DOI: 10.20419/2022.31.568
CC: 2700, 4100
UDK: 159.9:004.056

Psihološka obzorja / Horizons of Psychology, 31, 602–622 (2022)

Znanstveni pregledni prispevek / Scientific review article

Teorije in modeli v vedenjskih informacijskovarnostnih raziskavah

Špela Grilc, Kaja Prislan in Anže Mihelič*
Fakulteta za varnostne vede, Univerza v Mariboru

Povzetek: S pojasnjevanjem vloge uporabnikov v sistemu zagotavljanja informacijske varnosti se ukvarja vedenjska informacijska varnost, kjer se pri pojasnjevanju in napovedovanju vedenja uporabnikov izhaja iz različnih psiholoških, organizacijskih in kriminoloških teorij. Kljub številčnosti sistematičnih pregledov literature na področju informacijske varnosti med njimi ni mogoče zaslediti celostnega sistematičnega pregleda teorij, ki se uporabljajo v vedenjskih informacijskovarnostnih raziskavah. Namen pričujočega prispevka je ugotoviti, katere teorije so najpogosteje uporabljene v raziskavah, na katerih tematskih področjih se najpogosteje uporabljajo, kateri dejavniki so po posameznih sklopih teorij najpogosteje vključeni v raziskave in kateri so najpogosteje statistično značilni. Skladno s tem smo opravili dva sistematična pregleda literature za preteklih deset let. Ugotovitve kažejo, da med najpogosteje uporabljeni teoriji sodita varnostnomotivacijska teorija in teorija načrtovanega vedenja. Samoučinkovitost in zaznana uporabnost tehnologije sta dejavnika teh dveh teorij, ki sta pri napovedovanju samozaščitnega vedenja najpogosteje statistično značilna.

Ključne besede: informacijska varnost, kibernetska varnost, vedenjske teorije, sistematičen pregled literature

Theories and models in behavioral information security research

Špela Grilc, Kaja Prislan, and Anže Mihelič*
Faculty of Criminal Justice and Security, University of Maribor

Abstract: Behavioral information security is concerned with explaining the role of users in the information security system, drawing on various psychological, organizational, and criminological theories to explain and predict user behavior. Despite numerous systematic literature reviews on the field of information security, there is no comprehensive systematic review of the theories used in behavioral information security research. The purpose of this paper is to investigate which theories are most widely used in research, in which subject areas they are most used, which factors are most frequently included in research according to each set of theories, and which are most frequently statistically significant. Accordingly, we made two studies involving a systematic review of the literature over the past ten years. The findings suggest that the most used theories include the protection motivation theory and the theory of planned behavior. In these two theories, self-efficacy and perceived usefulness of the technology are factors, which are most often statistically significant in predicting self-protective behavior.

Keywords: information security, cybersecurity. behavioral theories, systematic literature review

*Naslov/Address: g. Anže Mihelič, Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova 8, 1000 Ljubljana,
e-mail: anze.mihelic@um.si

Tehnološki napredek in vsesplošna digitalizacija, ki narekujeta trende v razvoju sodobne družbe, poleg številnih prednosti, ustvarjata tudi neželene implikacije za varnost. Te se kažejo v razvoju vse bolj kompleksnih in sofisticiranih kibernetskih groženj, zaradi česar je informacijska varnost postala aktualna tema v strokovnih razpravah in znanstvenih raziskavah. Informacijska varnost je stanje oz. dobrina, ki je pomembna tako v domači oz. zasebni, kakor tudi organizacijski sferi, odvisna je od številnih dejavnikov (npr. tehnologij, uporabnikov, organizacij, procesov, politik), saj jo sestavljajo socialni in tehnični vidiki (Prislan idr., 2020). Pri tem sodobne razprave med najpomembnejše člene in hkrati tudi ranljivosti na področju informacijske varnosti umeščajo človeške oz. družbene dejavnike (Da Veiga in Eloff, 2007; Rocha Flores idr., 2014; Soomro idr., 2016). Kljub vse bolj naprednim tehnološkim varnostnim rešitvam, njihova uporaba ne vodi nujno do izboljšanja varnosti, saj so za informacijskovarnostne incidente največkrat odgovorni uporabniki. Njihova vedenja so zelo različna, imajo različne implikacije in so pod vplivom različnih dejavnikov. Pomembno vlogo v sistemu zagotavljanja informacijske varnosti imajo osebne lastnosti uporabnikov, njihove kognitivne sposobnosti, zaznava tveganj ter okolje, v katerem se nahajajo (Vicozi, 2018). Do incidentov lahko pride zaradi malomarnosti pri uporabi informacijskih sistemov in tehnologij, neozaveščenosti o informacijskih tveganjih, pozabljivosti, nepazljivosti ali nepremišljenosti uporabnikov (Njenga, 2017; Reason, 2000). Poleg malomarnosti in nevednosti oz. neozaveščenosti uporabnikov, ranljivost za informacijsko varnost organizacij predstavljajo tudi apatija in odpor uporabnikov do spoštovanja organizacijskih informacijskovarnostnih pravil in politik (Richardson idr., 2020; Safa idr., 2018).

Osrednja ideja vedenjske informacijske varnosti je obravnavanje človeških dejavnikov kot ranljivosti pri obvladovanju informacijske varnosti saj so napadi pogosto na način, da izkoriščajo človeške ranljivosti. Tveganj sicer ni mogoče popolnoma odpraviti, je pa možno z njimi upravljati in si prizadevati za njihovo čim manjšo pojavnost. Zato je ključnega pomena spodbujanje pozitivnega informacijskovarnostnega vedenja med uporabniki (Alohali idr., 2017). Pri tem je treba razumeti, kaj vpliva na vedenje uporabnikov in katere okoliščine lahko privedejo do napak oz. incidentov. Študije kažejo, da na to vplivajo različni dejavniki, kot so npr. odnos do vedenja, stališča glede tveganj in ukrepov, motivacija za samozaščitno vedenje, informacijskovarnostna ozaveščenost in kultura (Sadaf in Dhanapal, 2018) ter tudi socialne in druge zunanje okoliščine. Skladno z raznovrstnostjo pomembnih dejavnikov, ki vplivajo na vedenja in odnose uporabnikov, se v raziskovanju in pri pojasnjevanju uporabniških oz. vedenjskih vidikov v informacijski varnosti uporabljajo različne vedenjske teorije in modeli, ki ki jih raziskujemo v tem prispevku.

Namen prispevka je opraviti sistematični pregled literature, s katerim bomo identificirali najpogosteje uporabljene teorije in tematike v aktualnih vedenjskih informacijskovarnostnih raziskavah in izvedli pregled ugotovitev preteklih raziskav, ki so temeljile na teh teorijah. Prispevek bo odgovoril na naslednja raziskovalna vprašanja:

RV1: Katere teorije in modeli so najpogosteje uporabljeni v vedenjskih informacijskovarnostnih raziskavah?

RV2: Na katerih tematskih področjih se uporabljajo teorije in modeli v vedenjskih informacijskovarnostnih raziskavah?

RV3: Kateri dejavniki posameznih teorij in modelov so najpogosteje uporabljeni v raziskavah in kateri so najpogosteje statistično značilni?

Pregled preteklih raziskav

Na temo teorij, ki se uporabljajo v raziskavah s področja informacijske varnosti, je že bilo opravljenih nekaj sistematičnih pregledov literature, ki jih predstavljamo v tem poglavju. Prednost sistematičnega pregleda literature je v tem, da se lahko na podlagi metaanalize raziskav ugotovijo morebitne vrzeli v dosedanjih raziskavah, s tem se lahko postavi okvir za usmeritev novih raziskovalnih dejavnosti (Kitchenham in Charters, 2007). Sistematični pregledi omogočajo zmanjšanje velike količine informacij v manjše, razumljive enote (kar je še posebej pomembno pri ogromnih količinah informacij na informacijskovarnostnem področju), zbiranje kritičnih informacij in sintezo določenega vprašanja (Ganeshkumar in Gopalakrishnan, 2013).

V preteklosti je več prispevkov, ki vključujejo sistematične preglede literature obravnavalo upoštevanje zahtev informacijskovarnostne politike zaposlenih. Informacijskovarnostno politiko sestavljajo pravila, navodila in priporočila za varno rabo informacijskih sistemov v organizacijah. Organizacije sprejmejo informacijskovarnostne politike z namenom zagotoviti zaupnost, celovitost in razpoložljivost informacij in sistemov s katerimi upravljajo zaposleni. Spoštovanje ukrepov in pravil informacijskovarnostne politike viša stopnjo informacijske varnosti v organizacijah (Prislan in Bernik, 2019).

Mayer, Kunz in Volkamer (2017) so v sistematični pregled zajeli 13 prispevkov, objavljenih po letu 2013. Analizirali so uporabnost varnostnomotivacijske teorije, teorije načrtovanega vedenja, teorije generalne prevencije in modela sprejemanja tehnologij, z namenom oceniti statistično značilnost dejavnikov povezanih z varnostnim vedenjem iz več študij. Pregled je pokazal, da je 11 od 14 dejavnikov iz najpogosteje uporabljenih vedenjskih teorij mogoče povezati z zanesljivimi učinki v kontekstu informacijske varnosti. Kuppusamy idr. (2020) so skozi sistematičen pregled literature, ki je vključeval 29 prispevkov, želeli dobiti vpogled v najpogosteje uporabljene teorije, ki prispevajo k razumevanju spoštovanja politik informacijske varnosti. Ugotovili so, da izmed deset analiziranih teorij, med najpogosteje uporabljeni teoriji v študijah, ki so preučevale upoštevanje zahtev informacijskovarnostne politike sodita teorija načrtovanega vedenja in varnostnomotivacijska teorija. Nekoliko manj pogosto so uporabljene teorija generalne prevencije, teorija nevtralizacije in teorija socialnega nadzora. Izzive in stanje upoštevanja zahtev informacijskovarnostne politike zaposlenih s politikami informacijske varnosti so raziskali tudi Angraini idr. (2019), ki so v pregled vključili 53 prispevkov objavljenih med letoma 2014 in 2019. Pri tem so ugotovili, da so na omenjenem tematskem področju uporabne številne teorije, konkretno so

analizirali 29 teorij o človeškem vedenju in 13 organizacijskih teorij. Avtorji predlagajo izboljšanje teoretičnih izhodišč za preučevanje upoštevanja zahtev informacijskovarnostne politike z vključitvijo organizacijskih teorij oz. razvoj novega modela iz organizacijskih teorij in teorij človeškega vedenja. Sadaf in Dhanapal (2018) sta v sistematičen pregled literature vključila 200 prispevkov s področja upoštevanja zahtev informacijskovarnostne politike med letoma 2006 in 2016. Osredotočala sta se na pregled raziskovalnih zasnov, metodologij in okvirov, ki so se razvili v zadnjem desetletju. Prispevki, ki sta jih vključila v raziskavo, so temeljili na teoriji socialnega nadzora, varnostnomotivacijski teoriji in teoriji načrtovanega vedenja.

Med pogosto obravnavane teme, na katere se osredotočajo raziskovalci v sistematičnih pregledih sodijo tudi kršitve na področju politik informacijske varnosti. Njenga (2017) je s sistematičnim pregledom kršitev varnostnih politik informacijske varnosti v organizacijah želel izpostaviti in problematizirati kršitve varnosti pri uporabi informacijskih sistemov s strani zaposlenih v organizaciji. Ob analizi 19 različnih teorij je ugotovil, da je najbolj uporabna in najpogosteje uporabljena teorija, ki razlaga kršitve v različnih kontekstih, teorija generalne prevencije. Tudi varnostnomotivacijska teorija se je izkazala za priljubljeno v znanstvenih raziskavah. Kršitve na področju informacijske varnosti sta s sistematičnim pregledom raziskala tudi Parker in Flowerday (2020), ki sta v analizo vključila 25 člankov, objavljenih po letu 2010. Ugotovitve so pokazale, da so nekateri ljudje zaradi njihovih spletnih navad, vedenj pri delu s podatki, demografije, znanja o informacijski in komunikacijski tehnologiji ter osebnih lastnosti bolj dovzetni za napade na družbenih omrežjih z zvabljanjem (angl. *phishing*). Na podlagi ugotovitev sta predlagala model za zmanjšanje uspešnosti napadov z zvabljanjem, ki bi omogočil večjo ozaveščenost o dejavnikih, ki vplivajo na uporabnikovo dovzetnost za lažno predstavljanje na družbenih omrežjih.

V pregledih literature so se raziskovalci osredotočali tudi na temo vloge človeškega dejavnika v sistemu zagotavljanja informacijske varnosti v organizacijah. Sistematični pregled dimenzij povezanih z vedenjem uporabnikov so opravili Al-Harthy idr. (2020). V prispevku so poudarili pomembnost pozitivnega vedenja zaposlenih za uspešno varovanje organizacijskih podatkov, v sistematični pregled literature so zajeli 57 člankov objavljenih med letoma 2010 in 2019. Kot najbolj uporabne za razlago vedenja na področju informacijske varnosti so izpostavili tri teorije, to so varnostnomotivacijska teorija, teorija načrtovanega vedenja in teorija organizacijske kulture. Do podobnih ugotovitev so skozi sistematičen pregled literature prišli tudi Alohali idr. (2017), ki so se ukvarjali s preučevanjem dejavnikov, ki vplivajo na vedenje uporabnikov. V sistematičen pregled so vključili 74 prispevkov, objavljenih od leta 2010 naprej, podrobneje so se osredotočili na analiziranje teorije razumne akcije, razširjene verzije teorije načrtovanega vedenja, teorije generalne prevencije, varnostnomotivacijske teorije in modela sprejemanja tehnologije. Za izboljšanje ozaveščenosti uporabnikov so poudarili pomembnost nenehnega nadgrajevanja znanja, ki bi uporabnike preoblikovalo iz neozaveščenih oz. nizko ozaveščenih v varnostno naravnane.

Kot je razvidno iz predstavljenega pregleda literature, so pomanjkljivosti dosedanjih sistematičnih pregledov v osredotočanju na različne in zelo specifične informacijskovarnostne tematike (večina prispevkov se osredotoča na tematiko upoštevanja zahtev informacijskovarnostne politike, kršitev na področju politik informacijske varnosti in vlogo človeškega faktorja v sistemu zagotavljanja informacijske varnosti v organizacijah), kar onemogoča celosten vpogled v teoretična izhodišča, uporabna za pojasnjevanje in razumevanje vedenjskih vidikov na področju informacijske varnosti.

Prva študija: Identifikacija teorij in modelov

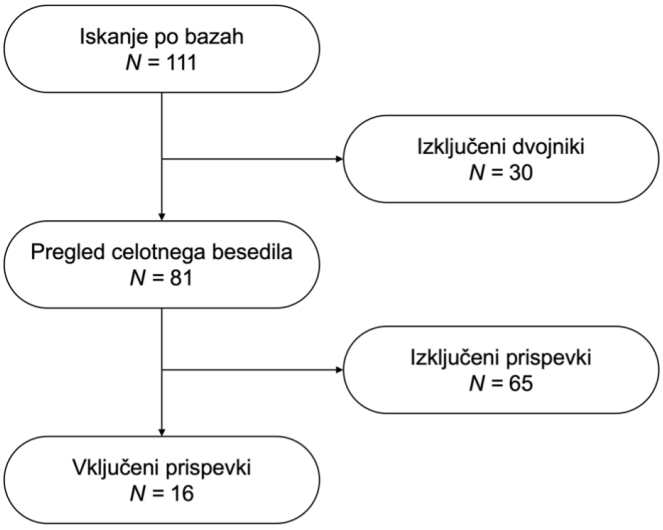
Metoda

V prvi študiji smo opravili sistematičen pregled literature, s katerim smo ugotovili, katere teorije se najpogosteje uporabljajo v vedenjskih informacijskovarnostnih raziskavah. Pregled je obsegal prispevke, objavljene po letu 2010, ki so vsebovali sistematične preglede literature s področja informacijske varnosti in so opisovali vedenjske teorije. Proces pregleda, s številom vključenih del v posameznem koraku, je prikazan na sliki 1.

Pregled literature smo izvedli v znanstvenih bibliografskih zbirkah *Web of Science* in *Scopus* med 8. in 27. 10. 2020. Iskalni niz je zajemal ključni besedi *informacijska varnost* in *sistematičen pregled literature*. Za poizvedbo je bil uporabljen iskalni niz v angleščini:

> *»information security« AND »systematic literature review«.*

Slika 1
Proces sistematičnega pregleda v prvi študiji



Iskanje je vrnilo skupno $N = 111$ zadetkov po letu 2010. V naslednjem koraku smo odstranili vse podvojene zadetke ter dela, ki niso vsebovala vedenjskih teorij. Vključitveni in izključitveni kriteriji v procesu sistematičnega pregleda so predstavljeni v tabeli 1. Končni rezultat je obsegal $N = 16$ zadetkov.

Rezultati

Skupno smo identificirali 16 člankov, ki so skupaj vključevali opise 26 teorij, in sicer: teorija načrtovanega vedenja (TPB); varnostnomotivacijska teorija (PMT); teorija generalne prevencije (GDT); teorija racionalne izbire (RCT); teorija socialnega nadzora (SBT); model sprejemanja tehnologij (TAM); model zdravstvenih prepričanj (HBM); teorija vpletenosti (IT); teorija aktivacije (NAT); teorija organizacijskega nadzora (OCT); teorija socialnega nadzora (SCT); kognitivna teorija (CET); model delovnih potreb in virov (EJDR); razširjeni model paralelnih procesov (EPPM); testna teorija (HRT); hevristično-sistematični model (HSM); integrirani vedenjski model (IBM); znanje, odnos in vedenje (KAB); teorija nevtralizacije (NT); teorija osebnih konstrukcij (PCT); teorija psihološke reaktance (PRT); teorija samodoločenosti (SDT); dvofaktorska motivacijska teorija (TFMT); teorija medosebnega vedenja (TIB); teorija organizacijskega vedenja (TOB) in teorija razumne akcije (TRA).

Da bi lahko odgovorili na prvo raziskovalno vprašanje (RV1): »*Katere teorije in modeli so najpogosteje uporabljeni v vedenjskih informacijskovarnostnih raziskavah*?«, smo nato preučili še, katere izmed teh 26 teorij se v analiziranih prispevkih najpogosteje pojavljajo. Za odgovor na RV1 smo izbrali teorije, ki so se v identificiranih sistematičnih pregledih literature ponovile najmanj *dvakrat*. Skladno z ugotovljenimi frekvencami smo v pregled vključili sedem najpogosteje uporabljenih teorij v vedenjskih informacijskovarnostnih raziskavah.

Odgovor na RV1: Iz tabele 2 je razvidno, da so se v analiziranih prispevkih, ki so vključevali sistematične preglede literature s področja informacijske varnosti, najpogosteje opisovale teorije PMT (sedemkrat), TPB (sedemkrat) in GDT (šestkrat). Sledile so teorije TAM (trikrat), RCT (trikrat) in SBT (trikrat). Najmanjkrat pa smo zasledili HBM (dvakrat).

Druga študija: Sistematičen pregled literature in metaanaliza

Metoda

V drugi študiji smo izvedli sistematičen pregled literature za teorije, ki smo jih identificirali kot najpogostejše v prvi študiji. Pregled je zajemal članke objavljene v revijah in konferenčne prispevke objavljene po letu 2010, ki so vsebovali kvantitativne raziskave izvedene na osnovi ene ali več teorij iz prve študije. Proces pregleda s številom vključenih del v posameznem koraku je prikazan na sliki 2.

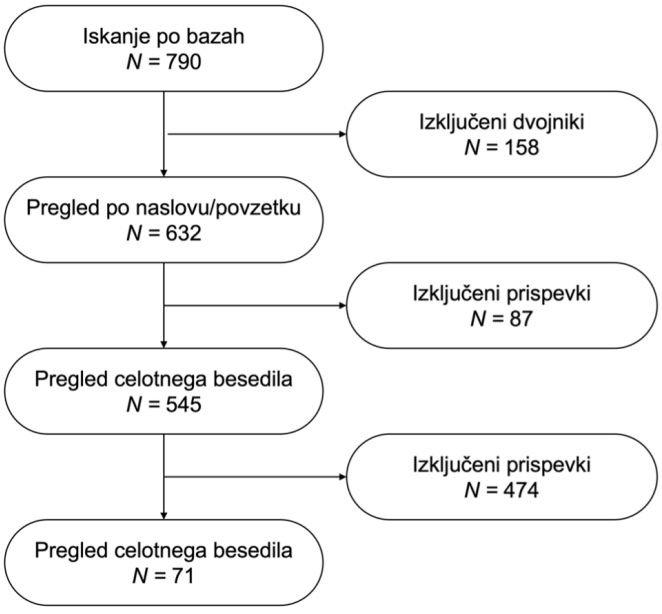
Tabela 1
Vključitveni in izključitveni kriteriji v prvi študiji

Vključitveni kriteriji	Izključitveni kriteriji
objavljeno v zadnjih desetih letih	objavljeno pred letom 2010
celotno besedilo članka dostopno raziskovalcem	celotno besedilo nedostopno
objavljeno v slovenskem ali angleškem jeziku	objavljeno v ostalih jezikih
članki, ki vsebujejo vedenjsko teorijo	članki, ki ne vsebujejo vedenjske teorije
članki s sistematičnim pregledom literature	članki, ki ne vsebujejo sistematičnega pregleda literature

Tabela 2
Frekvence pojavnosti teorij v analiziranih prispevkih po bazah.

Teorije	Web of Science	Scopus	Skupaj
PMT	4	3	7
TPB	4	3	7
GDT	4	2	6
TAM	2	1	3
RCT	1	2	3
SBT	1	2	3
HBM	1	1	2

Slika 2
Proces sistematičnega pregleda v drugem koraku



Pregled literature smo izvedli v znanstvenih bibliografskih zbirkah *Web of Science* in *Scopus* med 16. in 29. 1. 2021 za vsako teorijo posebej. Poizvedba je potekala v angleščini, kombinacija ključnih besed je bila določena po ključu: (*informacijska varnost* ALI *kibernetska varnost*) IN (*ime teorije* ALI *akronim teorije*).

Na primer, za teorijo PMT je bil tako uporabljen iskalni niz v angleščini:

(»information security« OR »ISec« OR »InfoSec« OR »cybersecurity« OR »cyber-security« OR »cyber security«) AND (»protection motivation« OR PMT).

Po tem ključu je bila izvedena poizvedba za vseh sedem identificiranih teorij.

Iskanje je vrnilo skupno $N = 790$ zadetkov. V naslednjih korakih smo odstranili vsa podvojena dela, dela, ki niso vsebovala izbranih vedenjskih teorij ter dela, ki niso vključevala kvantitativne empirične raziskave. Vključitveni in izključitveni kriteriji v procesu sistematičnega pregleda so predstavljeni v tabeli 3. Končni rezultat je zajel $N = 71$ unikatnih zadetkov. Vse izbrane prispevke sta zaradi zagotovitve višje zanesljivosti rezultatov vsebinsko pregledovala dva raziskovalca.

Rezultati

Največ ustreznih rezultatov je vrnila poizvedba za PMT (48 člankov). Sledita TPB (25 člankov) in TAM (devet člankov). Nekoliko manj rezultatov smo dobili z iskalnima nizoma HBM (šest člankov) in RCT (šest člankov). Najmanj ustreznih rezultatov smo dobili z GDT (tri članke). SCT nam ni vrnila nobenega rezultata, ki bi ustrezal našim vključitvenim in izključitvenim kriterijem in posledično ni bila vključena v nadaljnje delo. Ker so nekateri raziskovalni modeli vključevali več kot eno teorijo (npr. PMT in TPB), rezultati kažejo, da so bile posamezne teorije uporabljene skupno 97-krat v 71 različnih raziskovalnih modelih (člankih).

Tabela 3
Vključitveni in izključitveni kriteriji v drugem koraku

Vključitveni kriteriji	Izključitveni kriteriji
objavljeno v zadnjih desetih letih	objavljeno pred letom 2010
celotno besedilo članka dostopno raziskovalcem	celotno besedilo nedostopno
objavljeno v slovenskem ali angleškem jeziku	objavljeno v ostalih jezikih
članki v revijah ali konferenčni prispevki	ostale vrste dokumentov (poglavje knjige, pregled, uvodniki itd.)
raziskave, ki vsebujejo iskano vedenjsko teorijo	raziskave, ki ne vsebujejo iskane teorije
raziskave, ki tematsko ustrezajo našemu delu	raziskave, ki tematsko ne ustrezajo našemu delu
izvedena anketa	izvedeni intervjuji, eksperimenti, študija primera, teoretični pregledi in ostali
raziskave, ki vsebujejo konstrukte iskane teorije	raziskave, ki konstruktov niso vključevale

Vsakemu od identificiranih člankov smo po podrobnem pregledu in skladno z vsebino ter cilji posameznega članka dodelili besedno značko (npr. »upoštevanje pravil informacijskovarnostne politike ali »zlonamerna programska oprema«), ki predstavljajo tematska področja. Članke smo nato skupinili skladno z besednimi značkami in jih razvrstili glede na število člankov, ki so naslavljali enak ali podoben problem.

Odgovor na RV2: Najpogostejše so raziskave, ki naslavljajo problematiko upoštevanja pravil informacijskovarnostne politike. Predstavljajo 37,1 odstotka vseh raziskav. Na drugem mestu so raziskave, ki so preučevale splošno invormacijskovarnostno vedenje oz. izvajanje informacijskovarnostnih ukrepov. Gre za raziskave, ki niso natančno določile katero informacijskovarnostno vedenje preučujejo. Takšne raziskave predstavljajo 23,7 odstotka naših zadetko, medtem ko se je na točno določeno invormacijskovarnostno vedenje (npr. varno rabo spletnega bančništva, dojemljivost za zvabljanje, uporabo programske opreme za obvladovanje zlonamerne programske opreme) osredotočalo 11,3 odstotka raziskav. Na varno rabo tehnologij se je osredotočalo 10,3 odstotka raziskav, na sprejemanje (ali namero za sprejetje) novih tehnologij (npr. programske opreme za zaščito) 9,3 odstotka, medtem ko je dejansko uporabo posameznih tehnologij preučevalo 4,1 odstotka raziskav. Manjša deleža raziskav (2,1 odstotka) predstavljata raziskave, ki so preučevale stališča do določene tehnologije, in namero za kršenje pravil povezanih z informacijsko varnostjo.

Z drugo študijo smo odgovorili tudi na tretje raziskovalno vprašanje (RV3): »*Kateri dejavniki posameznih teorij in modelov so najpogosteje uporabljeni v raziskavah in kateri so najpogosteje statistično značilni?*« V nadaljevanju predstavljamo rezultate ločeno po posameznih teorijah. Vsak razdelek prikazuje tabelo z virom, temo posamezne raziskave, velikostjo vzorca, ciljno populacijo vzorca, vključene konstrukte raziskovalnega modela in odvisno spremenljivko. Prav tako v razdelkih predstavljamo graf s ključnimi konstrukti posamezne teorije in njihovo pogostost vključenosti v raziskovalne modele ter kako pogosto so posamezni dejavniki statistično značilni. Odstotek vključenosti nam pove, kako pogosto (oz. v koliko odstotkih raziskav) je bil konstrukt vključen v raziskovalni model. Statistična značilnost nam pove, ali je konstrukt statistično značilno povezan z odvisno spremenljivko oz. ali odvisno spremenljivko napoveduje statistično značilno (npr. vedenje ali namero).

Varnostnomotivacijska teorija

Varnostnomotivacijska teorija (angl. *protection motivation theory* – PMT) je teorija, ki je bila prvič predlagana leta 1983 (Rogers, 1983) in se je razvila iz HBM. Njen namen je pojasniti dejavnike, ki vplivajo na motivacijo ljudi za zaščito pred fizičnimi, psihološkimi in socialnimi grožnjami. PMT se je prvotno uporabljala za preučevanje strahu in v raziskovanju prepričevalnega komuniciranja. PMT predpostavlja, da je

z zaščitnim vedenjem povezanih pet osnovnih dejavnikov: 1) zaznana resnost posledic (posameznikovo dojemanje resnosti varnostnega tveganja oz. grožnje – višja kot je zaznana resnost, višja je pripravljenost posameznika, da se samozaščiti); 2) zaznana ranljivost (posameznikova ocena verjetnosti, da bo izpostavljen zlonamerni grožnji – višja kot je zaznana ranljivost, višja je pripravljenost posameznika, da se samozaščiti); 3) učinkovitost odziva (posameznikova zaznana učinkovitost potencialnih ukrepov za zmanjšanje nevarnosti – višja kot je učinkovitost odziva, višja je pripravljenost posameznika, da se samozaščiti); 4) samoučinkovitost (zaznana sposobnost posameznika, da se učinkovito samozaščiti oz. izvede ali uporabi zaščitni ukrep/vedenje – višja kot je samoučinkovitost, višja je pripravljenost posameznika, da se samozaščiti); 5) stroški (posameznikova ocena stroškov oz. nagrad ob samozaščitnem dejanju, ukrepu – višji kot so stroški, nižja je pripravljenost posameznika, da izvede ukrepe).

Identificirali smo 48 študij, ki so v svojih raziskovalnih modelih vključevale PMT. Povprečna velikost vzorca vseh raziskav je 394 anketirancev. Najpogostejši vzorec anket so bili zaposleni, drugi najpogostejši vzorec so bili študenti. PMT sestavlja pet napovednih dejavnikov, iz tabele 4 lahko razberemo, da so raziskave minimalno vključile en dejavnik, najpogosteje pa vseh pet dejavnikov (*Mo* = 5; *Me* = 4; *M* = 3,2).

Odgovor na RV3$_{PMT}$: Najpogosteje vključen dejavnik v raziskavah, ki temeljijo na PMT je samoučinkovitost, ki je drugi najpogosteje statistično značilen dejavnik. Raziskave najredkeje vključujejo stroške, ki so najpogosteje statistično značilen dejavnik. Najredkeje statistično značilen dejavnik je znaznana ranljivost. Tabela 5 prikazuje ostale podrobnosti analize rezultatov za PMT.

Teorija načrtovanega vedenja

Teorija načrtovanega vedenja (angl. *Theory of Planned Behavior* – TPB) je teorija, ki je bila prvič predlagana leta 1985 (Ajzen, 1985). Je nadgradnja teorije razumne akcije (angl. *Theory of Reasoned Action*). TPB predpostavlja, da na vedenje posameznika vpliva namera, na namero pa trije dejavniki: 1) odnos do vedenja (posameznikova osebna prepričanja in stališča o pomembnosti, primernosti določenega vedenja – bolj kot je pozitiven odnos do vedenja, višja je pripravljenost posameznika, da izvede določeno vedenje); 2) subjektivne norme (prepričanja posameznika o pričakovanjih drugih, njemu pomembnih, ljudi – višje kot so subjektivne norme, višja je pripravljenost posameznika, da izvede določeno vedenje; 3) zaznana kontrola vedenja (posameznikovo prepričanje, da je vedenje pod njegovim nadzorom (pogosto omenjena kot proces, ki vedenje olajša ali ovira) – višja kot je zaznana kontrola vedenja, višja je pripravljenost posameznika, da izvede določeno vedenje).

Identificirali smo 25 raziskav, ki so v svojih raziskovalnih modelih vključevale TPB. Povprečna velikost vzorca vseh raziskav je 322 anketirancev. Najpogostejši vzorec anket so bili zaposleni, drugi najpogostejši vzorec so bili študentje. TPB sestavljajo tri napovedni dejavniki, iz tabele 6 lahko razberemo, da so raziskave vključile minimalno en dejavnik TPB, najpogosteje pa so vključevale vse tri dejavnike (*Mo* = 3; *Me* = 2,5; *M* = 2,3).

Odgovor na RV3$_{TPB}$: Najpogosteje vključen dejavnik v raziskavah, ki so temeljile na TPB, je odnos do vedenja, ki je tudi najpogosteje statistično značilen dejavnik. Zaznana kontrola vedenja je v raziskave najmanj pogosto vključen dejavnik, ki je prav tako najredkeje statistično značilen dejavnik. Tabela 7 prikazuje ostale podrobnosti analize rezultatov za TPB.

Model sprejemanja tehnologij

Model sprejemanja tehnologij (angl. *Technology Acceptance Model* – TAM) je model, ki je bil prvič predlagan leta 1989 (Davis, 1989). Njegov namen je pojasniti, kaj vpliva na odločitev posameznika oz. njegovo pripravljenost uporabljati in sprejeti tehnologije (kamor sodijo tudi varnostni ukrepi ali rešitve). Temeljni model predpostavlja, da na vedenje vpliva namera, na namero pa vplivata dva dejavnika, in sicer: 1) zaznana enostavnost uporabe (višja kot je kompleksnost uporabe tehnologije, nižja je pripravljenost posameznika da uporablja tehnologijo) in 2) zaznana uporabnost (višja kot je uporabnost oz. priročnost in funkcionalnost tehnologije, večja je pripravljenost posameznika da uporablja tehnologijo).

Identificirali smo devet raziskav, ki so v svojih raziskovalnih modelih vključevale TAM. Povprečna velikost vzorca vseh raziskav je 230 anketirancev. Najpogostejši vzorec anket so bili uporabniki informacijskega sistema, drugi najpogostejši vzorec so bili študentje (tabela 8).

Odgovor na RV3$_{TAM}$: Oba osnovna dejavnika TAM sta bila vključena v vseh identificiranih raziskavah. Pogosteje je statistično značilen dejavnik zaznana uporabnost. Oba napovedna dejavnika TAM sta bila statistično značilna v več kot polovici primerov. Tabela 9 prikazuje ostale podrobnosti analize rezultatov za TAM.

Teorija racionalne izbire

Teorija racionalne izbire (angl. *Rational Choice Theory* – RCT) je teorija, ki je bila prvič predlagana leta 1968 (Becker, 1968). Njen namen je napovedati posameznikovo motivacijo in odločitev za vedenje. Teorija predpostavlja, da sta z racionalnim vedenjem povezana dva dejavnika, in sicer: koristi (posameznikovo dojemanje nagrad oz. koristi povezanih z želenim vedenjem – višje kot so koristi, višja je pripravljenost posameznika izvesti določeno vedenje) in 2) stroški (posameznikova ocena negativnih posledic oz. stroškov in tveganj povezanih z želenim vedenjem – višji kot so stroški, nižja je pripravljenost posameznika izvesti vedenje).

Identificirali smo šest raziskav, ki so v svojih raziskovalnih modelih vključevale RCT. Povprečna velikost vzorca vseh raziskav je 191 anketirancev. Ciljni vzorec vseh šestih raziskav so bili zaposleni, tako v javnem kot tudi zasebnem sektorju. RCT sestavljata dva napovedna dejavnika. Iz tabele 10 lahko razberemo, da so raziskave v polovici primerov vključile le en dejavnik, medtem ko so v polovici vključile oba (*Mo* = 1; *Me* = 1,5; *M* = 1,5).

Tabela 4

Raziskave, ki so v svoje raziskovalne modele vključevale PMT (PS – zaznana resnost posledic, PV – zaznana ranljivost, RE – učinkovitost odziva, SE – zaznana samoučinkovitost, C – zaznani stroški)

Vir	Tema	*n*	Sestava vzorca	Dejavniki	Odvisna spremenljivka
(Jaeger in Eckhardt, 2021)	situacijska IV ozaveščenost	107	zaposleni	PS, PV, RE, SE	namera za varno vedenje (zvabljanje)
(Aigbefo idr., 2020)	vpliv trdoživosti in navad na IV vedenje	294	zaposleni v SMEs	PS, PV	upoštevanje varnostnih postopkov
(Liu idr., 2020)	upoštevanje zahtev IVP	235	kitajski državni uslužbenci	PS, PV, RE, SE	upoštevanje zahtev IVP
(Leering idr., 2020)	neupoštevanje zahtev IV pravil	651	vladni uslužbenci	SE	nadaljevanje z neupoštevanjem pravil
(Yoo idr., 2020)	IV učinkovitost delovne skupine	536	zaposleni	SE	IV učinkovitost delovne skupine
(Jeon idr., 2021)	imanentna motivacija pri upoštevanju zahtev IVP	346	zaposleni v organizacijah, ki trenutno uporabljajo fasoo's EDRM sisteme	RE, SE	namera za upoštevanje zahtev IVP
(Kwak idr., 2020)	prijavljanje sporočil z usmerjenim zvabljanjem	386	izvajalci informacijske tehnologije	SE	verjetnost prijavljanja sporočil z usmerjenim zvabljanjem
(Williams in Joinson, 2020)	nadgrajevanje znanja o zvabljanju	157	člani Prolific	PS, PV, RE, SE	sposobnost prepoznave sporočil z zvabljanjem
(Giwah idr., 2020)	IV vedenja uporabnokov mobilnih telefonov	390	mobilni uporabniki	PS, PV, RE, SE, PC	namera za zaščito pred kršitvijo podatkov
(Vedadi in Warkentin, 2020)	skupinsko IV vedenje	214	zaposleni	PS, PV	namera za uporabo upravitelja gesel
(Verkijika, 2019)	izogibanje zvabljanju	231	uporabniki pametnih telefonov in/ali tabličnih računalnikov	SE	zvabljanju izogibajoče vedenje
(Abraham in Chengalur-Smith, 2019)	učinkovitost IV usposabljanj	210	študentje	PS, PV, SE	namera za preverjanje varnosti spletnih strani ob vpisu
(Hina idr., 2019)	upoštevanje zahtev IVP	301	zaposleni na visokošolskih ustanovah	PS, PV, RE, SE	namera za upoštevanje zahtev IVP
(Hooper in Blunt, 2020)	splošno IV vedenja	70	strokovnjaki za informacijsko tehnologijo	RE, SE	namera za splošno IV vedenje
(Grimes in Marquardson, 2019)	splošna IV vedenja na spletu	169	študentje na nižji ravni managementa	PS, PV, RE, SE	namera za uporaba ukrepov za varnost gesel
(Martens idr., 2019)	splošna namera za zaščito pred kibernetsko kriminaliteto	1181	strokovno raziskovalno podjetje, strokovnjaki	PS, PV, RE, SE	namera za zaščito pred prevarami, škodljivo programsko opremo in kibernetsko kriminaliteto
(Aurigemma in Mattson, 2019b)	upoštevanje zahtev IVP	254	zaposleni v ameriškem ministrstvu za obrambo	PS, PV, RE, SE	namera za upoštevanje zahtev IVP
(Nasir idr., 2019)	informacijsko-varnostna kultura in z njo povezano vedenje	604	študenti	SE	namera za upoštevanje zahtev IVP
(Iriqat idr., 2019)	upoštevanje zahtev IVP	151	zaposleni na univerzah	RE, SE	namera za upoštevanje zahtev IVP

Tabela 4 (nadaljevanje)

Vir	Tema	*n*	Sestava vzorca	Dejavniki	Odvisna spremenljivka
(Chang in Seow, 2019)	neupoštevanje zahtev IV politike	275	redno zaposleni v tajvanskih podjetjih	PS	namera za neupoštevanje zahtev IVP
(D'Arcy in Lowry, 2019)	upoštevanje zahtev IVP	77	zaposleni, računalniški strokovnjaki	SE	upoštevanje zahtev IVP
(Chen, Wu idr., 2018)	upoštevanje zahtev informacijskovanostne politike	231	zaposleni na univerzi	SE, PC	namera za upoštevanje zahtev IVP
(Torten idr., 2018)	vpliv ozaveščenosti na varnostno vedenje	408	strokovnjaki za informacijsko tehnologijo	PS, PV, RE, SE, PC	varna uporaba osebnega računalnika
(Blythe in Coventry, 2018)	izvajanje ukrepov za zaščito pred zlonamerno programsko opremo	526	zaposleni	PS, PV, RE, SE, PC	namera za izvajanje ukrepov za zaščito pred zlonamerno programsko opremo
(Jansen in van Schaik, 2018)	varna uporaba spletnega bančništva	1200	uporabniki spletnega bančništva	PS, PV, RE, SE, PC	previdnost pri uporabi spletnega bančništva
(Menard idr., 2018)	vpliv psihološkega lastništva in kolektivizma na motivacijo za zaščito	500	uporabniki	PS, PV, RE, SE, PC	namera za nezaščito informacij
(Chen, Chen in Wu, 2018)	ozaveščenost,motivacija in zmožnost za upoštevanje zahtev IVP	231	zaposleni na univerzi	SE	namera za upoštevanje zahtev IVP
(Jansen in van Schaik, 2015)	vloga strahu pri varni rabi spleta na primeru zvabljanja	786	uporabniki interneta	PS, PV, RE, SE, PC	motivacija za zaščito pre zvabljanjem
(Geil idr., 2018)	izvajanje ukrepov na področju kibernetske varnosti	138	kmetovalci	PS, PV, SE	varna uporaba računalnika
(Bélanger idr., 2017)	zgodnja posvojitev IVP	535	zaposleni na fakulteti in študentje	SE	namera za zgodnje upoštevanje IVP
(Menard idr., 2017)	motivacija uporabnikov za IV vedenje	785	zaposleni MTurk	PS, PV, RE, SE, PC	splošna namera za varno vedenje
(Jansen in van Schaik, 2017)	primerjava teorij za napovedovanje varne rabe spletnega bančništva	1200	uporabniki spletnega bančništva	PS, PV, RE, SE, PC	previdnost pri uporabi spletnega bančništva
(Laugesen in Hassanein, 2017)	sprejetje elektronskih osebnih zdravstvenih evidenc (ePHR)	230	bolniki in uporabniki brezpredhodnega tehničnega znanja ali izkušenj	RE, SE, PC	namera za sprejetje ePHR
(Warkentin idr., 2016)	trajanje IV vedenja	253	izkušeni uporabniki računalnikov, dodiplomski študenti na dveh univerzah	PS, PV, RE, SE	namera za nadaljevanja IV vedenja
(Chou in Chou, 2016)	problematično IV vedenje	505	učitelji	PS, PV, RE, SE, PC	problematično IV vedenje
(Tsai idr., 2016)	varna raba spleta	988	uporabniki MTurk	PS, PV, RE, SE, PC	namera za izvajanje varnostnih ukrepov
(Hanus in Wu, 2016)	vloga ozaveščenosti pri varni rabi osebnega računalnika	241	dodiplomski študentje poslovne šole	PS, PV, RE, SE, PC	varna uporaba osebnega računalnika

Tabela 4 (nadaljevanje)

Vir	Tema	*n*	Sestava vzorca	Dejavniki	Odvisna spremenljivka
(Safa idr., 2015)	zavestno skrbno IV ravnanje	212	strokovnjaki za informacijsko varnost in informacijsko tehnologijo	PV, SE	zavestno skrbno IV ravnanje
(Dang-Pham in Pittayachawan, 2015)	namera za izogibanje zlonamerni programski opremi	252	študentje visokošolskega študija	PS, PV, RE, SE, PC	namera za izogibanje zlonamerni programski opremi
(Barlette idr., 2015)	IV vedenja poslovodij majhnih in srednje velikih podjetij	258	poslovodje majhnih in srednje velikih podjetij	PS, PV, RE, SE, PC	namera za izvajanje varnostnih ukrepov
(Posey idr., 2015)	vloga organizacijske predanosti za zaščito informacijskih sredstev	380	zaposleni	PS, RE, PC	namera za varno vedenje
(Kim idr., 2014)	upoštevanje zahtev IVP	194	uporabniki informacijskih sistemov v organizacijah s politikami informacijske varnosti	RE, SE	namera za upoštevanje zahtev IVP
(Herath idr., 2014)	varnostne storitve kot mehanizem za spopadanje z (ne)varnostjo	134	dodiplomski študentje	PV, SE	namera za sprejem zunanjih mehanizmov za spopadanje z (ne)varnostjo
(Vance idr., 2012)	upoštevanja zahtev varnostnih postopkov za informacijske sisteme	210	zaposleni v državni upravi	PS, PV, RE, SE, PC	namera za upoštevanje IVP
(Bulgurcu idr., 2016)	vloga ozaveščenosti in racionalno utemeljenih prepričanj na upoštevanje zahtev IVP	464	zaposleni, ki uporabljajo informacijske vire svojih organizacij	SE	namera za upoštevanje zahtev IVP
(Ophoff in Lakay, 2018)	soočanje zlonamerno programsko opremo	118	naključni vzorec osebja in študentov na univerzi, zaposlenih	PS, PV, RE, SE, PC	namera za zaščito pred zlonamerno programsko opremo
(Bauer in Bernroider, 2015)	učinek programov ozaveščanja na informacijsko varnost	183	bančni uslužbenci	PS, PV, RE, SE	namera za varno vedenje
(Siponen idr., 2010)	upoštevanje zahtev IVP	917	zaposleni v podjetjih	PS, PV, RE, SE	namera za upoštevanje zahtev IVP

Tabela 5
Pogostost vključenosti posameznih dejavnikov PMT v raziskovalne modele (f), delež vključenosti (%), ter število primerov, v katerih so bili dejavniki statistično značilno povezani z odvisno spremenljivko (f_z) ter njihov delež ($\%_z$)

Dejavnik	f	%	f_z	$\%_z$
samoučinkovitost	44	92	33	75
zaznana resnost	31	65	16	52
zaznana ranljivost	31	65	12	39
učinkovitost odziva	31	65	21	68
stroški	18	38	14	78

Odgovor na $RV3_{RCT}$: Med obema dejavnika RCT so bile pogosteje vključene koristi, ki so tudi pogosteje statistično značilen dejavnik. Tabela 11 prikazuje ostale podrobnosti analize rezultatov za RCT.

Teorija generalne prevencije

Teorija generalne prevencije (angl. *General Deterrence Theory* – GDT) je kriminološka teorija, ki je bila prvič predlagana leta 1975 (Gibbs, 1975). Njen namen je preučiti vpliv sankcij oz. kazni na odvračanje posameznikov od deviantnega vedenja. Bistvo generalne prevencije je v strahu, saj ta vpliva na odnos, namen in vedenje ljudi ter lahko zmanjša njihovo vpletenosti v neželene oz. prepovedane in odklonske dejavnosti. Teorija predpostavlja, da posameznika od odklonskega vedenja odvračajo trije dejavniki: 1) strogost kazni (posameznik bo manj verjetno kršil pravila oz. ravnal deviantno, če bodo uporabljene stroge kazni); 2) gotovost kazni (posameznik bo manj verjetno kršil pravila oz. ravnal deviantno, če je tveganje, da ga ujamejo veliko); 3) hitrost kazni (posameznik bo manj verjetno kršil pravila oz. ravnal deviantno če bo verjel, da bo kazen hitra).

Identificirali smo tri raziskave, ki so v svojih raziskovalnih modelih vključevale GDT. Povprečna velikost vzorca vseh raziskav je 140 anketirancev. Najpogostejši vzorec anket so bili zaposleni. GDT sestavljajo tri napovedni dejavniki. Iz tabele 12 lahko razberemo, da so raziskave v svoje modele vključevale različno število dejavnikov, od le enega, do vseh treh (Mo = 2; Me = 2; M = 1,7).

Odgovor na $RV3_{GDT}$: Najpogosteje vključen dejavnik v raziskavah, ki so izhajale iz GDT, je strogost kazni, ki pa je bil le v dveh od treh primerov statistično značilen. Gotovost kazni in hitrost kazni sta bila vključena redkeje, pri čemer sta bila vsakokrat statistično značilna (hitrost kazni je bila vključena le enkrat). Tabela 13 prikazuje ostale podrobnosti analize rezultatov za GDT.

Model zdravstvenih prepričanj

Model zdravstvenih prepričanj (angl. *Health Belief Model* – HBM) je psihološki model, ki je bil prvič predlagan leta 1952 (Hochbaum idr., 1952). Njegov namen je pojasniti in napovedati dejavnike za samozaščitno vedenje. Prvotno se je uporabljal na področju zdravstvenega vedenja, kasneje se je uveljavil tudi na področju pojasnjevanja in raziskovanja varnostnega vedenja. Model predpostavlja, da je s samozaščitnim vedenjem povezanih šest dejavnikov oz. zaznava sledečih elementov: 1) tveganje (posameznikovo dojemanje negativnih posledic povezanih z vedenjem – višja kot je stopnja tveganja, višja je pripravljenost posameznika, da ravna samozaščitno); 2) resnost (posameznikovo dojemanje resnosti varnostnega tveganja oz. grožnje – višja kot je zaznana resnost, višja je pripravljenost posameznika, da ravna samozaščitno); 3) koristi (posameznikovo dojemanje nagrad oz. koristi povezanih z želenim vedenjem – višje kot so koristi, višja je pripravljenost posameznika, da ravna samozaščitno); 4) stroški (posameznikova ocena negativnih posledic oz. stroškov ob samozaščitnem dejanju, ukrepu – višji kot so stroški, nižja je pripravljenost posameznika, da izvede ukrepe), 5) spodbude (posameznikova zaznava spodbud za ukrepanje (npr. izobraževanje) – višje kot so spodbude, višja je pripravljenost posameznika, da se samozaščiti); 6) samoučinkovitost (angl. *self-efficacy*): zaznana sposobnost posameznika, da se učinkovito samozaščiti oz. izvede ali uporabi zaščitni ukrep/vedenje – višja kot je samoučinkovitost, višja je pripravljenost posameznika, da se samozaščiti).

Identificirali smo šest raziskav, ki so v svojih raziskovalnih modelih vključevale HBM. Povprečna velikost vzorca vseh raziskav je 446 anketirancev. Najpogostejši vzorec anket so bili zaposleni, ostali vzorci so bili različne populacije – uporabniki interneta, strokovnjaki in študenti. HBM sestavlja šest napovednih dejavnikov. Iz tabele 14 lahko razberemo, da so raziskave najpogosteje v svoje modele vključevale vseh šest dejavnikov in najmanj tri (Mo = 6; Me = 5; M = 4,7).

Odgovor na $RV3_{HBM}$: Najpogosteje vključen dejavnik v raziskavah, ki so temeljile na HBM, je zaznana resnost posledic. Najpogosteje statistično značilen dejavnik so zaznane koristi. Najredkeje so bili v raziskovalne modele vključeni dejavniki spodbude, zaznani stroški in zaznano tveganje, medtem ko sta bila slednja dva dejavnika tudi najmanj pogosto statistično značilna. Tabela 15 prikazuje ostale podrobnosti analize rezultatov za HBM.

Razprava

V pričujočem prispevku smo raziskali uporabo teoretičnih izhodišč v vedenjskih informacijskovarnostnih raziskavah. Ugotavljali smo, katere so najpogosteje uporabljene teorije v vedenjskih informacijskovarnostnih raziskavah, na katerih tematskih področjih se te teorije uporabljajo, kateri dejavniki posameznih teorij so najpogosteje uporabljeni v raziskavah ter kateri dejavniki so najpogosteje statistično značilni. V ta namen smo naredili dve raziskovalni študiji. S prvo študijo smo odgovorili na prvo raziskovalno vprašanje, z

Tabela 6
Raziskave, ki so v svoje raziskovalne modele vključevale TPB (ATT – stališča do vedenja, SN – subjektivne norme, PBC – zaznana kontrola vedenja)

Vir	Tema	*n*	Sestava vzorca	Dejavniki	Odvisna spremenljivka
(Wiafe idr., 2020)	vloga norm pri upoštevanju zahtev IVP	432	študenti	ATT	namera za upoštevanje zahtev IVP
(Jalali idr., 2020)	dovzetnost uporabnikov za zvabljanje	430	zaposlenih v treh bolnišničnih mrežah	ATT, SN, PBC	namera za upoštevanje zahtev IVP
(Klobas idr., 2019)	vloga varnostnih tveganj pri uporabi pametnih naprav	405	potencialni potrošniki	ATT, PBC	namera za uporabo pametnih naprav
(Hansen idr., 2018)	vloga tveganj pri napovedovanje potrošnikove uporabe družbenih medijev za transakcije	318	potrošniki	ATT, PBC	namera za uporabo storitev družbenih omrežij za finančne transakcije
(Ho idr., 2017)	vloga tveganj prri sprejemanju storitev v oblaku	170	višje vodstvo, upravljavci sistemov, osebje na področju informacijskih sistemov, menedžerji in drugi, ki sodelujejo pri odločanju v javnem in zasebnem sektorju	ATT, SN, PBC	namera za uporabo storitev v oblaku
(Mayer, Gerber idr., 2017)	ublažitev nasprotujočih ciljev v organizacijah	200	zaposleni	ATT, SN, PBC	upoštevanje zahtev IVP
(Cox, 2012)	varnost uporabnikov informacijskih sistemov	n.p.*	strokovnjaki, ki uporabljajo informacijsko tehnologijo v svojem delovnem okolju	ATT, SN, PBC	namera za upoštevanje ustreznih varnostnih ukrepov
(Hu idr., 2012)	vloga organizacijske kulture in vodstva na upoštevanje zahtev politike	148	zaposleni	ATT, SN, PBC	namera za upoštevanje zahtev IVP
(Hong in Furnell, 2019)	namera za IV vedenje med zaposlenimi	261	zaposleni v panogah informacijske tehnologije, financ, proizvodnje, logistike, nepremičnin, hotelov, restavracij in medijev	ATT, SN, PBC	namera za uporabo IV ukrepov
(Grimes idr., 2014)	vloga oblike spletnih strani na varno vedenje	173	študenti	ATT, SN, PBC	namera za varno vedenje
(Kranz in Haeussinger, 2014)	vloga endogenih dejavnikov na IV vedenje	444	začetni obiskovalci, zaposleni	ATT	namera za upoštevanje zahtev IVP
(Mussa in Cohen, 2013)	preudarnost pri kontroli dostopa v zdravstvu	47	zaposleni v zdravstvu	ATT, SN, PBC	namera za uporabo dobrih praks na področju kontrole dostopa
(Aigbefo idr., 2020)	vedenjska namera (vpliv trdoživosti in navad na IV vedenje)	294	zaposleni v SMEs	ATT, SN	upoštevanje varnostnih postopkov
(Hina idr., 2019)	upoštevanje zahtev IVP	301	zaposleni na visokošolskih ustanovah	ATT, SN	namera za upoštevanje zahtev IVP
(Sommestad idr., 2019)	upoštevanje zahtev IVP	645	beli ovratniki	ATT, SN, PBC	namera za upoštevanje zahtev IVP

Tabela 6 (nadaljevanje)

Vir	Tema	*n*	Sestava vzorca	Dejavniki	Odvisna spremenljivka
(Grimes in Marquardson, 2019)	splošna IV vedenja na spletu	169	študentje na nižji ravni managementa	SN	namera za uporaba ukrepov za varnost gesel
(Aurigemma in Mattson, 2019a)	prostovoljnost varnostnih ukrepov	227	posamezniki, ki so bili seznanjeni s specifičnim varnostnim problemom in sprejeto rešitvijo uporabe	ATT, SN	namera za varno vedenje (uporabo močnih gesel)
(Martens idr., 2019)	splošna namera za zaščito pred kibernetsko kriminaliteto	1181	strokovno raziskovalno podjetje, strokovnjaki	SN	namera za zaščito pred prevarami, škodljivo programsko opremo in kibernetsko kriminaliteto
(Aurigemma in Mattson, 2019b)	upoštevanje zahtev IVP	254	zaposleni v ameriškem ministrstvu za obrambo	ATT, SN, PBC	namera za upoštevanje zahtev IVP
(D'Arcy in Lowry, 2019)	upoštevanje zahtev IVP	77	zaposleni, računalniški strokovnjaki	ATT, SN	upoštevanje zahtev IVP
(Bélanger idr., 2017)	zgodnja posvojitev IVP	535	zaposleni na fakulteti in študentje	ATT, SN	namera za zgodnje upoštevanje IVP
(Aurigemma in Mattson, 2017)	vloga statusa na namero za upoštevanje groženj in nadzora	239	zaposleni na ministrstvu za obrambo	ATT, SN, PBC	namera za upoštevanje zahtev IVP
(Safa idr., 2015)	zavestno skrbno IV ravnanje	212	strokovnjaki za informacijsko varnost in informacijsko tehnologijo	ATT, SN, PBC	zavestno skrbno IV ravnanje
(Kim idr., 2014)	upoštevanje zahtev IVP	194	uporabniki informacijskih sistemov v organizacijah s politikami informacijske varnosti	ATT	namera za upoštevanje zahtev IVP
(Bulgurcu idr., 2016)	vloga ozaveščenosti in racionalno utemeljenih prepričanj na upoštevanje zahtev IVP	464	zaposleni, ki uporabljajo informacijske vire svojih organizacij	ATT	namera za upoštevanje zahtev IVP

*n.p. – podatka ni bilo mogoče zaslediti v članku (ni podatka).

Tabela 7

Pogostost vključenosti posameznih dejavnikov TPB v raziskovalne modele (f), delež vključenosti (%), ter število primerov, v katerih so bili dejavniki statistično značilno povezani z odvisno spremenljivko (f_z) ter njihov delež ($\%_z$)

Dejavnik	*f*	%	f_z	$\%_z$
odnos do vedenja	23	92	20	87
subjektivne norme	19	76	14	74
zaznana kontrola vedenja	14	56	10	71

Tabela 8

Raziskave, ki so v svoje raziskovalne modele vključevale TAM (PU – zaznana uporabnost, EoU – zaznana enostavnost uporabe)

Vir	Tema	*n*	Sestava vzorca	Vključeni konstrukti	Odvisna spremenljivka
(Ayyash idr., 2020)	sprejetje spletnih družbenih omrežij v sistemu e-učenja	370	palestinski študentje	PU, EoU	namera za uporabo spletnih družbenih omrežij v sistemu e-učenja
(Chatterjee idr., 2019)	preprečevanje kibernetske kriminalitete v pametnih mestih	315	udeleženci konferenc in delavnic	PU, EoU	uporaba tehnologij za preprečevanje kibernetske kriminalitete
(Tamjidyamcholo idr., 2016)	pripravljenost za sodelovanje v strokovnih virtualnih skupnostih	140	udeleženci ResearchGate – raziskovalci, uporabniki	PU, EoU	odnos do uporabe ResearchGate
(Trang idr., 2014)	vloga informacijske varnosti pri uporabi kolaborativnih tehnologij	121	vodje projektov	PU, EoU	namera za uporabo kolaborativnih tehnologij
(Dünnebeil idr., 2012)	sprejetje e-zdravja med zdravniki	117	ambulantni zdravniki	PU, EoU	namera za uporabo e-zdravja
(Addae idr., 2019)	uporabnost napovedne analitike pri razvoju učinkovitih modelov na področju prilagodljive kibernetske varnosti	384	študentje in predavatelji	PU, EoU	namera za uporabo personaliziranih tehničnih rešitev za zagotavljanje varnosti
(Shropshire idr., 2015)	začetno sprejetje IV vedenja	170	dodiplomski študentje, ki so se vpisali na začetni tečaj ekonomije	PU, EoU	namera za uporabo programa Perimeter Check
(Herath idr., 2014)	varnostne storitve kot mehanizem za spopadanje z (ne) varnostjo	134	dodiplomski študentje	PU, EoU	odnos do zunanjih mehanizmov za spopadanje z (ne)varnostjo
(Hansen idr., 2018)	vloga tveganj pri napovedovanje potrošnikove uporabe družbenih medijev za transakcije	318	potrošniki, uporabniki	PU, EoU	namera za uporabo storitev družbenih omrežij za finančne transakcije

Tabela 9

Pogostost vključenosti posameznih dejavnikov TAM v raziskovalne modele (f), delež vključenosti (%), ter število primerov, v katerih so bili dejavniki statistično značilno povezani z odvisno spremenljivko (f_z) ter njihov delež ($\%_z$)

Dejavnik	*f*	%	f_z	$\%_z$
zaznana uporabnost	9	100	7	78
zaznana enostavnost uporabe	9	100	6	67

drugo študijo smo odgovorili na drugi dve raziskovalni vprašanji. S tem smo dosegli vnaprej zastavljene cilje in zapolnili raziskovalno vrzel. V tem poglavju sledi razprava in primerjava ugotovitev s predhodnimi raziskavami.

S prvo študijo, ki je vključevala analizo preglednih prispevkov, smo ugotovili, da je v zadnjih desetih letih med najpogosteje uporabljenimi teorijami v vedenjskih informacijskovarnostnih raziskavah PMT, poleg te je zelo aktualna tudi TPB. Med šest najpogostejših teorij (poleg omenjenih) sodijo še GDT, TAM, RCT, SBT in HBM. Tovrstne ugotovitve so podobne izsledkom raziskave iz leta 2014, v kateri so Lebek idr. (2014) kot najpogosteje uporabljene teorije v informacijskovarnostnih raziskavah opredelili TPB, GDT, PMT in TAM (v tem vrstnem redu). Gre za teoretična izhodišča, ki zaokrožajo potek uporabnikove odločitve, da za samozaščitno vedenje. Uporabnik mora sprva imeti namen, da se bo samozaščitil oziroma spremenil ali prilagodil svoje vedenje (PMT, HBM). Varnostne rešitve (najpogosteje tehnološke) mora nato sprejeti in usvojiti (TAM) ter jih nato uporabljati oziroma jih vpeljati v vsakodnevno rutino (TPB, RCT). V organizacijskih razmerah lahko informacijskovarnostni incidenti povzročijo veliko škodo, zato so pogosto predpisane sankcije za kršitve varnostnih politik (GDT). Nabor omenjenih teorij tako na najbolj zgoščen in celovit način zaokroža področje vedenjskih vidikov informacijske varnosti.

Vedenjske raziskave na področju informacijske varnosti se osredotočajo predvsem na preučevanje kognitivnih procesov pri uporabnikih in njihov vpliv na (ne)upoštevanje zahtev informacijskovarnostne politike (Ormond idr., 2019). Tudi naši rezultati druge študije nakazujejo, da so raziskave, ki smo jih vključili v sistematičen pregled literature v zadnjih desetih letih najpogosteje preučevale upoštevanje pravil in politik s področja informacijske varnosti in splošnega informacijskovarnostnega vedenja. Gre za pričakovane rezultate, saj so informacijskovarnostne politike pomemben (in pogosto izčrpen) del večine organizacij in tako raziskovanje upoštevanja teh pravil predstavlja smiselno usmeritev raziskovalcev, saj upoštevanje pravil pomeni varno vedenje. Kljub temu pa ugotavljamo, da študije pogosto (lahko bi dejali skorajda izključno) nekritično predpostavljajo, da so respondenti seznanjeni z vsebino politik in da njihovo vsebino

Tabela 10

Raziskave, ki so v svoje raziskovalne modele vključevale RCT (PC – zaznani stroški; PB – zaznane koristi)

Vir	Tema	*n*	Sestava vzorca	Vključeni konstrukti	Odvisna spremenljivka
(Hu idr., 2010)	z računalniki povezane kršitve v organizacijah	207	zaposleni	PB	namera za storitev prekrška
(Kim in Han, 2019)	upoštevanje zahtev IVP	162	zaposleni	PC, PB	namera za upoštevanje zahtev IVP
(Aurigemma in Mattson, 2019b)	upoštevanje zahtev IVP	254	zaposleni v ameriškem ministrstvu za obrambo	PC, PB	odnos do upoštevanja zahtev IVP
(D'Arcy in Lowry, 2019)	upoštevanje zahtev IVP	77	zaposleni, računalniški strokovnjaki	PB	odnos do upoštevanja zahtev IVP
(Chen, Chen in Wu, 2018)	upoštevanje zahtev IVP	231	zaposleni na univerzi	PB	namera za upoštevanje zahtev IVP
(Han idr., 2017)	upoštevanje zahtev IVP	213	zaposleni	PC, PB	namera za upoštevanje zahtev IVP

Tabela 11

Pogostost vključenosti posameznih dejavnikov RCT v raziskovalne modele (f), delež vključenosti (%), ter število primerov, v katerih so bili dejavniki statistično značilno povezani z odvisno spremenljivko (f_z) ter njihov delež ($\%_z$)

Dejavnik	*f*	%	f_z	$\%_z$
zaznane koristi	6	100	2	33
zaznani stroški	3	50	2	67

Tabela 12

Raziskave, ki so v svoje raziskovalne modele vključevale GDT (SoP – zaznana strogost kazni, CoP – zaznana gotovost kazni, PCel – zaznana histrost kaznovanja)

Vir	Tema	*n*	Sestava vzorca	Vključeni konstrukti	Odvisna spremenljivka
(Park idr., 2017)	ozaveščenost na področju IV	123	dodiplomski študenti zdravstvene nege	SoP	namera za razkritje pacientovih informacij
(Iriqat idr., 2019)	upoštevanje zahtev IVP	151	zaposleni na univerzah	SoP, CoP	namera za upoštevanje zahtev IVP
(Chen idr., 2020)	upoštevanje zahtev IVP	146	zaposleni	SoP, CoP, PCel	upoštevanje zahtev IVP

dobro poznajo. Poznavanje pravil je namreč predpogoj za njihovo upoštevanje.

Podobno velja za številne raziskave, ki so raziskovale splošno informacijskovarnostno vedenje. Med indikatorji odvisnih spremenljivk je namreč pogosto mogoče zaslediti zelo splošne trditve o informacijski varnosti, kot na primer: »*Nadgradil bom varnostne ukrepe, da bi se bolje zaščitil na spletu*« (Tsai idr., 2016). Avtorji s tovstnimi trditvami predpostavljajo, da respondenti vedo kaj so varnostni ukrepi, kateri izmed njih se uporabljajo na spletu ter, da jih znajo uporabljati. Hkrati zajemajo zelo širok nabor ukrepov. Povprečnemu posamezniku ki pozna varnostne ukrepe se na tem mestu porajajo dodatna vprašanja – predvsem pa po *katerih* ukrepih snovalci raziskave sprašujejo. Respondenti morajo (podobno kot pri upoštevanu pravil informacijskovarnostne politike) najprej poznati ukrepe, da bi jih lahko uporabili in nato nadgradili. S tem se seveda odpira metodološko vprašanje veljavnosti nekaterih rezultatov – tako v primeru raziskovanja upoštevanja pravil informacijskovarnostne politike, kot tudi raziskav, ki se ne osredotočajo na specifične informacijskovarnostne ukrepe.

Z drugo raziskavo smo ugotavljali tudi najpogosteje vključene dejavnike po posameznih teorijah. V raziskavah, ki so temeljile na PMT, je najpogosteje vključen dejavnik samoučinkovitost, v raziskavah, ki so temeljile na TPB, je najpogostejši dejavnik stališče oz. odnos do vedenja. V raziskavah, ki so temeljile na TAM, je bila najpogosteje vključena zaznana uporabnost tehnologije, pri raziskavah, ki so vključevale RCT, je ta dejavnik zaznana korist določenega vedenja, ukrepa. Pri vseh štirih teorijah so omenjeni dejavniki tudi najpogosteje statistično značilni z vidika napovedovanja vedenja oz. vedenjske namere. V raziskavah, ki so bile osnovane na GDT, je bil najpogosteje vključen dejavnik strogost kazni, ki hkrati z dejavnikom gotovost kaznovanja najpogosteje s statistično značilnostjo napoveduje upoštevanje zahtev informacijskovarnostne politike. V raziskavah, ki so izhajale iz HBM, je bila zaznana resnost grožnje najpogosteje vključen dejavnik, koristi želenega vedenja so se izkazale kot najpomembnejši dejavnik, ki ima statistično značilen vpliv na vedenje. Takšni rezultati so podobni sklepom nekaterih drugih avtorjev, kot npr. Jansen in van Schaik (2018) za raziskave povezane s PMT, Nasir idr. (2018) za raziskave povezane s TPB, Alturki idr. (2020) za raziskave povezane s HBM, ter Chen idr. (2012) za raziskave povezane z GDT.

Tako ugotovitve naše raziskave, kot tudi raziskave drugih avtorjev nakazujejo na selektivno vključevanje posameznih dejavnikov uveljavljenih teorij v novonastajajoče modele. Gre za uveljavljeno raziskovalno prakso nadgrajevanja in izboljševanja obstoječih modelov v družboslovju, kar omogoča razvoj področja. Novorazviti modeli pogosto predstavljajo celovitejše in bolj osredotočene poglede na določeno izpostavljeno problematiko. Avtorji pa se le redko poslužujejo neposredne primerjave modela, ki ga predlagajo z uveljavljenim modelom (na istem vzorcu z

Tabela 13

Pogostost vključenosti posameznih dejavnikov GDT v raziskovalne modele (f), delež vključenosti (%), ter število primerov, v katerih so bili dejavniki statistično značilno povezani z odvisno spremenljivko (f_z) ter njihov delež ($\%_z$)

Dejavnik	*f*	%	f_z	$\%_z$
strogost kazni	3	100	2	67
gotovost kazni	2	67	2	100
hitrost kazni	1	33	1	100

Tabela 14

Raziskave, ki so v svoje raziskovalne modele vključevale HBM (PS – zaznana resnost posledic, PC – zaznani stroški, PB – zaznane koristi, SE – zaznana samoučinkovitost, PT – zaznano tveganje, CtA – spodbude)

Vir	Tema	*n*	Sestava vzorca	Vključeni konstrukti	Odvisna spremenljivka
(Dodel in Mesch, 2019)	splošno kibernetsk-ovarnostno vedenje	1850	izraelski uporabniki interneta	PS, PB, PC, SE	dejanska uporaba antivirusne programske opreme
(Williams idr., 2014)	splošno IV vedenje	144	strokovnjaki, ki delajo vsakodnevno z računalnikom	PT, PS, PB, PC. CtA SE	namera za IV vedenje
(Humaidi idr., 2014)	upoštevanje zahtev IVP	256	zaposleni zdravstveni delavci	PT, PS, PB, PC, CtA, SE	upoštevanje zahtev IVP
(Geil idr., 2018)	izvajanje ukrepov na področju kibernetske varnosti	138	kmetovalci	PT, PS, PB, PC, CtA, SE	varna uporaba uporaba osebnega računalnika
(Hanus idr., 2016)	vloga ozaveščenosti pri varni rabi osebnega računalnika	241	dodiplomski študentje poslovne šole	PT, PS, SE	varna uporaba osebnega računalnika
(Mussa in Cohen, 2013)	preudarnost pri kontroli dostopa v zdravstvu	47	zaposleni v zdravstvu	PS, PB, CtA	namera za uporabo dobrih praks na področju kontrole dostopa

istimi indikatorji). Tovrstne primerjave so pogoste na drugih področjih znanosti (npr. v računalništvu), kjer raziskovalci na istih podatkih testirajo učinkovitost novorazvite metode tako, da jo primerjajo z znanimi metodami. V kolikor bi primerljiv (prilagojen) pristop pogosteje uporabili v družboslovju, bi lahko izboljšali interpretabilnost rezultatov in lažje ter bolje utemeljili učinkovitost novih modelov za pojasnjevanje človeškega vedenja.

Iz sklopa teorij, ki preučujejo samozaščitno vedenje, med najpogosteje uporabljeno teorijo sodi PMT. Pri tem pregled literature pokaže, da ima na varnostno oz. samozaščitno vedenje največji vpliv samoučinkovitost. Iz sklopa teorij, ki preučujejo sprejetje tehnologij, se je v končni pregled uvrstil le TAM. Ugotovili smo, da ima na sprejetje tehnologije največji vpliv zaznana uporabnost tehnologije. V tretjem sklopu teorij, ki preučujejo upoštevanje zahtev informacijskovarnostne politike, je najpogosteje uporabljena TPB. Pri tem ima na upoštevanje zahtev politike največji vpliv odnos do vedenja, ki se je izkazal za najpogosteje statistično značilen dejavnik.

V obstoječi literaturi ni mogoče zaslediti splošnega in celostnega pregleda teoretičnih izhodišč v vedenjskih informacijskovarnostnih raziskav in dejavnikov, ki so povezani z vedenjem uporabnikov. Zato smo izvedli raziskavo, ki je vključevala dve študiji na področju vedenjskih informacijskovarnostnih teorij. Gre za eno redkih raziskav, ki je na podlagi obsežnega sistematičnega pregleda literature preučila pogostost uporabe teoretičnih izhodišč in uporabnost ter statistično značilnost dejavnikov po posameznih teorijah. Poznavanje najpogosteje uporabljenih teorij in dejavnikov je pomembno tako za raziskovalce, pri načrtovanju raziskav o vlogi človeških dejavnikov v sistemu informacijske varnosti v prihodnje, kot tudi stroko s področja izobraževanja in ozaveščanja o informacijski in kibernetski varnosti. Strokovnjaki, ki se ukvarjajo z upravljanjem in načrtovanjem informacijske varnosti, lahko uporabijo izsledke naših študij za naslavljanje tistih vidikov, ki so najbolj pomembni oz. vplivni za vedenje uporabnikov.

Omejitve raziskave in predlogi za nadaljnje delo

Kljub sistematični izvedbi, so s študijama, povezane nekatere omejitve. Prvič, vsi prispevki niso bili javno dostopni, zaradi česar do nekaterih nismo uspeli pridobiti dostopa in jih ni bilo mogoče pregledati v celoti. Drugič, iskalni niz kljub premišljeni postavitvi ne more biti vseobsegajoč. Tako obstaja možnost, da ni zajel nekaterih prispevkov. Tretjič, čeprav sta bibliografski zbirki *Web of Science* in *Scopus* obsežni, obstaja možnost, da nekateri aktualni prispevki niso indeksirani v omenjenih zbirkah in tako niso zajeti v naš pregled literature. Četrtič, ugotavljanje pogostosti statistične značilnosti posameznih konstruktov, ki so vsakokrat merjeni z različnimi indikatorji na različno reprezentativnih vzorcih, lahko vpliva na pristranskost rezultatov obravnavanih študij in posledično interpretacije naših rezultatov.

Na podlagi ugotovitev naših študij so vidne tudi priložnosti za nadaljnje raziskave, ki se kažejo na dveh področjih: področju preglednih študij in področju izvirnih študij. Na področju preglednih študij bi bilo v prihodnje smiselno identificirane raziskave skupiniti glede na odvisno spremenljivko in jih analizirati po omenjenih skupinah. Nadalje bi bila smiselna analiza indikatorjev posameznih konstruktov teorij, ki jih raziskovalci vključujejo v svoje empirične raziskave. Indikatorji, ki nepopolno ali napačno odražajo dejansko vsebino konstrukta, kot ga je predvidela teorija, lahko pomembno vplivajo na rezultate. Podobno bi bilo smiselno tudi skupiniti raziskave glede na populacijo na kateri je bila opravljena raziskava. Omenjene podrobnejše analize bi ponudile bolj celovit vpogled v dejansko stanje raziskav na tem področju.

Na področju izvirnih študij pa se kaže predvsem raziskovalna verzel na področju upoštevanja zahtev informacijskovarnostnih politik v podjetjih in raziskav, ki niso osredotočene na točno določeno varnostno vedenje – splošne informacijskovarnostne raziskave. Prihodnje raziskave bi se pred ugotavljanjem upoštevanja zahtev informacijskovarnostnih politik morale osredotočiti na stopnjo poznavanja zaposlenih o informacijskovarnostnih politikah. Na področju splošnega informacijskovarnostnega vedenja pa bi bilo v prihodnjih študijah smiselno nasloviti probleme razumljivosti in osredotočenosti indikatorjev odvisnih konstruktov. Tako so na tem področju na mestu metodološke raziskave, ki bi nadgrajevale obstoječa znanja in omogočile (bolj) veljavne in zanesljive rezultate v prihodnje.

Zaključek

Uporabniki s svojim vedenjem pri uporabi tehnologij, informacijskih sistemov in podatkov, predstavljajo ali najmočnejši ali pa najšibkejši člen informacijske varnosti. Za

Tabela 15

Pogostost vključenosti posameznih dejavnikov HBM v raziskovalne modele (f), delež vključenosti (%), ter število primerov, v katerih so bili dejavniki statistično značilno povezani z odvisno spremenljivko (f_z) ter njihov delež ($\%_z$).

Dejavnik	f	%	f_z	$\%_z$
zaznana samoučinkovitost	5	89	3	60
spodbude	4	67	3	75
zaznani stroški	4	67	2	50
zaznane koristi	5	83	5	100
zaznana resnost posledic	6	100	4	67
zaznano tveganje	4	67	2	50

ustrezno upravljanje uporabniškega vidika je treba razumeti, kaj vpliva na vedenja uporabnikov oz. njihovo pripravljenost izvajati priporočene varnostne ukrepe in spoštovati informacijskovarnostne politike ter pravila. V literaturi, ki razlaga vedenjske vidike v informacijski varnosti, je mogoče zaslediti različna teoretična izhodišča, ki so uporabna za pojasnjevanje in napovedovanje vedenja uporabnikov. V ta namen se uporabljajo tako psihološke, kakor tudi kriminološke in organizacijske teorije. S poznavanjem tovrstnih teorij lahko pojasnimo kaj vpliva na stališča uporabnikov, njihovo demotivacijo, odpor do upoštevanja politik, tehnologij ali pravil in kaj vpliva na njihovo dejansko končno vedenje. Na podlagi teh znanj je mogoče uporabnike lažje spodbuditi k pozitivnem vedenju, motivaciji in varnostni kulturi.

Literatura

Abraham, S. in Chengalur-Smith, I. S. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers and Security*, *87*, članek 101586.

Addae, J. H., Sun, X., Towey, D. in Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, *29*, 701–750.

Aigbefo, Q. A., Blount, Y. in Marrone, M. (2020). The influence of hardiness and habit on security behaviour intention. *Behaviour and Information Technology*, *41*(6), 1151–1170.

Ajzen, I. (1985). From intention to actions: A theory of planned behavior. V J. Kuhl in J. Beckman (ur.), *Action control: From cognition to behavior* (str. 11–39). Springer.

Al-Harthy, I. M., Rahim, F. A., Ali, N. in Singun, A. P. (2020). Dimensions of protection behaviors: A systematic literature review. *Journal of Theoretical and Applied Information Technology*, *98*(17), 3668–3697.

Alohali, M., Clarke, N., Furnell, S. in Albakri, S. (2017). Information security behavior: Recognizing the influencers. V *Proceedings of Computing Conference 2017, 18-20 July 2017, London, United Kingdom* (str. 844–853). IEEE.

Alturki, A., Alshwihi, N. in Algarni, A. (2020). Factors influencing players' susceptibility to social engineering in social gaming networks. *IEEE Access*, *8*, 97383–97391.

Angraini, Alias, R. A. in Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, 1216–1224.

Aurigemma, S. in Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers and Security*, *66*, 218–234.

Aurigemma, S. in Mattson, T. (2019a). Effect of long-term orientation on voluntary security actions. *Information and Computer Security*, *27*(1), 122–142.

Aurigemma, S. in Mattson, T. (2019b). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems*, *20*(12), 1700–1742.

Ayyash, M. M., Herzallah, F. A. T. in Ahmad, W. (2020). Towards social network sites acceptance in e-learning system: Students perspective at Palestine Technical University-Kadoorie. *International Journal of Advanced Computer Science and Applications*, *11*(2), 312–320.

Barlette, Y., Gundolf, K. in Jaouen, A. (20.–22. maj 2015). *Toward a better understanding of SMB CEOs' information security behavior: Insights from threat or coping appraisal* [prispevek na konferenci]. 20th Symposium of the Association Information and Management 2015, AIM 2015, Rabat, Morocco.

Bauer, S. in Bernroider, E. W. N. (2015). The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring. V *Proceedings of the Third International Conference on Human Aspects of Information Security, Privacy, and Trust*, *9190* (str. 154–164). Springer.

Becker, G. S. (1968). Crime and punishment: An economic approach. V G. S. Becker in W. Landes (ur.), *Essays in the economics of crime and punishment* (str. 1–54). Columbia University Press.

Bélanger, F., Collignon, S., Enget, K. in Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management*, *54*(7), 887–901.

Blythe, J. M. in Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87–97.

Bulgurcu, B., Cavusoglu, H. in Benbasat, I. (2016). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548.

Chang, K. C. in Seow, Y. M. (2019). Protective measures and security policy non-compliance intention: IT vision conflict as a moderator. *Journal of Organizational and End User Computing*, *31*(1), 1–21.

Chatterjee, S., Kar, A. K., Dwivedi, Y. K. in Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: From a citizen's perspective. *Information Technology and People*, *32*(5), 1153–1183.

Chen, X., Chen, L. in Wu, D. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, *58*(4), 312–324.

Chen, Y., Ramamurthy, K. in Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157–188.

Chen, L., Zhen, J., Dong, K. in Xie, Z. (2020). Effects of sanction on the mentality of information security policy compliance. *Revista Argentina de Clinica Psicologica*, *29*(1), 39–49.

Chen, X., Wu, D., Chen, L. in Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information and Management*, *55*(8), 1049–1060.

Chou, H. L. in Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, *65*, 334–345.

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858.

D'Arcy, J. in Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69.

Da Veiga, A. in Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361–372.

Dang-Pham, D. in Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers and Security*, *48*, 281–297.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340.

Dodel, M. in Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers and Security*, *86*, 75–91.

Dünnebeil, S., Sunyaev, A., Blohm, I., Leimeister, J. M. in Krcmar, H. (2012). Determinants of physicians' technology acceptance for e-health in ambulatory care. *International Journal of Medical Informatics*, *81*(11), 746–760.

Ganeshkumar, P. in Gopalakrishnan, S. (2013). Systematic reviews and meta-analysis: Understanding the best evidence in primary healthcare. *Journal of Family Medicine and Primary Care*, *2*(1), 9–14.

Geil, A., Sagers, G., Spaulding, A. D. in Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*, *21*(3), 317–334.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier.

Giwah, A. D., Wang, L., Levy, Y. in Hur, I. (2020). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital*, *21*(2), 215–233.

Grimes, M. in Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, *119*, 23–34.

Han, J. Y., Kim, Y. J. in Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers and Security*, *66*, 52–65.

Hansen, J. M., Saridakis, G. in Benson, V. (2018). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior*, *80*, 197–206.

Hanus, B. in Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. in Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61–84.

Hina, S., Panneer Selvam, D. D. D. in 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. *Computers and Security*, *87*, *članek* 101594.

Ho, S. M., Ocasio-Velázquez, M. in Booth, C. (2017). Trust or consequences? Causal effects of perceived risk and subjective norms on cloud technology adoption. *Computers and Security*, *70*, 581–595.

Hochbaum, G., Rosenstock, I. in Kegels, S. (1952). *Health Belief Model*. United States Public Health Service.

Hong, Y. in Furnell, S. (2019). Organizational formalization and employee information security behavioral intentions based on an extended TPB model. V *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), University of Oxford, United Kingdom, 3–4 June 2019* (str. 1–4). IEEE. https://doi.org/10.1109/CyberSecPODS.2019.8885405

Hooper, V. in Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour and Information Technology*, *39*(8), 862–874.

Hu, Q., Dinev, T., Hart, P. in Cooke, D. (2012). Managing employee compliance with information security policies. *Decision Sciences*, *43*(4), 615–659.

Hu, Q., Xu, Z., Dinev, T. in Ling, H. (2010). Why individuals commit computer offences in organizations: Investigating the roles of rational choice, self-control, and deterrence. V *PACIS 2010 Proceedings: 14th Pacific Asia Conference on Information Systems* (str. 1378–1389).

Humaidi, N., Balakrishnan, V. in Shahrom, M. (2014). Exploring user's compliance behavior towards health information system security policies based on extended health belief model. V *IC3e: 2014 IEEE Conference on e-Learning, e-Management and e-Services, Melbourne, Australia, 10-12 December 2014* (str. 30–35). IEEE.

Iriqat, Y. M., Ahlan, A. R. in Molok, N. N. A. (2019). Information security policy perceived compliance among staff in palestine universities: An empirical pilot study. V *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, Jordan, April 9-11* (str. 580–585). IEEE.

Jaeger, L. in Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429–472.

Jalali, M. S., Bruckes, M., Westmattelmann, D. in Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research*, *22*(1), članek e16775.

Jansen, J. in van Schaik, P. (2015). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information & Computer Security*, *23*(3), 302–316.

Jansen, J. in van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, *25*(2), 165–180.

Jansen, J. in van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371–383.

Jeon, S., Son, I. in Han, J. (2021). Exploring the role of intrinsic motivation in ISSP compliance: Enterprise digital rights management system case. *Information Technology and People*, *34*(2), 599–616.

Kim, H. L. in Han, J. (2019). Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective. *Information Technology and People*, *32*(4), 858–875.

Kim, S. H., Yang, K. H. in Park, S. (2014). An integrative behavioral model of information security policy compliance. *Scientific World Journal*, *2014*, članek 463870.

Kitchenham, B. in Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (EBSE 2007-001). Keele University and Durham University Joint Report.

Klobas, J. E., McGill, T. in Wang, X. (2019). How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers and Security*, *87*, članek 101571.

Kranz, J. J. in Haeussinger, F. J. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. V *Proceedings of the 35th International Conference on Information Systems ICIS 2014: Building a Better World through Information Systems, Auckland, New Zealand, December 14-17, 2014*. Association for Information Systems.

Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B. in Perumal, S. (2020). Systematic literature review of information security compliance behaviour theories. *Journal of Physics: Conference Series*, *1551*, članek 012005.

Kwak, Y., Lee, S., Damiano, A. in Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, *48*, *članek* 101343.

Laugesen, J. in Hassanein, K. (2017). Adoption of personal health records by chronic disease patients: A research model and an empirical study. *Computers in Human Behavior*, *66*, 256–272.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. in Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092.

Leering, A., van de Wijngaert, L. in Nikou, S. (2020). More honour'd in the breach: Predicting non-compliant behaviour through individual, situational and habitual factors. *Behaviour and Information Technology*, *41*(3), 519–534.

Liu, C., Wang, N. in Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, *54*(28), *članek* 102152.

Mark Grimes, G., Marquardson, J. in Nunamaker, J. F. (2014). Broken windows, bad passwords: Influencing secure user behavior via website design. V *20th Americas Conference on Information Systems (AMCIS 2014): Smart Sustainability: The Information Systems Opportunity, Georgia, USA, 7-9 August 2014* (str. 1862–1873). AIS/ICIS.

Martens, M., De Wolf, R. in De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150.

Mayer, P., Gerber, N., McDermott, R., Volkamer, M. in Vogt, J. (2017). Productivity vs security: Mitigating conflicting goals in organizations. *Information and Computer Security*, *25*(2), 137–151.

Mayer, P., Kunz, A. in Volkamer, M. (2017). Reliable behavioural factors in the information security context. V *ACM International Conference Proceeding Series, Part F1305*.

Menard, P., Bott, G. J. in Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230.

Menard, P., Warkentin, M. in Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security*, *75*, 147–166.

Mussa, C. in Cohen, M. (2013). Prudent access control behavioral intention: Instrument development and validation in a healthcare environment. V *19th Americas Conference on Information Systems (AMCIS 2013): Hyperconnected World: Anything, Anywhere, Anytime, Chicago, Illinois, USA, 15–17 August 2013* (str. 2820–2830). AIS/ICIS.

Nasir, A., Abdullah Arshah, R. in Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal*, *28*(3), 55–80.

Nasir, A., Abdullah Arshah, R. in Rashid Ab Hamid, M. (2018). The significance of main constructs of theory of planned behavior in recent information security policy compliance behavior study: A comparison among top three behavioral theories. *International Journal of Engineering & Technology*, *7*(2.29), 737–741.

Njenga, K. (2017). Understanding internal information systems security policy violations as paradoxes. *Interdisciplinary Journal of Information, Knowledge, and Management*, *12*, 1–15.

Ophoff, J. in Lakay, M. (2018). Mitigating the ransomware threat: A protection motivation theory approach. V H. Venter, M. Loock, M. Coetzee, M. Eloff in J. Eloff (ur.), *Information security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018: Communications in Computer and Information Science*, *973* (str. 163–175). Springer.

Ormond, D., Warkentin, M. in Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems*, *20*(12), 1794–1843.

Park, E. H., Kim, J. in Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers and Security*, *65*, 64–76.

Parker, H. J. in Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *SA Journal of Information Management*, *22*(1), 1–10.

Posey, C., Roberts, T. L. in Lowry, P. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214.

Prislan, K. in Bernik, I. (2019). *Informacijska varnost in organizacije* [Information security and organizations]. Univerzitetna založba Univerze v Mariboru.

Prislan, K., Mihelič, A. in Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLoS ONE*, *15*(9), članek e0238739.

Reason, J. (2000). Human error: Models and management. *British Medical Journal*, *320*(7237), 768–770.

Richardson, M. D., Lemoine, P. A., Stephens, W. E. in Waller, R. E. (2020). Planning for cyber security in schools: The human factor. *Educational Planning*, *27*(2), 23–39.

Rocha Flores, W., Antonsen, E. in Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers and Security*, *43*, 90–110.

Rogers, R. W. (1983). Cognitive and physiological process in fear appeals and attitude change: A revised theory of protection motivation. V J. Cacioppo in R. Petty (ur.), *Social Psychophysiology: A source book* (str. 153–176). Guilford Press.

Sadaf, H. in Dhanapal, D. D. (2018). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*, *60*(3), 201–211.

Safa, N. S., Maple, C., Watson, T. in Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, *40*, 247–257.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. in Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78.

Shropshire, J., Warkentin, M. in Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security*, *49*, 177–191.

Siponen, M., Pahnila, S. in Mahmood, M. A. A. (2010). Compliance with information security policies: An empirical investigation. *IEE Computer Society*, *43*(2), 64–71.

Sommestad, T., Karlzén, H. in Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*, *59*(4), 344–353.

Soomro, Z. A., Shah, M. H. in Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225.

Tamjidyamcholo, A., Kumar, S., Sulaiman, A. in Gholipour, R. (2016). Willingness of members to participate in professional virtual communities. *Quality and Quantity*, *50*(6), 2515–2534.

Torten, R., Reaiche, C. in Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers and Security*, *79*, 68–79.

Trang, S. T. N., Ruch, T. J. in Kolbe, L. M. (2014). Collaborative technologies in an inter-organizational context: Examining the role of perceived information security and trust on post-adoption. V R. H. Sprague, Jr. (ur.), *Proceedings of the 47th Annual Hawaii International Conference on System Sciences HICSS, Waikoloa, Hawaii, 6–9 January 2014* (str. 160–169). IEEE.

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J. in Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*, 138–150.

Vance, A., Siponen, M. in Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198.

Vedadi, A. in Warkentin, M. (2020). Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. *Journal of the Association for Information Systems*, *21*(2), 428–459.

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286–296.

Vicozi, M. (2018). *Vloga posameznika pri zagotavljanju informacijske varnosti* [The role of an individual in providing information security] [Magistrsko delo, Univerza v Ljubljani, Ekonomska fakulteta]. Repozitorij Univerze v Ljubljani. https://repozitorij.uni-lj.si/IzpisGradiva.php?id=104732

Warkentin, M., Johnston, A. C., Shropshire, J. in Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25–35.

Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N. in Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information and Computer Security*, *28*(5), 743–761.

Williams, E. J. in Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, *6*(1), 1–16.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E. in Duncan, B. K. (2014). Explaining users' security behaviors with the security belief model. *Journal of Organizational and End User Computing*, *26*(3), 23–46.

Yoo, C. W., Goo, J. in Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly: Management Information Systems*, *44*(2), 907–932.

Prispelo/Received: 7. 11. 2021
Sprejeto/Accepted: 8. 8. 2022