# Znanje o sigurnosti i potencijalno rizično ponašanje na Internetu među studentima sestrinstva u Puli

**Slacki, Rozi**

**Undergraduate thesis / Završni rad**

**2018**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Faculty of Medicine / Sveučilište Josipa Jurja Strossmayera u Osijeku, Medicinski fakultet**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:152:144695

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2024-07-17**

*Repository / Repozitorij:*

Repository of the Faculty of Medicine Osijek

zir.nsk.hr

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**

**MEDICINSKI FAKULTET OSIJEK**

**Studij sestrinstva**

**Rozi Slacki**

# ZNANJE O SIGURNOSTI I POTENCIJALNO RIZIČNO PONAŠANJE NA INTERNETU MEĐU STUDENTIMA SESTRINSTVA U PULI

**Završni rad**

**Osijek, 2018.**

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**

**MEDICINSKI FAKULTET OSIJEK**

**Studij sestrinstva**

**Rozi Slacki**

# ZNANJE O SIGURNOSTI I POTENCIJALNO RIZIČNO PONAŠANJE NA INTERNETU MEĐU STUDENTIMA SESTRINSTVA U PULI

**Završni rad**

**Osijek, 2018.**

Rad je ostvaren na Medicinskom fakultetu u Osijeku

Mentor rada: doc.dr.sc. Krešimir Šolić, dipl.ing.

Rad sadrži: 26 listova, 2 slike, 1 grafikon i 7 tablica

# SADRŽAJ

Stranica

# 1. UVOD

## 1.1. Definicija i nastanak interneta

Internet se može definirati kao svjetska računalna informacijska mreža, sastavljena od velikog broja manjih međusobno povezanih računalnih mreža, koja omogućava prijenos informacija između računala koji čine mrežu. Zato se za internet najčešće može čuti da je to „mreža svih mreža“(1).

Početak interneta veže se za 1969. godinu kada je Ministarstvo obrane SAD-a razvilo ARPANET (kratica od Advanced Research Project Agency, dok **NET** označava računalnu mrežu). Cilj te mreže bio je povezivanje određenog broja računala u SAD-u, kako bi se olakšalo prenošenje važnih informacija, s obzirom da je Hladni rat bio u ponom zamahu (2).

Ono što je tada bilo najbitnije jest da se mreža „ne sruši“, čak ni u slučaju da dio komunikacijskog dijela bude uništen, što znači da mreža mora nastaviti funkcionirati (2). To dovodi do današnjeg modela rada, gdje razgranata struktura interneta omogućuje komunikaciju između bilo koja dva udaljena računala, čak i u slučaju da dođe do kolapsa velikih dijelova mreže budući da poruka može zahvaljujući routerima putovati različitim putovima.

Projekt kojim je započeo razvoj weba potiče od ideje engleskog fizičara Tima Berners-Leeja, čiji je rad poslužio kao temelj i njemu i belgijskom znanstveniku Robertu Cailliau pa su 1993. godine u CERN-u u Švicarskoj osmislili prvu inačicu današnjeg WWW-a (World Wide Web) i prvi grafički orijentiran preglednik – Mosaic. Potom je predstavljen Netscape 1994. godine i Internet Explorer 1995. godine, potom nove brze mrežne arhitekture na kojima nastaju temelji interneta kakav danas poznajemo (3).

Postupno se s razvojem fiksne mreže razvija i mobilna internetska mreža pa danas, prema istraživanjima, čak 52% korisnika interneta dolazi s mobilnih uređaja. U prosjeku svakih 10 godina znanstvenici dođu do novog otkrića u mobilnoj internetskoj tehnologiji pa se tako 1979. godine prvi put spominje 1G (mogućnost poziva s mobilnog uređaja), 1991. godine 2G (uz pozive mogao se poslati SMS, a s vremenom i MMS, te je uveden mobilni internet s brzinama ispod 0,1 Mb/s), a 2001. godine 3G (mogućnost gledanja video sadržaja i mobilne televizije), dok se današnji standard od 4G uveo 2012. godine (brzine do 50 Mb/s).

### 1.2. Internet danas

Danas pomoću računala, tableta ili mobitela i zahvaljujući internetu možemo obaviti mnoštvo zadataka za koje nam je nekada trebalo više vremena i fizički odlazak na lice mjesta. Zahvaljujući internetu, možemo slati e-poštu, zvati i slati poruke u stvarnom vremenu (instant messaging, chat, VOIP), zabavljati se, kupovati, obavljati bankovne transakcije...

Internet se ne sastoji samo od „surfanja“, kako mnogi korisnici misle, već od nekoliko usluga i servisa, kao što su: (2)

- World Wide Web (www) – služi za pregledavanje web-stranica
- Chat – razgovori putem interneta
- E-mail – razmjena poruka
- VOIP – razgovori putem interneta
- Prijenos datoteka – FTP (file transfer protocol)
- Usenet – prenošenje novinskih članaka između novinskih grupa.

Da bi se ovim uslugama pristupalo što lakše i brže, znanstvenici i programeri svakodnevno rade na povećanju internet-brzine. Iako Hrvatska danas po statistikama ima jedan od najsporijih interneta u Europi s prosjekom od 12,5 Mb/s, svejedno je to sasvim dovoljno za svakodnevno uživanje u čarima interneta. Potrebno je napomenuti da Norveška, Danska i Švedska trenutno imaju i do 3 puta veće prosječne brzine spajanja na internet od Hrvatske, dok je svjetski lider Singapur s trenutnih 55 Mb/s u prosjeku. Lokalne mreže (LAN-ovi) ustanova rade na brzinama većim od 10 Gb/s između ključnih mrežnih uređaja, koji čine okosnicu lokalne mreže, to je takozvani backbone.

U području mobilnog interneta stvari za Hrvatsku stoje daleko bolje. S prosječnom brzinom od 34,4 Mb/s Hrvatska zauzima pohvalno 20. mjestu na svijetu s čak 72% ukupne površine pokrivene 4G mrežom, dok najbrže „surfaju“ Norvežani s prosječnom brzinom od 62,6 Mb/s.

Jedna od vodećih svjetskih istraživačkih tvrtki, Gartner, predviđa da će 2020. godine preko 20 milijardi uređaja biti povezano na internet. Televizori, hladnjaci, automobili, čak i pseće ogrlice, svi ti predmeti sve se više približavaju internetu te je zbog toga nastala potreba za novom generacijom bežičnog povezivanja - 5G. Peta generacija izgradit će se na temeljima koje su stvorili 4G LTE sustavi te će omogućiti brzine do 10 Gb/s.

### 1.3. Kako na internet?

Da bismo imali pristup internetu, potrebno je posjedovati uređaje koji to omogućuju, a ovisno o njima na internet se moguće spojiti: (4)

- Žičano

Uz pomoć DSL tehnologije omogućuje se stalan pristup internetu preko telefonske mreže. Najčešći oblik takvog povezivanja jest svima poznati ADSL. Računalo se povezuje preko mrežnog kabela na DSL uređaj, koji je najčešće kombinacija modema, usmjernika i pristupne točke, te omogućuje priključivanje nekoliko uređaja na internet (računalo, smart TV, HiFi sustavi, drugi usmjernik). Na taj se način veza dijeli i tvori malu lokalnu mrežu (LAN ili WLAN)

- Kabelska televizija (kabelski internet)

Kabelski internet može se ostvariti samo ako je uvedena kabelska televizija, tako da upotrebljava istu infrastrukturu. Potreban je kabelski modem, uređaj koji se priključuje na javnu televizijsku kabelsku mrežu kako bi se ona, osim za prijenos televizijskog signala, mogla koristiti i za internet komunikaciju.

- Bežično - mobilna širokopojasna mreža

Mobilna širokopojasna mreža, poznatija kao „podatkovna veza“ ili „mobilni podaci“, omogućuje brz bežični pristup internetu uz pomoć prijenosnih uređaja s bilo kojeg mjesta ukoliko je dostupan signal mobilne mreže.

Za povezivanje je potrebna SIM kartica (mala izmjenjiva kartica koja sadrži podatke o identitetu pretplatnika i sigurnosne informacije za pristup mobilnoj mreži) ili podatkovna kartica (elektronički sklop ugrađen u uređaj).

- Javni bežični internet (Wi-Fi)

Radi se o bežičnoj mreži gdje se podaci između uređaja prenose pomoću radiofrekvencija i odgovarajućih antena.

Kod bežičnog umrežavanja nema potrebe za kablovima i drugim mrežnim uređajima, korisnik se jednostavno spoji na hotspot, čvorište na koje se spajaju i drugi korisnici. Najčešći oblik takvog spajanja je WLAN, gdje se bežično spajamo mobitelima ili prijenosnim računalima na routere u vlastitim domovima, dok se u zadnje vrijeme sve češće može susresti i WAN tehnologija, spajanje na javne pristupne točke kakve se mogu naći na trgovima i drugim javnim mjestima.

### 1.4. Internet – dobro ili zlo?

*Slika 1.: Internet krađa*

*Izvor: www.evarazdin.hr*

Nažalost, kako je na neki način u prirodi sve uravnoteženo, tako se i za sve dobro vezano za internet uvijek može naći i jednako toliko štetnih argumenata.

Danas su sve moderne tehnologije povezane na internet. Međutim, dok ovaj digitalni svijet za neke predstavlja igralište, za druge je on baš poput bojnog polja. Internet je postao nezamjenjiv poslovni alat koji je pomogao da se ljudi širom svijeta zbliže. Primanje informacija i vijesti iz različitih krajeva svijeta, mogućnost kupovine i pristupačnost svega što nas zanima samo su jedan klik udaljeni. On ima ogroman potencijal i mnogo može ponuditi svojim korisnicima. Međutim, kao i sva tehnologija novijeg doba, internet pored svojih prednosti ima i mane (5,6).

Prednosti (5):

- brža komunikacija
- nepresušan izvor informacija
- bezbroj tečajeva iz svih disciplina (besplatnih ili plaćenih)
- zabava
- financijske transakcije.

Mane (5):

- ❖ Zloćudni programi

To su računalni programi koji mogu počiniti štetu na računalu. Mogu se podijeliti na:

- računalni virus - inficira datoteke i programe
- Trojanski konj - krađa korisničkih lozinki, brojeva kreditnih kartica, omogućavanje neovlaštenoj osobi potpuni nadzor nad zaraženim računalom
- računalni crv – štetni program koji se širi mrežom, najčešće elektroničkom poštom
- špijunski softver – prikuplja podatke korisnika na čijem je računalu
- oglašivački softver – zatrpava računalo oglasima
- Keylogger – praćenje korisnikovih unosa preko tipkovnice.

- ❖ Nesigurne mrežne linije

Korištenje interneta za bankarstvo, društveno umrežavanje ili neke druge usluge često čine osobne informacije ranjivima. Hakeri imaju mnoštvo načina da se domognu važnih informacija.

- ❖ Dobno neprikladni sadržaji

Jednostavan pristup najveća je prednost ovakvih sadržaja. U samo nekoliko klikova mišem razni sadržaji nenamijenjeni maloljetnoj populaciji na dohvat su ruke.

- ❖ Socijalizacija

Pored sigurnosti najveća mana interneta jest da umanjuje socijalne vrijednosti korisnika. Ljudi se izoliraju od stvarnog svijeta i utonu u digitalni (izmišljeni) svijet.

### 1.5. Kako se zaštititi

Postoji skup pravila ponašanja kako bismo se uspješno zaštitili od moguće internet-krađe, ali i oštećenja vlastite imovine. Dovoljno je u web-pretraživač upisati „sigurnost na internetu“ i pročitati predložene mjere opreza te ih upotrijebiti. Najčešći pojmovi su (7,8):

- ❖ Antivirus

Predlaže se instalacija jednog od pouzdanijih antivirusnih programa (Norton, AVG, Kaspersky, Avast), te njegovo redovno ažuriranje kako bi se spriječilo moguće inficiranje

uređaja. Također, ovdje se mogu uvrstiti i antispyware i antispam programi koji štite uređaje od zlonamjernog korištenja te krađe podataka s njih.

- Lozinka

Lozinka kao pristup, uglavnom svakom Internet-servisu, najvažniji je tajni podatak koji bi trebalo adekvatno zaštititi. Lozinka je ulaznica za sve privatne profile i račune, stoga ona mora biti složena i komplicirana za provaljivanje, a opet jednostavna za pamćenje. Preporučuje se korištenje kombinacije malih i velikih slova te brojki, nikako se ne preporuča korištenje jednostavnih lozinki poput 12345678, asdfghjkl ili datuma rođenja. Nadalje, lozinke ne bismo smjeli zapisivati, odavati drugima pa se također preporuča korištenje različitih lozinki za različite servise (10).

- Vatrozid

Vatrozid je još jedno softversko rješenje slično antivirusu, ali koje nadzire i zaustavlja neovlašteni promet prema računalu i s njega.

- Odjava

Prilikom završetka rada na javnom računalo obavezno se treba odjaviti te tako onemogućiti sljedećem korisniku da sazna Vaše osobne podatke.

- Internet-preglednik

Internet-preglednik trebao bi se redovno ažurirati, no ne bi trebala biti uključena opcija AutoComplete koja pamti e-mail adresu i lozinke. Također, treba izbjegavati logiranje na internet-stranice na koje Vas određene domene preusmjeravaju jer se vjerojatno radi o pokušaju krađe Vaših osobnih podataka.

### 1.6. Upotreba računala u medicini

Dok su ljudi prije bili primorani ići uvijek istom liječniku koji je jedini znao povijest njihovih bolesti i čuvao zdravstveni karton „kao oči u glavi“, danas stvari izgledaju malo drugačije. Uvođenjem informatičke tehnologije u medicinu stvaraju se velike baze podataka kako bi se podacima o pacijentu moglo pristupiti iz bilo koje zdravstvene ustanove svijeta. Zdravstveni karton više nije strogo čuvana tajna te se na taj način olakšava i ubrzava dijagnoza i liječenje samog pacijenta.

Postoji mnogo načina primjene računala u medicini. Jedan od najosnovnijih je i već navedeni, a tu spada i administrativna upotreba u svrhu financijskog i robnog knjigovodstva, evidencija lijekova, obrada teksta, statistika i sl.

Računala se koriste i u dijagnostičke svrhe gdje su opremljena odgovarajućim hardverom i softverom pa se koriste u kombinaciji s aparatima za dijagnostiku. Imaju široku primjenu u laboratorijima, u automatizaciji postupaka i obradi velikih količina podataka (11).

Međutim, koliko se god računalom pokušavalo zamijeniti ljudsko biće, ključnu ulogu još uvijek ima čovjek. Kako bi se određeni podaci našli u bazi podataka, netko ih mora ondje staviti, a to je obaveza kako doktora, tako i sestara. Stoga je važno posjedovati znanje o korištenju računala te biti upoznat s pozitivnim, ali i negativnim, stranama korištenja informatičke tehnologije, te se znati nositi s upotrebom novih tehnologija.

Internetska baza podataka o pacijentima dostupna je samo medicinskom osoblju, što znači da se informacije ne bi trebale odavati trećim stranama (12).

## 2. CILJ

U cilju upoznavanja navika studenata sestrinstva u Puli o ponašanju na računalu provedena je anketa validiranim upitnikom, u kojoj su studenti ispitani koliko su upoznati sa sigurnošću korištenja interneta, te o čuvanju vlastitih podataka.

Na temelju dobivenih odgovora može se zaključiti u kolikoj je mjeri tko potencijalno rizičan prilikom korištenja interneta.

# 3. METODA

## 3.1. Ustroj studija

Za potrebe ove studije provedeno je presječno istraživanje.

## 3.2. Ispitanici

U istraživanju je sudjelovalo 38 studenata Medicinskog fakulteta u Osijeku, s Odjela preddipomskog studija sestrinstva u Puli. Obuhvaćena su oba spola, a svi su ispitanici studenti treće godine preddiplomskog studija. Podaci su prikupljani tijekom srpnja 2017. godine.

## 3.3. Upitnik

U svrhu istraživanja korišten je validirani upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS), sastavljen od 33 pitanja koja se ocjenjuju bodovima od 1 do 5 na Likertovoj ljestvici. Upitnik se dijeli na dvije skale (13):

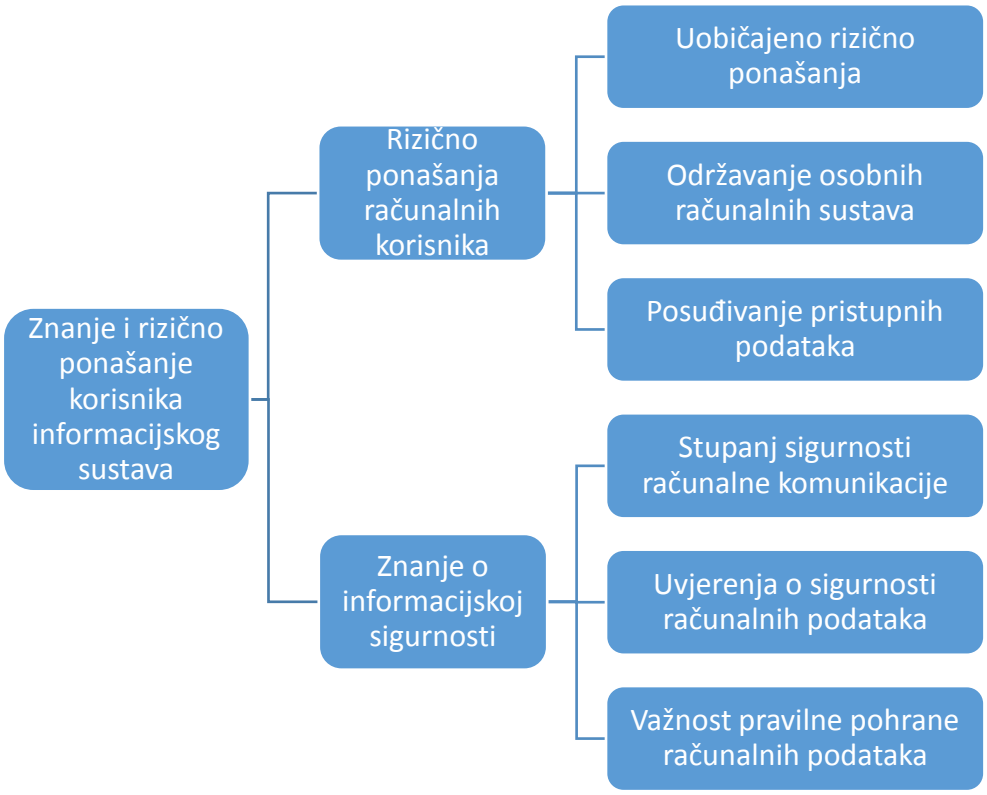
1. skala rizičnog ponašanja računalnih korisnika (k=17), koja se dodatno dijeli na 3 subskale:
    - subskala uobičajenih rizičnih ponašanja korisnika računala (k=6)
    - subskala održavanja osobnih računalnih sustava (k=6) i
    - subskala posuđivanja pristupnih podataka (k=5)
2. skala znanja o informacijskoj sigurnosti (k=16), koja se dodatno dijeli na 3 subskale:
    - subskala stupnja sigurnosti računalne komunikacije (k=5)
    - subskala uvjerenja o sigurnosti računalnih podataka (k=5) i
    - subskala važnosti pravilne pohrane računalnih podataka (k=6).

Radi daljnje analize ispitanici su ispunili i anketni upitnik s demografskim podacima (spol, dob, godina studija).

Upitnik je u cjelosti bio anoniman i svi su ispitanici bili upoznati s načinom ispunjavanja upitnika te je dobivena njihova suglasnost za sudjelovanje u istraživanju.

Za korištenje upitnika dobivena je dozvola autora s naputcima za njegovu primjenu.

*Slika 2.: Podjela anketnog upitnika na skale i subskale*




*Izvor: Izradila autorica 1. siječnja 2018.*

### 3.4. Statističke metode

Statistička obrada izvršena je u programu Microsoft Excell 2013 (verzija 15.0.4997.1000; Microsoft Corporation, Washington, SAD) korištenjem dodatka Analysis ToolPak. Rezultati ispitivanja prikazani su tablično i/ili grafički i to kategorijski podaci apsolutnom frekvencijom i proporcijom, a numerički aritmetičkom sredinom i standardnom devijacijom te po potrebi medijanom i interkvartilnim rasponom. Značajnost razlike numeričkih varijabli testirane su T-testom, povezanost kategorijskih varijabli testirana je Hi-kvadrat testom, a linearna povezanost Pearsonovim koeficijentom korelacije. Vrijednosti dobivene u statističkoj analizi smataju se značajnima ako su manje od $\alpha$=0,05.

### 3.5. Etička načela

Prije provedbe samog istraživanja dobivena je suglasnost Etičkog povjerenstva za istraživanje Medicinskog fakulteta u Osijeku (broj odobrenja: 2158-61-07-18-42, 12. ožujka 2018. godine).

# 4. REZULTATI ISTRAŽIVANJA

Provedenim istraživanjem došlo se do podataka potrebnih za statističku analizu. Upotrebom računalne tehnologije i softvera za statističku obradu podataka iz dobivenih rezultata možemo iščitati slijedeće:

## 4.1. Opća obilježja ispitanika

U istraživanju je sudjelovalo ukupno 38 polaznika preddiplomskog studija sestrinstva Medicinskog fakulteta u Osijeku, izdvojenog studija u Puli. U istraživanju je sudjelovalo ukupno 38 polaznika preddiplomskog studija sestrinstva Medicinskog fakulteta u Osijeku, izdvojenog studija u Puli U tablici 1. prikazana je distribucija po spolu, u njoj je vidljivo manje pripadnika muškog

U tablici 1. prikazana je distribucija po spolu, u njoj je vidljivo manje pripadnika muškog spola (Hi-kvadrat test, P = 0,26). U istoj je tablici prikazana i distribucija prema godini studija, prema kojoj je vidljivo da su samo 5 ispitanika apsolventi, dok 33 ispitanika pohađa treću godinu navedenog studija (Hi-kvadrat test, P = 0,37).

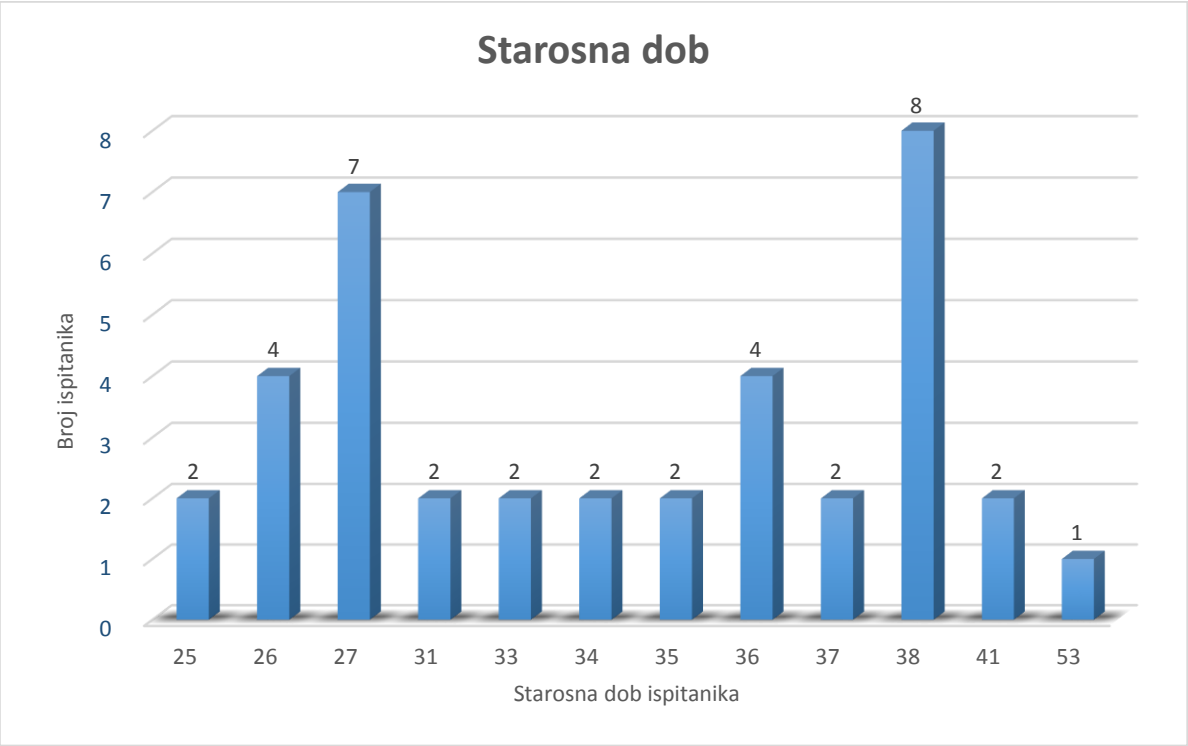
*Tablica 1.: Distribucija demografskih parametara uz *Hi-kvadrat test*

| ***Obilježje*** | **Kategorije** | **Broj (%) ispitanika** | ***P**** |
|---|---|---|---|
| *Spol ispitanika* | Ženski | 29 (76) | *0,26* |
| | Muški | 9 (24) | |
| *Godina studija* | Treća godina | 33 (87) | *0,37* |
| | Apsolventi | 5 (13) | |
| *Ukupno* | | 38 (100) | |

*Izvor: Izradila autorica 25. ožujka 2018.*

U grafikonu 1. prikazana je distribucija prema dobnoj skupini ispitanika. Izračunati medijan iznosi 34,5 godine, s interkvartilnim rasponom od 11 godina. Najmlađi ispitanik ima 25 godina, a najstariji 53 godine. Iz priloženog grafičkog prikaza može se uočiti raznolikost u dobnim skupinama.

*Grafikon 1.: Distribucija prema starosnoj dobi ispitanika*




*Izvor: Izradila autorica dana 1. siječnja 2018.*

### 4.2. Frekvencije odgovora na pojedina pitanja iz upitnika

U sljedećoj tablici (tablica 2.) ispitanici su odgovarali na pitanja koja opisuju uobičajena ponašanja korisnika računalnih informacijsko-komunikacijskih sustava. Raspon odgovora sezao je od „nikad“ do „uvijek“, te su ispitanici na osnovu svog ponašanja označili jedan od ponuđenih odgovora.

*Tablica 2: Učestalost rizičnog ponašanja*

| *Učestalost* | | | | | | |
|---|---|---|---|---|---|---|
| *Pitanje* | *Broj odgovora (%)* | | | | | |
| | Nikad | Rijetko | Ponekad | Često | Uvijek | *Ukupno* |
| *1. Posuđivanje službenih podataka* | 31 (81,6) | 4 (10,5) | 3 (7,9) | 0 (0) | 0 (0) | *38 (100)* |
| *2. Posuđivanje pristupnih podataka računala* | 15 (39,5) | 12 (31,6) | 9 (23,7) | 2 (5,3) | 0 (0) | *38 (100)* |
| *3. Posuđivanje pristupnih podataka e-pošte* | 26 (68,4) | 9 (23,7) | 3 (7,9) | 0 (0) | 0 (0) | *38 (100)* |
| *4. Posuđivanje kreditne kartice* | 31 (81,6) | 2 (5,3) | 5 (13,2) | 0 (0) | 0 (0) | *38 (100)* |
| *5. Otkrivanje tajnog PIN broja* | 37 (97,4) | 0 (0) | 1 (2,6) | 0 (0) | 0 (0) | *38 (100)* |
| *6. Korištenje različitih zaporki* | 3 (7,9) | 2 (5,3) | 11 (28,9) | 11 (28,9) | 11 (28,9) | *38 (100)* |
| *7. Ažuriranje antivirus programa* | 3 (7,9) | 5 (13,2) | 11 (28,9) | 9 (23,7) | 10 (26,3) | *38 (100)* |
| *8. Ažuriranje sustava* | 3 (7,9) | 6 (15,8) | 8 (21,1) | 13 (34,2) | 8 (21,1) | *38 (100)* |
| *9. Instaliranje raznih neophodnih programa* | 11 (28,9) | 16 (42,1) | 11(28,9) | 0 (0) | 0 (0) | *38 (100)* |
| *10. Djeljenje osobnih podataka na društvenim mrežama* | 26 (68,4) | 6 (15,8) | 6 (15,8) | 0 (0) | 0 (0) | *38 (100)* |
| *11. Odgovaranje na mailove nepoznatih pošiljatelja* | 37 (97,4) | 0 (0) | 1 (2,6) | 0 (0) | 0 (0) | *38 (100)* |
| *12. Otvaranje nepoznatih priloga* | 28 (73,7) | 5 (13,2) | 5 (13,2) | 0 (0) | 0 (0) | *38 (100)* |
| *13. Proslijeđivanje lančanih mailova* | 25 (65,8) | 10 (26,3) | 3 (7,9) | 0 (0) | 0 (0) | *38 (100)* |
| *14. Korištenje više adresa e-pošte* | 7 (18,4) | 6 (15,8) | 7 (18,4) | 13 (34,2) | 5 (13,2) | *38 (100)* |
| *15. Prijavljivanje na e-poštu s javnih mjesta* | 2 (5,3) | 11 (28,9) | 8 (21,1) | 10 (26,3) | 7 (18,4) | *38 (100)* |
| *16. Odjavljivanje nakon završetka rada* | 3 (7,9) | 2 (5,3) | 1 (2,6) | 7 (18,4) | 25 (65,8) | *38 (100)* |
| *17. Zaključavanje računala prilikom kraće odsutnosti* | 10 (26,3) | 6 (15,8) | 8 (21,1) | 4 (10,5) | 10 (26,3) | *38 (100)* |

U tablicama 3., 4. i 5. ispitanici su odgovarali na pitanja o informacijskoj sigurnosti.

*Tablica 3.: Stupanj sigurnosti*

| *Pitanje* | *Sigurnost* | | | | | |
|---|---|---|---|---|---|---|
| | *Broj odgovora (%)* | | | | | |
| | Potpuno nesigurno | Prilično nesigurno | Ne znam | Prilično sigurno | Potpuno sigurno | *Ukupno* |
| *18. Dopisivanje putem e-pošte* | 4 (10,5) | 10 (26,3) | 11 (29,0) | 13 (34,2) | 0 (0) | *38 (100)* |
| *19. Komunikacija na društvenim mrežama* | 6 (15,8) | 25 (65,8) | 2 (5,3) | 5 (13,2) | 0 (0) | *38 (100)* |
| *20. Komunikacija mobitelom* | 6 (15,8) | 16 (42,1) | 5 (13,2) | 11 (29) | 0 (0) | *38 (100)* |
| *21. Komunikacija žičnim telefonom* | 9 (23,7) | 10 (26,3) | 10 (26,3) | 9 (23,7) | 0 (0) | *38 (100)* |
| *22. Općenito internet komunikacija* | 8 (21,1) | 22 (57,9) | 4 (10,5) | 2 (5,3) | 2 (5,3) | *38 (100)* |

*Izvor: Izradila autorica dana 1. siječnja 2018.*

*Tablica 4.: Stupanj uvjerenja*

| *Pitanje* | *Uvjerenje* | | | | | |
|---|---|---|---|---|---|---|
| | *Broj odgovora (%)* | | | | | |
| | Nisam uvjeren/a | Možda | Ne znam | Prilično | Potpuno | *Ukupno* |
| *23. Krađa službenih podataka u školi* | 2 (5,3) | 15 (39,5) | 9 (23,7) | 12 (31,6) | 0 (0) | *38 (100)* |
| *24. Krađa privatnih podataka s računala* | 8 (21,1) | 13 (34,2) | 9 (23,7) | 8 (21,1) | 0 (0) | *38 (100)* |
| *25. Krađa privatnih podataka s mobitela* | 11 (29,0) | 18 (47,4) | 3 (7,9) | 6 (15,8) | 0 (0) | *38 (100)* |
| *26. Otuđenje novca s bankovnog računa* | 5 (13,2) | 24 (63,2) | 7 (18,4) | 2 (5,3) | 0 (0) | *38 (100)* |
| *27. Krađa identiteta na internetu* | 4 (10,5) | 16 (42,1) | 8 (21,1) | 5 (13,2) | 5 (13,2) | *38 (100)* |

*Izvor: Izradila autorica dana 1. siječnja 2018.*

*Tablica 5.: Stupanj važnosti*

| *Pitanje* | *Važnost* | | | | | |
|---|---|---|---|---|---|---|
| | *Broj odgovora (%)* | | | | | |
| | Potpuno nevažno | Prilično nevažno | Ne znam | Prilično važno | Izrazito važno | *Ukupno* |
| *28. Izrada pričuvnih kopija podataka* | 2 (5,3) | 0 (0) | 5 (13,2) | 25 (65,8) | 6 (15,8) | *38 (100)* |
| *29. Provjera tuđeg USB sticka od virusa* | 0 (0) | 2 (5,3) | 5 (13,2) | 25 (65,8) | 6 (15,8) | *38 (100)* |
| *30. Čuvanje zaporki u tajnosti* | 0 (0) | 0 (0) | 1 (2,6) | 18 (47,8) | 19 (50,0) | *38 (100)* |
| *31. Povremena promjena zaporke* | 0 (0) | 0 (0) | 4 (10,5) | 19 (50,0) | 15 (39,5) | *38 (100)* |
| *32. Odvajanje privatnih od zajedničkih podataka* | 0 (0) | 0 (0) | 5 (13,2) | 23 (60,5) | 10 (26,3) | *38 (100)* |
| *33. Čuvanje USB sticka od krađe* | 0 (0) | 0 (0) | 1 (2,6) | 18 (47,8) | 19 (50,0) | *38 (100)* |

*Izvor: Izradila autorica dana 1. siječnja 2018.*

Vrijedi izdvojiti iz skupine pitanja o učestalosti rizičnog ponašanja dva pitanja na koja su svi ispitanici, osim jednoga, odgovorili kako je čuvanje tajnog PIN broja izrazito važno, kao i zanemarivanje e-poruka nepoznatog pošiljatelja. Zanimljivo je da jedan ispitanik smatra kako je povremeno otkrivanje tajnog PIN broja sasvim normalno, što bi svakako trebalo biti zabrinjavajuće.

Vidljivo je također i kako su ispitanici u jednakom omjeru odgovorili na pitanje o zaključavanju računala prilikom kraće odsutnosti. Zanimljivo je da gotovo polovica ispitanika nikada ne zaključava računalo prilikom odsutnosti, što uvelike doprinosi zloporabi podataka.

Na trik pitanje kojim se pokušalo navesti ispitanike da napišu svoju zaporku za račun elektroničke pošte, a radi analize kvalitete zaporke, njih 6 (18,8%) odalo je svoju zaporku. Proporcija ispitanika koji su odali svoju zaporku u ovome istraživanju nešto je manja od 28,8% iz prethodnog referentnog istraživanja, no nije statistički značajno manja (Hi-kvadrat test, P = 0,06).

### 4.3. Usporedba ispitanika s prosječnim korisnikom interneta

Rezultati usporedbe ispitanika, studenata sestrinstva, s prosječnim rezultatima korisnika interneta u Hrvatskoj iz ranijeg istraživanja (15) pokazali su porazne rezultate (tablica 6.). U četiri subskale ispitanici su statistički značajno lošiji od prosjeka, dok se u dvije subskale značajno ne razlikuju. Studenti su lošiji u subskali koja ispituje koliko „Posuđuju pristupne podatke“ (Studentov T-test, P = 0,03), zatim u subskali koja opisuje „Održavanje osobnih računalnih sustava“ (Studentov T-test, P = 0,04), a lošiji su u subskali koja opisuje „Uobičajeno rizično ponašanje“ (Studentov T-test, P < 0,001). Lošiji su i u subskali koja ispituje „Uvjerenje o sigurnosti računalnih sustava“ (Studentov T-test, P = 0,003), što znači da su relativno lakovjerni. U subskali „Stupanj sigurnosti računalne komunikacije“ studenti iz ovog istraživanja nešto su kvalitetnije odgovorili od studenata iz prethodnog istraživanja (Studentov T-test, P = 0,28), dok su u subskali „Važnost pravilne pohrane podataka“ (Studentov T-test, P = 0,25) ipak malo popravili dojam.

*Tablica 6.: Usporedba s prosječnim korisnikom interneta*

| **Subskale** | ***Aritmetička sredina (standardna devijacija)*** | | **P*** |
|---|---|---|---|
| | *Studenti medicinskog fakulteta (n=38)* | *Referentne vrijednosti iz prethodnog* | |
| Posuđivanje pristupnih podataka | *4,60 (0,44)* | *4,74 (0,39)* | 0,03 |
| Održavanje osobnih računalnih sustava | *3,48 (0,68)* | *3,18 (0,91)* | 0,04 |
| Uobičajeno rizično ponašanje | *4,24 (0,46)* | *4,52 (0,43)* | <0,001 |
| Stupanj sigurnosti računalne komunikacije | *3,63 (0,76)* | *3,48 (0,83)* | 0,28 |
| Uvjerenje o sigurnosti računalnih sustava | *2,46 (0,83)* | *2,06 (0,79)* | 0,003 |
| Važnost pravilne pohrane podataka | *4,23 (0,47)* | *4,18 (0,68)* | 0,25 |

*Izvor: Izradila autorica 25. ožujka 2018.*

### 4.4. Usporedba rezultata prema dobi ispitanika

Rezultati analize korelacije starosne dobi ispitanika, studenata sestrinstva, i ocjena za pojedine subskale pokazali su statistički značajnu korelaciju samo za jednu subskalu. Statistički značajna, negativna korelacija vrlo visokog stupnja postoji između starosne dobi ispitanika i ocjene za subskalu „Uvjerenje o sigurnosti računalnih sustava“ (Spearmanov test korelacije, rho = -0,622, P = <0,001), što bi značilo da su stariji ispitanici lošije odgovorili, odnosno da su lakovjerniji po pitanju zaštite svoje privatnosti na internetu (tablica 7.).

Također je nađena niska negativna korelacija starosne dobi i ocjene „Uobičajenog rizičnog ponašanja“, no ona nije statistički značajna (Spearmanov test korelacije, rho = -0,254, P = 0,12), a pokazuje da se stariji ispitanici općenito rizičnije ponašaju od mlađih (tablica 7.).

*Tablica 7.: Usporedba po subskalama pitanja sa starosnom dobi*

| ***Subskale*** | **Starosna dob ispitanika** | | ***P**** |
|---|---|---|---|
| | rho | 95% CI od rho | |
| *Posuđivanje pristupnih podataka* | -0,000 | od -0,320 do 0,319 | *>0,99* |
| *Održavanje osobnih računalnih sustava* | -0,108 | od -0,413 do 0,219 | *0,52* |
| *Uobičajeno rizično ponašanje* | -0,254 | od -0,530 do 0,072 | *0,12* |
| *Stupanj sigurnosti računalne komunikacije* | 0,180 | od -0,148 do 0,473 | *0,28* |
| *Uvjerenje o sigurnosti računalnih sustava* | -0,622 | od -0,786 do 0,377 | *<0,001* |
| *Važnost pravilne pohrane podataka* | -0,151 | od -0,449 do 0,177 | *0,36* |

*Izvor: Izradila autorica 25.ožujka 2018.*

*Spearmanov test korelacije

# 5. RASPRAVA

U provedenom istraživanju sudjelovalo je 38 ispitanika preddiplomskog studija sestrinstva u Osijeku, od kojih je 9 ispitanika (24%) muškog roda, dok je 29 (76%) ženskog roda.

Pitanja u anketnom upitniku podijeljena su u dvije skupine: pitanja koja ispituju rizičnost ponašanja računalnih korisnika te pitanja u kojima se ispituje znanje o informacijskoj sigurnosti.

Iako se ne može sa sigurnošću utvrditi koliko je ispitanika trenutno zaposleno u zdravstvenim ustanovama, porazna i zabrinjavajuća činjenica je da je na pitanje o zaključavanju računala tijekom kraće odsutnosti od računala čak 10 ispitanika (26,3%) odgovorilo kako nikada ne zaključava računalo, što svakako doprinosi ugrožavanju tajnosti podataka koji se nalaze na njihovim računalima. Time ne samo da ugrožavaju tajnost podataka, već omogućuju neovlaštenim osobama da u odsustvu pažnje pristupe računalu i nad njime izvrše raznorazne manipulacije.

Prema dobivenim odgovorima iz anketnog upitnika, a uspoređujući s prethodnim istraživanjem provedenim na uzorku od 701 ispitanika (15), u kojemu je prosjek godina 32 (u ovom istraživanju prosjek godina je 33,3), može se obrazložiti sljedeće:

Od 6 predstavljenih subskala studenti preddiplomskog studija sestrinstva generalno su lošije odgovore dali u dvije subskale. Međutim, treba napomenuti kako su referentne vrijednosti dobivene usporedbom s prijašnjim rezultatima u četiri subskale statistički značajno odskočile od prijašnjeg istraživanja. U subskali koja ispituje uobičajeno rizično ponašanje, vidljiva je statistički najveća razlika, što i ne čudi kada se pogleda da se čak 5 od 38 (13,2%) ispitanika nikada ili rijetko odjavljuje s računala nakon završetka rada. Možda postotak od 13,2% ne zvuči kao velika brojka, ali ako se razmotri koliku težinu nosi samo pitanje, stvari izgledaju malo drugačije. Tu treba nadodati i da je na pitanje o zaključavanju računala prilikom kraće odsutnosti čak 16 (42,1%) ispitanika odgovorilo s „nikad“ ili „rijetko“. U subskali o sigurnosti računalnih sustava ispitanici su dali puno pozitivnije odgovore od prosjeka prošlog istraživanja, što ne mora nužno biti loše ako imaju nekakva nova saznanja o zaštiti vlastitih i poslovnih uređaja, kako računala, tako i mobitela, te drugih komunikacijskih uređaja koji imaju pristup internetu. Budući da je prošlo istraživanje zahvatilo veći broj starijih osoba, među kojima je bilo i dosta umirovljenika, koje su po prirodi skeptičnije u vezi s korištenjem računalne tehnologije te su slabije informirane po pitanju informacijske sigurnosti i zaštite podataka, ne

čudi podatak da se studenti iz ovog istraživanja osjećaju sigurnije prilikom korištenja navedene sigurnosti. To naravno može biti i dvosjekli mač ako se korisnik previše opusti, što u slučaju ovog istraživanja vidimo iz već objašnjenih pitanja o odjavljivanju i zaključavanju računala. Druge dvije subskale otkrivaju kako su studenti iz Pule malo „mekšeg srca“ kada je u pitanju posuđivanje pristupnih podataka, što naravno direktno utječe na sigurnost i diskreciju svih pacijenata, ali i njih samih. Održavanje osobnih računalnih sustava smatraju važnim, što doprinosi većoj zaštiti od virusa ili čak hakerskih napada na nezaštićena računala. U preostale dvije subskale, koje ispituju stupanj sigurnosti računalne komunikacije i važnost pravilne pohrane podataka, dobivene vrijednosti nisu statistički značajno različite od referentnih vrijednosti iz prethodnog istraživanja.

Analizom korelacije starosne dobi ispitanika i ocjena pojedinih subskala pokazalo se da su stariji ispitanici odgovorili lošije na pitanja o sigurnosti računalnih sustava, što znači da su manje skeptični u korištenje takvog oblika čuvanja podataka. Također je uočena negativna korelacija između starosne dobi i subskale „Uobičajeno rizično ponašanje“, što je čudno s obzirom da starije osobe nisu dovoljno upućene u informatičku tehnologiju pa bi se očekivalo da su oprezniji, kako je navedeno u referentnom istraživanju (14,15).

Također, na pitanje u kojemu se traži odavanje lozinke osobne e-pošte, 6 (18,8%) ispitanika odalo je svoju lozinku, što i nije baš pohvalno, ali uzevši u obzir rezultate prijašnjeg istraživanja gdje je 28% ispitanika bilo brzopleto, može se zaključiti da su studenti iz Pule nešto pažljiviji.

# 6. ZAKLJUČAK

Na temelju provedenog istraživanja došlo se do nekoliko bitnih zaključaka:

- Medicinske sestre/tehničari s preddiplomskog studija sestrinstva u Puli u usporedbi s prethodnim istraživanjem smatraju da su njihovi podaci na internetu dovoljno zaštićeni.

- Održavanje osobnih računalnih sustava smatraju važnijim od ispitanika iz prethodnog istraživanja.

- Određeni broj ispitanika ponekad vrlo rado ustupi pristupne podatke računala, pa i kreditnu karticu.

- U prosjeku se studenti iz Pule osjećaju nesigurnije prilikom komunikacije računalnom tehnologijom, što znači da su oprezniji.

- Svjesni su koliku važnost ima pravilna pohrana podataka.

- Odgovori na opća pitanja o mogućem rizičnom ponašanju otkrivaju da su ispitanici iz prethodnog istraživanja dali bolje odgovore.

- Stariji ispitanici slabije su educirani o korištenju računalne tehnologije, ali su svejedno manje skeptični, što nije razmjerno jedno drugome.

- Ukupno gledajući, studenti sestrinstva izdvojenog studija u Puli općenito su bolji u usporedbi s prosječnim korisnikom interneta u Hrvatskoj.

# 7. SAŽETAK

Cilj istraživanja: Provjera potencijalnog rizičnog ponašanja na računalu studenata sestrinstva u Puli anonimnom anketom u kojoj je ispitano koliko su studenti upoznati sa sigurnošću korištenja interneta te o čuvanju vlastitih podataka. Na temelju dobivenih odgovora te usporedbe s referentnim istraživanjem, odnosno prosječnim korisnikom interneta, može se zaključiti koliko je tko potencijalno rizičan prilikom korištenja interneta.

Nacrt studije: Ispitivanje je provedeno kao presječno.

Ispitanici i metode: U ispitivanju je sudjelovalo 38 studenata preddiplomskog studija sestrinstva. Ispitivanje je provedeno upotrebom validiranog znanstvenog upitnika „Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava“ (UZRPKIS) sastavljenog od 33 pitanja koja se ocjenjuju bodovima na Likertovoj ljestvici od 1 do 5, pri čemu ponuđeni odgovori imaju različita značenja.

Rezultati: Čak 97,4% studenata nikada ne otkriva tajni PIN bankovne kartice, a jednak postotak je i onih koji nikada ne odgovaraju na mailove nepoznatih pošiljatelja. Nažalost, samo 73,7% nikada neće otvoriti nepoznati privitak poslan mailom, 23,7% ispitanika rado će podijeliti pristupne podatke računalu, dok će se gotovo polovica, njih 44,7%, redovno prijaviti na račun e-pošte na javnom mjestu. Njih 63,2% misli da će mu možda netko ukrasti novac s bankovnog računa, a 26,4% prilično su ili potpuno uvjereni da će im netko ukrasti identitet na internetu. Porazan je podatak da čak 42,1% nikada ili gotovo nikada ne zaključava računalo bez nadzora, a njih troje (7,9%) nikada se ne odjavljuje s računala nakon završetka rada. Od šest subskala koje su obrađene, u dvije subskale interval odgovora lošiji je od referentnog istraživanja, dok su u četiri subskale pulski studenti pokazali bolje poznavanje računalne tehnologije.

Zaključak: Uspoređujući obrađeno istraživanje s prijašnjim istraživanjem, može se zaključiti kako se studenti preddiplomskog studija sestrinstva iz Pule ne ponašaju rizičnije na internetu od prosjeka, ali lakše odaju pristupne podatke računalu. Pozitivno je što su svjesniji važnosti zaštite svojih podataka te da su komunikacijski kanali nesigurni, ali svejedno prevelik je broj iznimaka koji kvare ukupan rezultat. Također, svjesniji su važnosti pravilne pohrane podataka.

Ključne riječi: internet, rizično ponašanje, zaštita podataka, sigurnost i privatnost na internetu

# 8. SUMMARY

Objectives: The aim of the research was to check upon the potential risky behaviour of nursing students in Pula by an anonymous opinion poll in which they were asked about the level to which they were familiar with the safety of Internet use and the preservation of personal information. Based on the obtained results, and in comparison to the reference research, i.e. the average Internet user, it can be concluded who is under potential risk while using the Internet and to what extent.

Study design: Cross-sectional study

Respondents and methods: There were 38 students of the university undergraduate study of nursing participating in this research. The research was conducted by using the validated questionnaire „Questionnaire on the knowledge and risky behaviour of information system users“ which consists of 33 questions evaluated by points on a five-point Likert scale. The answers offered have different meanings.

Results: As many as 97.4 % of students never reveal their secret bank card pin, and the same amount of them never answers to emails sent by unknown senders. Unfortunately, only 73.7 % of them would never open an unknown attachment sent by email. There are 23.7 % of respondents who would happily share their computer access data, while almost half of them, or 44.7 %, regularly log in to their email account in a public place. As many as 63.2 % of them think that someone could steal money from their bank account, while 26.4 % of them are quite or completely sure that someone could steal their identity on the Internet. It is a devastating data that even 42.1 % of them never or almost never lock their unattended computers, while three of them (7.9 %) never log out of their computers after finishing work. Out of the six processed subscales, there are two subscales where the answer interval is worse than in the reference research, while in the remaining four subscales the Pula students show a better understanding of computer technology.

Conclusion: By comparing the processed research to the former one it can be concluded that students of the undergraduate study of nursing in Pula do not behave riskier on the Internet than the average student, but they reveal their computer access data more easily. It is positive that they are aware of the importance of their personal data protection, and that communication channels are unsafe, but there are still a large number of exceptions that ruin the result. They are also more aware of the importance of correct data storage.

Key words: Internet, risky behaviour, data protection, safety and privacy on the Internet

# 9. LITERATURA


1. http://www.phy.pmf.unizg.hr/~dandroic/nastava/rm/spajanje_na_internet.pdf
2. https://hr.wikipedia.org/wiki/internet
3. https://informatika.buzdo.com/
4. https://lmonidc.weebly.com/povezivanje-na-internet.html
5. www.sigurnostnainternetu.hr
6. https://sites.google.com/site/sigurnostizastitanainternetu/prednosti-i-nedostaci-interneta
7. K. D. Mitnick, The Art of Deception - Controlling the Human Element of Security, John Wilwy & Sons, 2002.
8. M. A. Sasse, S. Brostoffand, and D. Weirich, "Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security" BT Technology Journal, vol. 19, pp. 122–131, July 2001.
9. S. Williams and S. Akanmu, "Relationship between Information Security Awareness and Information Security Threats", IJRCM, vol.3, pp. 115-119, August 2013.
10. K. Solic, H. Ocevcic and D. Blazevic, "Survey on Password Quality and Confidentiality", Automatika, vol. 56, Juny 2015.
11. Međunarodna asocijacija za medicinsku informatiku, Radna grupa 1: Preporuke Međunarodne asocijacije za medicinsku informatiku o edukaciji iz zdravstvene i medicinske informatike. Bilten Hrvatskog društva za medicinsku informatiku, posebno izdanje 2001; pp. 11
12. L. Bilić-Zulle, M. Petrovečki, Evaluation of Medical Informatics curriculum at the Rijeka University School of Medicine in Croatia. Stud Health Technol Inform, pp. 90-91, Rijeka 2002.
13. T. Velki, K. Solic and K. Nenadic, „Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS)", Psihologijske teme, vol. 24, pp. 401-424, December, 2015.
14. T. Velki, K. Solic and H. Ocevcic, "Development of Users' Information Security Awareness Questionaire (UISAQ) - Ongoing Work", Proceedings IEEE MIPRO, (Opatia), pp. 1417-1421, May 2014.
15. K. Šolić, T. Velki, T. Galba, „Empirical study on ICT system's users risky behavior and security awareness"//MIPRO Proceedings, pp. 1623-1626, Rijeka, 2015.

## Popis slika



## Popis grafikona



## Popis tablica

# 10. ŽIVOTOPIS

Ime i prezime: Rozi Slacki

Datum i mjesto rođenja: 21. veljače 1991. u Puli

Adresa: Splitska 2, Pula

Mobitel: 095/3977475

E-mail: rozislacki21@gmail.com

Obrazovanje:

- Osnovna škola Šijana 1997. – 2005. god.
- Srednja medicinska škola Pula 2005. – 2010. god.
- Preddiplomski studij sestrinstva Osijek – Pula 2014. god.