VARNOST UPORABNIKOV KIBERNETSKEGA PROSTORA: ANALIZA ZAZNAV MED PREBIVALCI V URBANIH IN RURALNIH OKOLJIH

GORAZD MEŠKO, KAJA PRISLAN IN ROK HACIN
Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija.
E-pošta: gorazd.mesko@fvv.uni-mb.si, kaja.prislan@fvv.uni-mb.si, rok.hacin@fvv.uni-mb.si

Povzetek V prispevku se osredotočamo na primerjavo varnosti uporabnikov kibernetskega prostora v urbanih in ruralnih okoljih. V študiji je sodelovalo 1.158 prebivalcev iz stotih občin po Sloveniji. Ugotovitve so pokazale, da so prebivalci urbanih in ruralnih okolij najpogosteje viktimizirani z naslednjimi kibernetskimi grožnjami: 1) pojavnimi okni, ki so z namenom pridobitve podatkov uporabnikov od njih zahtevali ponoven vpis uporabniškega imena in gesla, 2) elektronskimi sporočili z okuženimi priponkami in 3) lažnim spletnim oglaševanjem. Prebivalci v obeh okoljih so izpostavili tudi, da se počutijo najbolj ranljive pred prejetjem lažnega elektronskega sporočila z okuženo priponko ter da bi jim tovrstna grožnja in izsiljevanje z lastnimi seksualnimi vsebinami povzročili največ škode.

Ključne besede: kibernetske grožnje, viktimizacija, urbano okolje, ruralno okolje, Slovenija.

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/978-961-286-404-0.12
ISBN 978-961-286-404-0

Safety and Security of Cyberspace Users: Analysis of Perceptions among Residents from Urban and Rural Environments

Gorazd Meško, Kaja Prislan & Rok Hacin
University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia.
E-mail: gorazd.mesko@fvv.uni-mb.si, kaja.prislan@fvv.uni-mb.si, rok.hacin@fvv.uni-mb.si

Abstract The paper focuses on the comparison of safety and security of cyberspace users in urban and rural environments. The study involved 1,158 participants from 100 municipalities across Slovenia. Findings showed that residents of urban and rural settings were most frequently victimized with the following threats: 1) pop-up windows that required re-entering of the user name and password to obtain users' data, 2) receiving a fake e-mail with the infected attachment, and 3) fake online advertising. Residents in both environments highlighted that they feel most vulnerable to receiving a fake e-mail with the infected attachment. Moreover, they expose this threat and extortion with their own sexually explicit materials as those that would cause them the most harm.

Keywords: cyberthreats, victimisation, urban environment, rural environment, Slovenia.

https://doi.org/10.18690/978-961-286-404-0.12 DOI
978-961-286-404-0 ISBN
University of Maribor Press

1 Uvod

Kibernetska kriminaliteta sodi med najbolj razširjene oblike kriminalitete (Saunders, 2017), s katero so individualni uporabniki pogosteje viktimizrani kot pa v primeru klasičnih oz. konvencionalnih oblik kriminalitete (United Nations Office on Drugs and Crime, 2013). Raziskave namreč kažejo, da se je večina uporabnikov spleta že soočila s kibernetsko kriminaliteto zaradi vse večje razširjenosti kibernetskih groženj in visoke ranljivosti uporabnikov (Bissell, La Salle in Dal Cin, 2019; Symantec, 2019).

Znanstvenoraziskovalna sfera se z namenom spodbujanja učinkovitejših prevencijskih strategij aktivno ukvarja s proučevanjem različnih vidikov, povezanih z viktimizacijo in samozaščitnim vedenjem uporabnikov v kibernetskem prostoru. Značilnosti okolja, v katerem ljudje bivajo, predstavljajo enega izmed dejavnikov, ki se je v nekaterih tujih študijah izkazal kot povezan z verjetnostjo viktimizacije s kibernetsko kriminaliteto in sposobnostmi uporabnikov (Chang et al., 2016; European Commission, 2020; Ronis in Slaunwhite, 2019). V Sloveniji študije s področja kibernetske kriminalitete tovrstnih vidikov še niso analizirale, kljub temu pa se je že izkazalo, da prihaja do pomembnih razlik v razširjenosti in sami značilnosti kriminalitete v urbanih in ruralnih okoljih (Hacin in Eman, 2019). Skladno s tem se pojavlja vprašanje, kako prebivalci iz različnih okolij bivanja (urbano in ruralno) zaznavajo viktimizacijo v kibernetskem prostoru in kibernetske grožnje, saj je uporaba spleta neodvisna od fizičnih in socialnih značilnosti določenega okolja.

Z namenom analiziranja varnosti uporabnikov kibernetskega prostora v urbanih in ruralnih okoljih v nadaljevanju predstavljamo rezultate nacionalne študije, ki je vključevala analizo: 1) izkušenj uporabnikov z različnimi oblikami kibernetskih groženj, 2) njihovo zaznavo ranljivosti oziroma ogroženosti pri uporabi spleta ter 3) zaznavo nevarnosti groženj. Omenjeni vidiki so bili proučeni tako na vzorcu prebivalcev iz urbanih kakor tudi ruralnih okolij.

2 Nacionalna študija o varnosti uporabnikov kibernetskega prostora

Nacionalna študija o varnosti uporabnikov kibernetskega prostora je potekala v novembru in decembru 2019 na območju stotih občin po vsej Sloveniji. Uporabljen vprašalnik je bil predhodno pilotsko testiran na vzorcu študentov (Meško, Prislan in Hacin, 2019). Anketiranje so izvedli usposobljeni študenti Fakultete za varnostne vede Univerze v Mariboru. Sodelovanje v študiji je bilo prostovoljno in anonimno. Zbrani podatki so bili vneseni v program SPSS, s katerim so bile izvedene statistične analize podatkov.

V reprezentativni vzorec je bilo zajetih 1.158 posameznikov, kar predstavlja 0,05 % slovenskega prebivalstva (Statistični urad Republike Slovenije, 2020). Približno 55 % anketirancev je živelo v urbanih okoljih in več kot polovica vzorca so predstavljale ženske (53 %). Večina anketirancev je bila mlajših od 30 let in je imela dokončano srednjo šolo (42 %). Anketiranci internet največ uporabljajo za naključno in namerno brskanje po spletu.

2.1 Rezultati

Odgovori sodelujočih v anketiranju so predstavljeni v tabelah 1, 2 in 3. V tabeli 1 so predstavljeni rezultati izkušenj anketirancev z viktimizacijo v kibernetskem prostoru. Prebivalci v urbanih in ruralnih okoljih navajajo, da so bili v zadnjih 12 mesecih najpogosteje viktimizirani z naslednjimi kibernetskimi grožnjami: 1) pojavnimi okni, ki so z namenom pridobitve podatkov uporabnikov od njih zahtevali ponoven vpis uporabniškega imena in gesla, 2) elektronskimi sporočili z okuženo priponko in 3) lažnim spletnim oglaševanjem.

V tabeli 2 so predstavljeni rezultati zaznav ogroženosti prebivalcev urbanih in ruralnih okolij v kibernetskem prostoru (verjetnost viktimizacije). Prebivalci v urbanih in ruralnih okoljih se počutijo najbolj ranljive pred naslednjimi kibernetskimi grožnjami: 1) lažnimi elektronskimi sporočili z okuženo priponko, 2) zbiranjem in zlorabo njihovih osebnih podatkov, ki so objavljeni na spletu (npr. socialnih omrežjih), in 3) pojavnimi okni, ki bi z namenom pridobitve podatkov uporabnikov od njih zahtevali ponoven vpis uporabniškega imena in gesla.

V tabeli 3 so predstavljeni rezultati glede zaznave nevarnosti oz. resnosti kibernetskih groženj (možnih posledic viktimizacije). Prebivalci v urbanih in ruralnih okoljih zaznavajo: 1) izsiljevanje z lastnimi seksualnimi vsebinami, 2) elektronska sporočila z okuženo priponko in 3) zbiranje in zlorabo njihovih osebnih podatkov, ki so objavljeni na spletu (npr. socialnih omrežjih) kot najbolj škodljive oblike kibernetskih ogrožanj.

Tabela 1: Viktimizacija v preteklih dvanajstih mesecih

Spremenljivka (V zadnjih 12 mesecih …)	Urbano okolje						Ruralno okolje					
	Da		Ne		Ni odgovora		Da		Ne		Ni odgovora	
	N	%	n	%	n	%	n	%	n	%	n	%
sem bil žrtev spletne prevare pri uporabi kriptovalut.	13	2,0	614	96,7	8	1,3	6	1,1	515	98,7	1	0,2
sem bil žrtev izsiljevanja z lastnimi seksualnimi vsebinami.	17	2,7	617	97,2	1	0,2	3	0,6	518	99,2	1	0,2
sem bil žrtev ljubezenske prevare, kjer je storilec navezal stik z menoj na spletu z namenom pridobitve denarja.	17	2,7	616	97,0	2	0,3	11	2,1	510	97,7	2	0,4
sem bil žrtev spletne prevare pri igranju iger na spletu.	18	2,8	608	95,7	9	1,4	11	2,1	510	97,7	1	0,2
sem bil žrtev spletne prevare, kjer sem po e-pošti posredoval uporabniško ime in geslo lažnemu predstavniku organizacije (phishing).	21	3,3	612	96,4	2	0,3	8	1,5	513	98,3	1	0,2
sem bil žrtev spletne prevare, kjer sem posredoval uporabniško ime in geslo lažni spletni strani (pharming).	21	3,3	611	96,2	3	0,4	9	1,7	512	98,1	1	0,2
sem bil žrtev spletne prevare, ki je od mene zahtevala vnaprejšnje plačilo stroškov (nigerijska prevara).	32	5,0	602	94,8	1	0,2	20	3,8	501	96,0	1	0,2
je nekdo zbiral in zlorabil moje osebne podatke, ki so objavljeni na spletu (npr. socialnih omrežjih).	37	5,8	596	93,9	2	0,3	20	3,8	500	95,8	2	0,4
sem bil žrtev spletne prevare z uporabo lažne aplikacije.	38	6,0	595	93,7	2	0,3	25	4,8	495	94,8	2	0,4
sem bil žrtev prevare pri nakupovanju na spletu.	65	10,2	569	89,6	1	0,2	36	6,9	485	92,9	1	0,2
sem bil žrtev lažnega spletnega oglaševanja.	93	14,6	534	84,1	8	1,3	67	12,8	454	87,0	1	0,2
mi je nekdo posredoval lažno elektronsko sporočilo z okuženo priponko.	164	25,8	469	73,9	2	0,3	110	21,1	411	78,7	1	0,2
sem bil izpostavljen pojavnim oknom, ki so z namenom pridobitve podatkov uporabnikov od mene zahtevali ponoven vpis uporabniškega imena in gesla.	199	31,3	434	68,3	2	0,3	122	23,4	398	76,2	2	0,4

Vir: lastni.

Tabela 2: Zaznava ranljivosti/ogroženosti pred kibernetskimi grožnjami

Spremenljivka (Kako verjetno je, da boste v naslednjih 12 mesecih postali žrtev …)	Urbano okolje				Ruralno okolje			
	M	S.O.	Mediana	Modus	M	S.O.	Mediana	Modus
ljubezenske prevare, kjer bi storilec z vami navezal stik na spletu z namenom pridobitve denarja?	1,24	0,77	1	1	1,21	0,73	1	1
spletne prevare pri uporabi kriptovalut?	1,26	0,81	1	1	1,24	0,77	1	1
izsiljevanja z lastnimi seksualnimi vsebinami?	1,27	0,87	1	1	1,23	0,86	1	1
spletne prevare pri igranju iger na spletu?	1,40	0,99	1	1	1,38	1,01	1	1
spletne prevare, ki bi od vas zahtevala vnaprejšnje plačilo stroškov (nigerijska prevara)?	1,51	1,08	1	1	1,52	1,10	1	1
spletne prevare, kjer bi po e-pošti posredovali uporabniško ime in geslo lažnemu predstavniku organizacije (phishing)?	1,55	1,01	1	1	1,62	1,10	1	1
spletne prevare s sodelovanjem v lažni nagradni igri?	1,58	1,06	1	1	1,74	1,20	1	1
spletne prevare, kjer bi posredovali uporabniško ime in geslo lažni spletni strani (pharming)?	1,59	1,01	1	1	1,59	1,09	1	1
spletne prevare z uporabo lažne aplikacije?	1,70	1,01	1	1	1,78	1,06	1	1
lažnega spletnega oglaševanja?	1,89	1,29	1	1	1,96	1,37	1	1
spletne prevare pri nakupovanju na spletu?	2,08	1,29	2	1	2,04	1,37	2	1
pojavnih oken, ki z namenom pridobitve podatkov uporabnikov zahtevajo ponoven vpis uporabniškega imena in gesla?	2,11	1,31	2	1	2,17	1,40	2	1
če bi nekdo zbiral in zlorabil vaše osebne podatke, ki so objavljeni na spletu (npr. socialnih omrežjih)?	2,15	1,29	2	1	2,05	1,27	2	1
če bi vam nekdo posredoval lažno elektronsko sporočilo z okuženo priponko?	2,30	1,37	2	1	2,29	1,44	2	1

Lestvica: od 1 – To se zagotovo ne bo zgodilo do 7 – To se bo zagotovo zgodilo.
Vir: lastni.

Tabela 3: Zaznava nevarnosti/resnosti kibernetskih groženj

Spremenljivka (Kako velike posledice bi za vas nastale, če bi postali žrtev ...)	Urbano okolje				Ruralno okolje			
	M	S.O.	Mediana	Modus	M	S.O.	Mediana	Modus
spletne prevare pri igranju iger na spletu?	2,32	1,69	2	1	2,58	1,96	2	1
spletne prevare s sodelovanjem v lažni nagradni igri?	2,61	1,77	2	1	2,74	1,86	2	1
lažnega spletnega oglaševanja?	2,63	1,68	2	1	2,75	1,86	2	1
spletne prevare pri uporabi kriptovalut?	2,67	1,97	2	1	2,73	2,13	2	1
spletne prevare z uporabo lažne aplikacije?	2,97	1,82	3	1	3,04	1,89	3	1
ljubezenske prevare, kjer bi storilec z vami navezal stik na spletu z namenom pridobitve denarja?	3,01	2,19	2	1	3,21	2,34	2	1
spletne prevare, kjer bi posredovali uporabniško ime in geslo lažni spletni strani (pharming)?	3,15	1,97	3	1	3,29	2,08	3	1
pojavnih oken, ki z namenom pridobitve podatkov uporabnikov zahtevajo ponoven vpis uporabniškega imena in gesla?	3,30	1,88	3	2	3,21	1,92	3	1
spletne prevare, kjer bi po e-pošti posredovali uporabniško ime in geslo lažnemu predstavniku organizacije (phishing)?	3,30	2,03	3	1	3,50	2,16	3	1
spletne prevare, ki bi od vas zahtevala vnaprejšnje plačilo stroškov (nigerijska prevara)?	3,39	2,15	3	1	3,49	2,29	3	1
spletne prevare pri nakupovanju na spletu?	3,56	1,89	3	4	3,54	2,05	3	1
če bi nekdo zbiral in zlorabil vaše osebne podatke, ki so objavljeni na spletu (npr. socialnih omrežjih)?	3,59	1,96	3	3	3,59	2,00	3	2
če bi vam nekdo posredoval lažno elektronsko sporočilo z okuženo priponko?	3,68	2,00	3	3	3,72	2,10	3	1
izsiljevanja z lastnimi seksualnimi vsebinami?	3,70	2,47	3	1	3,74	2,62	3	1

Lestvica: od 1 – Sploh ne bi bilo posledic do 7 – Velike posledice.
Vir: lastni.

3 Zaključek

Rezultati raziskave so pokazali, da imajo prebivalci v ruralnih in urbanih okoljih različne izkušnje z viktimizacijo v kibernetskem prostoru, kar lahko pripišemo raznolikosti kibernetskih groženj. Ugotavljamo namreč, da se zaznana stopnja viktimizacije anketirancev okvirno giba med 1 in 31 %, pri čemer so bolj pogoste izkušnje s prevarami, povezanimi s pridobivanjem podatkov, vezanih na spletne račune, in razširjanjem zlonamerne programske opreme. S tega vidika se tveganja pojavljajo predvsem pri uporabi elektronske pošte in obiskovanju nepreverjenih spletnih strani, kjer lahko neprevidna komunikacija, odzivanje na spletna oglaševanja ali nepremišljeno izvajanje spletnih nakupov vodijo v zlorabe podatkov in finančnih virov. Med najmanj pogosto zaznane vrste kibernetskih groženj pa sodijo tiste, ki so povezane z redkejšimi spletnimi navadami (uporaba kriptovalut, deljenje eksplicitnih fotografij, igranje iger na spletu). Grožnje, s katerimi so bili uporabniki najpogosteje viktimizirani, prav tako zaznavajo kot bolj verjetne v prihodnosti, kar kaže na povezovanje med preteklimi izkušnjami in zaznavo ranljivosti. Ne glede na to pa med najnevarnejše kibernetske grožnje umeščajo tiste grožnje, ki sicer nujno ne sodijo med pogosto zaznane, vendar jim lahko povzročijo hujše finančne posledice ali pa resneje ogrozijo njihov ugled (izsiljevanja z eksplicitnimi vsebinami, okužbe z zlonamerno programsko opremo, zloraba osebnih podatkov, objavljenih na socialnih omrežjih). Primerjava rezultatov po omenjenih sklopih med vzorcema anketirancev (iz ruralnega in urbanega okolja) kaže na podobne zaznave, tako z vidika pretekle viktimizacije kot ranljivosti in resnosti kibernetskih groženj, kar predstavlja indic, da med skupinama ne obstajajo večje razlike. Kljub temu pa obstaja možnost, da okolje bivanja vpliva na druge okoliščine, povezane z viktimizacijo (kot so spletne navade, ozaveščenost, kompetence), kar bi veljalo podrobneje raziskati v prihodnjih raziskavah.

Na podlagi rezultatov tako ugotavljamo, da je stopnja viktimizacije z različnimi oblikami kibernetskih groženj relativno nizka, vendar raznolika, prav tako pa uporabniki ne zaznavajo visoke ranljivosti v kibernetskem prostoru, proučevanim grožnjam pa tudi ne pripisujejo resne nevarnosti. Tovrstne ugotovitve lahko nakazujejo na neobčutljivost uporabnikov na tveganja, povezana z uporabo kibernetskega prostora. Spodbudno pa je, da se zaznave v določeni meri razlikujejo glede na vrsto kibernetskih groženj, kar nakazuje na to, da se uporabniki zavedajo raznolikosti tveganj. Ob upoštevanju, da sodi kibernetska kriminaliteta med

najpomembnejše sodobne varnostne izzive in da ogroža slehernega uporabnika, bi bilo treba v prihodnje več pozornosti nameniti tudi razumevanju zaznave tovrstne problematike med uporabniki. Proučiti bi bilo treba tudi, kakšne so dejanske sposobnosti zaznavanja kibernetskih groženj in v kolikšni meri prihaja do razlik v dejanski in zaznani viktimizaciji. Obenem pa bi bilo treba na podlagi ugotovljenih sposobnostih in vedenjskih navad pri uporabi spleta ugotoviti tudi dejansko ogroženost uporabnikov ter nato stremeti k razvoju učinkovitejših, uporabnikovim okoliščinam, prilagojenih programov ozaveščanja. Pomembno vlogo pri oblikovanju splošni javnosti namenjenih priporočil in smernic varne uporabe kibernetskega prostora že imajo najrazličnejše za področje specializirane organizacije (npr. SI-CERT, Spletno oko, Varni na internetu), ki jih je treba javnosti še bolj približati.

Opombe

Pričujoče delo je nastalo v okviru temeljnega raziskovalnega projekta *Varnost uporabnikov kibernetskega prostora – kriminološke, viktimološke in preventivne perspektive* (J5-9345, 2018–2020), ki ga financira Javna agencija za raziskovalno dejavnost Republike Slovenije (ARRS). Projekt izvaja Fakulteta za varnostne vede Univerze v Mariboru, Slovenija.

Literatura

Bissell, K., LaSalle, R. in Dal Cin, P. (2019). *The cost of cybercrime: Ninth annual cost of cybercrime study. Unlocking the value of improved cybersecurity protection.* Pridobljeno na https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Chang, F. C., Miao, N. F., Chiu, C. H., Chen, P. H., Lee, C. M., Chiang, J. T. et al. (2016). Urban–rural differences in parental Internet mediation and adolescents' Internet risks in Taiwan. *Health, Risk and Society, 18*(3–4), 188–204. doi:0.1080/13698575.2016.1190002

European Commission. (2020). *Special Eurobarometer 499: Europeans' attitudes towards cyber security.* Pridobljeno na https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

Meško, G., Prislan, K. in Hacin, R. (2019). Varnost uporabnikov kibernetskega prostora. V G. Meško, R. Hacin in K. Eman (ur.), *5. Nacionalna konferenca o varnosti v lokalnih skupnostih: Uvod v razpravo o varnosti v urbanih in ruralnih okoljih: Konferenčni zbornik* (str. 121–128). Maribor: Univerza v Mariboru, Univerzitetna založba.

Ronis, S. in Slaunwhite, A. (2019). Gender and geographic predictors of cyberbullying victimisation, perpetration, and coping modalities among youth. *Canadian Journal of School Psychology, 34*(1), 3–21. doi:10.1177/0829573517734029

Saunders, J. (2016). Tackling cybercrime – The UK response. *Journal of Cyber Policy, 2*(1), 4–15.

Statistični urad Republike Slovenije (SURS). (2020). *Prebivalstvo po starosti in spolu, občine, Slovenija, polletno.* Pridobljeno na https://pxweb.stat.si/SiStatDb/pxweb/sl/10_Dem_soc/10_Dem_soc__05_prebivalstvo__10_stevilo_preb__20_05C40_prebivalstvo_obcine/05C4002S.px/

Symantec. (2019). *Internet security threat report.* Pridobljeno na https://www.symantec.com/security-center/threat-report

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. Pridobljeno na http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf