljam vsebine programa ozaveščanja. |
| Attitude towards behavior (AtB) | Označite svoje strinjanje z izjavami o spremljanju vsebin programa ozaveščanja Varni na internetu: <br>AtB1. Spremljanje vsebin programa ozaveščanja je zelo dobr a ideja. <br>AtB2. Spremljanje vsebin programa ozaveščanja bi bilo zelo pametno. <br>AtB3. Spremljanje vsebin programa ozaveščanja je zelo koristno. |
| Perceived behavioral control (PBC) | Označite svoje strinjanje z izjavami o spremljanju vsebin programa ozaveščanja Varni na internetu: <br>PBC1. Če želim, lahko spremljam vsebine programa ozaveščanja. <br>PBC2. Vem, kako spremljati vsebine programa ozaveščanja. <br>PBC3. Imam vse potrebno za spremljanje vsebin programa ozaveščanja. |
| Self-efficacy (SE) | Označite svoje strinjanje z izjavami o spremljanju vsebin programa ozaveščanja Varni na internetu: <br>SE1. Vsebine programa ozaveščanja je preprosto spremljati. <br>SE2. Brez težav bi lahko spremljal vsebine programa ozaveščanja. <br>SE3. Sposoben sem spremljati vsebine programa ozaveščanja brez posebnega napora. |
| Response efficacy (RE) | Označite svoje strinjanje z izjavami o spremljanju vsebin programa ozaveščanja Varni na internetu: <br>RE1. Spremljanje vsebin programa ozaveščanja znižuje uspešnost družbenega inženiringa. <br>RE2. Spremljanje vsebin programa ozaveščanja pomaga pri preprečevanju družbenega inženiringa. <br>RE3. Če spremljam vsebine programa ozaveščanja, je manj verjetno, da postanem žrtev družbenega inženiringa. |
| Trust in authorities (TiA) | Označite svoje strinjanje z izjavami o državnih organih (npr. policija, nacionalni odzivni center za kibernetsko varnost SI-CERT): <br>TiA1. Verjamem, da državni organi delujejo v mojem najboljšem interesu. <br>TiA2. Državne organi bi opredelil kot poštene. <br>TiA3. Zaupam državnim organom. |
| Perceived regulation (PR) | Označite svoje strinjanje z izjavami o ustreznosti pravne ureditve za boj proti družbenemu inženiringu: <br>PR1. Naša zakonodaja predvideva ustrezne ukrepe za boj proti družbenemu inženiringu. <br>PR2. Mednarodna zakonodaja predvideva ustrezne ukrepe za boj proti družbenemu inženiringu. <br>PR3. Država stori dovolj za boj proti družbenemu inženiringu. |
| Authorities performance (AP) | Označite svoje strinjanje z izjavami o aktivnosti državnih organov (npr. policija, nacionalni odzivni center za kibernetsko varnost SI-CERT) pri soočanju z družbenim inženiringom: <br>AP1. Državni organi se uspešno spopadajo z družbenim inženiringom. <br>AP2. Državni organi uspešno sodelujejo z uporabniki interneta pri reševanju družbenega inženiringa. <br>AP3. Državni organi uspešno preprečujejo družbeni inženiring. |
| Information sensitivity (IS) | Označite svoje strinjanje z izjavami o vaši aktivnosti na spletu: <br>IS1. Vsebino svoje elektronske pošte dojemam kot zelo občutljivo. <br>IS2. Podatke o tem, katere spletne strani obiskujem, dojemam kot zelo občutljive. <br>IS3. Podatke o tem, kaj delam na spletu, dojemam kot zelo občutljive. |
| Privacy concern (PC) | Označite svoje strinjanje z izjavami o vaših osebnih podatkih na spletu: <br>PC1. Zelo me moti, ko me spletne strani sprašujejo po osebnih podatkih. <br>PC2. Preden posredujem svoje osebne podatke preko spletu, vedno premislim dvakrat. <br>PC3. Zelo me skrbi, da spletne strani o meni zbira preveč osebnih podatkov. |
| Behavioral intention (BI) | Označite svoje strinjanje z izjavami o spremljanju vsebin programa ozaveščanja Varni na internetu: <br>BI1. V bližini prihodnosti nameravam spremljati vsebine programa ozaveščanja. <br>BI2. V bližini prihodnosti nameravam spremljati vsebine programa ozaveščanja. <br>BI3. V bližini prihodnosti bom spremljal vsebine programa ozaveščanja. |
Table 4. 5-point Likert scale.

| Score | English          | Slovenian          |
|-------|------------------|--------------------|
| 1     | Strongly disagree| Močno se ne strinjam|
| 2     | Disagree         | Se ne strinjam     |
| 3     | Neutral          | Nevtralno          |
| 4     | Agree            | Se strinjam        |
| 5     | Strongly agree   | Močno se strinjam  |

2.2 Data collection

We conducted the survey with the Slovenian translation of the questionnaire among individuals in Slovenia who were at least 15 years old between 6 January 2020 and 24 June 2020. Respondents were recruited through University of Maribor students who were asked to distribute the survey questionnaire to their family and friends. The students were not compensated for distributing the survey questionnaire. Also, the respondents 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. After excluding poorly completed responses (responses with over 50 percent of missing values or standard deviation equal to 0 for constructs perceived severity, perceived vulnerability, perceived threat, fear, subjective norm, attitude towards behavior, perceived behavioral control, self-efficacy, response efficacy, trust in authorities, perceived regulation, authorities performance, information sensitivity, and behavioral intention), we were left with 542 useful responses providing for a response rate of 27.9 percent as presented in Table 5.

Table 5. Sample with the number of distributed questionnaires, number of responses, and number of useful responses (N) after excluding poorly completed responses.

| ID   | Name                | Distributed questionnaires | Responses | N   |
|------|---------------------|----------------------------|-----------|-----|
| 1    | Individuals in Slovenia | 1982                      | 553       | 542 |

Due to the sensitive nature of the survey topic, safeguards were put in place to encourage participation and honest responses. First, the respondents were informed about the voluntariness and anonymity of participating in the survey. Next, the respondents were assured that the collected data will be used for research purposes only. No special incentives were offered to encourage participation in the survey.

The first page of the survey is presented in Table 6.
Dear Sirs!

You are cordially invited to participate in a study on social engineering and the Varni na internetu awareness campaign conducted by the University of Maribor. Estimated time to complete the survey is 6-10 minutes.

Social engineering refers to the use of deception in order to manipulate individuals to disclose confidential or personal information that may then be used for criminal purposes.

Don’t worry if you’re not sure what social engineering and the Varni na internetu awareness campaign are. A short presentation of the most problematic types of social engineering in the last year, and a presentation of the Varni na internetu awareness campaign are part of the survey.

Participation in the research is voluntary and anonymous. Data will be used exclusively for research purposes.

Contact person:
Simon Vrhovec <simon.vrhovec@um.si>

Kind regards,
Simon Vrhovec

---

3 RESULTS

3.1 Sample

Demographic characteristics of the sample are presented in Table 7.
Table 7. Demographic characteristics of the sample.

| Characteristic         | Value         | Frequency |
|------------------------|---------------|-----------|
| Gender                 |               |           |
| 1 – Male               |               | 225       |
| 2 – Female             |               | 315       |
| Missing                |               | 13        |
| Formal education       |               |           |
| 1 – High school or less|               | 348       |
| 2 – Bachelor’s degree  |               | 139       |
| 3 – Master’s degree    |               | 48        |
| 4 – PhD degree         |               | 5         |
| Missing                |               | 13        |
| Employment status      |               |           |
| 1 – Student            |               | 267       |
| 2 – Employed           |               | 240       |
| 3 – Unemployed         |               | 11        |
| 4 – Retired            |               | 20        |
| Missing                |               | 15        |
| Age                    |               |           |
| 15                     |               | 1         |
| 16                     |               | 3         |
| 17                     |               | 1         |
| 18                     |               | 7         |
| 19                     |               | 47        |
| 20                     |               | 71        |
| 21                     |               | 67        |
| 22                     |               | 31        |
| 23                     |               | 28        |
| 24                     |               | 18        |
| 25                     |               | 18        |
| 26                     |               | 15        |
| 27                     |               | 9         |
| 28                     |               | 8         |
| 29                     |               | 10        |
| 30                     |               | 19        |
| 31                     |               | 4         |
| 32                     |               | 10        |
| 33                     |               | 7         |
| 34                     |               | 3         |
| 35                     |               | 10        |
| 36                     |               | 3         |
| 37                     |               | 3         |
| 38                     |               | 7         |
| 39                     |               | 7         |
| 40                     |               | 5         |
| 41                     |               | 4         |
| 42                     |               | 8         |
| 43                     |               | 8         |
| 44                     |               | 8         |
| 45                     |               | 8         |
| 46                     |               | 4         |
| 47                     |               | 3         |
| 48                     |               | 9         |
| 49                     |               | 7         |
| 50                     |               | 10        |
| 51                     |               | 5         |
| 52                     |               | 8         |
| 53                     |               | 4         |
| 54                     |               | 7         |
| 55                     |               | 6         |
| 56                     |               | 2         |
| 57                     |               | 4         |
| 59                     |               | 2         |
| 60                     |               | 5         |
| 61                     |               | 3         |
| 62                     |               | 3         |
| 64                     |               | 1         |
| 65                     |               | 2         |
| 66                     |               | 2         |
| 68                     |               | 1         |
| 69                     |               | 1         |
| 73                     |               | 1         |
| 74                     |               | 1         |
| 75                     |               | 1         |
| 78                     |               | 1         |
| Missing                |               | 12        |
### 3.2 Frequencies

Frequencies of all variables for measured theoretical constructs are presented in Table 8.

| Variable | 1  | 2  | 3  | 4  | 5  | Valid | Missing | Total |
|----------|----|----|----|----|----|-------|---------|-------|
| IS1      | 14 | 93 | 200| 176| 69 | 552   | 1       | 553   |
| IS2      | 12 | 98 | 208| 169| 64 | 551   | 2       | 553   |
| IS3      | 10 | 85 | 153| 201| 97 | 546   | 7       | 553   |
| PC1      | 3  | 19 | 50 | 244| 236| 552   | 1       | 553   |
| PC2      | 2  | 26 | 51 | 201| 271| 551   | 2       | 553   |
| PC3      | 3  | 27 | 88 | 196| 237| 551   | 2       | 553   |
| TiA1     | 19 | 82 | 236| 186| 30 | 553   | 0       | 553   |
| TiA2     | 29 | 103| 236| 153| 29 | 550   | 3       | 553   |
| TiA3     | 35 | 103| 240| 142| 30 | 550   | 3       | 553   |
| AP1      | 13 | 116| 303| 103| 3  | 538   | 15      | 553   |
| AP2      | 14 | 104| 294| 117| 10 | 539   | 14      | 553   |
| AP3      | 17 | 146| 297| 72 | 3  | 535   | 18      | 553   |
| PR1      | 8  | 128| 252| 146| 3  | 537   | 16      | 553   |
| PR2      | 10 | 80 | 270| 164| 12 | 536   | 17      | 553   |
| PR3      | 26 | 211| 231| 62 | 7  | 537   | 16      | 553   |
| PV1      | 47 | 162| 185| 125| 15 | 534   | 19      | 553   |
| PV2      | 49 | 182| 115| 162| 29 | 537   | 16      | 553   |
| PV3      | 84 | 187| 183| 73 | 10 | 537   | 16      | 553   |
| PS1      | 24 | 94 | 129| 248| 42 | 537   | 16      | 553   |
| PS2      | 19 | 70 | 116| 270| 63 | 538   | 15      | 553   |
| PS3      | 13 | 52 | 118| 219| 136| 538   | 15      | 553   |
| PT1      | 18 | 147| 234| 127| 14 | 540   | 13      | 553   |
| PT2      | 27 | 159| 253| 93 | 8  | 540   | 13      | 553   |
| PT3      | 22 | 120| 244| 135| 18 | 539   | 14      | 553   |
| F1       | 37 | 165| 203| 111| 23 | 539   | 14      | 553   |
| F2       | 38 | 125| 193| 144| 38 | 538   | 15      | 553   |
| F3       | 39 | 143| 194| 129| 33 | 538   | 15      | 553   |
| SE1      | 8  | 55 | 177| 269| 28 | 537   | 16      | 553   |
| SE2      | 6  | 46 | 138| 317| 33 | 540   | 13      | 553   |
| SE3      | 5  | 32 | 136| 299| 63 | 535   | 18      | 553   |
| RE1      | 3  | 36 | 191| 262| 45 | 537   | 16      | 553   |
| RE2      | 6  | 20 | 167| 303| 43 | 539   | 14      | 553   |
| RE3      | 2  | 36 | 123| 292| 83 | 536   | 17      | 553   |
| PBC1     | 1  | 9  | 89 | 363| 76 | 538   | 15      | 553   |
| PBC2     | 8  | 59 | 187| 242| 43 | 539   | 14      | 553   |
| PBC3     | 10 | 45 | 168| 250| 66 | 539   | 14      | 553   |
| SN1      | 23 | 118| 223| 152| 22 | 538   | 15      | 553   |
| SN2      | 28 | 100| 239| 150| 20 | 537   | 16      | 553   |
| SN3      | 33 | 105| 223| 157| 20 | 538   | 15      | 553   |
| AtB1     | 3  | 12 | 68 | 336| 120| 539   | 14      | 553   |
| AtB2     | 2  | 6  | 67 | 321| 143| 539   | 14      | 553   |
| AtB3     | 2  | 4  | 72 | 309| 151| 538   | 15      | 553   |
| BI1      | 21 | 73 | 206| 208| 32 | 540   | 13      | 553   |
| BI2      | 21 | 74 | 181| 224| 38 | 538   | 15      | 553   |
| BI3      | 24 | 63 | 204| 206| 41 | 538   | 15      | 553   |
4 DISCUSSION

This paper presents the results of a survey about social engineering and the Varni na internetu awareness campaign. Future studies may focus on other factors associated with individuals’ motivation to follow awareness campaign materials. Such studies would be beneficial both to better explain the motivation of internet users to follow awareness campaigns, and to better understand the associations between different factors associated with it.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to the respondents who took their time to participate in our survey. We would also like to thank the students who helped with data collection, and Luka Jelovčan for data screening and entry.

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.

REFERENCES

[1] Catherine L. Anderson and Ritu Agarwal. 2010. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly 34, 3 (2010), 613–643.
[2] Matthew S. Crow, Jamie A. Snyder, Vaughn J. Crichlow, and John Ortiz Smykla. 2017. Community Perceptions of Police Body-Worn Cameras. Criminal Justice and Behavior 44, 4 (2017), 589–610. https://doi.org/10.1177/0093854816688037
[3] Damjan Fuis, Anže Mihelič, and Simon Vrhovec. 2019. Social Network Self-Protection Model: What Motivates Users to Self-Protect? Journal of Cyber Security and Mobility 8, 4 (2019), 467–492. https://doi.org/10.13052/jcsm2245-1439.844
[4] Jurjen Jansen and Paul van Schaik. 2018. Testing a model of precautionary online behaviour: The case of online banking. Computers in Human Behavior 87 (2018), 371–383. https://doi.org/10.1016/j.chb.2018.05.010
[5] Allen C. Johnston and Merrill Warkentin. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34, 3 (2010), 549. https://doi.org/10.2307/25756691
[6] Huigang Liang and Yajiong Xue. 2010. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association for Information Systems 11, 7 (2010), 394–413.
[7] D. Harrison McKnight, Vivek Choudhury, and Charles Kacmar. 2002. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. The Journal of Strategic Information Systems 11, 3-4 (2002), 297–323. https://doi.org/10.1016/S0963-8687(02)00020-3
[8] Gregory D. Moody, Mikko Siponen, and Seppo Pahnila. 2018. Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly 42, 1 (2018), 285–311. https://doi.org/10.25300/MISQ/2018/13853
[9] Augustine Osman, Francisco X. Barrios, Joylene R. Osman, Raelynn Schneekloth, and Josh A. Troutman. 1994. The Pain Anxiety Symptoms Scale: Psychometric properties in a community sample. Journal of Behavioral Medicine 17, 5 (1994), 511–522. https://doi.org/10.1007/BF01857923
[10] Hee Sun Park and Sandi W. Smith. 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. Human Communication Research 33 (2007), 194–218. https://doi.org/10.1111/j.1468-2958.2007.00296.x
[11] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27, 3 (2003), 425–478. https://doi.org/10.2307/30036540