*VARSTVOSLOVJE,*
*let. 16*
*št. 1*
*str. 5–15*

# Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo

**Igor Bernik, Blaž Markelj**

**Namen prispevka:**

Uporabniki različnih demografskih skupin vsakodnevno uporabljajo mobilne naprave v osebne in poslovne namene. Pri uporabi mobilnih naprav s pomočjo nameščene programske opreme in pri dostopanju do omrežij zanemarjajo varovanje informacij in večinoma ne delujejo v skladu s principi informacijske varnosti. Ob nevestni rabi mobilnih naprav je tveganje veliko. Ker so študenti velika skupina uporabnikov mobilnih naprav, ki vstopa v poslovni svet, smo izvedli raziskavo, kako le-ti uporabljajo mobilne naprave, koliko poznajo grožnje in uporabo možnih varnostnih zaščit. S tem znanjem organizacije lahko pripravimo na trenutne in prihajajoče informacijskovarnostne izzive.

**Metode:**

Predstavljene ugotovitve temeljijo na deskriptivnih dognanjih, izhajajočih iz pregleda virov in izvedene raziskave med študentsko populacijo ter analizirane s pomočjo statističnih metod.

**Ugotovitve:**

Študenti slabo poznajo načela varne uporabe mobilnih naprav, programske opreme zanje ter groženj in varnostnih rešitev. Glavne ugotovitve raziskave, izvedene 2012, pokažejo nizko stopnjo zavedanja in poznavanja groženj, ki pretijo uporabnikom mobilnih naprav ter nizko stopnjo uporabe varnostnih rešitev. Mobilne naprave postajajo mesto, kjer se shranjujejo in obdelujejo osebni in poslovni podatki. Pri mobilnih napravah je meja med osebnimi in poslovnimi podatki popolnoma izginila. Zato je pri uporabi mobilnih naprav priporočljivo spoštovati informacijskovarnostna priporočila in s tem zagotoviti ustrezno zaščito podatkov, do katerih imamo dostop.

**Omejitve/uporabnost raziskave:**

Znanstvene objave na temo, ki jo obravnavamo v prispevku, so redke. Navedb primerov širših razsežnosti zlorab iz prakse, preiskovanja kriminalitete in dejanskih sodnih obravnav pa je malo.

**Praktična uporabnost:**

Skozi izsledke ugotavljamo načine uporabe mobilne naprave, zavedanje groženj in uporabo varnostnih rešitev.

**Izvirnost/pomembnost prispevka:**

Menimo, da je delo na področju uporabe mobilnih naprav originalno in na izviren način obravnava predstavljeno problematiko.

**UDK: 004.056:621.395.721.5**

**Ključne besede:** mobilne naprave, grožnje, varnost, študenti

**Ensuring the Security of Information by Understanding User Behaviour on a Mobile Device**

**Purpose:**

Mobile devices are used every day by users from various demographic groups, both for personal and business purposes. Users neglect information security and generally do not operate according to the principles of information security while using the mobile devices by using the installed software and accessing networks. When using the mobile devices in unconscious manner the risk is high. Since the students are a very large group of users of mobile devices, we conducted a survey among them on how they use their mobile devices, and how much do they know of the threats and the use of possible security features.

**Design/Methods/Approach:**

The presented results are based on descriptive findings resulting from the review of resources and on the research conducted among the student population and subsequently analysed by statistical methods.

**Findings:**

Students have poor knowledge of the safe use of mobile devices, the software for them, threats and security solutions. The main findings of the survey, conducted in 2012, show low level of awareness and knowledge of threats to mobile security of smart phones and low level of utilization of security solutions. Mobile devices are becoming a place to store and process personal and business data. In the case of mobile devices the boundary between personal and business data is disappearing completely. Therefore, when using mobile devices it is advisable to observe safety information and recommendations in order to ensure adequate protection of the data to which we have access.

**Research Limitations/Implications:**

Scientific publications on the topic under discussion in this paper are rare. Allegations of abuse cases from practice, investigation of crime and the actual court case law is limited.

**Practical Implications:**

Through the results of the descriptive analysis and done research ways to use mobile devices are found, as well as the awareness of the threat and use of security solutions.

**Originality/Value:**

There is no access to comparative research, so the work on the use of mobile devices is original, since it addresses the issue presented in an original way.

**UDC: 004.056:621.395.721.5**

**Keywords:** mobile device, threats, security, students

# 1 UVOD

Zaradi naprednih razvitih mobilnih omrežij in mobilnih naprav[1] je možen stalen dostop do informacij v informacijskih sistemih, ki so potrebne za posamezne odločitve. Mobilne naprave s pomočjo mobilnih omrežij in različne programske opreme posameznemu uporabniku omogočajo nepozabno uporabniško izkušnjo (Greene, Tamborello in Micheals, 2013). Te niso priljubljene zgolj pri osebah, ki se gibljejo v poslovnem svetu, temveč celotni populaciji. Tako kot v realnem svetu, je za vzdrževanje stikov treba komunicirati; komuniciranje pa poteka prek družabnih portalov, tudi s pomočjo mobilnih naprav. Orodja, ki so namenjena dodatni zaščiti, pa so za uporabnike trenutno bolj ovira kot korist. Za mobilni dostop do kibernetskega prostora uporabljamo različne mobilne naprave, med katerimi so v zadnjem obdobju najbolj priljubljeni pametni telefoni. Po raziskavah podjetja International Data Corporation (2011) se v svetovnem merilu prodaja pametnih mobilnih telefonov povečuje za 55 % na leto. Raziskava, ki jo je leta 2011 objavila organizacija Ponemon Institute (2011) in je bila izvedena z namenom ugotoviti, kako dobro se uporabniki (državljani ZDA) zavedajo vprašanj varnosti in zasebnosti pri rabi pametnih telefonov, prikazuje, da uporabniki v večji meri (poleg telefoniranja) uporabljajo pametne telefone za prenose podatkov s spleta. Zanimivo je ekvivalentno število namena uporabe, največ izpraševancev ima pametne telefone tako za osebno kot poslovno rabo. Med mladimi pa je posebej zaželena neprestana povezanost s spletom in s tem omogočena dostopnost prenosa sporočil ali možnost uporabe številnih naprednih storitev družabnih omrežij (Facebook, Google Chat, Twiter idr.). Ker bodo le-ti v naslednjih letih aktivno vstopili v poslovna okolja in vanje prenašali svoje navade, menimo, da je za pripravo ustreznih strategij zagotavljanja t. i. mobilne varnosti v poslovnem okolju študentska populacija ustrezna testna skupina.

Programska oprema za mobilne naprave se prav tako razvija izredno hitro, predvsem z namenom privabiti uporabnike in povečati prodajo. Mladi prepogosto pozabljajo na pasti, ki jim pretijo, ko uporabljajo mobilne naprave, in tudi na potrebo po dodatni zaščiti, da bi se izognili pastem kibernetskega prostora. Tako je Ponemon Institute (2012) decembra 2012 objavil rezultate raziskave ugotavljanja tveganj v organizacijah, tako pri napravah kot informacijski infrastrukturi, ki jih uporabljajo končni uporabniki. Kot največje tveganje za varnost informacijske tehnologije in sistemov v organizacij je 70 % izpraševancev izbralo mobilne naprave. V rezultatih so primerjave za leto 2010, ko jih je tako odgovorilo le 9 %, za leto 2011 pa 48 %. Na drugem mestu v raziskavi iz leta 2012 (67 %) so mobilne aplikacije neznanega izvora, kar nakazuje na kontinuirano rast števila tistih, za katere mobilne naprave niso zgolj uporabno sredstvo, ampak tudi grožnja (varnostno tveganje) za informacijsko tehnologijo in sisteme organizacije.

1 *Med mobilne naprave uvrščamo predvsem naprave, ki imajo prilagojene operacijske sisteme, kot so iOS, Android, BlackBerry OS ali Windows mobile, in so prenosljive (mobilni telefoni, tablični računalniki itd.). V to kategorijo se lahko uvrsti vse naprave, ki se lahko prenašajo in pri katerih je dostop do interneta mogoč brez fizične povezave (tudi prenosniki, prenosne igralne konzole, industrijski čitalci itd.), medtem ko v skupino mobilnih telefonov spadajo tako mobilni telefoni, ki so namenjeni zgolj klicanju in pisanju kratkih sporočil, kot tudi pametni mobilni telefoni, ki predstavljajo sodobno komunikacijsko napravo, saj poleg klicanja prek mobilnih omrežij omogočajo še kopico dodatnih funkcij, ki so podobne funkcijam osebnega računalnika.*

Mobilna naprava je lahko tudi tarča programske opreme, ki se nenadzorovano namesti v napravo, kot je npr. škodljiva programska oprema in druge grožnje (*spyware*, *botnets*, *bluetooth connection* in okužbe v socialnih omrežjih (Leavitt, 2011)). Rezultati raziskave podjetja Lookout (2011) kažejo, da je bilo v drugi polovici leta 2011 povečano število groženj, temelječih na aplikacijah programa *malware*, predvsem v primerjavi s programi *spyware*; za 14 %. Poročilo Juniper Networks (2011) navaja, da se je od poletja 2010 za 400 % povečalo število mobilnih naprav, ki delujejo na platformi Android in so se okužile s škodljivo programsko opremo. V poročilu zasledimo tudi, da ima 85 % uporabnikov na svojem mobilnem telefonu neuporabno zaščito, saj si (nekateri) proizvajalci programske opreme za mobilne naprave dovolijo vgraditi »zadnja vrata« in potem brez vednosti uporabnika upravljajo nastavitve programske opreme na mobilni napravi ali pa le-ta samodejno pošilja podatke o tem, kje naprava je (npr. GPS lokacija). Tudi v poročilu Juniper Networks (2013) iz leta 2013 je navedeno veliko povečanje groženj mobilnim napravam. Poročilo je sestavljeno na podlagi enoletnega kontinuiranega spremljanja razvoja in pojavljanja groženj mobilnim napravam. Tako se je količina škodljive programske opreme od marca 2012 pa do marca 2013 povečala za 614 %.

Nepoznavanje delovanja programske opreme in zmožnosti, ki jih omogoča programska oprema mobilne naprave, povzroči, da postanemo potencialna tarča kibernetske kriminalitete. Zavedanje groženj in posledic, ki pretijo uporabnikom mobilnih naprav, je pomembno tudi zaradi zavedanja potrebe po zagotavljanju zadostne kibernetske zaščite. Nekatere zaščite bi dandanes morale biti uporabnikom samoumevne (npr. koda PIN za kartico SIM, zaklepanje povezave *Bluetooth* in zaklepanje mobilnih naprav), pa niso.

Med študenti slovenskih fakultet smo izvedli raziskavo z naslovom »Zavedanje groženj mobilnim napravam«. Namen raziskave je ugotoviti, v kolikšni meri se mladi zavedajo nevarnosti/groženj, ki jim pretijo, in kakšne varnostne rešitve uporabljajo. Cilji raziskave so bili pridobiti podatke o namenu, načinu in vrsti uporabe mobilnih naprav ter posledično o njihovem poznavanju načina rabe, groženj in zaščiti. S stališča poznavanja groženj in varnega upravljanja z mobilnimi napravami sklepamo tudi na uporabnikovo dovzetnost in poznavanje kibernetske kriminalitete.

## 2 METODA

Raziskava je bila izvedena s pomočjo spletnega vprašalnika, ki je bil objavljen na portalu »1ka« (www.1ka.si). Vprašalnik je bil aktiven 21 dni leta 2012. Študenti so bili o raziskavi/vprašalniku informirani prek elektorske pošte, Facebook profilov in osebno. Vprašalnik je sestavljen tako, da je mogoče ugotoviti, kako in s kakšnim namenom se uporabljajo mobilne naprave in katere vrste mobilnih naprav ter programskih rešitev se uporabljajo. V vprašalniku so vprašanja postavljena tako, da iz rezultatov dobimo vpogled v poznavanje in uporabo varnostnih rešitev ter poznavanje in zavedanje groženj, ki pretijo ob uporabi mobilnih naprav. Analiza podatkov je bila narejena s programskim orodjem SPSS. Obravnavali smo 281 izpolnjenih vprašalnikov.

Med izpraševanci je bilo največ starih od 21 do 25 let, sledi starostna skupina študentov do 20 let, 61,5 % žensk in 63,2 % takih, ki imajo zaključeno srednješolsko izobrazbo, 36,8 % je podiplomskih študentov.

Ugotavljali smo poznavanje načinov rabe mobilnih naprav. Ker pa način rabe izhaja tudi iz vrste naprave, smo ugotavljali, katere vrste mobilnih naprav uporabljajo izpraševanci. Tabela 1 prikazuje uporabo različnih tipov mobilnih naprav.

**Tabela 1: Tip uporabljanih mobilnih naprav**

| **Vzorec**, $n = 282$ | ***n*** | **%** |
|---|---|---|
| Klasični mobilni telefon in prenosni računalnik | 79 | 28,01 |
| Pametni telefon | 76 | 26,95 |
| Pametni telefon in prenosni računalnik | 56 | 19,86 |
| Klasični mobilni telefon | 48 | 17,02 |
| Klasični mobilni telefon, tablični računalnik in prenosni računalnik | 9 | 3,19 |
| Pametni telefon, tablični računalnik in prenosni računalnik | 7 | 2,48 |
| Klasični mobilni telefon in pametni telefon | 4 | 1,42 |
| Klasični mobilni telefon, pametni telefon, tablični računalnik in prenosni računalnik | 1 | 0,35 |
| Pametni telefon in tablični računalnik | 1 | 0,35 |
| Tablični računalnik | 1 | 0,35 |

Iz tabele 1 je razvidno, da je največji odstotek tistih, ki istočasno uporabljajo klasični mobilni telefon (te danes v veliki meri tudi omogočajo povezavo v splet) ter prenosni računalnik; skoraj 27 % pa je takih, ki že uporabljajo pametni telefon. S skoraj 20 % pa jim sledijo izpraševanci, ki uporabljajo tako pametni telefon kot prenosni računalnik.

Tabela 2 prikazuje namen uporabe mobilne naprave. Več kot polovica (58,3 %) uporablja mobilne naprave v zasebne namene, medtem ko je četrtina takih, ki sočasno uporabljajo mobilne naprave v zasebne in službene namene.

**Tabela 2: Namen uporabe mobilne naprave**

| **Vzorec**, $n = 216$ | ***n*** | **%** |
|---|---|---|
| Samo za zasebne potrebe | 126 | 58,3 |
| Za zasebne in tudi službene potrebe | 56 | 25,9 |
| Za zasebne in službene potrebe | 31 | 14,4 |
| Za službene in delno tudi zasebne potrebe | 1 | 0,5 |
| Samo za službene potrebe | 2 | 0,9 |

Glede na populacijsko strukturo izpraševancev (študenti) so bili takšni podatki pričakovani. Zaskrbljujoče pa je dejstvo, da je dokaj visok odstotek tistih, ki uporabljajo mobilne naprave za zasebne in službene potrebe, še posebno, če je to ista mobilna naprava. Problem nastane, ko kombiniramo med zasebnim in službenim (predvsem dostop do podatkov) ter s tem ne usklajujemo potrebe po

zagotavljanju zadostne kibernetske varnosti. Podoben primer najdemo tudi v raziskavi organizacije Ponemon Institute (2011), kjer je rezultat kombinacije osebne in poslovne rabe ravno tako velik (40 %). Iz obeh raziskav lahko trdimo, da je in bo (s prihodom novejših in naprednejših mobilnih naprav) težko postaviti ločnico med zasebno in profesionalno uporabo mobilnih naprav.

## 2.1 Ugotavljanje ogroženosti uporabnikov

Za zavedanje potreb po zagotavljanju zadostne stopnje informacijske varnosti pri uporabi mobilnih naprav je smiselno poznati grožnje. Tabela 3 tako prikazuje grožnje, ki jih izpraševanci poznajo.

**Tabela 3: Poznavanje groženj**

| | DA | | NE | |
|---|---|---|---|---|
| | ***n*** | **%** | ***n*** | **%** |
| Kraja naprave (*n* = 246) | 220 | 89,4 | 26 | 10,6 |
| Okužba z malwareom (*n* = 236) | 79 | 33,5 | 157 | 66,5 |
| Okužba s spywareom (*n* = 239) | 107 | 44,8 | 132 | 55,2 |
| Okužba preko aplikacije (*n* = 243) | 157 | 64,6 | 85 | 35 |
| Phishing (*n* = 235) | 68 | 28,9 | 167 | 71,1 |
| Okužba z rootkitom (*n* = 229) | 32 | 14 | 197 | 86 |
| Drive By Downloads (avtomatični prenos aplikacije ob odprtju brskalnika) (*n* = 233) | 103 | 44,2 | 130 | 55,8 |
| Odtujitev podatkov (*n* = 234) | 152 | 65 | 82 | 35 |
| Okužba brskalnika, ki ob obisku določene spletne strani avtomatsko naloži malware in posledično aktivira reklamne vsebine in s tem onesposobi napravo. (*n* = 238) | 117 | 49,2 | 121 | 50,8 |
| Prestrezanje komunikacije (tudi prenosa podatkov) (*n* = 237) | 137 | 57,8 | 100 | 42,2 |
| Vdori prek Bluetootha (*n* = 238) | 186 | 78,2 | 52 | 21,8 |
| Virusi (*n* = 242) | 201 | 83,1 | 41 | 16,9 |
| Plačilne prevare (*n* = 239) | 167 | 69,9 | 72 | 30,1 |
| Avtomatsko oddajanje podatkov (*n* = 237) | 132 | 55,7 | 105 | 44,3 |
| Sledenje (*n* = 242) | 189 | 78,1 | 53 | 21,9 |

Poznavanje in zavedanje posameznih groženj, ki pretijo uporabnikom pametnih mobilnih telefonov, je bistvenega pomena tudi s stališča informacijske varnosti. Ni presenetljivo, da je kraja med vsemi naštetimi na prvem mestu s skoraj 90 %. Vsekakor pa je presenetljivo dejstvo, da so grožnje, kot npr. *malware* in *spyware* ter okužbe z *rootkitom*, slabo poznane. Predvsem glede na dejstvo, da raziskave, kot so npr. Lookut (2011), Juniper Networks (2011) in McAfee (2013), v svojih poročilih opozarjajo na strmo povečanje okužb z omenjenimi grožnjami.

Zaradi zavarovanja pametnega mobilnega telefona pred raznovrstnimi grožnjami moramo poznati (vsaj) osnovne varnostne ukrepe (tabela 4). Izpraševanci odgovarjajo, da najpogosteje uporabljajo kodo PIN za kartico SIM, kar je tudi pričakovano. Tako varnostno rešitev vgradi v kartico SIM že tisti, pri katerem zakupite uporabo mobilne telefonije.

**Tabela 4: Uporaba varnostnih rešitev**

| | Uporabljam | | Poznam, vendar ne uporabljam | | Ne poznam | |
|---|---|---|---|---|---|---|
| | *n* | % | *n* | % | *n* | % |
| PIN za SIM kartico (*n* = 212) | 190 | 89,6 | 21 | 9,9 | 1 | 0,5 |
| PIN za dostop do aplikacij na pametnem telefonu (*n* = 206) | 44 | 21,4 | 117 | 56,8 | 45 | 21,8 |
| Enkripcija podatkov (*n* = 206) | 12 | 5,8 | 112 | 54,4 | 82 | 39,8 |
| Avtentikacija ob uporabi določenih funkcij (*n* = 208) | 27 | 13 | 90 | 43,3 | 91 | 43,8 |
| Oddaljeno brisanje vsebin (*n* = 206) | 14 | 6,8 | 84 | 40,8 | 108 | 52,4 |
| Antivirusna zaščita (*n* = 207) | 61 | 29,5 | 102 | 49,3 | 44 | 21,3 |
| VPN povezava (*n* = 206) | 14 | 6,8 | 84 | 40,8 | 108 | 52,4 |
| Arhiviranje vsebin pametnega telefona (*n* = 205) | 40 | 19,5 | 91 | 44,4 | 74 | 36,1 |
| Centralni nadzor pametnega telefona (določanje politike uporabe) (*n* = 205) | 13 | 6,3 | 83 | 40,5 | 109 | 53,2 |
| Omogočeno sledenje pametnega telefona v primeru kraje (*n* = 207) | 42 | 20,3 | 104 | 50,2 | 61 | 29,5 |
| Izobraževanje (*n* = 204) | 53 | 26 | 84 | 41,2 | 67 | 32,8 |

Skrbi dejstvo, da veliko izprašanih pozna možnost uporabe kode PIN za dostop do posameznih aplikacij na pametnem telefonu, vendar je ne uporablja (56,8 %). Pametni mobilni telefoni to omogočajo že v osnovi, uporabiti je potrebno le ustrezne nastavitve. Varnostno rešitev oddaljenega brisanja vsebine mobilnega pametnega telefona lahko uporabimo v primeru izgube ali kraje mobilnega pametnega telefona, vendar pozna to možnost samo 40 % izprašanih (a je niso oziroma je ne nameravajo uporabiti), 52 % izprašanih pa te varnostne rešitve sploh ne pozna. Naštete možnosti zavarovanja mobilne naprave bi uporabniki lahko pridobili z ustreznim izobraževanjem, ki je lahko splošno, za vse modele zavarovanja mobilnih naprav, ali specifično, usmerjeno v posamezne modele in določene programske rešitve. Glede na rezultate, več kot 42 % izpraševancev izobraževanje, kot varnostno možnost, pozna, vendar je ne uporablja; skoraj 39 % pa te rešitve ne pozna.

Ocenjevanje verjetnosti uporabe različnih načinov prenosa podatkov na pametnem mobilnem telefonu smo razdelili v tri skupine oz. faktorje. V te skupine smo umestili spremenljivke (uporaba načinov prenosa podatkov na pametnem

mobilnem telefonu), ki so jih ocenjevali na Likertovi lestvici od 1 do 5 (1 = Nikoli, 5 = Vedno). Izvedena faktorska analiza (tabela 5) z metodo glavnih komponent razvrsti spremenljivke v tri faktorje (pri pravokotni rotaciji Varimax z normalizacijo Kaiser). Prvi faktor smo poimenovali »Nezavarovana omrežja«. V okviru tega faktorja obstaja največja verjetnost uporabe brezplačnih nezavarovanih javnih omrežij, sledi uporaba domačega z geslom nezavarovanega omrežja in nato drugi načini prenosa podatkov. V okviru drugega faktorja, ki smo ga poimenovali »Zavarovana omrežja«, smo iskali pogostost uporabe zavarovanih omrežij pri prenosu podatkov. V sklopu tega faktorja najbolj pogosto uporabljajo domače brezžično omrežje, ki je varovano z geslom, sledi službeno zavarovano omrežje. Tretji faktor smo poimenovali »Internetni ponudniki«. V okviru tega faktorja je najbolj pogosta uporaba Internetnih modulov (ponudnikov) za prenos podatkov, sledi *Blutetooth* povezava.

**Tabela 5: Faktorska analiza pogostosti uporabe različnih načinov prenosa podatkov**

*Faktorska analiza Prenos podatkov*

| | | | | | |
|---|---|---|---|---|---|
| Cronbachov koeficient alfa: 0,655<br>Kaiser-Meyer-Olkinova mera ustreznosti vzorčenja: 0,680 | | | | | |
| **F1: Nezavarovana omrežja** | | | | | |
| Cronbachov koeficient alfa: 0,617 | | | | | |
| Odstotek pojasnjene variance: 26,9 % | **F1** | F2 | F3 | Aritm. sr. | St. odkl. |
| Povprečna vrednost: 1,93; standardni odklon: 0,912 | 0,825 | | | 1,71 | 1,198 |
| Drugo | 0,718 | | | 1,65 | 1,016 |
| Brezplačna javna brezžična omrežja, ki niso varovana z geslom (brezplačne javno dostopne točke) | 0,579 | | | 2,30 | 1,263 |
| **F2: Zavarovana omrežja** | | | | | |
| Cronbachov koeficient alfa: 0,568<br>Odstotek pojasnjene variance: 22,9 %<br>Povprečna vrednost: 2,64; standardni odklon: 1,309 | | | | | |
| | F1 | **F2** | F3 | Aritm. sr. | St. odkl. |
| Službeno brezžično omrežje, ki je varovano z geslom | | 0,828 | | 2,00 | 1,456 |
| Domače brezžično omrežje, ki je varovano z geslom | | 0,820 | | 3,26 | 1,636 |
| **F3: Internetni ponudniki** | | | | | |
| Cronbachov koeficient alfa: 0,348 | | | | | |
| Odstotek pojasnjene variance: 18,6 % | | | | | |
| Povprečna vrednost: 2,94; standardni odklon: 1,095 | | | | | |
| | F1 | F2 | **F3** | Aritm. sr. | St. odkl. |
| Modul ponudnika interneta (Mobitel, Simobil, Tuš idr.) | | | 0,860 | 2,97 | 1,566 |
| Bluetooth povezava | | | 0,540 | 2,90 | 1,201 |

Stopnja zanesljivosti lestvice je izračunana s Cronbachovim koeficientom alfa, ki z vrednostjo 0,655 zagotavlja srednjo zanesljivost, skupna pojasnjena varianca vseh faktorjev pa je 68,4 % (tabela 5). Na podlagi predstavljenih ugotovitev in pregleda virov pa v nadaljevanju ugotavljamo načine zagotavljanja varnosti uporabnikom mobilnih naprav.

## 3 DISKUSIJA

Na podlagi teoretičnih spoznanj ugotavljamo, da sta uporaba in uporabnost mobilnih naprav v porastu, hkrati pa tudi informacijskovarnostne grožnje. Nameni uporabe mobilnih naprav so različni, najbolj pogost je v povezavi z možnostjo neprestane komunikacije in neprestane dostopnosti do informacij. Na področju programske opreme imamo številne aplikacije, ki omogočajo, da si uporabniki s pomočjo informacij, ki jih prenesejo iz kibernetskega prostora, olajšajo delo.

Pri vsej popularnosti mobilnih naprav se uporabniki premalo zavedajo, da morajo sami poskrbeti za njihovo varno rabo in zaščito podatkov, tako na napravi kot med prenosom le-teh. Poznavanje groženj, ki pretijo uporabnikom mobilnih naprav, in uporaba varnostnih ukrepov je zato bistvenega pomena. Iz poznavanja groženj izhaja uporaba potrebnih varnostnih rešitev, ob nepoznavanju groženj pa se pod vprašaj postavlja tudi posameznikovo poznavanje in uporaba varnostnih rešitev.

Predstavljene ugotovitve raziskave pokažejo, da izpraševanci slabo poznajo grožnje mobilnim napravam. Grožnje, ki jih poznajo, so splošne, medtem ko je poznavanje naprednih groženj, ki so na področju mobilnih naprav najbolj v porastu, slabo. Ravno tako je z uporabo varnostnih ukrepov. Najpogostejša je uporaba preprostih zaščitnih možnosti, ki jih na področju mobilnih naprav poznamo že dalj časa (npr. koda PIN), medtem ko je uporaba in poznavanje napredne zaščite nezadostno. Zanimiva je ugotovitev, da kljub poznavanju številnih nevarnosti, ki grozijo uporabnikom mobilnih naprav, ti še vedno ne verjamejo, da se lahko grožnja zgodi tudi njim. To pomeni, da nevarnosti zavestno zanemarjajo. Rezultati raziskave kažejo, da vprašani v največji meri uporabljajo mobilno napravo zato, da lahko komunicirajo z vrstniki. Programska oprema oz. načini uporabe pa se razlikujejo.

Uporaba mobilnih naprav se bo, glede na trenutne trende, povečevala še naprej. Vedno več bo naprednih aplikacij, ki bodo uporabnikom nudile hitrejši dostop do podatkov. Pri obilici raznovrstnih mobilnih naprav in programske opreme ne smemo pozabiti na pomen zasebnosti, varovanja informacij in vzpostavitve celovite kibernetske varnosti. V središče zagotavljanja omenjenega je treba postaviti izobraževanje in ozaveščanje uporabnikov. Uporabnike je potrebno seznaniti z varnostnimi načeli rabe mobilnih naprav, razširiti njihovo poznavanje raznovrstnih groženj in morebitnih posledic ob njihovi uresničitvi ter poudariti pomen zaščitnih ukrepov. Ko se grožnja enkrat uresniči, poti nazaj ni več, zato je treba za kibernetsko varnost poskrbeti že prej. To lahko večinoma storimo že z nekaj osnovnimi koraki uporabe tehničnih rešitev in znanja varne uporabe mobilnih naprav. Najbolj običajni ukrepi so redno zaklepanje naprave (s PIN-om, vzorcem, prstnim odtisom) (Mooney, Parham in Cairney, 2013), uporaba varnostnih reši-

tev (npr. antivirusni program), tudi tistih, ki so brezplačno dostopne na spletu, uporaba zaščitenih omrežij in kriptiranega prenosa podatkov (Teulf, Zefferer in Stromberger, 2013). Pri dostopanju do spletnih portalov in prenosu različnih aplikacij s spleta je potrebno uporabljati različna in varna gesla ter predhodno preveriti varnost mest in aplikacij, do katerih dostopamo.

Moderna tehnologija nam odpira vrata v svet dodatnih možnosti, ki jih nudi kibernetski prostor. Pri vsem tem pa ne smemo pozabiti na zdravo pamet uporabe moderne tehnologije, neprestano izobraževanje o uporabi le-te in se zavedati, da poleg dobrih stvari, ki jih tehnologija prinaša, vedno z njo prihajajo tudi nevarnosti.

## LITERATURA


Greene, K. K., Tamborello, F. P. in Micheals, R. J. (2013). Computational cognitive modeling of touch and gesture on mobile multitouch devices: Applications and challenges for existing theory. V M. Kurosu (ur.), *Human-computer interaction: Interaction modalities and techniques* (str. 449–455). Heidelberg: Springer.

International Data Corporation. (2011). *IDC – Press release.* Pridobljeno na http://www.idc.com/getdoc.jsp?containerId=prUS22871611http://www.idc.com/getdoc.jsp?containerId=prUS22871611

Juniper Networks. (2011). *Malicious mobile threats report 2010/2011*. Pridobljeno na http://www.juniper.net/us/en/dm/interop/go

Juniper Networks. (2013). *Juniper Networks third annual mobile threats report.* Pridobljeno na http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf

Leavitt, N. (2011). *Mobile security: Finally a serious problem?* Largo: University of Maryland. Pridobljeno na http://www.computer.org/portal/web/computingnow

Lookout. (2011). *Lookout mobile threat report*. Pridobljeno na https://www.mylookout.com/mobile-threat-report

McAfee. (2013). *McAfee® labs threats report: Third quarter 2013.* Santa Clara: McAfee. Pridobljeno na http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q3-2013.pdf

Mooney, J. L., Parham, A. G. in Cairney, T. D. (2013). Your guide to authenticating mobile devices. *Journal of Corporate Accounting & Finance, 24*(5), 51–68.

Ponemon Institute. (2011). *Second annual cost of cyber crime study: Benchmark study of U.S. companies*. Traverse City: Ponemon Institute. Pridobljeno na http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf

Ponemon Institute. (2012). *2013 state of the endpoint.* Traverse City: Ponemon Institute. Pridobljeno na http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

Teulf, P., Zefferer, T. in Stromberger, C. (2013). Mobile device encryption systems. V L. J. Janczewski, H. B. Wolfe in S. Shenoi (ur.), *Security and privacy protection in information processing systems* (str. 203–216). Heidelberg: Springer.

**O avtorjih:**

**Dr. Igor Bernik**, docent, predstojnik Katedre za informacijsko varnost in prodekan za izobraževalno dejavnost na Fakulteti za varnostne vede Univerze v Mariboru. E-mail: igor.bernik@fvv.uni-mb.si

**Blaž Markelj**, predavatelj informacijske varnosti na Fakulteti za varnostne vede Univerze v Mariboru. Doktorski študent varstvoslovja. E-mail: blaz.markelj@fvv.uni-mb.si