Kategorizacija uporabnikov na podlagi njihovega z informacijsko varnostjo povezanega znanja, stališčin vedenja: pilotna študija

Damjan Fujs[1], Simon Vrhovec[2], Damjan Vavpotič[1]
[1]Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana 2Univerza V Mariboru, Fakulteta za varnostne vede, Kotnikova 8, 1000 Ljubljana poštni naslov ustanove damjan.fujs@fri.uni-lj.si, simon.vrhovec@um.si, damjan.vavpotic@fri.uni-lj.si

Izvleček

V tem prispevku predstavljamo pristop za kategorizacijo uporabnikov, ki temelji na preverjenem vprašalniku o človeških vidikih informacijske varnosti (HAIS-Q). Na tej podlagi smo izvedli razvrščanje uporabnikov (N = 165). Analiza je pokazala tri skupine uporabnikov (uporabniki z nizkim, zmernim in visokim tveganjem). Izračunali smo indeks silhuete (0,44) za potrditev kakovosti razvrščanja, ki kaže na ustrezno kakovost razvrščanja. Naš pristop (kombinacija HAIS-Q in razvrščanja v skupine) omogoča prilagojeno usposabljanje 1) uporabnikov, ki dosežejo najnižje vrednosti pri HAIS-Q in 2) uporabnikov, ki dosegajo splošno nizko tveganje, vendar se na nekaterih področjih odrežejo nekoliko slabše. V primerjavi s sorodnimi pristopi je naša prednost enostavnost uporabe in ublažitev pristranskosti, saj je pristop namenjen analiziranju skupin in ne posameznikov. Poleg tega naš pristop omogoča razvrščanje na podlagi prioritizacije spremenljivk, medtem ko obstoječe raziskave obravnavajo vse spremenljivke enako pomembne.

Ključne besede: kibernetska varnost, informacijska varnost, inženirstvo zahtev, segmentacija uporabnikov.

Abstract

In this paper, we present an approach for user categorization based on the established Human Aspects of Information Security Questionnaire (HAIS-Q). Clustering based on HAIS-Q data (N = 165) was performed. In doing so, three groups of users were identified (low, moderate and high-risk users). The silhouette measure of cohesion and separation (0.44) was conducted to validate the quality of clustering. A fair cluster quality was indicated. Our approach (a combination of HAIS-Q and clustering) allows for the tailored training of 1) users who achieve the lowest values in HAIS-Q and 2) users who achieve overall high results but perform slightly worse in certain focus areas. In comparison to similar approaches, our advantage is the ease of use and mitigation of social desirability bias since the approach is designed to analyze user groups only. Additionally, our approach allows for focus area (variable) prioritization while existing studies consider all variables to be of equal value.

Keywords: Cyber security, information security, requirements engineering, user segmentation

1 UVOD

Pomanjkanje ustrezne informacijske varnosti lahko vodi v izgubo dobička in slab ugled organizacije (Roy Sarkar, 2010). Da bi dobili vpogled v dejansko stanje informacijske varnosti moramo implementirati ustrezne merilne mehanizme (Prislan et al., 2020), kot so kvantitativne in kvalitativne metrike (Fujs et al., 2020, 2019). Informacijska varnost se je tradicionalno zagotavljala s pomočjo tehničnih varnostnih mehanizmov (kot so npr. požarni zidovi), kljub temu, pa ne smemo zanemariti pomembnosti človeških vidikov zagotavljanja varnosti (Wiley et al., 2020). Da bi uporabniki z informacijskimi sistemi ravnali varno, morajo biti ustrezno usposobljeni, pri čemer pa univerzalni pristopi niso optimalni, saj ne upoštevajo varnostnih karakteristik posameznega uporabnika (Fujs et al., 2020).

Namen pričujočega prispevka je odgovoriti na zastavljena raziskovalna vprašanja: 1) kako oceniti človeške vidike informacijske varnosti? 2) kako kategorizirati uporabnike na tej podlagi? 3) kako nam ti rezultati lahko pomagajo pri prilagojenem usposabljanju?

2 ČLOVEŠKI VIDIKI INFORMACIJSKE VARNOSTI

Varnostne funkcije programske opreme so bile tradicionalno uvedene na koncu procesa razvoja programske opreme, brez upoštevanja uporabnikovih - z varnostjo povezanih karakteristik (Wiley et al., 2020). Cˇ e se je pojavila ranljivost, so jih razvijalci naslovili z varnostnimi popravki (Niazi et al., 2020). Pravilno nastavljene tehnične rešitve so učinkovite, vendar ne zadostne, da bi zagotovile celovito informacijsko varnost, saj obstajajo razlike med uporabniki v njihovem znanju, stališčih in vedenju glede informacijske varnosti (Neigel et al., 2020). V ta namen je bil razvit vprašalnik, ki meri ozaveščenost o informacijski varnosti (v nadaljevanju HAIS-Q; angl. Human Aspects of Information Security Questionnaire). HAIS-Q obravnava uporabnikovo z varnostjo-povezano znanje, stališča do varnosti in varno vedenje (Parsons et al., 2017), ki se osredotoča na sledečih sedem področij: *UISO* (uporaba socialnih omrežij), *UIN* (uporaba interneta), *POI* (poročanje o incidentih), *RZI* (ravnanje z informacijami), *UMN* (uporaba mobilnih naprav), *UEP* (uporaba e-pošte) in *UGE* (upravljanje gesel). Raziskave so pokazale, da je HAIS-Q dober napovedovalec človeških vidikov informacijske varnosti, saj uporabniki, ki so dosegali v povprečju višji indeks ozaveščenosti o informacijski varnosti, so bili uspešnejši v poskusih o zvabljanju (angl. *pshishing*) (Parsons et al., 2017). Podobno je bilo ugotovljeno v raziskavi o razlikah glede kibernetske higiene med moškimi in ženskami, kjer so s pomočjo regresijskih modelov ugotovili dobro napovedno moč posameznih dejavnikov oz. področij iz HAIS-Q (Neigel et al., 2020). HAIS-Q je bil uporabljen v še eni od študij glede razlik med demografskimi spremenljivkami (natančneje spol), kjer so ugotovili, da obstajajo statistično pomembne razlike med spoloma glede ozaveščenosti o informacijski varnosti (Wiley et al., 2020). Poleg ozaveščenosti o informacijski varnosti, imata pomembno vlogo tudi splošna organizacijska in varnostna kultura, kar pomeni, da če dvignemo splošno organizacijsko kulturo, dvignemo tudi varnostno kulturo (Wiley et al., 2020).

3 KATEGORIZACIJA UPORABNIKOV

Koncept kategorizacije (v literaturi poimenovan tudi kot *segmentacija*) je uporaben z vidika identifikacije različnih tipov uporabnikov. Beseda segmentacija se dandanes uporablja na področju računalniškega vida, vendar je bila prvotno uporabljena (in se še uporablja) na področju marketinga za identifikacijo različnih skupin uporabnikov Tolley (1975). V okviru našega pristopa bomo uporabili kategorizacijo uporabnikov, saj bomo na ta način identificirali različne uporabnike (npr. ranljive), na podlagi katerih bomo lahko predlagali prilagojena usposabljanja. Usposabljanja na področju informacijske varnosti so pomembna, saj težijo k njenemu izboljšanju (Neigel et al., 2020). V literaturi so poudarjeni številni pristopi za kategorizacijo uporabnikov na podlagi varnostnih karakteristik. Xiao (2021) kategorizira uporabnike pametnih mobilnih telefonov na podlagi spola ter tipa operacijskega sistema. Poleg tega, lahko kategorizacijo na podlagi spola zasledimo tudi v ostalih študijah, glej npr. (Wiley et al., 2020; Neigel et al., 2020; Parsons et al., 2017). Cain et al. (2018) raziskujejo vpliv starosti na poznavanje kibernetske higiene, pri čemer ugotavljajo, da obstoječi neprilagojeni pristopi za usposabljanje uporabnikov ne izboljšujejo znanja in vedenja uporabnikov. Anichiti et al. (2021) kategorizirajo uporabnike na podlagi njihovega znanja o kibernetski varnosti hotelov, pri čemer se za razliko od ostalih prej omenjenih avtorjev, osredotočajo na pripadnost generaciji - rojeni v različnih obdobjih (npr. generacija x, y in z). Poleg tega lahko v literaturi zasledimo kategorizacijo uporabnikov na podlagi vlog, ki jih imajo v organizacijah (Sarkar et al., 2020).

Optimalne skupine uporabnikov je nemogoče identificirati *a priori* brez podatkov, zato je pomembno, da izhajamo iz zbranih podatkov. V našem prispevku se osredotočamo na kategorizacijo uporabnikov na podlagi njihovih tveganj glede informacijske varnosti. Z vidika prilagojenih usposabljanj je treba imeti v mislih, da je manjše skupine lažje obvladovati. Namen gručenja na nivoju skupin je dvoplasten. Personalizirana usposabljanja so v realnem oziroma industrijskem okolju finančno breme, kar pomeni, da si velika večina tovrstnih usposabljanj ne more privoščiti. Na ta način iščemo razmerje med »realnimi« in »idealnimi« razmerami na področju informacijske varnosti. Zaradi tega je bolje, da izobražujemo uporabnike na nivoju skupin.

4 METODA

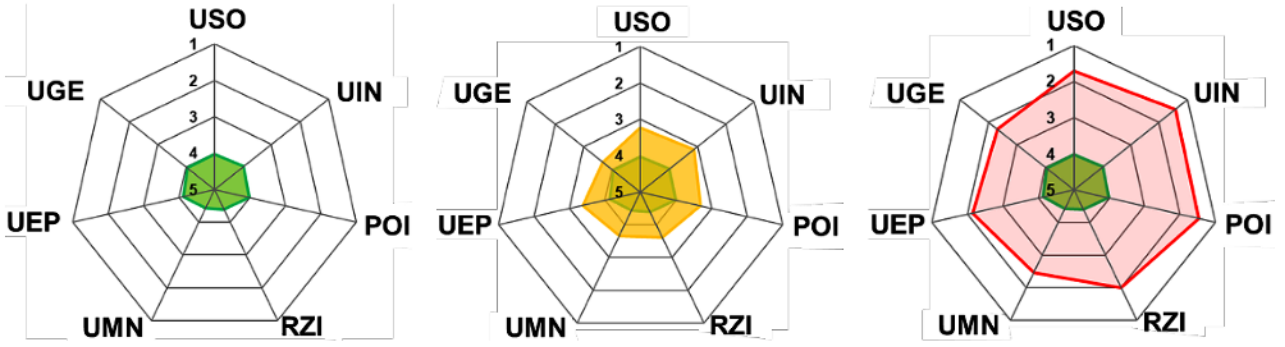
Za potrebe našega pristopa smo analizirali rezultate ankete 165 uporabnikov informacijskih sistemov ene izmed slovenskih univerz. V sklopu informacijskovarnostnih študij so študenti zelo primerna populacija za preučevanje informacijske varnosti (Aurigemma et al., 2019). Študenti so pogosti uporabniki informacijske tehnologije (mobilne naprave, aplikacije, socialna omrežja itd.) (Aurigemma et al., 2019) in so s tem tudi varnostno poudarjeni. Hkrati Hewitt in White (2020) med študenti opažata pomanjkanje zavedanja o informacijski varnosti, kar pa je značilno tudi za celotno populacijo uporabnikov informacijskih storitev (Falessi et al., 2018; Hameed and Arachchilage, 2021).V okviru našega pristopa smo prilagodili in prevedli HAIS-Q. HAIS-Q zajema 63 spremenljivk oziroma vprašanj, ki na Likertovi lestvici od 1 (se sploh ne strinjam) do 5 (se popolnoma strinjam) merijo ozaveščenost o informacijski varnosti. Raziskava je bila izvedena februarja 2021. Anketiranci so bili obveščeni, da je raziskava anonimna in prostovoljna. Vabilo k raziskavi je bilo poslano na 964 študentskih e-naslovov, pri čemer smo dosegli 17 % odziv. Zbrani podatki so bili kvalitativno pregledani. Glede na to, da ni bilo odstopanj, smo vse spremenljivke ohranili za nadaljnje analize. Podrobnejša demografska slika anketirancev je prikazana v Tabeli 1. 63 spremenljivk je bilo združenih v sedem faktorjev. Teh sedem faktorjev je bilo uporabljenih za potrebe razvrščanja v skupine (angl. *clustering*). Poleg tega smo izvedli tudi razvrstitev spremenljivk znotraj gruče glede na pomembnost, kar predstavlja dodano vrednost, saj obstoječi pristopi obravnavajo vse spremenljivke kot enako pomembne (Parsons et al., 2017). Za potrebe razvrščanja v skupine na podlagi HAIS-Q smo izbrali algoritem *TwoStep*, ki omogoča samodejno (ali vnaprej podano) identifikacijo primernega števila skupin (Tan, 2019). Dodatna prednost algoritma je iterativnost, saj lahko razvrščamo skupine, dokler identificiramo najbolj optimalno rešitev za preučevani primer. Za preverbo kakovosti razvrščanja smo izmerili indeks silhuete (angl. Silhouette index), ki lahko zavzame vrednost od -1 do 1, pri čemer 1 pomeni optimalno vrednost, saj so razdalje znotraj gruč kratke in razdalje med gručami velike (Celestino et al., 2018).

Tabela 1: **Demografske značilnosti vzorca na podlagi 165 anketirancev, pri čemer povprečna starost znaša 24 let.**

	Število #	Odstotek %
Vrsta študija		
Redni	136	83,0
Izredni	29	17,0
Stopnja in letnik študija		
1. letnik dodiplomskega študija	78	48,0
2. letnik dodiplomskega študija	18	11,0
3. letnik dodiplomskega študija	28	17,0
1. letnik podiplomskega študija	19	11,0
2. letnik podiplomskega študija	19	11,0
Doktorski študij	3	2,0
Spol		
Moški	48	29,0
Ženski	117	71,0
Življenjsko okolje		
Mestno	91	55,0
Podeželsko	74	45,0

5 REZULTATI IN RAZPRAVA

Slika 1 prikazuje polarni grafikon z identificiranimi skupinami na podlagi razvrščanja v skupine (TwoStep). Indeks silhuete znaša 0,44, kar pomeni, da je kakovost razvrščanja v skupine ustrezna. Iz Slike 1 lahko razberemo, da uporabniki z nizkim tveganjem dosegajo najboljše rezultate pri posameznih področjih HAIS-Q. Te skupine uporabnikov uporabimo za primerjavo med ostalima dvema skupinama. Upoštevajte, da je lestvica na polarnih grafikonih obrnjena, saj želimo prikazati odstopanje od normalnosti (torej od nizkega tveganja). Namen je identificirati stanje informacijske varnosti na sedmih področij od MSO do UGE ter nato vsakemu uporabniku, katerega znanje je na določenem področju pomanjkljivo, ponuditi namensko usposabljanje, da vrzeli s področja zapolnijo. Z vidika prilagojenega usposabljanja so najbolj zanimivi uporabniki z zmernim in/ali visokim tveganjem, saj najbolj odstopajo od normalnega oziroma zaželenega. Pristop je zasnovan na način, da se uporabnike izobražuje na tistih področjih, ki jih najslabše pokrivajo – oziroma tam kjer je odstopanje največje. Od podatkov oziroma gručenja pa je odvisno, v katero skupino bo posameznik uvrščen. Prednosti gručenja pred klasičnim skupinskim treningom sta predvsem finančna optimizacija in učinkovitejše usposabljanje saj vsakega uporabnika pošljemo na največ eno usposabljanje, pri čemer tovrstni način



a) Uporabniki z nizkim tveganjem (*N* = 137)
b) Uporabniki z zmernim tveganjem (*N* =24)
c) Uporabniki z visokim tveganjem (*N* =4)

Slika 1: **Primerjava skupin uporabnikov pri izbranih področjih človeških vidikov informacijske varnosti. Uporabniki z nizkim tveganjem (a) služijo kot merilo za primerjavo med ostalima dvema skupinama uporabnikov (b, c).**

zagotavlja tudi manj prekrivanj. Usposabljanja ki temeljijo na gručenju sicer niso tako prilagojena kot pri individualni obravnavi, vendar gre za nek kompromis med učinkovitostjo in stroški. Cilj izobraževanja mora biti doseganje nizkega tveganja. Da bi podrobneje razumeli dinamiko izbranih področij HAIS-Q znotraj gruče, predstavljamo Tabelo 2, v kateri izpostavimo pomembnost posameznega področja znotraj gruče.

Namen Tabele 2 je izpostaviti povprečne vrednosti izbranih področij HAIS-Q znotraj posamezne gruče. V primeru razvrstitev spremenljivk znotraj gruče glede na pomembnost gre za standardno meritev na skali od 0 do 1, ki se izračuna na podlagi statistične značilnosti posamezne spremenljivke znotraj gruče (Tkaczynski, 2016). Za lažji prikaz smo izbrali pet stopenj (naraščajoče z 0.2), pri čemer vrednosti manjše od 0.6 ni. Bolj, kot se vrednosti na barvni lestvici približujejo 1, bolj je spremenljivka statistično pomembna znotraj posamezne gruče. Na ta način omogočimo identifikacijo usposabljanja, ne samo za uporabnike z visokim tveganjem, ampak tudi za tiste, ki imajo splošno nizko tveganje, vendar na določenih področjih dosegajo odstopanje (npr. UIN in POI pri uporabniki z nizkim tveganjem).

V primerjavi s sorodnimi pristopi (Parsons et al., 2017), naš pristop omogoča 1) kategorizacijo uporabnikov na podlagi HAIS-Q spremenljivk in ne samo sodeč po demografskih karakteristikah, kot je npr. spol, izobrazba itd. S tem naslavljamo enega izmed pomembnih faktorjev pristranskosti pri evalvaciji informacijske varnosti (Wiley et al., 2020; Roy Sarkar, 2010), saj je znano, da je mogoče pristranskost znižati na način, da uporabnike vključimo v skupine (Kwak et al., 2019) ali pa da ne zbiramo vseh demografskih podatkov (Larson, 2019), če to res ni nujno. 2) prednost uporabe algoritma TwoStep je, da lahko vnaprej podamo število skupin in na podlagi parametrizacije najdemo optimalno število skupin ter pripadajočih enot/uporabnikov. S tem naslovimo optimizacijo stroškov usposabljanja, saj je manjše skupine lažje obvladovati in da s pomočjo prilagaja-

Tabela 2: **Razvrstitev spremenljivk znotraj gruče glede na pomembnost. Vrednosti v oklepajih predstavljajo povprečno vrednost posameznega področja informacijske varnosti.**

Uporabniki z nizkim tveganjem	Uporabniki z zmernim tveganjem	Uporabniki z visokim tveganjem	Legenda:
(N=137) 83.0 %	(N=24) 14.5 %	(N=4) 2.4 %	(barvna lestvica pomembnosti)
UIN (3.98)	USO (3.24)	UIN (1.44)	1.0
USO (4.03)	UMN (3.66)	USO (1.72)	0.8
POI (4.02)	UIN (3.12)	POI (1.47)	0.6
RZI (4.40)	UEP (3.37)	UMN (2.47)	0.4
UEP (4.13)	POI (3.31)	RZI (2.00)	0.2
UMN (4.43) UGE (4.05)	RZI (3.61) UGE (3.68)	UGE (2.31) UEP (2.14)	0.0

nja usposabljamo samo tiste skupine, ki jima manjka neka kompetenca.

V nadaljnjem delu bi nadgradili naš pristop s prilagajanjem varnostnih zahtev na podlagi kategorizacije, kar pomeni, da bi bilo smiselno razviti priporočilni sistem na podlagi katerega bi priporočali 1) tehnične varnostne funkcionalnosti ali 2) zahteve v smislu prilagojenih usposabljanj. Poleg tega pa bi nadgradili metodologijo za oceno rezultatov našega pristopa.

Kot vsaka raziskava, ima tudi pričujoči prispevek določene omejitve, ki jih je pri interpretaciji treba upoštevati. Prvič, vzorec študentov ni bil naključen, saj so anketiranci prihajali iz ene izmed slovenskih univerz. To pomeni, da ugotovitev ne moremo posploševati na vso populacijo študentov. Drugič, raziskavo bi bilo smiselno izvesti tudi med ostalo „ne-študentsko“populacijo (npr. zaposleni v podjetju). S tem bi dobili bolj celovit in raznovrsten vpogled v človeške vidike informacijske varnosti. Tretjič, bilo bi smiselno izvesti raziskavo na večjem vzorcu. Ne glede na to, pa velja omeniti, da je večina sorodnih raziskav narejena na vzorcih podobne velikosti (Tkaczynski, 2016; Parsons et al., 2014; Farooq et al., 2021; Hewitt and White, 2020; Cheolho et al., 2012)).

LITERATURA

[1] Anichiti, A., Dragolea, L. L., Hârs, an, G. D. T., Haller, A. P., and Butnaru, G. I. (2021). Aspects regarding safety and security in hotels: Romanian experience. *Information*, 12(1):1–22.

[2] Aurigemma, S., Mattson, T., and Leonard, L. (2019). Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications. *AIS Transactions on Replication Research*, 5:1–21.

[3] Cain, A. A., Edwards, M. E., and Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42:36–45.

[4] Celestino, A. E. M., Cruz, D. A. M., Sánchez, E. M. O., Reyes, F. G., and Soto, D. V. (2018). Groundwater quality assessment: An improved approach to K-means clustering, principal component analysis and spatial analysis: A case study. *Water (Switzerland)*, 10(4):1–21.

[5] Cheolho, Y., Hwang, J.-W., and Rosemary, K. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education,* 23(4):407–415.

[6] Falessi, D., Juristo, N., Wohlin, C., Turhan, B., Münch, J., Jedlitschka, A., and Oivo, M. (2018). Empirical software engineering experts on the use of students and professionals in experiments. *Empirical Software Engineering*, 23(1):452–489.

[7] Farooq, A., Dubinina, A., Virtanen, S., and Isoaho, J. (2021). Understanding dynamics of initial trust and its antecedents in password managers adoption intention among young adults. *Procedia Computer Science*, 184:266–274.

[8] Fujs, D., Mihelič, A., and Vrhovec, S. L. R. (2019). The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pages 1–10, New York, NY, USA. ACM.

[9] Fujs, D., Vrhovec, S., and Vavpotič, D. (2020). Bibliometric mapping of research on user training for secure use of information systems. *Journal of Universal Computer Science,* 26(7):764–782.

[10] Hameed, M. A. and Arachchilage, N. A. G. (2021). The role of self-efficacy on the adoption of information systems security innovations: a meta-analysis assessment. *Personal and Ubiquitous Computing*.

[11] Hewitt, B. and White, G. L. (2020). Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *Journal of Computer Information Systems*, 00(00):1–11.

[12] Kwak, D. H., Holtkamp, P., and Kim, S. S. (2019). Measuring and controlling social desirability bias: Applicati- ons in information systems research. *Journal of the Association for Information Systems*, 20(4):317–345.

[13] Larson, R. B. (2019). Controlling social desirability bias. *International Journal of Market Research*, 61(5):534– 547.

[14] Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., and Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers and Security,* 92:101731.

[15] Niazi, M., Saeed, A. M., Alshayeb, M., Mahmood, S., and Zafar, S. (2020). A maturity model for secure requirements engineering. *Computers and Security*, 95:101852.

[16] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, 66:40–51.

[17] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, 42(May):165–176.

[18] Prislan, K., Mihelič, A., and Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLoS ONE*, 15(9 September):1–28.

[19] Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, 15(3):112–133.

[20] Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., and Wu, D. T. (2020). The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information Systems Research*, 31(4):1240–1259.

[21] Tan, S. C. (2019). Improving association rule mining using clustering-based discretization of numerical data. In *2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018*, pages 18–22, Mon Tresor, Mauritius. IEEE.

[22] Tkaczynski, A. (2016). Segmentation Using Two-Step Cluster Analysis. In Dietrich, T., Rundle-Thiele, S., and Kubacki, K., editors, *Segmentation in Social Marketing: Process, Methods and Application*, pages 109–125.

[23] Tolley, S. B. (1975). Identifying Users through a Segmentation Study. *Journal of Marketing*, 39(2):69–71.

[24] Wiley, A., McCormac, A., and Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers and Security*, 88.

[25] Xiao, Q. (2021). Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study. *Telematics and Informatics*, 58 (May 2020):101535.

▪

Damjan Fujs je doktorski študent in asistent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegova raziskovalna področja zajemajo varnost informacijskih sistemov (IS), metodologije razvoja IS, prilagojeno usposabljanje in izobraževanje za varno rabo IS ter kibernetsko in informacijsko varnost. Trenutno je član programskega odbora dveh konferenc: 1) Dnevi slovenske informatike (DSI 2021) in 2) The Sixth International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2021).

▪

Simon Vrhovec je izredni profesor na Univerzi v Mariboru. Leta 2015 je doktoriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. V letih 2018 in 2019 je sopred- sedoval mednarodni konferenci Central European Cybersecurity Conference(CECC). Od leta 2019 je član usmerjevalnega odbora European Interdisciplinary Cybersecurity Conference (EICC) ter član uredniškega odbora revije Journal of Cyber Security and Mobility. Njegova glavna raziskovalna področja so človeški dejavniki v kibernetski varnosti, razvoj varne programske opreme, agilne metode, odpor do sprememb in zdravstvena informatika

▪

Damjan Vavpotič je izredni profesor na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegovo raziskovalno delo vključuje področja metodologije razvoja programske opreme in njihovega sprejemanja vključno z razvojem varnih informacijskih sistemov, sprejemanje metod e-učenja ter napredne metode analize podatkov v zdravstvu in turizmu. Je član programskih odborov mednarodnih konferenc s področja računalništva in informatike. Objavil je več kot 50 člankov v revijah in na konferencah. Za leto 2019 je prejel nagrado TheaSinclair Award for Journal Article Excellence pri podjetju Sage Publishing.

PRILOGA (VPRAŠALNIK)

Tabela 3: Vprašalnik o človeških vidikih informacijske varnosti (HAIS-Q) v slovenskem jeziku, ki je povzet po Parsons et al. (2017). Simbol (*) nakazuje, da je merska lestvica obrnjena. Trditve so bile merjene na podlagi petstopenjske Likertove lestvice (od 1 - se sploh ne strinjam do 5 - se popolnoma strinjam). Pomen kratice indikatorja: _z (znanje), _s (stališče) in _v (vedenje).

Konstrukt	Indikator	Trditev
UGE	UGE1_z*	Sprejemljivo je, da uporabljam enaka gesla za moja socialna omrežja in za moje univerzitetne račune.
	UGE1_s*	Varno je uporabljati enaka gesla za socialna omrežja in za univerzitetne račune.
	UGE1_v	Uporabljam različna gesla za moja socialna omrežja in univerzitetne račune.
	UGE2_z*	Svoja univerzitetna gesla smem deliti s kolegi.
	UGE2_s	Ni dobro deliti mojih univerzitetnih gesel s kolegi, tudi če me prosijo za to.
	UGE2_v*	Svoja univerzitetna gesla delim s kolegi.
	UGE3_z	Univerzitetna gesla bi morala biti sestavljena iz črk, številk in simbolov.
	UGE3_s	Varno je imeti univerzitetno geslo, ki je sestavljeno samo iz črk.
	UGE3_v	Za univerzitetna gesla uporabljam kombinacijo črk, številk in simbolov.
UEP	UEP1_z*	Klikniti smem na katerokoli povezavo v e-pošti od ljudi, ki jih poznam.
	UEP1_s*	Vedno je varno klikniti na povezave v e-pošti od ljudi, ki jih poznam.
	UEP1_v	Na povezave v e-pošti ne klikam le zato, ker prihaja od nekoga, ki ga poznam.
	UEP2_z	Ne smem klikniti na povezavo v e-pošti, ki prihaja od neznanega pošiljatelja.
	UEP2_s*	Nič slabega se ne more zgoditi, če kliknem na povezavo v e-pošti, ki prihaja od neznanega pošiljatelja.
	UEP2_v*	Če e-pošta od neznanega pošiljatelja izgleda zanimivo, kliknem na vključeno povezavo.
	UEP3_z*	Priponke v e-pošti neznanih pošiljateljev smem odpreti.
	UEP3_s	Tvegano je odpreti priponko v e-pošti neznanega pošiljatelja.
	UEP3_v	Ne odpiram priponk v e-pošti, če mi pošiljatelj ni znan.
UIN	UIN1_z*	Na svoj delovni računalnik smem prenesti katerokoli datoteko, če mi to pomaga pri mojih nalogah.
	UIN1_s	Prenašanje datotek na moj delovni računalnik je lahko tvegano.
	UIN1_v*	Na svoj delovni računalnik prenašam katerekoli datoteke, ki mi pomagajo pri mojih nalogah.
	UIN2_z	Med delom naj nebi dostopal do določenih spletnih strani.
	UIN2_s	Le zato, ker lahko med delom dostopam do spletne strani, to še ne pomeni, da je varna.
	UIN2_v*	Ko med delom dostopam do interneta, obiščem katerokoli spletno stran želim.
	UIN3_z*	Svoje podatke lahko vnesem na katerokoli spletno stran, če mi to pomaga pri mojih nalogah.
	UIN3_s*	Če mi to pomaga pri mojih nalogah, ni pomembno, katere podatke vnesem na spletno stran.
	UIN3_v	Preden začnem vnašati podatke ocenim varnost spletnih strani.
USO	USO1_z	Nastavitve zasebnosti na mojih računih na socialnih omrežjih moram redno pregledovati.
	USO1_s	Nastavitve zasebnosti na mojih računih na socialnih omrežjih je dobro redno pregledovati.
	USO1_v*	Ne pregledujem redno nastavitev zasebnosti na svojih računih na socialnih omrežjih.
	USO2_z	Ne morejo me izključiti iz fakultete zaradi mojih objav na socialnih omrežjih.
	USO2_s*	Ni pomembno, če na socialnih omrežjih objavim nekaj, česar sicer ne bi javno izjavil.
	USO2_v	Na socialnih omrežjih ne objavim ničesar brez razmisleka o morebitnih negativnih posledicah.
	USO3_z*	Na socialnih omrežjih smem o svojem delu objaviti karkoli želim.
	USO3_s	Na socialnih omrežjih je tvegano objaviti določene informacije o mojem delu.
	USO3_v*	Na socialnih omrežjih objavljam karkoli želim o svojem delu.
UMN	UMN1_z	Pri delu na javnih krajih je treba imeti svoj prenosnik ves čas pri sebi.
	UMN1_s*	Pri delu v kavarni bi bilo varno pustiti svoj prenosnik za minuto brez nadzora.
	UMN1_v*	Pri delu na javnem kraju pustim svoj prenosnik brez nadzora.
	UMN2_z*	Občutljive z delom povezane datoteke smem pošiljati preko javnega omrežja Wi-Fi.
	UMN2_s	Občutljive z delom povezane datoteke je tvegano pošiljati čez javno omrežje Wi-Fi.
	UMN2_v*	Občutljive z delom povezane datoteke pošiljam čez javno omrežje Wi-Fi.
	UMN3_z	Pri delu z občutjivimi dokumenti moram zagotoviti, da neznanci ne morejo videti na zaslon mojega prenosnika.
	UMN3_s	Tvegano je dostopati do občutljivih z delom povezanih datotek na prenosniku, če lahko neznanci vidijo na moj zaslon.
	UMN3_v	Preverim, da neznanci ne morejo videti na zaslon mojega prenosnika, če delam z občutljivimi dokumenti.
RZI	RZI1_z*	Občutljive izpise na papirju lahko zavržemo na enak način kot neobčutljive.
	RZI1_s*	Občutljive izpise na papirju je varno zavreči z odlaganjem v koš za smeti.
	RZI1_v	Ko je treba zavreči občutljive izpise na papirju, poskrbim, da so razrezani ali uničeni.
	RZI2_z	Če na javnem kraju najdem USB ključek, ga ne smem priključiti v svoj delovni računalnik.
	RZI2_s*	Če na javnem kraju najdem USB ključek, se ne more zgoditi nič slabega, če ga priključim v svoj delovni računalnik.
	RZI2_v	V svoj delovni računalnik ne bi priključil na javnem mestu najdenega USB ključka.
	RZI3_z*	Občutljive izpise na papirju smem čez noč pustiti na svoji mizi.
	RZI3_s	Tvegano je pustiti občutljive izpise na papirju čez noč na moji mizi.
	RZI3_v*	Občutljive izpise na papirju puščam na moji mizi, ko me ni tam.
POI	POI1_z	Če opazim, da se nekdo v prostorih fakultete obnaša sumljivo, bi moral to prijaviti.
	POI1_s*	Če se ne menim za nekoga, ki se obnaša sumljivo v prostorih fakultete, se ne more zgoditi nič slabega.
	POI1_v	Če bi videl, da se nekdo obnaša sumljivo v prostorih fakultete, bi nekaj ukrenil glede tega.
	POI2_z	Ne smem zanemariti pomanjkljivega odnosa do varnosti s strani mojih kolegov.
	POI2_s*	Nič slabega se ne more zgoditi, če zanemarim pomanjkljiv odnos do varnosti, ki ga ima kolega.
	POI2_v*	Če bi opazil, da se moj kolega ne zmeni za varnostna pravila, ne bi ukrepal.
	POI3_z*	Poročanje o varnostnih incidentih je neobvezno.
	POI3_s	Tvegano je zanemariti varnostne incidente, tudi če se mi zdijo nepomembni.
	POI3_v	Če bi opazil varnostni incident, bi ga prijavil.