VARSTVOSLOVJE,
letn. 20
št. 1
str. 25–44

Analiza vedenja uporabnikov spletnega bančništva

Kaja Prislan, Branko Lobnikar

Namen prispevka:

Namen prispevka je analizirati vedenjske vzorce uporabnikov in varnostna tveganja, ki se pojavljajo pri uporabi spletnega bančništva. V prispevku so predstavljeni temeljni in aplikativni teoretični okvirji ter modeli pojasnjevanja vedenja uporabnikov spletnega bančništva, na podlagi rezultatov empirične raziskave pa so izoblikovani predlogi za izboljšanje programov informiranja in ozaveščanja uporabnikov za varno uporabo spletnega bančništva.

Metode:

Izhajajoč iz okvirov vedenjskih teorij in usmeritev bank za varno uporabo spletnega bančništva je bila izvedena raziskava med uporabniki v Sloveniji (n = 210). Zbiranje podatkov je potekalo s pomočjo spletnega anketiranja. Proučili smo, kako uporabniki ob rabi spletnega bančništva skrbijo za varnost lastnih elektronskih naprav, gesel, digitalnih potrdil in na kakšen način skrbijo za varnost na spletu ter katere druge samozaščitne ukrepe pri tem uporabljajo.

Ugotovitve:

Rezultati kažejo, da so anketiranci dobro ozaveščeni o nevarnostih pri uporabi spletnega bančništva, vendar kljub temu še vedno zaznavamo neprimerne prakse pri zaščiti ključnih podatkov. Ugotavljamo tudi nizko stopnjo samoiniciativnosti pri uporabi varnostnih ukrepov, zato je zavzetost uporabnikov ključni izziv, ki ga je treba nasloviti za dvig stopnje varnosti pri uporabi spletnega bančništva.

Omejitve raziskave:

Omejitve raziskave izhajajo iz majhnega vzorca udeležencev raziskave, vsebinsko pa je raziskava osredinjena na proučevanje vedenja uporabnikov spletnega bančništva in ukrepov, vezanih na tovrstno storitev. Drugi vidiki zagotavljanja varnosti in vedenja uporabnikov pri rabi spleta in interneta v prispevku niso analizirani.

Praktična uporabnost:

Ugotovitve raziskave so uporabne tako za ponudnike spletnega bančništva, njihove uporabnike kot tudi za vse zainteresirane in tiste, ki se ukvarjajo s procesi krepitve varne uporabe informacijske tehnologije.

Izvirnost/pomembnost prispevka:

Študija analizira vedenje uporabnikov spletnega bančništva s pomočjo različnih vedenjskih teorij, ki so bile osnova za oblikovanje vprašalnika, uporabljenega v raziskavi. Uporabljena metoda lahko predstavlja osnovo za bodoče raziskovanje vedenja uporabnikov tako na področju spletnega bančništva kot drugih spletnih storitev.

UDK: 004.056+336.71:004.738.5

Ključne besede: banke, spletno bančništvo, varnost, vedenje uporabnikov, samozaščita

Analysis of Online Banking Users Behaviour

Purpose:

The purpose of the paper is to analyse behavioural patterns of users and the security risks that occur when using online banking. The paper presents basic and applied theoretical frameworks and models for explaining the behaviour of online banking users. Based on the results of the empirical research, proposals for improving the awareness programs for users regarding security of online banking were developed.

Design/Methods/Approach:

Based on frameworks of behavioural theories and guidelines for the safe use of online banking, a survey was conducted among users in Slovenia ($n = 210$). Data were collected through online survey. We analysed how users take care of their safety and security when using online banking services, how they protect their electronic devices, passwords, digital certificates and what other self-protection measures they use.

Findings:

The results show that respondents are well aware of the dangers associated with online banking, but nonetheless they still engage in risk-taking and fail to protect their key data properly. We also observe low level of self-initiative and commitment for the use of additional security measures. Therefore, user engagement is a key challenge that needs to be addressed in order to raise the level of online banking security.

Research Limitations:

The limitations of the research derive from a small sample and the limited focus of the survey. The research is focused on studying the behaviour of online banking users and measures related to such services. Other aspects of information security and users behaviour when using the internet and online services are not analysed in the paper.

Practical Implications:

The paper and research findings are useful for both online banking providers and their users, as well as for those who are in any way interested in the topic or involved in the process of reinforcing the safe use of information technology.

Originality/Value:

The study analyses the behaviour of online banking users through various behavioural theories and models, which formed the basis for the questionnaire used in the survey. The method presented in the paper can serve as a basis for future exploration of user behaviour both in the area of online banking and in other online services.

UDC: 004.056+336.71:004.738.5

Keywords: bank, online banking, security, safety, users' behaviour, self-protection

1 UVOD

Spletno in mobilno bančništvo[1] je v zadnjem desetletju postalo splošno dostopna in razširjena finančna storitev. V 27 državah EU je trenutna stopnja razširjenosti spletnega bančništva med prebivalci 49 %, se pa stanje močno razlikuje med državami (v sedmih državah je na primer večja od 70 %, v Sloveniji pa je 35 %) (Statista, 2018). Raziskava Ameriške centralne banke (Board of Governors of the Federal Reserve System, 2013) je pokazala, da približno 74 % lastnikov bančnih računov uporablja spletno in 29 % mobilno bančništvo. Spletno bančništvo opisujemo kot sklop procesov, v okviru katerih se stranka preko spleta prijavi v sistem banke s pomočjo spletnega brskalnika in osebne elektronske naprave: v okviru tega lahko izvaja transakcije, plačuje račune ali upravlja oseben bančni račun (Jassal in Sehgal, 2013). Na ta način stranke prihranijo čas in bančne storitve opravijo na bolj preprost način. Glavne prednosti spletnega bančništva v primerjavi s klasičnim bančništvom so *udobnost* (možnost oddaljenega dostopa, dostopnost 24 ur na dan), *dostopnost* (iz katerekoli lokacije, na kateri se posameznik počuti varno ali nujno potrebuje storitve), *hitrost* (obdelava podatkov, upravljanje s storitvami poteka hitreje kot v klasičnem pristopu, transakcije pa so opravljene enako hitro), *učinkovitost* (izvedejo se lahko skoraj vse storitve in vse oblike upravljanja z računom in vse možne transakcije) in *zanesljivost* (transakcije se izvajajo na zahtevan in pričakovan način) (Khan, 2014). Pomemben vidik spletnega bančništva pa je tudi varnost te storitve, ki je osrednja tema tega prispevka. Ker med storilci kibernetske kriminalitete nasploh prevladuje finančna motivacija, so storitve elektronskega poslovanja in spletnega bančništva ena izmed glavnih tarč napadov, ogroženi pa so tako uporabniki kot banke. To dokazuje velika količina finančnih prevar, goljufij, vdorov in napadov, izvedenih na sisteme ali podatke, povezane z bančnim poslovanjem (npr. primer vdora v banko JP Morgan leta 2014 ali napadi skupine MoneyTaker na ruske in ameriške banke v letu 2017).

Poleg banke, ki mora poskrbeti za ustrezno tehnično varnost aplikacij in procesov, povezanih s spletnim bančništvom, je odgovornost za varnost tudi na uporabniku, ki je dolžan storitve uporabljati v skladu z navodili ponudnika in koncepti varnega vedenja na spletu. Čeprav je primarna odgovornost za zagotavljanje varnosti na banki, je za preprečevanje škodnih primerov pomemben predvsem uporabnik, saj se večina groženj uresniči s pomočjo preslepitve uporabnikov. Ko govorimo o tveganih vedenjih uporabnikov storitev spletnega bančništva, največjo težavo predstavlja njihovo neznanje glede zaščite ali neozaveščenost oz. napačne percepcije glede groženj. Ker do škodnih primerov pogosto pride zaradi napak in ranljivosti na strani uporabnika, je namen prispevka analizirati vedenje uporabnikov spletnega bančništva in ugotoviti, kakšna so glavna tveganja, ki izhajajo iz tega, in kaj bi bilo treba storiti, da bi bila uporaba bolj varna in učinkovita.

1.1 Varnost in spletno bančništvo

Pri varnostnih tveganjih v povezavi s spletnim bančništvom ločujemo med zaznavo varnostnih tveganj s strani uporabnikov ter dejanskimi oškodovanji. Gre

1 *Elektronsko bančništvo zajema spletno in mobilno bančništvo.*

za enak odnos, kot ga v kriminologiji poznamo med strahom pred kriminaliteto in dejansko viktimizacijo. Po podatkih Eurobarometer Cybersecurity 390 (European Commission, 2012) skoraj 30 % uporabnikov interneta navaja, da se ne čutijo sposobne oz. kompetentne za varno uporabo spleta, 40 % uporabnikov spletnega bančništva pa je zaskrbljenih glede varnosti – najbolj jih skrbi zloraba ali kraja osebnih podatkov. Britanska raziskava (D'Ardenne in Toomse-Smith, 2014) je pokazala, da so glavni razlogi neuporabe spletnega bančništva povezani ravno s pomisleki glede varnosti – tisti, ki spletnega bančništva ne uporabljajo, so v večini primerov (85 %) prepričani, da storitve niso varne, najbolj se bojijo hekerskih vdorov in prevar. Velik odstotek anketirancev, ki spletnega bančništva ne uporablja, vendar jih zanima, je priznal, da se ne počuti sposobne varno uporabljati te storitve. Čeprav je strah med uporabniki spletnega bančništva pogost pojav, ne gre za neupravičene percepcije, saj so nevarnosti pri uporabi spletnega bančništva zelo konkretne.

Finančno poročilo iz Velike Britanije navaja, da je država v letu 2016 zaradi zlorab spletnega bančništva uradno zabeležila več kot 137-milijonsko škodo v funtih, celotna škoda nastala zaradi zlorabe bančnih kartic pa znaša skoraj petkrat več. Skupaj so zabeležili skoraj dva milijona primerov finančnih prevar (Financial Fraud Action UK, 2017). Raziskava organizacije Verizon (2015) pa ugotavlja, da eden izmed 25 prejemnikov phishing[2] sporočil, ki sicer sodijo med najpogostejše tehnike preslepitve uporabnikov, nasede prevari. Izmed prejemnikov neznanih sporočil kar 11 % ljudi odpre prejeto priponko, 25 % pa jih deli svoja uporabniška gesla z drugimi ljudmi. Primerov uresničenih groženj v povezavi z bančnim poslovanjem je ogromno, v nadaljevanju pa kot ilustracijo predstavljamo nekatere najbolj odmevne primere, ki nazorno prikazujejo način delovanja in tehnike storilcev. Julija 2015 je bila na primer razkrita oz. zaznana velika organizirana akcija napadov na uporabnike večjih evropskih in ameriških bank. Uporabljena so bila phishing elektronska sporočila, ki so vsebovala vstavljeno zlonamerno kodo. Ob zagonu se je na uporabnikov računalnik namestil trojanski virus, ki so ga strokovnjaki poimenovali kot Dyre malware, s katerimi so storilci zbirali finančne podatke uporabnikov in organizacij. Z uspešnimi prevarami so od organizacij uspešno ukradli več kot milijon ameriških dolarjev, po ocenah pa je bilo prizadetih več kot 1.000 bank po vsem svetu, okužbo pa so storilci za pridobitev vstopa v sisteme organizacij kombinirali z DDOS napadi. Omenjen virus je po tehniki zelo podoben škodljivi programski opremi ZEUS (Murdoc, 2015). Ta se je prvič pojavil leta 2007, v obtoku pa je bil več let (do 2010). Tudi ta se je kot zagonska koda širil preko elektronskih sporočil, ob namestitvi pa deloval kot vohunski program, ki je spremljal aktivnosti in beležil osebne podatke ter gesla za vstop v spletne bančne račune. V to organizirano prevaro je bilo vpletenih več sto ljudi, ki so skupaj banke, stranke in organizacije oškodovali za 70 milijonov dolarjev. Poleg opisanih primerov je znan tudi SpyEye trojanski konj, ki je na podoben način kot prejšnja dva okužil 1,4 milijona računalnikov in omogočil vdor v 10.000 spletnih bančnih

2 *Phishing je tehnika lažnega predstavljanja, zavajanja in manipuliranja z uporabniki, ki je namenjena pridobivanju zaupnih podatkov. Pod pretvezo, da sporočilo pošilja legitimna oseba ali ustanova se uporabnika pozove k posredovanju osebnih in drugih podatkov ali k obisku lažne spletne strani, preko katere se uporabnik okuži z zlonamernim programom.*

računov. V dveh letih delovanja se je na trgu pojavilo več verzij tega virusa, ki so se prodajale na temnem spletu (Jackson Higgins, 2014).

Poleg uporabnikov spletnega bančništva med pogoste tarče sodijo tudi banke in zaposleni v finančnih ustanovah. Februarja 2015 je bilo na primer razkrito delovanje mednarodne organizirane kriminalne združbe imenovane »Carbanak«, sestavljene iz evropskih, ruskih, ukrajinskih in kitajskih hekerjev, ki se je v obdobju dveh let infiltrirala v 30 bank po svetu in se pri tem skupno okoristila za več kot milijardo dolarjev. Mediji so dogodek poimenovali kot »kibernetski rop brez primere«. Za razliko od klasičnih primerov spletnih prevar so storilci v tem primeru napadli banke in bančne uslužbence in ne njihove stranke oz. uporabnike. V tem času so za izvedbo aktivnosti uporabljali različne zlonamerne kode Carberp Trojan, Anunak in Carbanak, pri čemer so se nekatere izmed teh prodajale tudi v spletnem kriminalnem podzemlju. Storilci so imeli natančno predstavo o tem, katere zaposlene v bankah je treba izkoristiti, da so lahko pridobili vstop v kritične dele informacijskih bančnih sistemov. Čas izkoriščanja določenega sistema je v povprečju trajal med dvema in štirimi meseci, v tem času so natančno proučili infrastrukturo in njihove sisteme, preverjali programsko opremo, ki jo uporabljajo banke, in se na ta način izognili detekciji. V osnovi so napadi temeljili na phishing prevari preko elektronske pošte, s katero so zaposlene okužili z namensko izdelano programsko kodo. Z njeno pomočjo so na sisteme bank naložili dodatne programe, ki so jim nato omogočili oddaljen nadzor in vstop v strežnike (Kaspersky Lab, 2015).

Ker gre za globalne grožnje, se s tovrstnimi prevarami in tveganji soočamo tudi v Sloveniji. Januarja 2015 so bile na primer stranke šestih slovenskih bank tarča phishing prevar, napadi pa so bili dolgotrajni in zelo premišljeni oz. dobro organizirani. V sporočilih so storilci stranke pozvali k obisku lažne, na videz legitimne spletne strani, kjer so od njih zahtevali vnos osebnih podatkov in enkratnih gesel za dostop do spletnega bančnega računa. V tem primeru so se banke na prevare odzvale hitro, s poudarkom na obveščanju in opozarjanju svojih strank. Nekatere so nadgradile obstoječe varnostne mehanizme, medtem ko se vse strinjajo, da so obstoječi ukrepi zadostni in da je uspešnost takšnih groženj odvisna od njihovih strank (Grosman, 2015). O vse večji nevarnosti in agresivnosti storilcev poroča tudi slovenski CERT, ki vsako leto zazna veliko količino napadov oz. prevar, povezanih z uporabniškimi računi. V zadnjem poročilu o omrežni varnosti (SI-CERT, 2016) lahko preberemo, da je bilo uradno prijavljenih 283 primerov phishing prevar in 40 primerov zlorab uporabniških računov, goljufij in prevar nasploh pa je bilo več kot 900.

2 POMEN VEDENJSKIH TEORIJ ZA KREPITEV VARNOSTI UPORABE SPLETNEGA BANČNIŠTVA

Banke zaradi vse več primerov ogrožanj svojih storitev postopke za krepitev varnosti usmerjajo v uporabnike (gre za t. i. *user-centered security approach)*. Pri upravljanju vedenja ljudi je namreč treba upoštevati dejstvo, da ljudje sami ustvarjamo situacije, v katerih smo lahko oškodovani, zato lahko največ za lastno varnost naredimo ravno sami z ustreznim samozaščitnim vedenjem (Kreuger in

Kerney, 2006). Na odločanje in vedenje uporabnikov v kontekstu varnosti sicer vplivajo številni elementi. Te pojasnjujejo različne vedenjske teorije in pristopi, kot sta na primer teorija razumne akcije in teorija načrtovanega vedenja (angl. *Theory of reasoned action* (TRA) in *Theory of planned behaviour* (TPB)). Teoriji opisujeta, da je vedenje posameznika odvisno od njegovih namenov in motivov, ki pa so v veliki meri pogojeni z njegovimi normami in odnosom do nekega pojava. Kadar ima posameznik močna prepričanja (npr. glede tveganj in nevarnosti), pozitiven odnos (npr. zaupanje v varnostne rešitve) in močno ponotranjene norme (npr. glede lastne odgovornosti do varnosti), je tudi namen izvesti neko dejavnost (npr. zaščititi se) večji (Khan, Alghathbar, Nabi in Khurram, 2011). Če se nadalje osredotočimo na temeljne vedenjske teorije, je treba poudariti, da je prepričanjem, odnosu in normam Bandura (1977) pri pojasnjevanju posameznikovega vedenja dodal še ključno spremenljivko – tj. »občutek samonadzora«. Ta pojasnjuje, da se posameznik lažje odloči za neko aktivnost, kadar ima večji občutek nadzora oz. kontrole nad situacijo. V skupino pojasnjevalnih teorij vedenja posameznika je smiselno dodati tudi teorijo PMT (angl. *Protection motivation theory*), ki pojasnjuje, kako se ljudje vedemo v primeru zaznave tveganj. Uporaba samovarovalnih ali samozaščitnih ukrepov je po tej teoriji odvisna od osebne percepcije posameznika in ne od njegove dejanske ogroženosti. Za zaščito se bo posameznik odločil, kadar bo ocenil, da je stopnja ranljivosti, verjetnost uresničenja grožnje in možnost samoučinkovitega zavarovanja dovolj visoka, največji vpliv na aktivnost posameznika pa ima strah, ki je odvisen od zaznane ranljivosti in nevarnosti (Rogers, 1975). Ljudje sicer pogosto tveganja podcenjujemo in precenjujemo lastne sposobnosti, sploh kadar se primerjamo z drugimi subjekti, razlog pa je v subjektivnih ocenah, ki temeljijo na omejenih informacijah, pomanjkljivem znanju in hevristikah (miselne bližnjice pri odločanju). V povezavi s teorijo PMT se pri proučevanju vedenja ljudi glede na zaznana tveganja pogosto uporablja model HBM (angl. *Health belief model*), ki se ukvarja z analiziranjem odnosov in razumevanjem vedenja ljudi ob zaznavi tveganj, z namenom njihovega upravljanja oz. usmerjanja. Je psihološki model, ki poskuša pojasniti in predvideti vedenje ljudi, primarno na področju zdravja (ob zaznavi zdravstvenih tveganj), v zadnjem času pa se je izjemno uveljavil tudi pri analizah odzivov na varnostna tveganja oz. varnostnega vedenja ljudi. Model predpostavlja, da je vedenje odvisno od štirih elementov: *zaznane verjetnosti* (da se bo grožnja uresničila), *zaznane nevarnosti* (škoda, ki jo lahko povzroči grožnja), *zaznane koristi* (koristi ob neupoštevanju pravil oz. neuporabi varnostnih ukrepov) in *zaznanih ovir* (verjetnost uspeha preprečitve grožnje). Ta prepričanja ljudi vplivajo na njihovo pripravljenost izvesti določeno aktivnost oz. akcijo (Rosenstock, 1974). Študija, ki sta jo na podlagi modela HBM v kontekstu elektronskega bančništva izvedla Davinson in Sillence (2014), kaže, da je med uporabniki zaznana verjetnost uresničenja goljufij (prevar) zelo majhna, čeprav so izkazali relativno visoko stopnjo poznavanja teh goljufij. Večina uporabnikov meni, da se grožnja njim ne more zgoditi, če pa se ta zgodi, pa niso osebno odgovorni zanjo. Anketiranci v tej študiji so izkazali prepričanje, da je za posledice morebitnih incidentov odgovorna banka in čeprav niso vsi prepričani, da bo banka to odgovornost dejansko prevzela, menijo, da sami finančnih izgub ne bodo utrpeli. Kljub temu, da poznajo najpomembnejše

varnostne kontrole, večine teh ne uporabljajo, saj menijo, da so preveč zamudne in realno nepotrebne. Veliko anketirancev v omenjeni raziskavi (Davinson in Sillence, 2014) tudi meni, da varnostne kontrole ne morejo preprečiti groženj, kar potrjuje vpliv predpostavke o samoučinkovitosti na vedenje. S to študijo se je pokazalo, da je stopnja zaznane škode in koristi varnega vedenja zelo nizka in da to vodi v ravnodušno, celo malomarno vedenje uporabnikov.

Poleg modela HBM med uveljavljene modele na področju proučevanja varnostnega vedenja ljudi, ki izhajajo iz opisanih vedenjskih teorij, sodi tudi model KABP (angl. *Knowledge, Attitude, Belief, and Practice*), ki poudarja pomen ozaveščenosti in kompetentnosti uporabnikov. Glede na predpostavke modela ima največjo vlogo pri spreminjanju vedenja ljudi njihovo znanje, poleg tega pa še njihov odnos in osebna stališča, ki jih imajo do nekega področja (torej motivacija, zaznana samoučinkovitost, norme ipd.) (Mcllwraith, 2006). Po priporočilih tega vedenjskega modela je za spreminjanje vedenja ljudi najprej treba razumeti vzroke njihovega trenutnega obnašanja; to pomeni, da je treba najprej oceniti trenutno stanje, identificirati odstopanja in pomanjkljivosti in nato programe ozaveščanja oblikovati na podlagi teh ugotovitev. V tem kontekstu je treba oceniti: (a) kaj ljudje vedo (znanje); (b) kaj si mislijo (prepričanja – odnose in norme) in (c) kaj dejansko počno v praksi (vedenje) (Mcllwraith, 2006). Z uporabo modela se identificirajo ovire, ki zavirajo zaželeno vedenje, ocenijo stališča ljudi do neke problematike in ugotovi, kakšna je stopnja njihovega znanja ter kompetenc na določenem področju (Gumucio, 2011). Z uporabo modela lahko ugotovimo, ali so nevarne vedenjske prakse posledica pomanjkljivega znanja ali neustreznih odnosov. Model KAPB je bil uspešno uporabljen tudi pri proučevanju zagotavljanja informacijske varnosti v slovenskem prostoru (Lobnikar, Prislan, Markelj in Banutai, 2012).

Če z vidika zagotavljanja varnosti uporabnikov spletnega bančništva želimo doseči trajne spremembe v njihovem vedenju in oblikovati ustrezna priporočila, ki bi prispevala k bolj varnemu vedenju, je treba dobro razumeti opisane koncepte. Z vidika varnosti je še posebej pomembno, da se posameznik počuti odgovornega za svoje vedenje in posledice; da pozna tveganja in načine zaščite, še posebej pomembno pa je, da zmore uresničiti pričakovanja. Večina opisanih teorij in modelov namreč med ključne dejavnike, ki vplivajo na vedenje ljudi in njihovo motivacijo spremeniti vedenje, uvršča občutek samoučinkovitosti oz. zmožnosti nadzora. V tem kontekstu se je razvil tudi termin računalniška samoučinkovitost (Compeau in Higgins, 1995; Davis, Bagozzi in Warshaw, 1989), ki se nanaša na samooceno posameznika glede lastnih sposobnosti opraviti neko nalogo ali aktivnost, za katero so potrebne določene računalniške kompetence.

Če pri pojasnjevanju vedenjskih dimenzij spletnega bančništva izhajamo iz opisanih vedenjskih teorij, lahko sklenemo, da internet in informacijska tehnologija zaradi vsesplošne razširjenosti in enostavne uporabe pri ljudeh pogosto vzbujata občutek lažne varnosti, večjega samonadzora in manjše ogroženosti, kot je realno. Ljudje se pri uporabi tehnologije nemalokrat počutijo samozavestno, pri uporabi spletnega bančništva pa storitve uporabljajo doma, kjer se nasploh počutijo varno, kar še dodatno poglablja napačne občutke in predstave (Davinson in Sillence, 2014). Kadar posamezniki delujejo izven nadzorovanega okolja in ne zaznavajo realnih posledic groženj in tveganih vedenj, je njihova motivacija do uporabe

samozaščite veliko nižja, saj jo zaznavajo kot nepotreben poseg v njihovo svobodo in funkcionalnost storitev (Mihelič in Vrhovec, 2017). Wash (2010) navaja, da imajo ljudje tudi nasploh v odnosu do informacijske varnosti pogosto napačne kognitivne oz. mentalne modele in predstave – v določenih situacijah (npr. izguba oz. kraja gesla) ne vidijo večje nevarnosti, ampak naivno menijo, da ne bodo oškodovani. Prav tako ljudje radi prenašajo odgovornost za lastno varnost na tretje osebe (npr. banke, tehnično pomoč) ali pa se preveč zanašajo na tehnične kontrole.

Na podlagi predstavljenih izzivov, ki so povezani z vedenjem uporabnikov pri zaznavi varnostnih tveganj in pregleda priporočil, ki jih banke podajajo svojim strankam za večjo varnost spletnega bančništva[3], smo zasnovali raziskavo, v kateri smo proučili vedenje uporabnikov spletnega bančništva v Sloveniji.

3 OPIS UPORABLJENE METODE, VZORCA IN VPRAŠALNIKA

Vprašalnik, s katerim smo zbrali podatke, izhaja iz spoznanj opisanih vedenjskih teorij ter modelov KABP in HBM. Vsebina je oblikovana na podlagi priporočil bank. Vedenje uporabnikov spletnega bančništva smo ocenjevali s petimi vsebinskimi sklopi, ki jih je sestavljalo 32 trditev:

a. Prvi sklop »*Varnost elektronske naprave*« se nanaša na stopnjo varnosti uporabnikovega računalnika, preko katerega dostopa do spletne banke

3 *Glavna priporočila, ki jih svojim strankam dajejo banke v slovenskem prostoru glede zaščite pri uporabi spletnega bančništva (Banka Koper, Gorenjska banka, Abanka, NLB, Hypo Alpe Adria):*

- *Uporaba varnostnih programov za zaznavanje škodljive programske opreme na elektronski napravi, ki se uporablja za dostop do spletne banke.*
- *Posodabljanje programske opreme.*
- *Uporaba varnih spletnih povezav (ssl, https) in preverjanje avtentičnosti certifikata spletne strani banke.*
- *Preverjanje pošiljateljev e-sporočil in ignoriranje tistih, ki prihajajo od nepoznanih virov.*
- *Varna hramba zaupnih podatkov in nosilcev podatkov za dostop do uporabniških računov.*
- *Uporaba izključno preverjene programske opreme iz zanesljivih virov.*
- *Redno preverjanje stanja na bančnem računu.*
- *Varna hramba digitalnega potrdila. Priporočeno je, da se digitalno potrdilo hrani na ločenem mediju, v primeru hrambe na računalniku pa naj bo zaščiteno z močnim geslom in onemogočen njegov izvoz.*
- *Varno upravljanje z gesli. Gesla naj bodo dovolj dolga in kompleksna, redno menjana in poznana samo lastniku. Gesla naj ne bodo nikoli zapisana na vidnem mestu. Uporabljajo naj se različna gesla za različne uporabniške račune.*
- *Po uporabi se je priporočljivo vedno odjaviti iz spletnega računa in zapreti brskalnik. Ta mora biti nastavljen tako, da ne shranjuje gesel in uporabniških imen.*
- *Izdelava kopij digitalnega potrdila in zasebnega ključa ter shranjevanje na ločenem mediju.*
- *Ustrezna konfiguracija požarnega zidu, ki odkriva in preprečuje potencialno nevarne povezave.*
- *Varna uporaba spleta, ki zajema obiskovanje zgolj preverjenih spletnih strani.*
- *Varna hramba generatorja gesel. Tako kot digitalno potrdilo naj bo generator hranjen ločeno od naprave, preko katere se dostopa do bančnega računa.*
- *Uporaba dodatnih varnostnih nastavitev, npr. dodatnih varnostnih gesel za potrjevanje plačil, limita uporabe, sms obveščanja, osebnega vstopnega pozdravnega sporočila.*
- *Spremljanje opozoril organizacij in bank glede varnostnih popravkov in aktualnih groženj.*
- *Uporaba spletnega bančnega računa na varni napravi. Naprava, s katero se uporablja bančni račun, naj bo v osebni lasti (ne javni računalnik), priporočeno pa je, da se uporablja ločen spletni brskalnik in da se naprava ne povezuje v omrežja za prenos torrent datotek.*
- *Skrb za zaupnost ključnih podatkov. Podatkov, povezanih s spletnim bančnim računom, (številka kreditne kartice, uporabniško ime, geslo, certifikat/potrdilo, OTP geslo) ni priporočljivo deliti z drugimi osebami, še posebej pa ne preko elektronske pošte ali telefona.*

(npr., kako je poskrbljeno za zaščito, v kakšne namene se uporablja).

b. Drugi sklop »*Varnost na spletu*« ocenjuje stopnjo varnosti uporabnika pri uporabi spleta in omrežja (npr., kateri spletni mehanizmi se uporabljajo pri dostopu do spletne banke, na kakšen način, kakšna je ozaveščenost o spletnih prevarah).
c. Tretji sklop »*Upravljanje z gesli*« analizira kakovost uporabnikovih gesel in ostalih mehanizmov za dostop do računov (npr. izbiranje, shranjevanje, posredovanje gesel).
d. Četrti sklop »*Upravljanje z digitalnimi potrdili*« se nanaša na zaščito certifikatov in generatorjev gesel (npr., na kakšen način se varujejo, shranjujejo in konfigurirajo potrdila ter uporabljajo varnostni mehanizmi ponudnika).
e. Peti sklop »*Samozaščita*« ocenjuje proaktivnost in motiviranost uporabnika (npr. uporaba dodatnih varnostnih mehanizmov, informiranje in samoiniciativnost uporabnika).

Vsakega izmed petih sklopov so sestavljala vprašanja, ki prakso uporabnikov ocenjujejo z dihotomnimi odgovori (da/ne) ali petstopenjskimi lestvicami (vrednosti od 0 do 4). Spremenljivke, s katerimi smo ocenjevali posamezno področje, smo utežili s stopnjevalnimi tako, da se lahko vsako izmed petih področij indeksira. Vsak možni odgovor v vprašalniku je v osnovi utežen z vrednostmi 0 ali 4 (za dihotomna vprašanja) in od 0 do 4 pri petstopenjskih lestvicah. Odgovore smo utežili tako, da se vrednost 0 dodeli odgovorom, ki opisujejo skrajno negativno oz. neželeno vedenje, vrednost 4 pa najboljše možne prakse. Na ta način lahko s seštevkom odgovorov anketirancev izračunamo končni indeks varnostnega vedenja. Minimalno lahko anketiranec zbere 0 točk, maksimalno pa 100 točk, kar predstavlja najvišji nivo varnosti oz. učinkovitega varnostnega vedenja. Pri vsakem izmed petih sklopov področij je možno zbrati 20 točk, na tej podlagi pa lahko ocenimo tudi indeks varnega vedenja na posameznih področjih. Stopnjo varnosti smo ocenili za vsakega anketiranca posebej, s seštevkom vrednosti odgovorov.

Socialno-demografske značilnosti udeležencev smo ugotavljali s pomočjo sedmih vprašanj, ki so se nanašala na splošne osebnostne značilnosti (spol, starost, status, ponudnik spletne banke), predhodno viktimizacijo, občutek varnosti ob rabi spletnega bančništva in občutek odgovornosti ter uporabo mobilnega bančništva.

Podatke smo marca 2015 zbrali s pomočjo spletnega anketiranja, vabilo za sodelovanje pa smo razširjali s pomočjo različnih spletnih omrežij in preko elektronske pošte.

3.1 Opis vzorca

V analizo smo vključili vprašalnike tistih anketirancev, ki so v celoti odgovorili na vsebinska vprašanja – teh je bilo skupaj 210. Vsi anketiranci so uporabniki spletnega bančništva (največ uporabnikov uporablja NLB Klik – 46 %, Abanet – 12 % in Bank@net – 8 % uporabnikov spletne banke). Demografske značilnosti vključenega vzorca so predstavljene v tabeli 1.

Tabela 1: Opis demografskih značilnosti vzorca

		N	Odstotek
Spol (*N* = 190)	Moški	88	46
	Ženski	102	54
Starost (*N* = 190); povprečna starost = 35, 7	Do 25	29	15,3
	26-35	80	42,1
	36-50	58	30,5
	Nad 50	23	12,1
Status (*N* = 186)	Zaposlen	122	66
	Nezaposlen	20	11
	Študent	30	16
	Upokojen	14	8
Osebna izkušnja s phishing prevaro (*N* = 189)	Da	37	20
	Ne	152	80
Občutek varnosti pri uporabi spletnega bančništva (*N* = 190)	Da	165	87
	Ne	25	13
Odgovornost za varnost spletnega bančništva (*N* = 191)	Uporabnik	103	54
	Ponudnik/banka	88	46
	Država	0	0
Uporaba mobilnega bančništva (*N* = 191)	Da	37	19
	Ne	154	81

4 PREDSTAVITEV IN INTERPRETACIJA REZULTATOV RAZISKAVE

V študiji nismo ugotavljali stopnje viktimiziranosti slovenskih uporabnikov spletnega bančništva pri uporabi te finančne storitve, je pa 13 % anketirancev poročalo, da se pri uporabi te storitve ne počuti varno in da jih je imelo 20 % izkušnjo s phishing prevaro pri uporabi spletne banke. V nadaljevanju predstavljamo ugotovitve raziskave, ki kažejo na možnosti za viktimizacijo – predstavljamo tvegana vedenja, ki na strani uporabnika kažejo na ranljivost za prevaro. Najprej so predstavljeni rezultati v obliki opisnih statistik, zatem pa še primerjave med posameznimi demografskimi skupinami, vključenimi v raziskavo. Rezultate predstavljamo združene v posamezne vsebinske sklope, kot so bili predstavljeni v metodološkem delu prispevka (varnost elektronskih naprav, varnost na spletu, upravljanje z gesli, upravljanje z digitalnimi potrdili in samozaščitno vedenje uporabnikov spletnega bančništva).

V tabeli 2 so najprej prikazani rezultati odgovorov na vprašanja, ki se vežejo na varnost elektronske naprave, ki jo anketiranci uporabljajo za spletno bančništvo.

Tabela 2: Varnost elektronske naprave

N = 210		*N*	Odstotek
1. Ali spletno banko uporabljate na istem računalniku oz. napravi, ki jo uporabljate za spletno brskanje, branje novic, sodelovanje v socialnih omrežjih in podobno?	0 (Da)	198	94
	4 (Ne)	12	6
2. Ali napravo, preko katere dostopate do spletne banke, uporabljate tudi za dostop do zabavnih video vsebin (npr. torrent) in vsebin za odrasle?	0 (Da)	141	67
	4 (Ne)	69	33
3. Ali imate na elektronski napravi za dostop do spletne banke nastavljen ločen/poseben uporabniški račun brez skrbniških oz. administratorskih pravic (t. i. »root access«)?	4 (Da)	70	33
	0 (Ne)	140	67
4. Ali je naprava, na kateri imate nameščen digitalni certifikat oz. preko katere dostopate do spletne banke, v času neuporabe in mirovanja ustrezno zavarovana pred nepooblaščeno uporabo s strani drugih, tudi poznanih oseb (npr. naprava je fizično varna pred krajo, zaklenjena z geslom, šifrirana ipd.)?	4 (Da)	168	80
	0 (Ne)	42	20
5. Ali ste se pri ponudniku spletne banke pozanimali o vseh možnih (tudi dodatnih) varnostnih ukrepih, ki so vam na voljo, in jih potem tudi uporabili pri svojem poslovanju s spletno banko?	4 (Da)	88	42
	0 (Ne)	122	58

Pri uporabi naprave, ki jo anketiranci uporabljajo za storitve spletnega bančništva, lahko med tvegana vedenja uvrstimo naslednje ugotovitve: 94 % anketirancev spletno banko uporablja na istem računalniku, ki ga uporablja tudi za osebno rabo (spletno brskanje, družabna omrežja itd.), 67 % anketirancev napravo, na kateri uporablja spletno banko, uporablja tudi za dostop do zabavnih vsebin, torrent datotek in vsebin za odrasle, 67 % anketirancev ne uporablja ločenega uporabniškega računa za dostop do spletne banke, 58 % anketirancev pa se pri ponudniku spletne banke ni pozanimalo o dodatnih varovalnih mehanizmih. 80 % anketirancev navaja, da je njihova naprava, preko katere dostopajo do spletne banke, varna pred nepooblaščeno uporabo s strani tretjih oseb (varna pred krajo, zaklenjena, šifrirana). V tabeli 3 so prikazani rezultati analize, ki so se vezali na varno uporabo spleta.

Tabela 3: Varnost pri uporabi spleta

N = 205		*N*	Odstotek
1. Ali za dostop do spletne banke uporabljate isti spletni brskalnik kot za opravljanje drugih spletnih aktivnosti?	0 (Da)	140	68
	4 (Ne)	65	32
2. Ali se vedno odjavite in zaprete brskalnik potem, ko končate z uporabo spletne banke?	4 (Da)	177	86
	0 (Ne)	28	14
3. Ali ste kdaj komu preko elektronske pošte posredovali svoje osebne podatke, vezane na poslovanje s spletno banko, kot npr. številko kreditne kartice, uporabniško ime, geslo ali certifikat?	0 (Da)	11	5
	4 (Ne)	194	95
4. Ali vedno preverite pošiljatelja elektronskega sporočila (takoj izbrišete sporočila neznanih pošiljateljev) in ste zelo previdni pri odpiranju priponk?	4 (Da)	195	95
	0 (Ne)	10	5
5. Ali v »nastavitvah« spletnega brskalnika redno preverjate veljavnost (datum poteka) in avtentičnost (prstni odtis oz. »hash« SHA in MD5) vašega digitalnega potrdila?	4 (Da)	68	33
	0 (Ne)	137	67

Pri uporabi spleta med ugotovitve, ki opisujejo tvegano vedenje, sodi ugotovitev, da 68 % anketirancev za dostop do spletne banke uporablja isti spletni brskalnik kot za opravljanje drugih osebnih in službenih aktivnosti, ter ugotovitev,

da 67 % anketirancev ne preverja veljavnosti in avtentičnosti digitalnega potrdila. Kljub tem ugotovitvam pa lahko povzamemo tudi nekaj spodbudnih rezultatov: 86 % anketirancev vedno zapre spletni brskalnik po uporabi spletne banke, 95 % anketirancev preko e-pošte ne posreduje svojih osebnih podatkov, vezanih na uporabo spletne banke, 95 % anketirancev prav tako ustrezno preverja izvor elektronskih sporočil in so previdni pri ravnanju/odpiranju s priponkami. V tabeli 4 so predstavljeni rezultati opisne statistke pri vsebinskem sklopu, ki se je nanašal na upravljanje z gesli.

Tabela 4: Upravljanje z gesli pri spletnem bančništvu

N = 199		*N*	Odstotek
1. Kakšna gesla uporabljate za vstop v vašo spletno banko? Ocenite, kaj je značilno za geslo, ki ga uporabljate. Izberite en odgovor.	0 (Geslo, ki si ga lahko hitro zapomnim (npr. letnice, roj. dnevi)	29	15
	1 (Smiselne in enostavne kombinacije besed in števil)	36	18
	2 (Daljše fraze, sestavljene iz črk, številk in simbolov.)	57	29
	3 (Dolga gesla, sestavljena iz naključnih znakov)	32	16
	4 (PIN kodo in enkratno geslo identifikacijske kartice/naprave)	45	23
	Povprečje/standardni odklon (2,1/1,3)		
2. Kako pogosto menjate geslo za vstop v vašo spletno banko?	0 (Nikoli)	67	34
	1 (Redko (npr. do 1-krat na leto))	57	29
	2 (Občasno (npr. vsaj 2-krat na leto))	30	15
	3 (Pogosto (npr. vsaj 4-krat na leto))	29	15
	4 (Zelo pogosto (npr. vsak mesec))	16	8
	Povprečje/standardni odklon (1,3/1,3)		
3. Kje imate shranjeno geslo za vstop v spletno banko?	0 (Na istem osebnem računalniku)	6	3
	1 (Na mobilni napravi, ki je v redni uporabi)	4	2
	2 (Zapisano imam na papirju)	26	13
	3 (Na ločeni elektronski napravi, ki ni v redni uporabi)	11	6
	4 (Nikjer ga nimam zapisanega, sem si ga zgolj zapomnil/a	152	76
	Povprečje/standardni odklon (3,5/1,0)		
4. Ali isto oz. podobno geslo, ki ga imate za dostop do spletne banke, uporabljate tudi pri katerem drugem uporabniškem računu?	0 (Da)	51	26
	4 (Ne)	148	74
5. Ali ste kdaj komu zaupali svoje geslo za vstop v spletno banko (četudi je to znana oseba)?	0 (Da)	23	12
	4 (Ne)	176	88

Pri analizi zagotavljanja varnosti gesel za dostop do spletne banke ugotavljamo naslednja najpogostejša uporabniška tveganja: približno tretjina anketirancev uporablja preprosta gesla, ki so sestavljena iz smiselnih in enostavnih fraz, 62 % anketirancev nikoli ali pa samo enkrat letno menja geslo za dostop do spletne banke, 26 % anketirancev pa isto geslo uporablja tudi na drugih uporabniških računih. Pri tem si 76 % anketirancev gesla za dostop do spletne banke ni zapisalo/shranilo, 88 % anketirancev gesla še ni zaupalo nikomur.

Naslednji vsebinski sklop se je vezal na upravljanje z digitalnimi potrdili, ki jih uporabniki uporabljajo pri spletnem bančništvu. Rezultati so prikazani v tabeli 5.

Tabela 5: Upravljanje z digitalnimi potrdili pri spletnem bančnem poslovanju

N = 197		*N*	Odstotek
1. Ali imate generator gesel (OTP), žeton oz. dodatno varnostno geslo za potrjevanje transakcij varno shranjeno pred izgubo, krajo, nepooblaščeno uporabo?	4 (Da)	116	59
	0 (Ne)	81	41
2. Ali pri izvajanju transakcij uporabljate dodatno varnostno geslo, s katerim potrdite izvedbo nakazila?	4 (Da)	136	69
	0 (Ne)	61	31
3. Ali imate aktivirano SMS obveščanje v primeru prijave v spletni bančni račun oz. v primeru izvedbe finančnih transakcij preko spletne banke?	4 (Da)	88	45
	0 (Ne)	109	55
4. Ali imate na spletni banki določen limit porabe, ki omejuje vaše transakcije?	4 (Da)	121	61
	0 (Ne)	76	39
5. Kje imate shranjeno vaše digitalno potrdilo?	0 (Na istem računalniku)	99	66
	4 (Na pametni kartici, USB-ju)	52	34

Pri delu z digitalnimi potrdili smo prav tako ugotovili nekatera tvegana vedenja. Na primer 41 % anketirancev generatorja gesel nima varno shranjenega pred izgubo oz. zlorabo, 55 % anketirancev nima aktiviranega SMS-obveščanja v primeru izvedbe transakcij preko spletne banke, 66 % anketirancev pa ima digitalno potrdilo shranjeno na isti napravi, preko katere dostopa do spletne banke. Med pozitivna vedenja v tem vsebinskem sklopu lahko uvrstimo ugotovitvi, da 69 % anketirancev uporablja dodatno varnostno geslo za potrditev transakcij in da ima 61 % anketirancev določen limit porabe. Zadnji vsebinski sklop se je vezal na vedenje uporabnikov spletnega bančništva in je prikazan v tabeli 6.

Tabela 6: Samozaščita uporabnikov

N =192	0 (Sploh ne drži)	1 (Ne drži)	2 (Niti/niti)	3 (Drži)	4 (Popolnoma drži)	Povp.	*SD*
1. Stalno preverjam pravilnost vnesenega URL-ja in varnost povezave (https://), preden vstopim v spletno banko.	28 (15 %)	28 (15 %)	33 (17 %)	55 (29 %)	48 (25 %)	2,3	1,4
2. Operacijski sistem in aplikacije na napravi, preko katere dostopam do spletne banke, so stalno posodobljene.	2 (1 %)	13 (7 %)	33 (17 %)	83 (43 %)	61 (32 %)	3	0,9
3. Na napravi, preko katere dostopam do spletne banke, imam vedno aktivirane in posodobljene varnostne ukrepe (npr. antivirusni program in požarni zid).	4 (2 %)	8 (4 %)	16 (8 %)	73 (38 %)	91 (47 %)	3,2	0,9

Tabela 6: Nadaljevanje

N =192	0 (Sploh ne drži)	1 (Ne drži)	2 (Niti/niti)	3 (Drži)	4 (Popolnoma drži)	Povp.	*SD*
4. Redno spremljam stanje na svojem bančnem računu in ugotavljam morebitna odstopanja.	1 (1 %)	4 (2 %)	17 (9 %)	78 (41 %)	92 (48 %)	3,3	0,8
5. Redno spremljam varnostna obvestila in opozorila ponudnika spletne banke ter drugih varnostnih organizacij (npr. SI-CERT, Varni na Internetu, Safe-si, Policija).	10 (5 %)	30 (16 %)	36 (19 %)	76 (40 %)	40 (21 %)	2,7	1,1

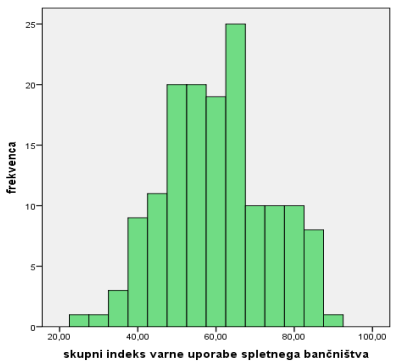
Pri uporabi spletne banke kar 46 % anketirancev ne preverja pravilnosti/avtentičnosti spletne povezave, hkrati pa 40 % anketirancev ne spremlja varnostnih obvestil in opozoril ponudnika spletnega bančništva ali drugih varnostnih organizacij. Ugotovili smo, da ima 75 % anketirancev ustrezno posodobljene aplikacije in operacijske sisteme na napravi, preko katere dostopa preko spletne banke, da ima 85 % anketirancev na napravi nameščen posodobljen antivirusni program ter da 89 % anketirancev redno preverja stanje na spletnem bančnem računu. V tabeli 7 so prikazani sumarni rezultati o stopnji varnosti pri uporabi spletnega bančništva.

Tabela 7: Izračunani indeksi varnega vedenja pri uporabi spletnega bančništva

Varnost naprave	7,62 (od 20)
Varnost na spletu	13,72 (od 20)
Upravljanje z gesli	13,51 (od 20)
Upravljanje z digitalnimi potrdili	10,23 (od 20)
Samozaščita	14,48 (od 20)
Skupen indeks vseh anketirancev	**59,56 (od 100)**

Na sliki 1 je prikazana porazdelitev indeksa stopnje varnosti uporabnikov spletnega bančništva. Vidimo lahko, da je dobra četrtina anketirancev (25,7 %) uvrščena v skupino z nizko stopnjo varnega vedenja (sumarni rezultat pod 50), 16,2 % anketirancev pa se je uvrstilo v skupino z zelo visoko stopnjo varnostnega vedenja (sumarni rezultat nad 75).

Slika 1: Porazdelitev indeksa varnega vedenja



V nadaljevanju smo rezultate podrobneje analizirali in proučili razlike oz. analizirali varianco med posameznimi skupinami anketirancev (statistično značilnost rezultatov smo proučili s testom ANOVA).

V tabeli 8 je predstavljena primerjava zgoraj prikazanih vsebinskih sklopov glede na posamezne starostne skupine. Ugotavljamo, da obstajajo statistično značilne razlike med posameznimi starostnimi skupinami (pri tem moramo upoštevati omejitev, da so posamezni podvzorci majhni, kar predstavlja omejitev v tem delu interpretacije rezultatov analize) pri »varnosti na spletu«, »varnosti gesel« in »samozaščiti«. Najboljše rezultate dosegajo višje starostne skupine, najmanj varna je starostna skupina do 25 let. Za varnost naprave najslabše skrbi starostna skupina 26–35 let, najboljše pa tisti nad 50 let. Višje starostne skupine so manj varne pri uporabi gesel in digitalnih potrdil, medtem ko so mlajše skupine najmanj zavzete pri samozaščiti. Generalno gledano pa se indeks varnosti po posameznih skupinah stopnjuje, kar pomeni, da se z višanjem starosti izboljšuje tudi varno vedenje uporabnikov.

Tabela 8: Vpliv starosti varnost pri uporabi spletnega bančništva

Starost	Varnost naprave (indeks)*	Varnost na spletu (indeks)**	Gesla (indeks)**	Digitalna potrdila (indeks)	Samozaščita (indeks)**	Indeks skupaj (povprečje)**
Do 25 (*N* = 29)	7,31	13,65	12,45	10,21	12,8276	56,4483
26–35 (*N* = 80)	6,75	13,00	13,15	10,26	14,2875	57,4500
36–50 (*N* = 58)	8,27	14,14	14,836	9,69	15,3966	62,3276
nad 50 (*N* = 23)	9,21	15,13	12,83	11,21	14,9565	63,3478
ANOVA (F--statistika/p)	2,612/0,053	2,852/0,039	3,915/0,01	0,565/0,64	3,579/0,015	2,774/0,043

**p-vrednost < 0,1; **p-vrednost < 0,05*

Poleg starostnih skupin smo rezultate po vsebinskih sklopih primerjali tudi med drugimi kategorijami anketirancev. Pri primerjavi med spoloma glede varnosti pri uporabi spletne banke smo z uporabo t-testa ugotovili, da na primer na področju samozaščite moški dosegajo boljše rezultate (t-test = 1,99; Sig. = 0,048). Drugih statistično značilnih razlik nismo potrdili, so se pa kljub temu pokazala določena odstopanja, ki jih je smiselno omeniti. Ugotovili smo na primer, da v povprečju slabše rezultate dosegajo tisti, ki jih je bolj strah (največje razlike je opaziti pri varnosti digitalnih potrdil in samozaščiti). Uporabniki, ki imajo manj informacij o pravilni rabi in nevarnosti, se počutijo bolj ogrožene. Primerjava med statusnimi skupinami je pokazala, da najslabše rezultate dosegajo študenti (mlajša starostna skupina), ki najslabše skrbijo za varnost elektronske naprave. Upokojenci najboljše rezultate dosegajo pri uporabi spleta (najmanj nezaposleni), zaposleni in nezaposleni pa bolj skrbijo za samozaščito (najmanj upokojenci).

5 RAZPRAVA IN ZAKLJUČEK

Čeprav je primarna odgovornost za varnost spletnega bančništva na banki, je za preprečevanje škodnih primerov pomembno predvsem ustrezno vedenje uporabnikov, saj se večina groženj uresniči ravno s pomočjo izkoriščanja človeškega

faktorja. Kot kažejo primeri iz prakse, preslepitev uporabnikov in nizka stopnja samozaščite vplivata na uspešnost prevar, povezanih z zlorabami spletnega bančništva. Največjo težavo z uporabniškega vidika predstavljajo napačne predstave glede ogroženosti ali sposobnosti samozaščite, kar se pri uporabnikih pojavlja primarno zaradi pomanjkljivega znanja ali neozaveščenosti. Poleg slabe informiranosti pa težave ustvarja tudi pomanjkanje občutka odgovornosti za varnost bančnih storitev, ki posledično vodi v manjšo zavzetost oz. motiviranost za samozaščito. V uvodnem poglavju smo predstavili podatke o tveganjih, ki so jim uporabniki spletnega bančništva izpostavljeni pri uporabi te finančne storitve. Čeprav v študiji nismo ugotavljali pogostosti viktimizacije slovenskih uporabnikov spletnega bančništva, podatki kažejo, da je petina anketirancev že bila soočena s prevaro, kljub vsemu pa je stopnja zaznave tveganja med anketiranci nizka. To je lahko povezano s pretirano samozavestjo oziroma pretiranim zaupanjem v lastne sposobnosti ali pa tudi z zaupanjem v banko, ki nudi to storitev. Pomanjkanje zavzetosti uporabnikov in določena tveganja v vedenjskih vzorcih, ki jih izpostavljajo v prispevku povzete vedenjske teorije in modeli, smo ugotovili tudi v empirični raziskavi med uporabniki spletnega bančništva v Sloveniji. Vedenje uporabnikov smo analizirali skozi prizmo priporočil, ki jih dajejo banke svojim strankam, in pri tem ugotovili, da uporabniki osnovne varnostne ukrepe izvajajo le deloma. Ugotovili smo, da 10 % uporabnikov sploh ne skrbi za varnost naprav, ki jih uporabljajo pri spletnem bančništvu, pri slabi četrtini (23,8 %) je ta varnost zelo nizka, zgolj 27,6 % uporabnikov pa uporablja napravo, za katero lahko ocenimo, da je zadovoljivo varna. Uporabniki sicer menijo, da je njihova naprava fizično varna pred neavtorizirano rabo, vendar velika večina ne skrbi za osnovne varnostne ukrepe (npr. uporaba ločenih računov) in ne pozna dodatnih varovalnih mehanizmov, ki jih ponuja banka. Slabih 13 % uporabnikov spletnega bančništva ne poskrbi za varnost spletnega okolja, ki ga uporablja za spletno bančništvo, pri 43,9 % anketirancev je varnost nizka, pri 43,4 % anketirancev pa ustrezno visoka. Anketiranci na primer ne uporabljajo ločenih spletnih brskalnikov, kot je priporočeno, in ne preverjajo veljavnosti digitalnih potrdil, poročajo pa recimo, da so previdni pri ravnanju s tveganimi elektronskimi sporočili. Nekoliko bolj spodbudne rezultate smo ugotovili pri sklopu, ki se je nanašal na varnost in ustreznost gesel, še vedno pa je odstotek tveganja vedenja visok, saj 11 % anketirancev sploh ne poskrbi za varnost ključnih podatkov, dobra četrtina pa to naredi zelo površno oz. slabo. Kot velika težava se je izkazala neustrezna struktura gesel in njihovo menjavanje. Pri četrtem sklopu smo ugotovili, da z digitalnim potrdilom varno ravna samo 15,2 % anketirancev, kar slaba četrtina anketirancev pa se je uvrstila v kategorijo tistih uporabnikov, ki sploh ne poskrbijo za varnost digitalnih potrdil. Ena tretjina uporabnikov se je uvrstila v skupino, za katero je značilno tvegano vedenje, glavno težavo pa predstavlja predvsem neustrezno shranjevanje digitalnih potrdil. Generalno gledano smo najbolj spodbudne rezultate ugotovili pri uporabi varnostnih aplikacij, saj večina anketirancev uporablja ustrezno zaščito pred zlonamernimi programi, veliko je tudi takšnih, ki redno spremljajo varnostna opozorila bank in preverjajo svoje stanje na bančnem računu. Na podlagi opisanih rezultatov ugotavljamo, da je ločevanje naprav, uporabniških računov, spletnih brskalnikov in finančnih/

zasebnih podatkov neustrezno – uporabniki uporabljajo iste naprave/brskalnike/uporabniške račune/podatke v zasebne in finančne namene. S tem pa je tveganje okužbe pred zlonamerno programsko opremo, kljub nekaterim programskim zaščitam, ki jih uporabljajo, bolj verjetno. Uporabniki spletnega bančništva se lahko s škodljivo kodo namreč okužijo že ob preprostem brskanju po spletu, neprevidnem ravnanju z elektronsko pošto, obiskovanju nepreverjenih spletnih strani in nalaganju nepreverjenih vsebin s spleta. To še posebej velja izpostaviti, saj večina uporabnikov spletnega bančništva uporablja za to storitev iste naprave in brskalnike, kot za ostalo poizvedovanje, vključno z dostopi do vsebin za odrasle in zabavnih video vsebin (preko torrent povezav). Če povzamemo, najslabše rezultate uporabniki dosegajo na področju zagotavljanja varnosti naprav in digitalnih potrdil, najboljše pa na področju varne uporabe spleta in pri samozaščiti. Skupni indeks stopnje ozaveščenosti nakazuje, da so uporabniki spletnega bančništva v Sloveniji srednje varni – 58 % anketirancev se je uvrstilo v srednji nivo varnosti (25–75 točk). Analiza razlik med posameznimi skupinami uporabnikov je pokazala, da do največjih odstopanj v varnostnem vedenju prihaja med starostnimi skupinami, pri čemer starejši anketiranci izkazujejo bolj varne vedenjske prakse kot mlajši uporabniki. Med najpomembnejše sklepe raziskave sodi ugotovitev, da uporabniki niso samoiniciativni pri iskanju dodatnih informacij o varnostnih nastavitvah, več kot polovica uporabnikov pa ne uporablja dodatnih varovalnih mehanizmov in jih to tudi ne zanima. Ob upoštevanju teh rezultatov ugotavljamo, da so vzroki za tvegana vedenja anketirancev povezani z njihovim neustreznim odnosom, pomanjkanjem občutka odgovornosti in nezavzetostjo oz. nemotiviranostjo.

Rezultati raziskave nam torej pomagajo razumeti vedenje uporabnikov spletnega bančništva, kar je nujno pri razvoju programov njihovega ozaveščanja s področja varne uporabe te finančne storitve. Model KABP sicer poudarja tako pomen ozaveščenosti kot kompetentnosti uporabnikov spletnega bančništva pri krepitvi varnostno zaželenega vedenja. Glede na opisan model ima največjo vlogo pri spreminjanju vedenja ljudi znanje, k temu pa je treba dodati še odnos, ki ga imajo uporabniki do te storitve (Mcllwraith, 2006). Da posamezniki spremenijo vedenje, je treba najprej doseči, da tveganja ozavestijo – v skladu z opisano teorijo PMT, ki pojasnjuje, kako se ljudje vedemo v primeru zaznave tveganj. Uporaba samovarovalnih ali samozaščitnih ukrepov je po tej teoriji odvisna od osebne percepcije posameznika in ne od njegove dejanske ogroženosti. Za zaščito se bo tako posameznik odločil, kadar bo subjektivno ocenil, da je stopnja ranljivosti, verjetnost nevarnosti in možnost samoučinkovitega zavarovanja velika (Rogers, 1975). Na tej podlagi lahko ob upoštevanju raziskave sklenemo, kaj konkretno bi bilo dobro v programih za krepitev varnostno primernega vedenja pri uporabi spletnega bančništva posebej poudariti. Ti programi bi se tako morali posvečati predvsem krepitvi zavedanja, da je ločevanje naprav, uporabniških računov in spletnih brskalnikov pomemben vidik zagotavljanja varnosti spletnega bančništva, okrepiti bi bilo treba obveščanje uporabnikov o možnih dodatnih varovalnih mehanizmih, s posebnim poudarkom na preverjanju avtentičnosti spletnih povezav in digitalnih potrdil. Za pomanjkljive so se izkazale tudi prakse pri shranjevanju generatorjev gesel in digitalnih potrdil. Kot že omenjeno, je

ključnega pomena, da se izboljša zavzetost uporabnikov in spodbudi njihova samoiniciativnost pri zagotavljanju lastne varnosti. To dokazuje tudi pogosto prepričanje uporabnikov, da je za njihovo varnost v prvi vrsti odgovorna banka (teh je kar 46 %), kar kaže na to, da se jih veliko ne čuti osebno odgovorne za varnost pri uporabi bančnih storitev.

Ob zaključku razprave je treba omeniti, da varnost elektronskega bančništva ni omejena zgolj na spletne storitve, saj je v porastu tudi mobilno bančništvo, ki ustvarja kar nekaj novih in dodatnih dilem, ki izhajajo iz uporabe mobilnih naprav. Zato je v prihodnje treba okrepiti zavedanje o varni uporabi spletnega bančništva tudi na področju mobilnih naprav. Markelj in Bernik (2015) pri raziskovanju ozaveščenosti uporabnikov mobilnih naprav v Sloveniji namreč prihajata do skrb vzbujajočih ugotovitev glede slabega uporabniškega zavedanja in varnostnega ukrepanja. Ugotavljata, da večina uporabnikov ne uporablja (oz. se ne zaveda prednosti) že nameščenih varnostnih mehanizmov, ki jih dobimo ob nakupu mobilne naprave. Ker se pri uporabi spletnega bančništva najbolj tvegano vedejo mladi uporabniki, je tej starostni skupini treba posvetiti še posebno pozornost. Ne glede na to, s kakšno napravo uporabniki dostopajo do bančnega računa preko spleta, je za izboljšanje varnosti treba okrepiti predvsem ukrepe, povezane s krepitvijo odgovornih vedenjskih praks. Ob predpostavki, da banke dobro skrbijo za tehnično varnost tovrstne storitve, se morajo programi ozaveščanj in usposabljanj osredotočiti na kompetence uporabnikov za prepoznavanje groženj na spletu (predvsem phishing sporočil in socialnega inženiringa) ter ustrezno samozaščitno ukrepanje.

UPORABLJENI VIRI

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215.

Board of Governors of the Federal Reserve System. (2013). *Consumers and mobile financial services 2013.* Pridobljeno na https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf

Compeau, D. R. in Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189.

D'Ardenne, J. in Toomse-Smith, M. (2014). Supporting people interested in using online banking research findings. Pridobljeno na http://natcen.ac.uk/media/563041/user-friendly-pathways_supporting-people-research_final--nov2014.pdf

Davinson, N. in Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*, *72*(2), 154–168.

Davis, F. D., Bagozzi, R. P. in Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

European Commission. (2012). *Cyber security report* (Special Eurobarometer 390). Pridobljeno na http://archives.strategie.gouv.fr/cas/system/files/ebs_390_en1.pdf

Financial Fraud Action UK. (2017*). Financial fraud data for 2016 published*. Financial Fraud Action UK. Pridobljeno na https://www.financialfraudaction.org.uk/news/2017/03/30/financial-fraud-data-for-2016-published/

Grosman, G. (12. 3. 2015). Kako so hekerji spremenili spletno bančništvo. *Večer*. Pridobljeno na http://novice.najdi.si/predogled/novica/4ae67dd363151dbeb247c430ae453d6b/Večer/Gospodarstvo/Kako-so-hekerji-spremenili-spletno--bančništvo

Gumucio, S. (2011). *The KAP survey model (knowledge, attitude & practices).* Pridobljeno na https://www.spring-nutrition.org/publications/tool-summaries/kap-survey-model-knowledge-attitudes-and-practices

Jackson Higgins, K. (2014). SpyEye creator got „sloppy," then got nabbed. *DARKReading*. Pridobljeno na https://www.darkreading.com/attacks-breaches/spyeye-creator-got-sloppy-then-got-nabbed/d/d-id/1141236

Jassal, K. R. in Sehgal, R. K. (2013). Online banking security flaws: A study. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(8), 1016-1021 .

Kaspersky Lab. (2015). Carbanak APT – the great bank robbery. Pridobljeno na htt p://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf

Khan, B., Alghathbar, K. S., Nabi, S. I. in Khurram, M. (2011). Effectiveness of information security awareness method based on psychological theories. *African Journal of Business Management*, *26*(5), 10862–10868.

Khan, H. U. (2014). E-banking: Online transactions and security measures. *Research Journal of Applied Sciences, Engineering and Technology*, *7*(19), 4056–4063.

Kreuger, H. A. in Kerney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296.

Lobnikar, B., Prislan, K., Markelj, B. in Banutai, E. (2012). Informacijskovarnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji. *Varstvoslovje*, *14*(3), 345–363.

Markelj, B. in Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*, *20*, 84–89.

Mcllwraith, A. (2006). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness*. Hampshire: Grower.

Mihelič, A. in Vrhovec, S. (2017). Explaining the employment of information security measures by individuals in organizations: The self-protection model. V I. Bernik, B. Markelj in S. Vrhovec (ur.), *Advances in cybersecurity* (str. 23–34). Maribor: University of Maribor Press.

Murdoc, J. (2015). UK online banking users hit with Dyre malware phishing attacks. *V3*. Pridobljeno na https://www.v3.co.uk/v3-uk/news/2416828/uk-online-banking-users-hit-with-dyre-malware-phishing-attacks

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Consumer Psychology*, *91*(1), 93–114.

Rosenstock, I. M. (1974). The health belief model and preventive health behavior. *Health Education Monographs*, *2*(4), 354–386.

SI-CERT. (2016). *Poročilo o omrežni varnosti za leto 2015*. Pridobljeno na https://www.cert.si/letna_porocila/porocilo-o-omrezni-varnosti-za-leto-2015/

Statista. (2018). *Online banking penetration in selected European markets in 2016*. Pridobljeno na https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/

Verizon. (2015). *2015 data breach investigation report*. Pridobljeno na http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

Wash, R. (2010). Folk models of home computer security. V *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*. New York: ACM Press. Pridobljeno na https://cups.cs.cmu.edu/soups/2010/proceedings/a11_Walsh.pdf

O avtorjih:

Dr. Kaja Prislan, docentka za varnostne vede na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: kaja.prislan@fvv.uni-mb.si

Dr. Branko Lobnikar, izredni profesor za varnostne vede na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: branko.lobnikar@fvv.uni-mb.si