# Ispitivanje svjesnosti srednjoškolaca Medicinske škole u Osijeku o privatnosti i zaštiti na Internetu

**Vojnović, Nemanja**

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**
**MEDICINSKI FAKULTET OSIJEKA**

**Sveučilišni preddiplomski studij sestrinstva**

**Vojnović Nemanja**

# ISPITIVANJE SVJESNOSTI SREDNJOŠKOLACA MEDICINSKE ŠKOLE U OSIJEKU O PRIVATNOSTI I ZAŠTITI NA INTERNETU

**Završni rad**

**Osijek, 2017.**

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**
**MEDICINSKI FAKULTET OSIJEKA**

**Sveučilišni preddiplomski studij sestrinstva**

**Vojnović Nemanja**

# ISPITIVANJE SVJESNOSTI SREDNJOŠKOLACA MEDICINSKE ŠKOLE U OSIJEKU O PRIVATNOSTI I ZAŠTITI NA INTERNETU

**Završni rad**

**Osijek, 2017.**

Rad je ostvaren u Medicinskoj školi Osijek

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

Rad sadrži: 35 listova , 7 tablica i  1 sliku

**Predgovor**

Zahvaljujem se mentoru doc. dr. sc. Krešimiru Šoliću koji me je svojim znanjem, iskustvom, idejama i smjernicama motivirao tijekom pisanja završnoga rada. Želim zahvaliti Medicinskoj školi Osijek i profesorici informatike Vesni Suvali na pomoći tijekom provođenja anketiranja, te mojoj obitelji na pruženoj podršci, razumijevanju i pomoći tijekom školovanja

I. **SADRŽAJ**

## II. POPIS TABLICA

## III. POPIS KRATICA

ARPANET – Agencija za napredne istraživačke projekte (od engl. Advanced Research Projects Agency, net od engl. Network)

WWW / World Wide Web – „svjetska mreža“

CERN - Europsko vijeće za nuklearna istraživanja (od engl. The European Organization for Nuclear Research)

CARNet – Hrvatska akademska i istraživačka mreža (od engl. Croatian Academic and Research Network)

PIN - tajni osobni broj bankovne kartice (od engl. Personal Identification Numbe)

e-pošta – elektronička pošta (od engl. Electronic mail)

UZPK - Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava

# 1.UVOD

## 1.1 Povijest interneta

Povijest Interneta započinje 1969. godine stvaranjem računalne mreže ARPANET (Agencija za napredne istraživačke projekte, net od engl. network) koju je stvorilo američko Ministarstvo odbrane s ciljem povezivanja određenog broja računala u SAD-u radi ostvarivanja vojne nadmoći nad Sovjetskim savezom tijekom Hladnog rata (1). Sljedeći je korak bilo stvaranje mreže sačinjene od više mreža koja bi funkcionirala i ako dio komunikacijskog sustava bude uništen u slučaju vojnog sukoba. Iako je Internet nastao kao rezultat vojnih potreba, daljnjim razvojem odlučili su komercijalizirati uporabu Interneta tako da su devedesetih godina prošloga stoljeća mnogi dobavljači internetskih usluga izgradili svoje mreže (2).

Današnji izgled Interneta nastao je revolucionarnim izumom internetskog programa World Wide Web kojeg su 1990. godine razvili engleski programer Tim Barners-Lee i Robert Cailliau u CERN-u (Europsko vijeće za nuklearna istraživanja) u Švicarskoj (3). World Wide Web temeljio se na programskom jeziku koji je pretvarao tekst, slike i druge izvore u tzv. hipertekst koji su drugi mogli čitati pomoću WWW preglednika (4,5). Internet kao svjetski sustav međusobno povezanih računalnih mreža smatra se jednim od najvećih otkrića modernog čovječanstva. Ove je godine navršio 49 godina postojanja, a počeci u Hrvatskoj vežu se za 1991. kad je osnovan CARNet (Hrvatska akademska i istraživačka mreža) kojemu je tad glavni zadatak bio spojiti znanstvenike u Hrvatskoj s ostatkom svijeta, a već do 2012. godine u Hrvatskoj je bilo registrirano 2,7 milijuna korisnika (6).

## 1.2 Internet danas

Internet nosi naziv *mreža svih mreža* jer se sastoji od milijuna akademskih, poslovnih, kućnih i vladinih mreža koje međusobno razmjenjuju informacije te omogućuju prijenos velike količine podataka (6). Svi oblici informacija (slika, zvuk, tekst) u digitaliziranom se obliku pohranjuju i prenose između korisnika. Dalekosežne su posljedice njegove primjene u svim granama ljudskoga djelovanja. Tako je Internet u ekonomiji omogućio elektroničko bankarstvo i poslovanje, oglašavanje i katalošku prodaju, u kulturi i obrazovanju

pristup obrazovnim sadržajima, virtualnim knjižnicama i muzejima, u znanosti pristup bazama podataka i trenutačnu razmjenu najnovijih spoznaja, u medicini dijagnostiku bolesti te vođenje zahvata na daljinu (7). Najnovije primjene Interneta usmjerene na digitalnu distribuciju radijskih i televizijskih programa, glazbe, filma, knjiga, računalnih igara, za govornu komunikaciju i uspostavu videokonferencija dokaz su današnjih tendencija ujedinjavanja različitih platformi za distribuciju i razmjenu informacija (6).

Razvojem informacijske i komunikacijske tehnologije, Internet je postao osnova današnje komunikacije. No, unatoč svim prednostima koje donosi, istovremeno uzrokuje rizik za osobnu sigurnost i privatnost korisnika. Napredne tehnologije omogućavaju razvoj novih usluga u informacijsko-komunikacijskoj mreži što pogoduje razvoju informacijskog društva i stvaranja trenda personalizacije koji omogućuje proizvođačima novih aplikacija uslugu prilagođavanja svakom pojedinom korisniku. Personalizacija omoguće bolju uslugu no od korisnika zahtijeva znatnu količinu osobnih podataka pri čemu može doći do povrede privatnosti (7). Sveprisutnost Interneta u svakodnevnom životu uzrokovala je da virtualni svijet postane dio stvarnog svijeta, a da ljudi ponekad toga nisu ni svjesni. Današnja djeca nose naziv „digitalna generacija“ jer već od dvije godine starosti koriste moderne uređaje za igru, gledanje videa i zabavu (8). Takav trend nosi i pozitivne i negativne strane. Pozitivne su strane postojanje i korištenje aplikacija uz koje dijete brže uči i razvija kognitivne funkcije dok su negativne strane te što takav oblik i način odrastanja kod djeteta može izazvati niz problema, od izolacije i problema s društvenom prilagodbom do ovisnosti o Internetu. Kako odrastaju, djeca se sve bolje razumiju u suvremenu tehnologiju tako da im je lako izmanipulirati roditelje oko svoje aktivnosti na Internetu (9).

Osim što Internet sadrži korisne informacije također je izvor nasilnog sadržaja, govora mržnje, grubosti, vulgarnosti i sl. Pojavom širokopojasnog Interneta (način povezivanja na internet koji omogućuje velike brzine prijenosa podataka) svakom računalu omogućen je pristup Internetu, čak i prijenosnim računalima u pokretu, putnim računalima u automobilu ili pokretnim (mobilnim) telefonima dok se neki uređaji povezuju optičkim kabelima ili satelitskom vezom (4).

### 1.3 Cyber kriminal

Cyber kriminal (od engl. Cybercrime) relativno je nov pojam, a predstavlja oblik kriminalnog ponašanja kod kojeg se uz pomoć kompjuterske tehnologije, Interneta i

informacijskih sustava omogućava izvršenje krivičnog djela gdje se računalo i računalna mreža upotrebljavaju kao sredstvo ili cilj izvršenja. Internet obiluje kriminalnim aktivnostima u rasponu od digitalnog piratstva, narušavanja koncepta autorskih prava „skidanja“ (od engl. Download) glazbe, filmova, knjiga, igrica do trgovine oružjem, ljudima, identitetima, ljudskim organima sve do pornografije, prostitucije, krađe novca s bankovnih računa i sl. Kada je pojedinac cilj cyber kriminala, računalo se smatra alatom, a ne ciljem. Iskorištavaju se ljudske slabosti poput stranica koje inače pretražuje te se tako dolazi do važnih podataka. Oštećenje koje nastaje psihološko je i neopipljivo što otežava pravni postupak protiv počinitelja čak i kada se zna njegov identitet (10).

Najpoznatiji način prijevare je takozvano „pecanje“ (od engl. Phishing), a predstavlja mrežnu krađu identiteta u kojem pošiljatelj navodi žrtvu da otkrije osobne informacije (obično financijske) na lažnoj internetskoj stranici. Poruka koja predstavlja „udicu“ (od engl. Hook) može izgledati kao obavijest iz banke, zahtjev policije, internetske trgovine i sl., što bi moglo navesti žrtvu da klikne na poveznicu. Izgled, adresa i sadržaj lažne internetske stranice do koje dovodi poveznica su podosta autentične originalnoj stranici, ali lokator sadržaja (od engl. Uniform Resource Locator – URL) je drukčiji (11). Brojke Phishinga u porastu su svakim danom. U 2005. godini ukupan broj prijavljenih prijevara bio je 173063 da bi taj broj u 2016. godini iznosio 1380432. Također je poznata zloupotreba neželjene e-pošte (od engl. Spam) što predstavlja svaku poruku koja je distribuirana masovno bez zahtjeva korisnika. U spamu pošiljatelj šalje bezbrojne poruke korisnicima u kojima reklamira proizvode, lažne osvojene nagrade, privatne stranice i privatne poruke koje vode do stranica s pornografskim sadržajem i sl. jer će se u milijunima primatelja gotovo sigurno naći pojedinac koji će naručiti proizvod ili kliknuti lažnu stranicu što može daljnje dovesti do gubitka privatnih podataka (12,13). No opasnost ne prijeti samo na Internetu. Postoje određene skupine koje prate društvene mreže na kojima je prisutno sve više populacije gdje izlažu svoje privatne podatke od adrese stanovanja do imovinskog stanja, načina života, broja telefona i potencijalno su izloženi riziku da postanu meta otmice, krađe i silovanja. Dok odrasli sami odgovaraju za svoju nepromišljenost, posljedice po djecu mogu biti katastrofalne jer su lakovjernija te mogu postati žrtve cyber nasilja.

### 1.4 Sigurnost i privatnost

Sigurnost na Internetu označuje tajnost i cjelovitost osobnih podataka, sigurnost

vlastitog računala, web i mail prometa. Preko raznih načina prijevare, hakerskih napada i malicioznog softvera (računalnog programa s ilegalnom namjerom) podaci korisnika mogu biti kompromitirani. Za smanjenje rizika od spomenutog, potrebno je povećanje svijesti korisnika o potencijalnim prijetnjama na Internetu te određena količina znanja, informatičke pismenosti, informiranosti te odgovornosti u smislu održavanja računala i mreže kako bi se izbjegle spomenute situacije. Korisnici na Internetu postaju sve nesmotreniji i neoprezniji jer često nisu niti svjesni potencijalnog rizika kojemu su izloženi. Prema općim zahtjevima informacijske sigurnosti, potrebno je postići stanje povjerljivosti, cjelovitosti te raspoloživosti podatka, a ono se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom (14).

Podatke je potrebno zaštititi na odgovarajući način, kroz zaštitu komunikacijskih kanala kojima se prenose podaci, zaštita pohrane tih podataka, kontrola pristupa osoba koje te podatke posjeduju i koriste. Tehnička rješenja fizičke i programske zaštite uz razvijene sigurnosne procedure i automatizaciju sigurnosnih kopija danas su na visokoj razini, međutim utjecaj korisnika na sigurnost, iako je znatna, tek je zadnjih godina prepoznata, a rješenja problema kontrole i edukacije korisnika tek su u zasnivanju (14).

Postojala je ideja o zakonima koji bi zaštitili djecu na Internetu no upravo zbog svoje raširenosti, tehnički je postalo nemoguće u potpunosti nadzirati Internet. Kako tehnologija napreduje, ljudi se sve više oslanjaju na Internet kako bi pohranili neke osobne podatke kao što su podaci o kreditnoj kartici i sve dok je tako, kriminalci će pokušavati ukrasti te podatke. Cyber kriminal postaje sve više prijetnja ljudima širom svijeta i potrebno je podizanje svijesti o tome kako se informacije štite te koje taktike kriminalci koriste kako bi se mogle ukrasti te informacije. Godišnje se provede 1,5 milijuna cyber-napada što znači da je to dnevno više od 4000 napada, odnosno 170 napada svaki sat (15). Svatko tko koristi Internet iz bilo kojeg razloga može biti žrtva zbog čega je važno biti svjestan kako se zaštititi na Internetu.

Prvo sustavno istraživanje pomoću validiranog upitnika kao znanstvenog instrumenta mjerenja napravljeno je prije tri godine u Hrvatskoj (16,17) na srednjoškolskoj populaciji. Cilj je bilo dobiti neke nove zaključke o potencijalno rizičnom ponašanju i svijesti o sigurnosti među učenicima srednjih škola. Sudionici te studije bili su sredjnoškolci iz triju različitih škola: ekonomska škola, trgovačka škola i gimnazija. U daljnjem tekstu koristit će se rezultati i podaci iz navedenog istraživanja.

## 2. CILJEVI ISTRAŽIVANJA

Ciljevi su ovog istraživanja validiranim upitnikom ispitati stupanj znanja o pitanjima informacijske sigurnosti i privatnosti među učenicima Medicinske škole Osijek te ispitati koliko je njihovo ponašanje na Internetu potencijalno rizično.

# 3. ISPITANICI I METODE

## 3.1. Ustroj studije

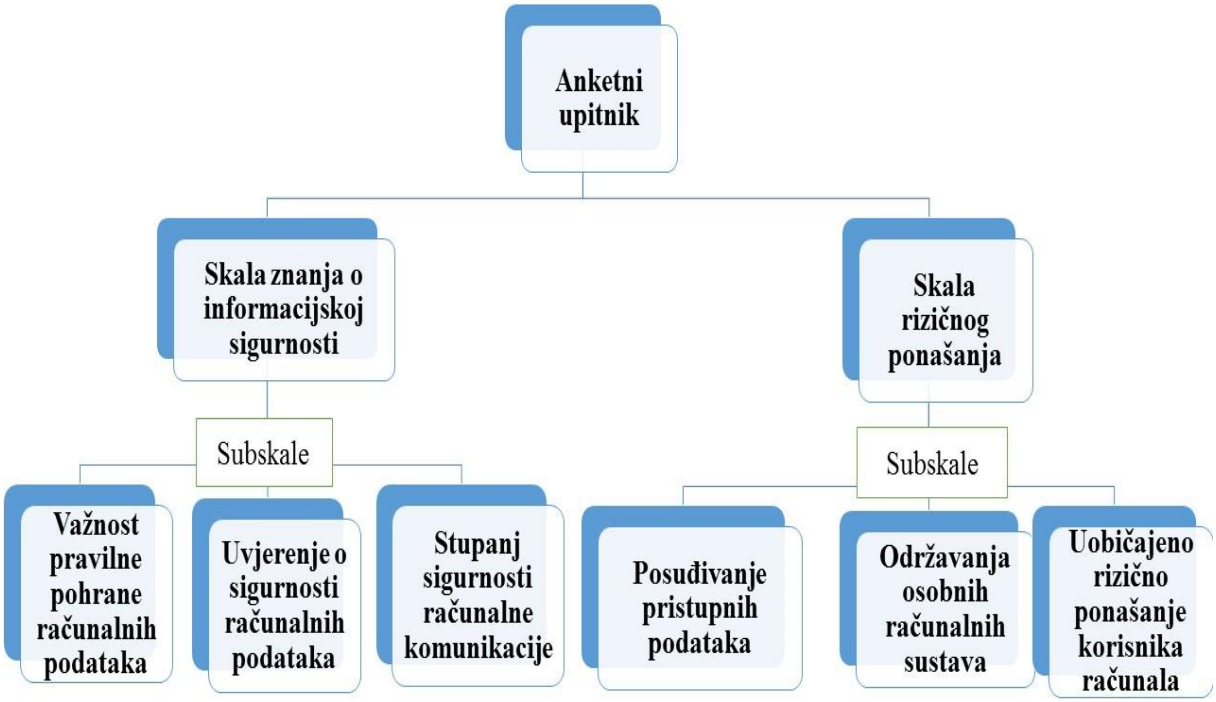
Provedeno je istraživanje ustrojeno kao presječno istraživanje.

## 3.2. Ispitanici

Ispitanici su bili učenici Medicinske škole Osijek, prvog i drugog razreda, svih dobnih skupina, koji su pristali sudjelovati u istraživanju. Istraživanje je provedeno tijekom svibnja 2017. godine. Sudjelovala su dva prva razreda i jedan drugi razred.

## 3.3. Metode

Kao instrument istraživanja korišten je validirani znanstveni upitnik Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK) koji se sastoji od 33 pitanja grupiranih u šest subskala. Odgovori se procjenjuju bodovima na Likertovoj skali od 1 do 5 pri čemu ponuđeni odgovori imaju različita značenja (npr. učestalost, stupanj sigurnosti, stupanj uvjerenja, stupanj važnosti te sigurnost osobnih podataka). Autori navedenog upitnika su Krešimir Šolić, Tena Velki i Hrvoje Očevćić, znanstvenici sa sveučilišta u Osijeku. Za korištenje upitnika dobivena je dozvola autora te upute o načinu korištenja istoga. Primjenjen je i anketni list s demografskim podacima (dob, spol, razred, zanimanje) i pitanje o odavanju zaporke za račun elektroničke pošte radi analize i procjene. Anketa je bila anonimna. Svi ispitanici su dobili Obavijest ispitanika o istraživanju te kada izraze i potpišu suglasnost o istraživanju bit će pojašnjeno kako ispuniti upitnik. To je istraživanje dio projekta „Safer Internet Centre Croatia: Making internet a good and safe place“ , Agreement Number: INEA/CEF/ICT/A2015/115320 financiranog od strane Europske Komisije. Projekt vodi Centar za nestalu i zlostavljanju djecu te je za istraživanje ishođena dozvola institucija na kojima će se provoditi uz potvrdu o etičnosti ispitivanja (18).




**Slika 1.** Prikaz skala i subskala Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava

### 3.4. Statističke metode

Za statističku obradu podataka rabljen je program MedCalc for Windows (Version 17.8, MedCalc Software bvba, Mariakerke, Belgium). Rezultati ispitivanja su prikazani tabelarno. Kategorijski podaci predstavljeni su apsolutnim i relativnim frekvencijama. Numerički su podatci opisani aritmetičkom sredinom i standardnom devijacijom u slučaju raspodjele koje slijede normalu, odnosno medijanom i interkvartilnim rasponom u slučaju kada ne slijede normalnu raspodjelu. Povezanost kategorijskih varijabli testirat će se Hi-kvadrat testom, po potrebi Fisherovim egzaktnim testom. Razlike numeričkih varijabli su testirane Studentovim T- testom. Vrijednosti dobivene u statističkoj analizi smatrat će se značajnim ako su manje od $\alpha=0,05$

### 3.5 Etička načela

Prije provedbe istraživanja dobivena je suglasnost Centra za nestalu djecu i etičkoga povjerenstva Medicinske škole Osijek.

Ispitanici su u istraživanju sudjelovali dobrovoljno, nakon što su im usmenim i pisanim putem pružene informacije o temi, svrsi i ciljevima istraživanja. Prije ispunjavanja upitnika ispitanici su potpisali suglasnost o pristanku na sudjelovanje u istraživanju. Podaci su prikupljeni anonimnim upitnikom u sklopu nastave informatike te je svim ispitanicima pri svakom odsječku bila zajamčena anonimnost, odnosno podatci dobiveni anketnim upitnikom ni na koji se način nisu mogli povezati s osobnim podatcima ispitanika.

# 4. Rezultati

## 4.1 Demografske osobine ispitanika

Statističkom analizom obrađeni su podaci prikupljeni od 92 učenika Medicinske škole Osijek. Pretežito je bilo učenika od 15 i 16 godina, a značajno manje njih od 17 godina (Hi-kvadrat test, P < 0,001) (**Tablica 1.**).

Od ukupnog broja ispitanika, značajno je manje muških učenika (Hi-kvadrat test, P < 0,001) (**Tablica 1.**).

**Tablica 1**. Ispitanici prema dobnim skupinama

| | | **Broj (%) učenika** | **P*** |
|---|---|---|---|
| **Dob kategorije** | **15 godina** | 44 (47,8) | <0,001 |
| | **16 godina** | 41 (44,5) | |
| | **17 godina** | 7 ( 7,6 ) | |
| **Spol** | **M** | 15 (16,3) | <0,001 |
| | **Ž** | 77 ( 83,6) | |
| | **Ukupno** | 92 (100,0) | |

***Hi-kvadrat test**

Iz **tablice 2**. može se uočiti kako je bilo nešto više ispitanika iz prvoga razreda. (Hi-kvadrat test, P = 0,067) (**Tablica 2**).

**Tablica 2.** Ispitanici prema razredima

| | | **N** | **%** | **P*** |
|---|---|---|---|---|
| **Razred** | **Prvi razred** | 55 | 59,7 % | 0,067 |
| | **Drugi razred** | 37 | 40,2 % | |
| | **Ukupno** | 92 | 100,0 % | |

***Hi-kvadrat test**

### 4.2. Frekvencija odgovora na pojedino pitanje

U tablici frekvencija odgovora na pojedina pitanja o učestalosti određenog ponašanja može se uočiti kako je veliki postotak njih u pitanjima 1 , 3, 4, 5, 11, 12, 13 odgovorilo sa odgovorom *nikad* (**Tablica 3**.).

**Tablica 3.** Frekvencija odgovora na pitanja koja ispituju

***obrnuto kodirana pitanja**

| **Pitanje** | Broj (%) odgovora na pojedino pitanje o učestalosti | | | | | |
|---|---|---|---|---|---|---|
| | nikad | rijetko | ponekad | često | uvijek | ukupno |
| **p1* Posuđivanje zaporki / lozinki** | 76 (82,6) | 11 (11,9) | 3 (3,2) | 0 | 2 (2,1) | 92 (100,0) |
| **p2* Posuđivanje pristupnih podataka za kućno računalo** | 38 (41,3) | 26 (28,2) | 17 (18,4) | 6 (6,5) | 5 (5,4) | 92 (100,0) |
| **p3* Posuđivanje zaporke za pristup e-mail adresi** | 71 (77,1) | 16 (17,3) | 5 (5,4) | 0 | 0 | 92 (100,0) |
| **p4* Posuđivanje PIN-a debitne/kreditne kartice** | 88 (95,6) | 3 (3,2) | 1 (1,1) | 0 | 0 | 92 (100,0) |
| **p5* Otkrivanje pina (tijekom plaćanja karticom u trgovini** | 89 (96,7) | 2 (2,1) | 1 (1,1) | 0 | 0 | 92 (100,0) |
| p6 Korištenje različitih zaporki za različite sustave (mail, računalo, facebook itd.) | 8 (8,6) | 21 (22,8) | 18 (19,5) | 17 (18,4) | 28 (30,4) | 92 (100,0) |
| p7 Održavanje zaštite kućnog računala / nadogradnja antivirusnih programa | 7 (7,6) | 22 (23,9) | 23 (25,0) | 18 (19,5) | 22 (23,9) | 92 (100,0) |
| p8 Vršenje nadogradnje programa i operativnog sustava | 11 (11,9) | 25 (27,1) | 29 (31,5) | 15 (16,3) | 12 (13,0) | 92 (100,0) |
| **p9* Instaliranje nepoznatih / neophodnih programa** | 32 (34,7) | 39 (42,3) | 17 (18,4) | 3 (3,2) | 1 (1,1) | 92 (100,0) |
| **p10* Postavljanje osobnih podataka na društvenim mrežama** | 47 (51,0) | 30 (32,6) | 11 (11,9) | 4 (4,3) | 0 | 92 (100,0) |
| **p11* Odgovaranje na mail nepoznatim pošiljateljima** | 82 (89,1) | 8 (8,6) | 2 (2,1) | 0 | 0 | 92 (100,0) |
| **p12* Otvaranje priloga od nepoznatih pošiljatelja** | 69 (75,0) | 17 (18,4) | 4 (4,3) | 1 (1,1) | 1 (1,1) | 92 (100,0) |
| **p13* Slanje ili prosljeđivanje lančanih mailova** | 76 (83,6) | 6 (6,5) | 5 (5,4) | 3 (3,2) | 2 (2,1) | 92 (100,0) |
| p14 (Korištenje više e-mail adresa) | 41 (44,5) | 13 (14,1) | 14 (15,2) | 9 (9,7) | 15 (16,3) | 92 (100,0) |
| **p15* (Prijavljivanje na e-mail ili facebook sa javnih mjesta)** | 9 (9,7) | 22 (23,9) | 13 (14,1) | 26 (28,2) | 22 (23,9) | 92 (100,0) |
| p16 ( Odjavljivanje sa informacijskog sustava pri završetku rada – u školi, poslu itd.) | 9 (9,7) | 23 (25,0) | 13 (14,1) | 25 (27,1) | 22 (23,9) | 92 (100,0) |
| p17 ( Zaključavanje računala prilikom odlaska na toalet ili pauzu ) | 4 (4,3) | 9 (9,7) | 7 (7,6) | 15 (16,3) | 57 (61,9) | 92 (100,0) |

U tablici frekvencije odgovora na pitanja iz znanja i svjesnosti o stupnju sigurnosti računalne komunikacije ističu se se pitanje o važnosti bezuvjetnog čuvanja svojih zaporki i pitanja o čuvanju USB-a sa važnim podacima od krađe na koja je veliki postotak njih odgovorio *izrazito važno* (**Tablica 4.**).

**Tablica 4.** Frekvencija odgovora na pitanja koja ispituju znanje i svjesnost (nastavak na sljedećoj stranici)

| **Pitanje** | Broj (%) odgovora na pojedino pitanje o stupnju sigurnosti | | | | | |
|---|---|---|---|---|---|---|
| | potpuno nesigurno | prilično nesigurno | ne znam | prilično sigurno | potpuno sigurno | ukupno |
| **P18* Dopisivanje putem e-maila** | 2 (2,1) | 40 (43,4) | 29 (31,5) | 21 (22,8) | 0 | 92 (100,0) |
| **P19* Komunikacija putem društvenih mreža** | 2 (2,1) | 23 (25,0 ) | 16 (17,3) | 44 (47.82%) | 7 (7,6) | 92 (100,0) |
| **P20* Komunikacija mobitelom (razgovori, SMS)** | 15 (16,3) | 50 (54,3) | 17 (18,4) | 10 (10,8) | 0 | 92 (100,0) |
| **P21* Komunikacija žičnim telefonom** | 12 (13,0) | 46 (50,0) | 24 (26,0) | 6 (6,5) | 3 (3,2) | 92 (100,0) |
| **P22* Komunikacija putem interenta (npr. Skype, Viber)** | 2 (2,1) | 32 (34,7) | 28 (30,4) | 29 (31,5) | 1 (1,1) | 92 (100,0) |
| | Broj (%) odgovora na pojedino pitanje o uvjerenju | | | | | |
| | nisam uvjeren/a | možda | ne znam | prilično | potpuno | ukupno |
| P23 Krađa podataka sa računala u školi | 24 (26,0) | 30 (32,6) | 15 (16,3) | 21 (22,8) | 2 (2,1) | 92 (100,0) |
| P24 Krađa privatnih poruka sa kućnog računala | 31 (33,6) | 28 (30,4) | 15 (16,3) | 15 (16,3) | 3 (3,2) | 92 (100,0) |
| P25 Krađa privatnih podataka sa mob. Uređaja | 17 (18,4) | 32 (34,7) | 9 (9,7) | 27 (29,3) | 7 (7,6) | 92 (100,0) |
| P26 Krađa novca sa računa u banci | 36 (39,1) | 18 (19,5) | 16 (17,3) | 15 (16,3) | 7 (7,6) | 92 (100,0) |
| P27 Krađa identiteta na internetu (npr. facebook, e-mail) | 15 (16,3) | 21 (22,8) | 16 (17,3) | 33 (35,8) | 6 (6,5) | 92 (100,0) |

| | Broj (%) odgovora na pojedino pitanje o važnosti | | | | | |
|---|---|---|---|---|---|---|
| | potpuno nevažno | prilično nevažno | ne znam | prilično važno | izrazito važno | ukupno |
| P28 Izraditi pričuvnu kopiju podataka | 2 (2.1) | 1 (1.1) | 15 (16,3) | 43 (46,7) | 30 (32,6) | 92 (100,0) |
| P29 Provjeriti tuđi USB stick od virusa | 1 (1.1) | 3 (3,2) | 14 (15,2) | 34 (36,9) | 40 (43,4) | 92 (100,0) |
| P30 Bezuvjetno čuvanje svojih zaporki | 0 | 0 | 7 (7,6) | 21 (22,8) | 64 (69,5) | 92 (100,0) |
| P31 Periodički mijenjati zaporke novima | 1 (1,1) | 7 (7,6) | 12 (13.04%) | 37 (40,2) | 34 (36,9) | 92 (100,0) |
| P32 Odvajati podatke prikupljene za školu od privatnih podataka | 1 (1.1) | 12 (13,0) | 14 (15.2) | 39 (42,3) | 26 (28,2) | 92 (100,0) |
| P33 Čuvati od krađe svoj USB stick sa važnim podacima | 0 | 1 (1.0) | 7 (7,6) | 21 (22,8) | 62 (67.3) | 92 (100,0) |

***obrnuto kodirana pitanja**

### 4.3. Usporedbe (ovisno o ciljevima)

U tablici broj 5 opisane su usporedbe po subskalama na pitanja koja ispituju znanje i svjesnost prema razredu. Na temelju rezultata, prvi razred je značajno bolji, odnosno manje posuđuju pristupne podatke u odnosu na drugi razred (Studentov T-test, P = 0,049). U ostalim subskalama nema značajne razlike.

**Tablica 5.** Usporedba po subskalama na pitanja koja ispituju znanje i svjesnost prema razredu

| **Subskale** | **Aritmetička sredina (standardna devijacija)** | | P* |
|---|---|---|---|
| | Prvi razred (N=55) | Drugi razred (N=37) | |
| Posuđivanje pristupnih podataka | 4,72 ( 0,31 ) | 4,56 ( 0,46 ) | **0,049** |
| Održavanje osobnih računalnih sustava | 3,19 ( 0,74 ) | 3,37 ( 0,78 ) | 0,266 |
| Uobičajeno rizično ponašanje | 4,26 ( 0,47 ) | 4,11 ( 0,55 ) | 0,165 |
| Stupanj sigurnosti računalne komunikacije | 2,72 ( 0,60 ) | 2,73 ( 0,60 ) | 0,938 |
| Uvjerenje o sigurnosti računalnih sustava | 2,45 ( 0,90 ) | 2,64 ( 1,07 ) | 0,360 |
| Važnost pravilne pohrane podataka | 4,13 ( 0,60 ) | 4,34 ( 0,48 ) | 0,078 |

***studentov T-test**

U tablici broj 6 prikazana je usporedba po subskalama prema spolu. Iz tablice je vidljiva statistički značajna razlika pri čemu je ženski spol u odnosu na muški više uvjeren da postoji realna opasnost da će im netko ukrasti podatke na Internetu (Studentov T-test, P = 0,037)

**Tablica 6.** Usporedba po subskalama na pitanja koja ispituju znanje i svjesnost prema spolu

| **Subskale** | **Aritmetička sredina (standardna devijacija)** | | P* |
|---|---|---|---|
| | Spol | | |
| | Učenici (N = 15) | Učenice (N = 77) | |
| Posuđivanje pristupnih podataka | 4,57 ( 0,31 ) | 4,67 ( 0,39 ) | 0,351 |
| Održavanje osobnih računalnih sustava | 3,03 ( 0,72 ) | 3,31 ( 0,76 ) | 0,191 |
| Uobičajeno rizično ponašanje | 4,35 ( 0,52 ) | 4,17 ( 0,50 ) | 0,208 |
| Stupanj sigurnosti računalne komunikacije | 2,89 ( 0,60 ) | 2,69 ( 0,60 ) | 0,240 |
| Uvjerenje o sigurnosti računalnih sustava | 2,05 ( 0,93 ) | 2,62 ( 0,96 ) | **0,037** |
| Važnost pravilne pohrane podataka | 3,98 ( 0,64 ) | 4,26 ( 0,54 ) | 0,078 |

***studentov T-test**

U tablici broj 7 prikazana je usporedba po subskalama sa prosječnim vrijednostima iz prethodnoga istraživanja (N = 355). Na temelju rezultata, učenici Medicinske škole manje posuđuju pristupne podatke u odnosu na prethodno istraživanje (Studentov T-test, P = 0,006). Vidljiva je statistički značajna razlika o uvjerenju u sigurnost računalnih sustava i važnosti pravilne pohrane podataka, naime učenici Medicinske škole su uvjereniji u mogućnosti krađe podataka i pridaju veću važnost pravilnoj pohrani podataka u odnosu na prethodno istraživanje.

**Tablica 7.** Usporedba po subskalama na pitanja koja ispituju znanje i svjesnost s prosječnim vrijednostima iz prethodnog istraživanja (prosječne vrijednosti, N = 355)

| **Subskale** | **Aritmetička sredina (standardna devijacija)** | | P* |
|---|---|---|---|
| | Vrijednosti na cijelom uzorku (N = 92) | Vrijednosti iz prethodnog istraživanja (N = 355) | |
| Posuđivanje pristupnih podataka | 4,65 ( 0,38 ) | 4,77 ( 0,37 ) | **0,006** |
| Održavanje osobnih računalnih sustava | 3,27 ( 0,76 ) | 3,33 ( 0,82 ) | 0,526 |
| Uobičajeno rizično ponašanje | 4,20 ( 0,51 ) | 4,12 ( 0,58 ) | 0,728 |
| Stupanj sigurnosti računalne komunikacije | 2,74 ( 0,59 ) | 2,67 ( 0,81 ) | 0,437 |
| Uvjerenje o sigurnosti računalnih sustava | 2,53 ( 0,98 ) | 2,27 ( 0,92 ) | **0,018** |
| Važnost pravilne pohrane podataka | 4,21 ( 0,56 ) | 3,86 ( 0,76 ) | **<0,001** |

***studentov T-test**

Na trik pitanje o odavanju zaporke za račun elektroničke pošte radi analize odgovorilo je 86 učenika ( 93,4 % )

## 5. RASPRAVA

Rizično ponašanje srednjoškolaca te njihovo znanje o pitanjima iz područija računale sigurnosti su uspoređena sa rezultatima iz prethodnog istraživanja uzetog kao referentne vrijednosti za srednjoškolce (20). U ponašanju su značajno lošiji pri posuđivanju podataka (P = 0,006) dok su u znanju značajno bolji te pridaju veću važnost pravilnoj pohrani podataka. U ostalim subskalama nije bilo značajne razlike (Tablica 7).

Među ispitanicima Medicinske škole bilo je 93,4% učenika koji su odgovorili na trik pitanje o odavanju zaporke za račun elektroničke pošte radi analize i procjene dok je 77,7 % (N = 355) učenika odgovorilo na to pitanje iz referentnih vrijednosti. Samo 28,8 % (N = 701) odraslih je odgovorilo na to pitanje što je mogući pokazatelj da su odrasli u slučaju sigurnosti svojih podataka skeptičniji i odgovorniji kad je u pitanju odavanje podataka. U studijama je prikazano da mladi korisnici imaju lozinke bolje kvalitete, a slično je s korisnicima koji su tehnički potkovani. Iako je u tom istraživanju visok postotak njih napisao svoju lozinku, u upitniku na pitanje o važnosti periodičnog mijenjanja lozinke njih 36,9 % odgovorilo je da je to izričito važno dok je na pitanje o učestalosti korištenja različitih zaporki za različite sustave (mail, računalo itd.) njih 22,8 % odgovorilo da rijetko koristi različite zaporke (za e-mail, društvene mreže itd.) (Tablica 3). Iako to ne mora biti veliki sigurnosti problem ako osoba nigdje nema lozinku zapisanu nego je pamti, propust nastaje ako netko do te lozinke dođe na drugi način, tada svi sustavi sa istim pristupom bivaju ugroženi. Privatnost ili povjerljivost uz tajnost i dobru kvalitetu lozinke jedna su od važnijih svojstava sigurnosti (21).

U odnosu na spol postoji statistički značajna razlika (P = 0,037) pri čemu je ženski spol u odnosu na muški više uvjeren da postoji realna opasnost kako će im netko ukrasti podatke na Internetu (Tablica 6). S obzirom na današnju popularnost društvenih mreža na internetu velika je količina osobnih podataka dostupna svima. Malo ljudi to zna, ali kada jednom nešto objavite na Internetu, taj podatak uvijek ostaje tamo tj. nikada u potpunosti ne možete povući objavljeno (22). 51,0 % učenika izjavilo je da nikada ne postavljaju osobne podatke na društvene mreže (Tablica 3). Ako pretpostavimo da su učenici iskreno odgovarali na postavljena pitanja, s obzirom da im je osigurana anonimnost, može se reći kako se savjesno ponašaju no realnost je ipak malo drugačija jer ljudi nisu svjesni koliko je Internet postao njihova svakodnevnica.

Društvene mreže potiču na otkrivanje te razmjenu informacije i fotografija putem Interneta a upravo je taj izvor podataka otvorio vrata prevarantima (23,24,25). Uspoređujući podatke koji ispituju znanje i svjesnost prema razredima može se uočiti primjetna razlika kod posuđivanja pristupnih podataka prvoga razreda u odnosu na drugi (P = 0,049), odnosno drugi razred se ponaša rizičnije dok za ostale subskale nema značajne razlike (Tablica 5).

Pogledamo li rezultate frekvencija odgovora na pojedina pitanja o učestalosti određenog ponašanja možemo uočiti kako su ispitanici na prvih pet obrnuto kodiranih pitanja (prva subskala) odgovorili s *nikad,* što predstavlja najbolju ocjenu (Tablica 3) 82,6 % učenika nikada ne posuđuje lozinku prijateljima iz razreda (npr. za vrijeme informatike).

41,3 % njih nikada ne posuđuje pristupne podatke za kućno računalo dok njih 5,4 % uvijek posuđuje. 77,1 % nikada nije dalo pristupne podatke za e-mail adresu svojim prijateljima rođacima. 95,6 % njih nikada ne posuđuje podatke kreditne ili debitne kartice dok njih 96,7 % pokriva PIN prilikom kupovine u trgovini. 41,3 % njih nikada ne posuđuje pristupne podatke za kućno računalo dok njih 5,4 % uvijek posuđuje no na pitanje održavaju li zaštitu kućnog računala nadogradnjom antivirusnog programa 23,9 % ih je odgovorilo da to rijetko rade a njih 7,6 % izjasnilo se da to nikada ne radi (Tablica 3). To je rizični faktor u lancu sigurnosti jer problem ne mora biti fizička krađa PIN-a ili kartice. Sve je veći rizik gubitka PIN-a posebno kod ljudi koji kupuju online i koriste direktno podatke svoje kartice kao način plaćanja. S tom je svrhom bio osmišljen socijalni inženjering, a predstavlja način manipulacije ljudima u svrhu otkrivanja njihovih povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih manipulator inače ne bi mogao doći. Napadači se tom tehnikom služe jer im nije potrebna fizička krađa kartice, a uvjerljivost dobijaju primjerice putem e-mail adrese. Da bi se zaštitili od takvih programa potrebno je koristiti antivirusni program s najnovijom nadogradnjom (26). Na pitanje prijavljivanja na e-mail ili Facebook račun s javnih mjesta 23,9 % odgovorilo je da to uvijek čine (Tablica 3). Bežične mreže (od engl. Wi-Fi) sve su rasprostranjenije širom gradova putem kojih se korisnik spaja jednim klikom na uređaj. Jedan od sofisticiranijih načina za krađu podataka je „Zli blizanac“ (od engl. Evil twin) a predstavlja pristupnu točku (bežičnu mrežu) koja izgleda kao legitimna. Korisnik se na istu spoji no ne može pristupiti na Internet već zapravo izlaže sebe riziku potencijalnom gubitku podataka. Takva vrsta napada može se koristiti za krađu lozinki korisnicima koji ne sumnjaju, bilo praćenjem njihovih veza ili krađe identiteta što uključuje postavljanje lažnih web stranica i privlačenje ljudi tamo (26). 2016. godine zabilježen je napad u Izraelu gdje je pojedinac uspješno preuzeo čitav grad preko lažne bežične mreže. Iako je nakraju uhićen, podatak govori da treba biti oprezan i na mjestima koje

smatramo sigurnim (27).

Na preostalih 16 pitanja koja ocijenjuju znanje učenici su imali zadovoljavajuće rezultate te su pokazali veću razinu znanja u odnosu na referentne vrijednosti (Tablica 4). 54,3 % ih smatra da je komunikacija putem mobilnog telefona (razgovori, SMS) prilično nesiguran način komunikacije. 34,7 % ih smatra da je komunikacija putem Interneta (Skype, Viber itd.) prilično nesiguran način komunikacije. Po pitanju sigurnosti podataka o važnosti i bezuvjetnom čuvanju svojih zaporki 69,5 % učenika odgovorilo da je to izrazito važno, a na pitanje koje se ticalo izrađivanja pričuvne kopije važnih podataka 46,7 % ih je odgovorilo da je prilično važno izraditi pričuvnu kopiju (Tablica 4).

Od različitih opasnosti na internetu možemo se zaštiti i metodom zdravoga razuma. Pojednostavljeno, kao što u svakodnevnom životu ne dajemo osobne podatke i povjerljive dokumente nepoznatim osobama i ne zalazimo u nesigurne dijelove grada noću tako se trebamo ponašati i na Internetu. Treba koristiti njegove sigurne mogućnosti i obraćati pozornost na potencijalno rizično ponašanje. Provedeno istraživanje i primjena validiranog upitnika mogla bi pomoći u planiranju edukacije i poboljšanju sigurnosnih aspekata kod učenika

Dosadašnja istraživanja koja se bave informacijskom sigurnošću pokazali su kako je čovjek čimbenik koji narušava informacijsku sigurnost sustava. Utjecaj korisnika na cjelokupnu sigurnost informacijskog sustava je značajan no kako tehnologija napreduje te je sve više korisnika na internetu, a cyber kriminal je u porastu potrebna su daljnja istraživanja koja će dovesti do novih saznanja o korisnicima i poboljšati postojeći stupanj sigurnosti (27).

# 6. ZAKLJUČAK

Temeljem provedenog istraživanja i dobivenih rezultata mogu se izvesti sljedeći zaključci:

- U usporedbi s referentnim vrijednostima iz prethodnoga istraživanja kod učenika Medicinske škole Osijek postoji statistički značajna razlika u ponašanju dok su u znanju iznadprosječni. Njihovo je ponašanje na Intenetu rizičnije, ali u znanju su znatno bolji

- Učenice su generalno pažljivije i skeptičnije u odnosu na učenike kada je u pitanju krađa privatnih podataka

- Prvi su razredi pažljiviji kad je u pitanju posuđivanje privatnih podataka u odnosu na drugi razred

- Učenici srednjih škola češće otkrivaju svoje lozinke u odnosu na starije

Iako su učenici pokazali odgovarajuću razinu znanja o sigurnosti na internetu, uočena je riskanta razina ponašanja učenika Medicinske škole Osijek u odnosu na referentne vrijednosti. Potrebno je informirati i povećati svijest o mogućim rizicima na internetu te provoditi daljnju edukaciju učenika svih srednjih škola.

## 7. SAŽETAK

**Cilj istraživanja:** Validiranim upitnikom ispitati stupanj znanja o pitanjima informacijske sigurnosti i privatnosti među učenicima Medicinske škole Osijek te ispitati koliko je njihovo ponašanje na Internetu potencijalno rizično.

**Nacrt studije:** Istraživanje je provedeno kao presječno.

**Ispitanici i metode:** U istraživanju su sudjelovali učenici i učenice dva prva i jednog drugog razreda Medicinske škole Osijek. Kao instrument istraživanja korišten je validirani znanstveni upitnik *Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava* koji se sastoji od 33 pitanja koja se procjenjuju bodovima na Likertovoj skali od 1 do 5 pri čemu odgovori imaju različita značenja. Istraživanje je provedeno tijekom svibnja 2017. godine

**Rezultati:** Obradom podataka 92 ispitanika Medicinske škole Osijek primjetna je razlika kako je ženski spol u odnosu na muški više uvjeren da postoji opasnost kako će im netko ukrasti podatke na netu**.** S obzirom na razred prvi razredi su pažljiviji u odnosu na drugi razred kad je u pitanju posuđivanje privatnih podataka. Vidljiva je statistički značajna razlika o uvjerenju u sigurnost računalnih sustava i važnosti pravilne pohrane podataka, naime učenici Medicinske škole su uvjereniji u mogućnosti krađe podataka i pridaju veću važnost pravilnoj pohrani podataka u odnosu na referentne vrijednosti prethodna istraživanja.

**Zaključak:** Iako su učenici pokazali odgovarajuću razinu znanja o sigurnosti na Internetu, uočena je nešto rizičnija razina ponašanja učenika Medicinske škole Osijek u odnosu na referentne vrijednosti. Potrebno je informirati i povećati svijest o mogućim rizicima na internetu te provoditi daljnju edukaciju učenika svih srednjih škola.

**Ključne riječi:** Internet, sigurnost, rizično ponašanje, cyber kriminal, privatnost

## 8. SUMMARY

**Study goal:** The aim of the research was to assess by means of a validated questionnaire the level of the knowledge about the information-technology system and online safety issues associated with privacy among the students of the Medical School in Osijek as well as to make an assessment of the extent to which their behaviour on the Internet is potentially risky.

**Study design:** The conducted study was implemented as a cross – sectional study.

**Research paricipants and methods:** The students of the Medical School in Osijek who took part in the research on the voluntary basis were the classes of the year-one students and one class of the year-two students both female and male respondents. The research was carried out by means of a validated scientific questionnaire " The questionnaire on the knowledge and risky behaviour of the users on information-technology system" (UISAQ) that includes 33 questions/statements divided into six subgroups measured in numerical values/points against a Likert Scale with a range from 1 to 5 where the responses are given different values. The respondents were given a choice of 4 pre-coded statements on demography-associated information. The research was conducted in May 2017.

**Results:** The collected data regarding 92 respondents were processed to indicate that the female respndents are significantly more aware that their personal details on the Internet might be stolen, as opposed to the male respondends. Statistically, in comparison with the findings of the previous surveys, the students of the Medical School in Osijek behave significantly different with regard to giving their personal details associated with the access to the internet.

**Conclusion:** Although the pupils showed an adequate level of knowledge on Internet safety, the level of behaviour of the students at the Osijek Medical school was noticed relative to the reference values. It is necessary to inform and raise awareness of possible risks on the Internet and to carry out further education.

**Keywords:** Internet, safety, risky behaviour, cybercrime, privacy

## 9. LITERATURA

1. Abbate JA. Inventing the Internet. Cambridge: MIT Press; 1999.

2**.** Douglas CO, Internetworking With TCP/IP. 6th Edition. USA: Prentice Hall; 2000.

3. T. Berners-Lee/CN, HyperText and CERN . WorldWideWeb: Proposal for a HyperText Project, 12 November 1990. Dostupno na adresi: http://www.internet-guide.co.uk/WorldWideWebProposalforaHyperTextProject.html. Datum pristupa stranici: 12.09.2017

4. Leksikografski zavod Miroslav Krleža. Hrvatska enciklopedija. Dostupno na adresi: http://www.enciklopedija.hr/natuknica.aspx?ID=27653#start. Datum pristupa stranici 12.09.2017

5. Kim B.-K. Internationalizing the Internet: The Co-evolution of influence and Technology. 6th ed. Cheltenham, UK and Northampton: Edward Elgar; 2006.

6. Castells MA. Internet galaksija:razmišljanja o Internetu, poslovanju i društvu. 1.izd. Zagreb: Jesenski i Turk; 2003., str.28

7. Al-Gahtani SA, King MA. Attitudes, Satisfaction and Usage: Factors Contributing to Each in the Acceptance of Information Technology. Behavior and Information Technology. 1999;277-297-18.

8. Despotovic ZO, Hossfeld TO, Kellerer WO., Lehrieder FR, Oechsner SI, Michel MA. Mitigating Unfairness In Locality-Aware Peer-To-Peer Networks. International Journal Of Network Management. 2011;21:3-20.

9. Turow JO. Lilach NI. The Internet and the Family 2000: The View From Parents, the View From Kids. From Report Series. No.13, The Annenberg Public Policy Center of the University of Pennsylvania. 2000

10. Moore RO. Cyber crime: Investigating High-Technology Computer Crime. 2. izd. Cleveland, Mississippi: Anderson Publishing. 2005

11. Zulfikar RA. Phishing attacks and countermeasures. U: Stavroulakis PE, Stamp MA, urednik. Handbook of Information and Communication Security. In Stamp, Mark & Stavroulakis (2010) str. 433-448

12. Dragičević D. Kompjuterski kriminalitet i informacijski sustavi. Zagreb: IBS; 2004

13. Cournane AL , Hunt RA. An analysis of the tools used for the generation and prevention of spam. Computers & Security, vol. 23, pp. 154-166, 2004.

14. Narodne Novine 79/07 Zakon o informacijskoj sigurnosti, Osnovne odredbe. (http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, Datum pristupa: 13.09.2017.)

15. Clarke RI. Cyber War. 1 izd. New York: HarperCollins; 2010
16. T. Velki, K. Solic and H. Ocevcic, „Development of Users Information Security Awareness Questionaire (UISAQ) – Ongoing Work“ , Proceedings IEE MIPRO, (Opatia), pp. 1417-1421, May 2014
17. K. Parsons et. Al, „The Human Aspect of Information Security Questionnaire (HAIS-Q): Two further validation studies“, Computer&Security,vol. 66, pp. 40-51, May 2017
18. Centar za sigurniji internet Dostupno na adresi: http://www.csi.hr/ Datum pristupa stranici: 03.08.2017
19. T. Velki, K. Solic and H. Ocevcic, „Empirical study on the risky behavior and security awareness among secondary school pupils – validation and preliminary results“, Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017.
20. K. Solic, H. Ocevcic and D. Blazevic, „Survey on Password Quality and Confidentiality“, Automatika, vol. 56, Juny 2015
21. Summers, G. (2004). Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5.
22. I. Sege. Where everybody knows your name. Boston.com, April 27, 2005.
23. Varga M. Zaštita elektroničkih podataka. Tehnički glasnik. 2011;5;61-73.
24. The Facebook. Privacy policy. Dostupno na: http://facebook.com/policy.php, August 2005. Datum pristupa 10:09:2017
25. Lowry TO. To catch a cyber thief. USA Today, Feb. 17, 1999,
26. Vice video documentaries. Motherboard digital media. Dostupno na: https://motherboard.vice.com/en_us/article/jpgngb/a-hacker-took-over-tel-avivs-public-wi-fi-network-to-prove-that-he-could. Datum pristupa: 13.09.2017
27. Mitnick K. D. The Art of Deception – Controlling the Human Element of Security, John Wilwy & Sons, 2002

## 10. ŽIVOTOPIS

**Ime i prezime:** Vojnović Nemanja

**Datum i mjesto rođenja:** 16.06.1993. Vukovar, Republika Hrvatska

**Adresa:** Vlahe Bukovca 64, Vukovar

**Telefon:** 098 / 9941 / 891

**E-mail:** nvojnovic.vu@gmail.com

**Obrazovanje:**

- 2008. završio Drugu osnovnu školu Vukovar

- 2012. maturirao u Medicinskoj školi Osijek

- 2013. upis na Sveučilišni preddiplomski studij Sestrinstva

## 11. PRILOZI