Ispitivanje privatnosti među studentima studija medicinsko laboratorijske dijagnostike

Martinović, Marina

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
MEDICINSKI FAKULTET OSIJEK
PREDDIPLOMSKI SVEUČILIŠNI STUDIJ MEDICINSKO LABORATORIJSKA DIJAGNOSTIKA

Marina Martinović

ISPITIVANJE PRIVATNOSTI MEĐU STUDENTIMA STUDIJA MEDICINSKO LABORATORIJSKE DIJAGNOSTIKE

Završni rad

Osijek, 2019.

Rad je ostvaren na Medicinskom fakultetu u Osijeku među studentima preddiplomskog studija Medicinsko laboratorijske dijagnostike.

Mentor rada: doc. dr. sc. Krešimir Šolić

Rad ima 28 listova, 3 tablice i 3 slike.

PREDGOVOR

Zahvaljujem mentoru doc. dr. sc. Krešimiru Šoliću, dipl.ing. koji je svojom ažurnošću i brojnim savjetima uvelike olakšao i pomogao pisanje ovoga rada. Zahvaljujem kolegama i svim prijateljima na pomoći, savjetima i podršci tijekom studija. Ponajviše zahvaljujem svojoj obitelji koja me pratila i bodrila kroz čitavo školovanje, kao i svom dečku koji me uvijek nesebično podržavao tijekom studija.

SADRŽAJ

1. Uvod

U današnje je vrijeme internet važan resurs u svim organizacijama te je stoga potrebno posvetiti pozornost računalnoj sigurnosti i svjesnosti. Internet je dostupan svima, no edukacija o njemu nije. U doba nevjerojatne brzine dijeljenja podataka i informacija, činjenica da se osobni podaci vrlo često nađu na meti zlouporabe i krađe nimalo ne začuđuje. Sve se više povećava potreba za korištenjem interneta u svakodnevnom životu te je gotovo nemoguće izbjeći komunikaciju, poslovanje, a samim time i dijeljenje informacija bez interneta. Dobre strane ovakve komunikacije dovode do sve bržeg širenja internetske mreže, ali je zbog toga važno raditi na povećanju sigurnosti i privatnosti svih korisnika interneta.

1.1. Povijest interneta

Počeci interneta sežu u 1960-te godine u vrijeme Hladnog rata kada su se SAD i SSSR natjecali u širenju svoga utjecaja na svijet. Ministarstvo obrane SAD-a osnovalo je Agenciju za napredne istraživačke projekte (ARPA) u sklopu koje je djelovao Ured za tehniku obrade informacija (IPTO). IPTO je financirao istraživanja u području računalnih znanosti pokrećući američka sveučilišta i istraživačke laboratorije na izgradnju strateške komunikacijske mreže koja bi omogućila slanje poruka. U to su vrijeme tri znanstvenika na tri različita mjesta u svijetu neovisno razmišljali o istoj tehnologiji: Leonard Kleinrock bio je prvi koji je razvio temeljne principe „komunikacije paketa*"*. Svoje ideje razvio je u laboratorijima MIT-a 1961. godine te su one predstavile važnu prekretnicu u razvoju interneta. Donald Davies također je mislio da je za postizanje komunikacije između računala potrebna brza izmjena poruka u kojoj se dugačke poruke dijele na manje dijelove koji se šalju odvojeno kako bi se smanjio rizik od zagušenja. Te dijelove nazvao je „paketima*"*, a ta je tehnika dobila naziv „komunikacija paketa". Daviesov dizajn mreže primijenili su znanstvenici ARPA-e. Internet je zapravo nastavak računalne mreže uspostavljene u Sjedinjenim Američkim Državama, koja je povezivala četiri „superračunala" telefonskom mrežom. Ta prva računalna mreža uopće nazvana je ARPANET (ARPA NETwork) i pokrenuta je 1969. godine. Znanstvenici su izgradili ARPANET s namjerom da to bude mreža koja će uspješno raditi i u slučaju da dio mreže bude oštećen. Takav koncept bio je važan vojnim organizacijama koje su proučavale načine da održe komunikacijske mreže u funkciji i u slučaju nuklearnog rata.

Prvotno zamišljen da omogućuje visoku učinkovitost u komunikaciji između istraživačkih centara, sveučilišta i vladinih agencija SAD-a, internet je ubrzo prerastao u internacionalnu mrežu dostupnu svima. Sa sve više sveučilišta i institucija koji su se spajali na ARPANET 1970-ih, korisnici su uvidjeli potrebu razvijanja standarda za put kojim će podaci biti prenošeni internetom (1, 2).

1.2. Internetska mreža

Internet nije jedna računalna mreža. Sastoji se od mnoštva lokalnih, regionalnih i globalnih računalnih mreža međusobno povezanih različitim vezama, telefonskim linijama, optičkim kabelima, mikrovalnim, radijskim i satelitskim vezama. O internetu govorimo kao o cjelini zbog mogućnosti umrežavanja više računala koja međusobno mogu komunicirati na način jasan krajnjem korisniku. Često se kaže da je internet „mreža svih mreža", ali ta izjava nije istinita jer nisu sve mreže dio interneta. Mnoge su mreže u tvrtkama ostale izvan interneta iz praktičnih i sigurnosnih razloga. Pravila koja reguliraju rad računalnih mreža nazivaju se protokoli, a onaj koji koristi internet još od 1973. godine jest TCP/IP protokol (3).

1.3. Internetska mreža u Hrvatskoj

Hrvatska akademska i istraživačka mreža (CARNET) najveća je računalna mreža unutar hrvatske domene *.hr*. Nju je tijekom 1992. godine pokrenulo Ministarstvo znanosti i tehnologije Republike Hrvatske. CARNET nudi pristup internetu i sustavu e-pošte jednak onome koji nude komercijalni davatelji internetskih usluga. Razlika je u tome što Vlada RH omogućuje CARNET-u da studentima, profesorima i ostalim članovima hrvatske akademske i istraživačke zajednice te usluge pruža bez novčane naknade (3).

1.4. Sigurnost na internetu

Javna dostupnost informacijsko-komunikacijskih usluga na internetu, osim što je doprinijela nebrojenim novim mogućnostima za njegove korisnike, istovremeno je uzrokovala i novi rizik za osobnu sigurnost i privatnost korisnika. Jedan od načina smanjivanja rizika jest

povećanje svijesti te edukacija o sigurnosnim pitanjima kod korisnika informacijskih sustava. Današnja sveprisutnost interneta uzrokovala je da i virtualni svijet postane realan dio svačijeg života, no način odnošenja prema osobnim, privatnim podacima daleko se razlikuje u virtualnom i realnom svijetu.

Nove usluge na internetu (aplikacije, elektronički zdravstveni sustav, internetske trgovine, bankarstvo...), koje su svakim danom sve više prisutne i potrebne za održavanje komunikacije, često zahtijevaju od korisnika mnogo, a nerijetko i previše osobnih informacija. Dijeljenjem informacija raste i rizik zlouporabe ili krađe. Dosadašnja istraživanja pokazala su da je čovjek, kao korisnik informacijskih sustava, najkritičniji sigurnosni element u informacijskom sustavu. Istovremeno, ne postoji pouzdan način kojim se mjeri rizičnost čovjekova ponašanja u vidu narušavanja sigurnosti informacijskog sustava. Korisnici informacijsko-komunikacijskih sustava neoprezni su i nesmotreni, često nesvjesni postojećih rizika. Nažalost, njihovo neznanje ne uzrokuje veći oprez prilikom dijeljenja osobnih informacija, već ignoriranje potencijalnih rizika bez razumijevanja opasnosti koje mogu donijeti (4).

1.5. Zaštita osobnih podataka na internetu

Sve učestalije korištenje podataka s interneta potaknulo je pitanje zaštite baze podataka i njihovih sadržaja, odnosno prava njihovih autora. Internet je doveo do uspostavljanja nevidljivog nadzora pomoću uređaja sposobnih da presreću prijenos svih podataka u komunikaciji. Za presretanje podataka putem interneta nije dovoljno biti spojen na računalnu mrežu, već je potrebno imati odgovarajući alat kojim će se moći vidjeti paketi koji se prenose određenim komunikacijskim kanalom od pošiljatelja prema primatelju. Prije stavljanja podataka na internetske servise treba dobro promisliti. Jednom stavljeni podaci na internet zauvijek ostaju tamo. Podaci koji se prenesu na udaljeno računalo, tj. na server, zauvijek ostaju kod vlasnika servera. Danas postoje servisi na internetu koji vraćaju podatke koji su bili objavljeni na internetu prije više od 10 godina (5).

Najpoznatiji internet servisi, odnosno društvene mreže, koji se kod nas trenutno koriste su Facebook i Instagram. Njihova su sučelja jednostavna za korištenje, mogućnosti su iz dana u dan sve veće i načini komunikacije stalno napreduju. Budući da donose mnogo mogućnosti za

samovoljno dijeljenje privatnih informacija, korisnici, pogotovo mlađi, uopće ne razmišljaju o opasnostima dijeljenja istih.

Zaštita osobnih podataka u Republici Hrvatskoj te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka uređuje se Zakonom o provedbi Opće uredbe o zaštiti podataka. Svrha zaštite osobnih podataka zaštita je privatnog života, ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka (6).

1.6. Sigurnost i zaštita korisničkog imena i zaporke

Važno je dobro odabrati korisničko ime i zaporku kako bi se spriječila zlouporaba privatnih podataka. Odabir kvalitetne i sigurne zaporke ponekad nije jednostavan, a od velike je važnosti za većinu platformi kojima se služimo. Opasnosti su mnoge – od toga da nam netko načini financijsku štetu do nešto lakših nematerijalnih krađa koje povrjeđuju privatnost.

1.6.1. Lozinka *(password)*

Zaporka ili lozinka tajna je riječ ili kraći niz slova, brojeva i simbola koji se koriste za provjeru identiteta korisnika kako bi se moglo pristupiti sigurnim podacima ili drugim resursima. Povijesno gledano, lozinke se koriste oduvijek. U početku verbalno, kako bi se ostvarila prava pristupa imovini ili znanju, a u modernim se vremenima korisničkim imenom i lozinkom obično koriste ljudi tijekom procesa zapisivanja koji kontrolira pristup zaštićenim računalnim operacijskim sustavima, mobilnim telefonima, dekoderima kabelske televizije, bankomatima i slično. Tipični korisnik računala ima lozinke za mnoge svrhe: prijavljivanje na račune, e-mail adrese, pristup aplikacijama, bazama podataka, mrežama, web-lokacijama itd. (7).

1.6.2. Kako izabrati lozinku?

Za izbor dobre lozinke važno je pratiti nekoliko savjeta. Važno je da lozinka bude „lako pamtljiva“. Neka to bude nešto specifično kako bi uvijek moglo biti na umu, ali ne i očito da svatko može pogoditi. Treba odabrati neki pamtljiv, dugačak izraz ili izreku te zaporku kreirati od cijelog

izraza ili samo njegovih prvih slova. Primjerice, preuzimanjem početnih slova svake riječi neke fraze i naizmjeničnim ili nasumičnim stavljanjem velikih i malih slova. Važno je izbjegavati jednostavne zaporke poput brojeva ili slova u nizu, riječi iz rječnika i slično. Naime, postoje liste riječi za koje hakeri znaju da su često korištene kao lozinke, stoga im to uvelike olakšava pristup. Također, važno je ne koristiti istu lozinku na svim postojećim računima. Postoje razni servisi koji traže prijavu s korisničkim imenom i lozinkom kojima je jedina svrha „upad“ u ostale račune korisnika, nadajući se da će korisnik upisati istu lozinku. Zapisivanje lozinke nije najbolja ideja, ali ako je to već potrebno, poželjno bi bilo zapisati je na papir ili u bilježnicu koja je dobro spremljena od pristupa drugih ljudi. Ne treba koristiti kombinacije na tipkovnici jer većina rječnika koji se koriste za otkrivanje lozinki sadrže najčešće kombinacije. Važno je koristiti kombinaciju veličine slova kad god je to moguće. Čak i ako se odabere jednostavan pojam za lozinku, raznovrsnost znakova znatno otežava pristup provalnicima. Najbolja je metoda korištenje vlastitog algoritma za kreiranje lozinke. Primjerice, odabrati prva četiri znaka od imena stranice na koju se registrirate i dodati zadnje četiri znamenke broja telefona neke osobe. Navedeni se algoritam uvijek može dodatno razraditi da se od svakog slova odabere sljedeće ili prethodno u abecedi, kombiniranjem velikih i malih slova i slično. Što je više koraka u kreiranju algoritma, to je zaporka sigurnija (6).

1.6.3. Passphrase

Passphrase je niz riječi ili drugog teksta koji se koristi za kontrolu pristupa računalnom sustavu, programu ili podacima. Slična je upotrebi lozinke (*password*), ali je općenito dulja za dodatnu sigurnost. Često se koristi za kontrolu pristupa kriptografskim programima i sustavima, kao i za rad s njima. *Passphrase* se koristi na istom principu kao i tradicionalna lozinka, no izraz je uglavnom dulji od tradicionalnih lozinki. Dok lozinke često mogu biti kratke, *passphrases* imaju veću minimalnu duljinu, u praksi 20-30 znakova, što pruža veću sigurnost. Pravila za njihova kreiranja razlikuju se od pravila kreiranja tradicionalne lozinke. Sustavi koji koriste kraće lozinke često zabranjuju stvarne riječi ili nazive, stoga su lozinke obično slučajan niz znakova. Nasuprot tome, veća duljina *passphrase*-a omogućuje stvaranje lako pamtljive fraze, a ne kriptične serije slova, brojeva i simbola (8).

1.7. Mobilni uređaji

Svjedoci smo naglog razvoja i širenja popularnosti mobilnih uređaja, prvenstveno pametnih telefona i tableta, pa takvi uređaji postaju sve zanimljiviji napadačima. Operativni sustavi (OS) namijenjeni za pametne telefone uvode niz sigurnosnih mjera i mehanizama kako bi se umanjio rizik i uklonile ranjivosti koje bi omogućile napad uređaja i podataka na njemu. Službene trgovine namijenjene za distribuciju aplikacija provode niz mjera koje izdvajaju zlonamjerne i ranjive aplikacije kako bi se osiguralo da krajnjim korisnicima budu ponuđene samo aplikacije koje zadovoljavaju traženi sigurnosni standard. Neke od trenutno najpopularnijih aplikacija, uključujući društvene mreže, koriste se nizom osjetljivih podataka, ponajprije identitetom i lokacijom, stoga je vrlo važno da se kod takvih aplikacija poduzimaju sve mjere kako bi se zaštitila privatnost osobnih podataka korisnika (9).

Budući da je i dalje čovjek najslabija karika u razini zaštite sigurnosti privatnih podataka, najveća mogućnost napada na osobne podatke na mobilnim uređajima je nesmotrenost vlasnika koji ostavlja uređaj bez nadzora ili nepovjerljivim osobama daje pristup zaporkama na osobnom mobilnom uređaju. U doba kada mnoge informacije možemo čuvati na mobitelu, a preko njega povezati velik broj internet servisa (mail, društvene mreže, bankarstvo...), važno je jednaku važnost posvetiti zaštiti podataka na mobilnom uređaju kao i onima na osobnom računalu.

1.8. Informatika i informacijski sustav u laboratoriju

Laboratorijski informacijski sustav (LIS) u užem je smislu program koji omogućuje unos, obradu i pohranu podataka nastalih kao rezultat laboratorijskih pretraga. Međutim, pod pojmom *LIS* često podrazumijevamo i računalnu opremu potrebnu za odvijanje svih procesa, bazu podataka, pripadajuće programe automatskih analizatora i program koji omogućuje komunikaciju između analizatora i LIS-a. Iako takvi programi nisu novost u medicinskim laboratorijima, razvoj novih tehnologija dramatično utječe na mogućnosti koje oni pružaju laboratorijskim stručnjacima i svim ostalim korisnicima u sustavu zdravstvene skrbi i zdravstvenog osiguranja. Danas na svjetskom tržištu postoji niz tvrtki koje nude laboratorijske informacijske sustave i nije uvijek jednostavno procijeniti koji od dostupnih programa u potpunosti zadovoljava specifične potrebe pojedinog laboratorija. Neki proizvođači nude cjelovita rješenja za velike bolnice ili čak mreže

zdravstvenih ustanova, dok su drugi specijalizirani za neka uska područja i prilagodljivi manjim ustanovama. U konačnici je svaki LIS jedinstven i ustrojen po mjeri laboratorija (3).

1.8.1. Zaštita podataka unutar LIS-a

LIS može funkcionirati unutar laboratorija izoliran od ostatka bolnice, može biti uklopljen u bolnički informacijski sustav (BIS) ili čak može povezivati u mrežu više laboratorija. Moderni LIS sustavi najčešće se koriste mrežnim (eng. *Web*) preglednicima kao klijentima. Na taj način omogućen je upis i dohvat podataka iz LIS-a na bilo kojem računalu s instaliranim mrežnim preglednikom. Iz sigurnosnih je razloga pristup LIS-u strogo ograničen. Takva su ograničenja nužna radi zaštite povjerljivih medicinskih informacija, tj. prava bolesnika na privatnost i tajnost podataka. Zbog toga se pravo pristupa LIS-u dodjeljuje samo ovlaštenim osobama koje se u sustav prijavljuju uporabom kombinacije korisničkog imena i zaporke (3).

2. Cilj

Cilj je ovog istraživanja ispitati razinu zaštite privatnosti, razinu svjesnosti i rizičnosti ponašanja među studentima Preddiplomskog sveučilišnog studija Medicinsko laboratorijske dijagnostike koristeći validirani upitnik djelomično zasnovan i na metodama socijalnog inženjeringa te usporediti znanje i ponašanje ispitanika prema demografskim obilježjima, dobi i spolu.

3. Ispitanici i metode

3.1. Ustroj studije

Studija je dizajnirana kao presječna studija.

3.2. Ispitanici

Podaci su prikupljeni tijekom svibnja 2019. godine. Ispitanici su bili studenti Preddiplomskog studija Medicinsko laboratorijske dijagnostike Medicinskog fakulteta u Osijeku. Sudionici su podijeljeni u dvije dobne skupine: prva skupina od 18 do 21 godine i druga skupina od 22 do 25 godina starosti. Sudjelovale su osobe oba spola, a u istraživanju je sudjelovalo 59 ispitanika.

3.3. Metode

Svaki student, tj. ispitanik riješio je *online* validirani upitnik čiji su autori Tena Velki i Krešimir Šolić, uz njihovu prethodnu dozvolu za korištenje. Upitnik ispituje rizična ponašanja i znanja računalnih korisnika. Prvi dio upitnika sastoji se od općih demografskih podataka o osobama (spol, dob, obrazovanje). Idući slijed pitanja provjerava koliko su ispitanici upoznati s određenim temama koje se tiču korištenja računala, interneta i zaštite privatnosti. U tom dijelu upitnika od ispitanika se traži da, ako žele, upišu svoju e-mail adresu kako bi primali obavijesti, kao i to da prihvate Uvjete korištenja koji su im priloženi. Nadalje, pred ispitanicima se nalaze primjeri uobičajenih situacija gdje ispitujemo rizično ponašanje, znanje i svjesnost o opasnostima korištenja interneta. Naposljetku, ispitanicima je postavljeno testno/“trik“ pitanje o odavanju najkorištenije zaporke.

Pitanja unutar upitnika podijeljena su u tri skale: skala rizičnog ponašanja, skala znanja i skala svjesnosti. Ispitanici su odgovarali na nekoliko pitanja unutar svake skale te je izvedena prosječna ocjena za svaku od njih. Pitanja se procjenjuju bodovima na Likertovoj skali od 1 do 5

pri čemu (ovisno o skali) ponuđeni odgovori imaju različita značenja (npr. učestalost, stupanj sigurnosti, stupanj uvjerenja, stupanj važnosti...).

3.4. Statističke metode

Statistička analiza učinjena je standardnim statističkim metodama. Svi prikupljeni kategorijski podaci predstavljeni su apsolutnim i relativnim frekvencijama, dok su numerički podaci opisani aritmetičkom sredinom i standardnom devijacijom, a u slučaju raspodjela koje ne slijede normalnu razdiobu medijanom i interkvartilnim rasponom. Rezultati su prezentirani u tablicama i grafikonima.

Za usporedbu kategorijskih podataka unutar skupina i među skupinama korišten je Hi-kvadrat test, dok su razlike između dvije nezavisne skupine numeričkih podataka testirane neparametrijskim Mann-Whitney U testom.

Statistička analiza učinjena je programskim sustavom MedCalc (inačica 16.12.0, MedCalc Software bvba), uz odabranu razinu značajnosti od α=0,05. Sve su P vrijednosti dvostrane.

3.5. Etička načela

Prije provođenja ovog istraživanja dobivena je suglasnost Etičkog povjerenstva Sveučilišta J. J. Strossmayera u Osijeku Medicinskog fakulteta Osijek (KLASA: 602-04/19-08/04; URBROJ: 2158-61-07-19-42; Osijek, 30. travnja 2019.)

4. Rezultati

4.1. Opća obilježja sudionika

U istraživanju je sudjelovalo ukupno 59 ispitanika, pri čemu je njih 48 (81,4 %) ženskog spola, što je značajno više (Hi-kvadrat test, $P < 0,001$) od ispitanika muškog spola, kojih je bilo 11 (18,6 %). Ispitanici su bili studenti prve, druge i treće godine preddiplomskog studija, starosne dobi između 18 i 25 godina, podijeljeni u dvije starosne skupine: njih 32 (54,2 %) je bilo u mlađoj skupini (u dobi od 18 do 20 godina) te njih 27 (45,8 %) u starijoj skupini (u dobi od 21 do 25 godina) (Hi-kvadrat test, $P = 0,65$).

4.2. Ukupne ocjene

Odgovori na opća pitanja o znanju i svjesnosti, kao i opća pitanja o korištenju interneta, prikazani su u Tablici 1.

Više od dvije trećine ispitanika svoje je znanje o sigurnosti i privatnosti te svoje opće tehničko znanje o računalima procijenila kao dobro. Tri četvrtine ispitanika izjasnilo se da je imalo neku vrstu edukacije po pitanju zaštite privatnosti. Također, većina ispitanika koristi internet pola svog života te svakodnevno 2 do 3 sata (Tablica 1).

Drugi dio upitnika pokušava ispitanika navesti na pristanak primanja obavijesti te antivirusnog *software*-a na svoj e-mail te ih stoga navodi da ga i upišu. Sedam (11,9 %) ispitanika navelo je da želi primati obavijesti, devet (15,3 %) ispitanika navelo je da bi voljelo primiti besplatni antivirusni *software* na e-mail, a čak devet (15,3 %) njih ostavilo je i svoju e-mail adresu. Nakon toga ispitanicima su predstavljeni Uvjeti korištenja (*Terms of conditions*) koje su trebali pročitati i odgovoriti slažu li se s njima ili ne. Uvjete korištenja prihvatilo je 49 (83,0 %) ispitanika.

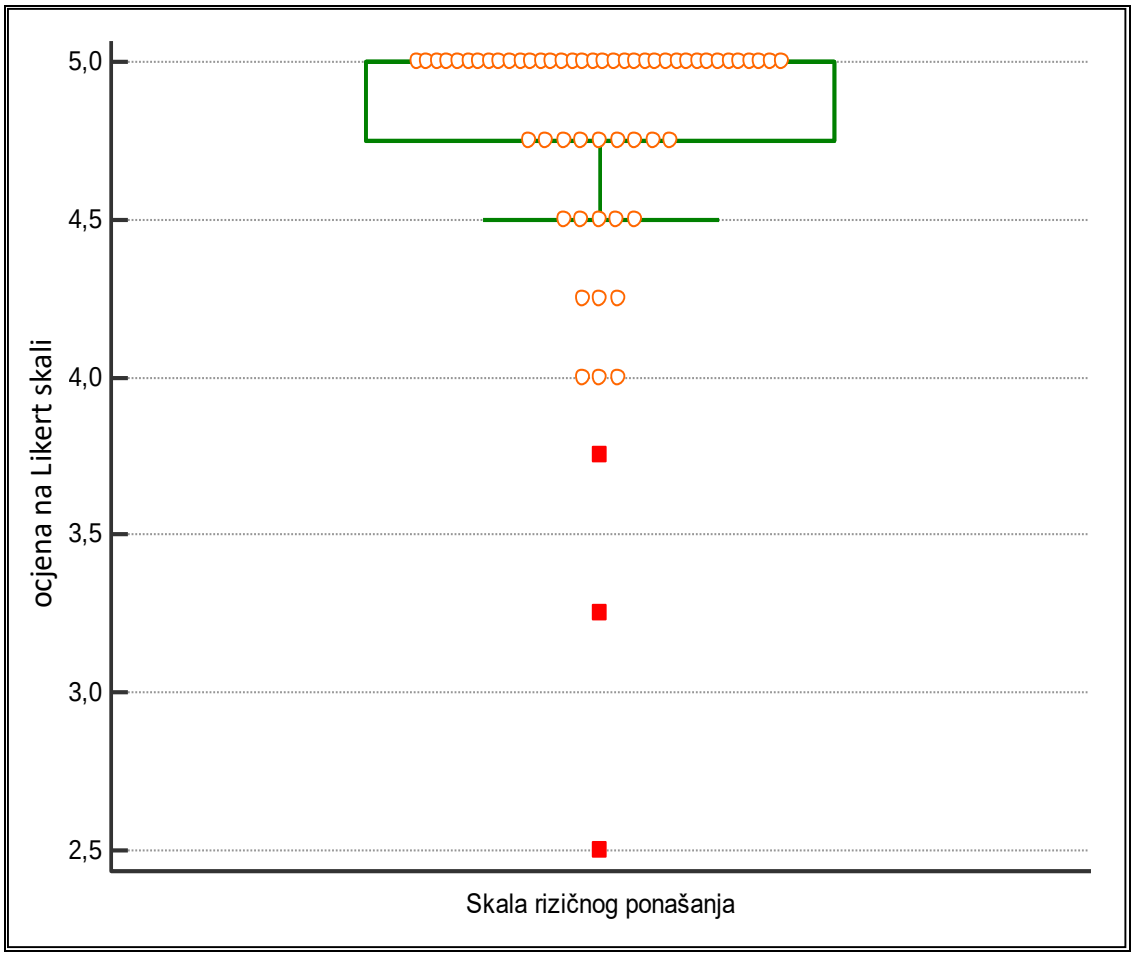
Tablica 1. Distribucija odgovora općih pitanja o znanju prema procjenama ispitanika

Pitanje	**Odgovor**	**Broj (%) ispitanika**	**P***
Procjena vlastitog znanja o sigurnosti i privatnosti	loše	13 (22,0 %)	**0,49**
	dobro	42 (71,2 %)	
	odlično	4 (6,8 %)	
Procjena općeg tehničkog znanja o računalima	loše	11 (18,6 %)	**0,49**
	dobro	42 (71,2 %)	
	odlično	6 (10,2 %)	
Prijašnja edukacija po pitanju zaštite	da	44 (74,6 %)	>**0,99**
	ne	15 (25,4 %)	
Otkad koristite internet	nekoliko godina	8 (13,6 %)	**0,49**
	pola svog života	41 (69,5 %)	
	otkad znam za sebe	10 (17,0 %)	
Koliko dnevno koristite internet	manje od jedan sat	0 (0 %)	**0,58**
	2 do 3 sata	23 (39,0 %)	
	4 do 5 sati	16 (27,1 %)	
	između 5 i 10 sati	15 (25,4 %)	
	više od 10 sati	5 (8,5 %)	
Ukupno		59 (100 %)	

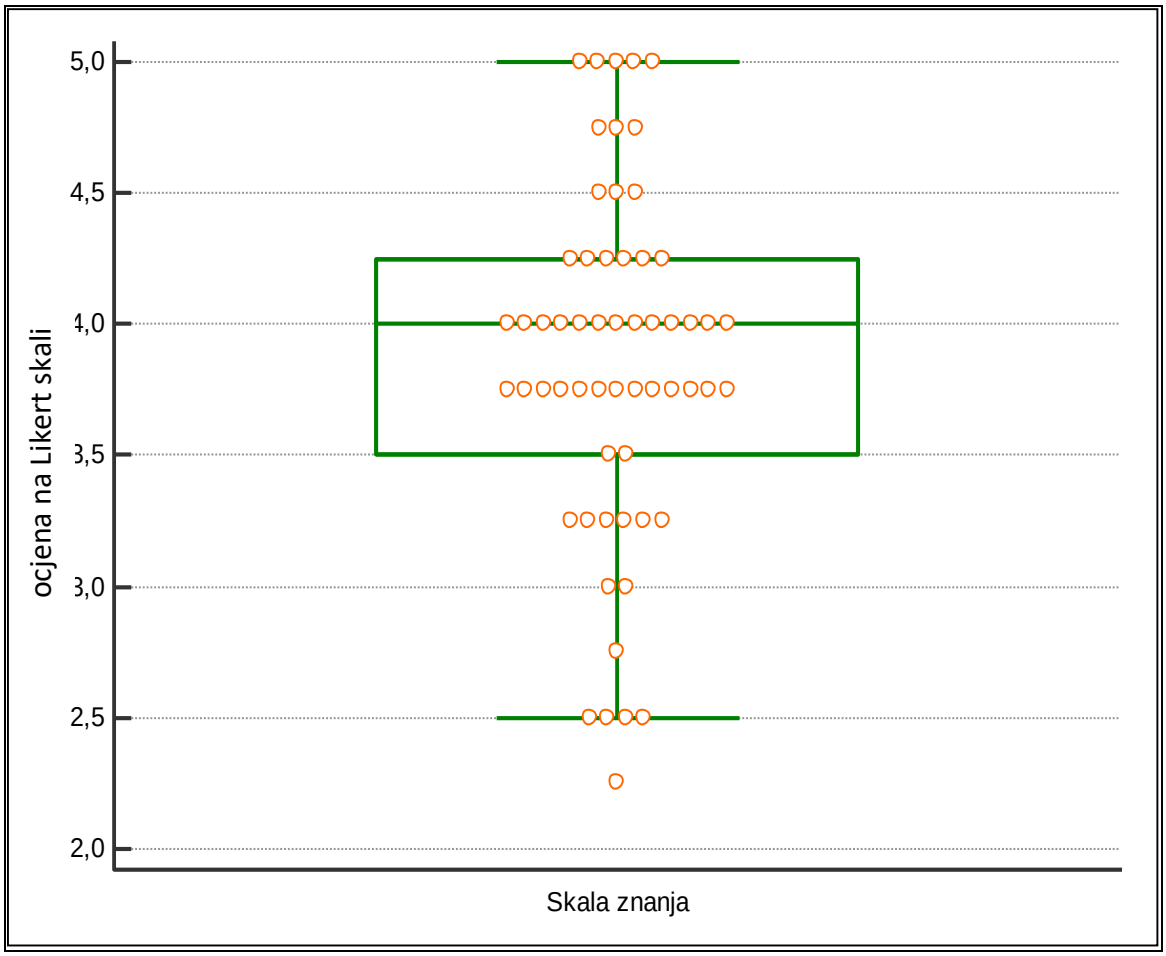
*Hi-kvadrat test

Prosječne vrijednosti ocjena po subskalama pokazale su da su ispitanici oprezni u rizičnim situacijama, a da svoje znanje i svjesnost ocjenjuju nešto iznadprosječnim ocjenama (Slika 1-3).

Prosječna ocjena ispitanika po skali rizičnog ponašanja iznosi 4,7 (0,5) [aritmetička sredina (standardna devijacija)] (Slika 1). Prosječna ocjena po skali znanja iznosi 3,8 (0,7) [aritmetička sredina (standardna devijacija)] (Slika 2). Prosječna ocjena po skali svjesnosti (o opasnostima) iznosi 3,5 (1,1) [aritmetička sredina (standardna devijacija)] (Slika 3).

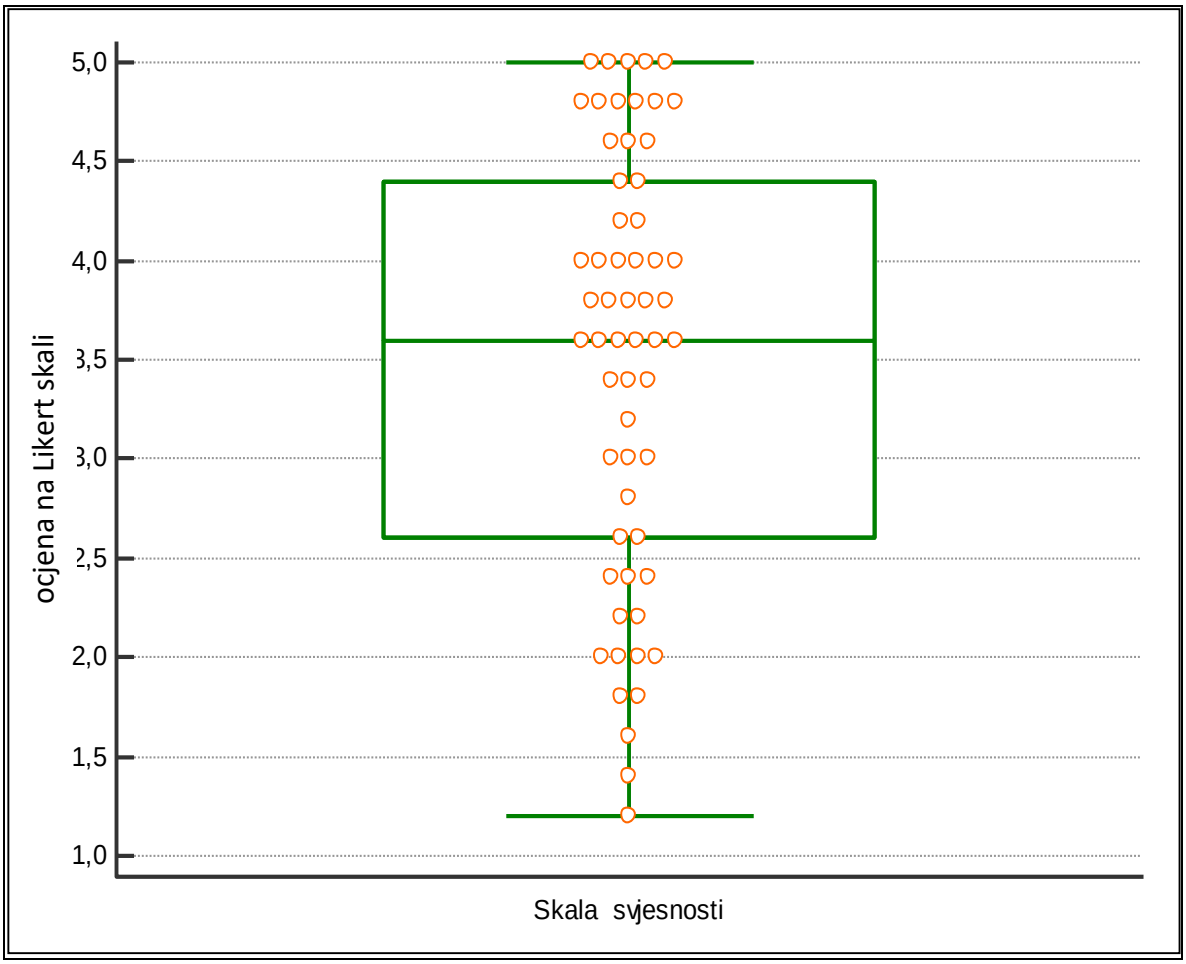


Slika 1. Prikaz ocjena na skali rizičnog ponašanja, box-and-whiskers dijagram



Slika 2. Prikaz ocjena na skali znanja, box-and-whiskers dijagram

Posljednje pitanje u upitniku navodi ispitanike na odavanje svoje najčešće korištene lozinke. Od 59 ispitanika njih troje (5,1 %) odalo je svoju pravu lozinku, njih 11 (18,6 %) je napisalo kako ne želi dati lozinku ili su podijelili lažnu, dok su ostali to polje ostavili praznim.



Slika 3. Prikaz ocjena na skali svjesnosti, box-and-whiskers dijagram

4.3. Usporedba prema spolu

Rezultati usporedbe prosječnih ocjena po pojedinoj skali prema spolu pokazali su da su žene značajno svjesnije potencijalnih rizika na internetu (Mann-Whitney test, P = 0,04) u usporedbi s muškarcima. Nije dobivena statistički značajna razlika između ženskih i muških ispitanika u skalama (rizičnog) ponašanja, odnosno znanja o rizicima (Tablica 2).

Tablica 2. Usporedba ocjena pojedinih skala prema spolu

Skale	**Medijan (interkvartilni raspon)**		**P***
	Muškarci /n=11	**Žene /n=48**	
Ponašanje	5,0 (od 5,0 do 5,0)	5,0 (od 4,5 do 5,0)	0,10
Znanje	3,8 (od 3,0 do 4,0)	4,0 (od 3,8 do 4,3)	0,07
Svjesnost	2,4 (od 2,0 do 3,7)	3,8 (od 3,1 do 4,6)	**0,04**

*Mann-Whitney test

4.4. Usporedba prema dobi

Rezultati usporedbe prosječnih ocjena po pojedinoj skali prema spolu pokazali su da su mlađi studenti značajno svjesniji potencijalnih rizika na internetu (Mann-Whitney test, P = 0,006) u usporedbi sa starijim studentima. Nije dobivena značajna razlika prema dobi u skalama (rizičnog) ponašanja, odnosno znanja o rizicima (Tablica 3).

Tablica 3. Usporedba ocjena pojedinih skala prema dobi

Skale	**Medijan (interkvartilni raspon)**		**P***
	od 18 do 21 /n=32	**od 22 do 25 /n=27**	
Ponašanje	5,0 (od 4,5 do 5,0)	5,0 (od 4,8 do 5,0)	0,66
Znanje	3,8 (od 3,4 do 4,3)	4,0 (od 3,6 do 4,3)	0,74
Svjesnost	4,0 (od 3,4 do 4,8)	3,0 (od 2,3 do 3,8)	**0,006**

*Mann-Whitney test

5. Rasprava

U istraživanju je sudjelovalo 59 ispitanika Preddiplomskog studija Medicinsko laboratorijske dijagnostike Medicinskog fakulteta u Osijeku. Ispitanici su bili studenti prve, druge i treće godine preddiplomskog studija, oba spola te podijeljeni u dvije starosne skupine.

Anketna pitanja dala su uvid u vlastite procjene ispitanika o njihovom općem poznavanju sigurnosti na internetu kao i saznanja o njihovom korištenju interneta kako tijekom dana, tako i tijekom života. Na opća pitanja o sigurnosti i tehničkom poznavanju računala i interneta većina studenata, njih dvije trećine, odgovorila je s prosječnom ocjenom „dobro“. Pomalo zabrinjava činjenica da je čak četvrtina studenata navela da nikada dosad nisu prošli nikakvu vrstu edukacije po pitanju zaštite na internetu. Nije sigurno jesu li studenti nesvjesni edukacija koje tijekom školovanja prolaze ili doista ne susreću dovoljno edukacijskih sadržaja po pitanju tehničkih znanosti i rizika koje one donose. Većina ispitanika koristi internet pola svojega života, a čak 17 % njih koristi internet otkad znaju za sebe. Takvi podaci ukazuju na još veću potrebu za edukacijom tijekom redovnog školovanja, kao i podizanje svijesti o opasnostima među roditeljima maloljetnika koji u sve ranijoj dobi počinju samostalno koristiti internet.

Anketni upitnik podijeljen je u tri skale; ponašanje, znanje i svjesnost, koje su služile kao varijable za usporedbu rezultata s demografskim obilježjima studenata (spol, dob) u ovome istraživanju. Rezultati nisu pokazali statistički značajne razlike između spolova na skalama ponašanja i znanja. Na skali svjesnosti dobivena je statistički značajna razlika između spolova gdje su žene znatno svjesnije rizika koji vladaju internetom. Na skali ponašanja i znanja također nije uočena razlika između dvaju dobnih skupina (18-20 godina, 22-25 godina) dok se na skali svjesnosti mlađa skupina pokazala statistički značajno svjesnijom rizika od starije skupine studenata.

Zadnje pitanje upitnika ispituje koliko je lako navesti ispitanike na odavanje svoje najčešće korištene lozinke pod isprikom da će se na taj način provjeriti njezina kvaliteta i sigurnost. Većina ispitanika ostavila je to polje praznim, što bi i trebao biti očekivan i ispravan odgovor. S druge strane, 14 (23,7%) ispitanika dalo je odgovor. Najčešći odgovori bile su prepoznatljivo lažne lozinke ili su samo napisali da ne žele dati lozinku, no troje ispitanika (5,1 %) je, čini se, ostavilo svoju pravu, odnosno stvarnu lozinku.

U usporedbi s drugim istraživanjem na istu temu (10), većina rezultata odgovara prijašnjim rezultatima. Općenito, žene su uvijek pokazivale veću razinu sigurnosti, što su potvrdili i rezultati ove ankete. Prijašnji su rezultati također pokazali različite rezultate s obzirom na obrazovanje, gdje se najveća razlika u ponašanju pokazala pri usporedbi rezultata ispitanika sa završenom srednjom školom i magisterijem. Budući da su svi ispitanici ove ankete na putu prema magisteriju, ne začuđuju rezultati s iznadprosječnim ocjenama. Za razliku od prijašnjih istraživanja u kojima je čak 28,8 % ispitanika odalo svoje lozinke, ovo istraživanje pokazalo je da su studenti puno svjesniji te je svoju pravu lozinku odalo tek troje ljudi (5,1 %).

Postoji nekoliko mogućih nedostataka ovoga istraživanja. Jedan od njih je mali broj ispitanika. Rezultati bi zasigurno pokazali širu i specifičniju sliku da su u istraživanju sudjelovali i studenti drugih sveučilišta. Osim što se ne može saznati jesu li odane lozinke uistinu prave i aktivne, studenti Medicinskog fakulteta u Osijeku tijekom svog studija djelomično su upoznati s pojmom socijalnog inženjeringa, odnosno manipuliranjem ljudima u svrhu otkrivanja povjerljivih informacija do kojih se uglavnom dolazi prijevarom, stoga su možda opreznije odgovarali na pitanja o odavanju privatnog e-maila i lozinke (11).

Iako distribucije ocjena po pojedinim skalama pokazuju kako su ocjene relativno visoke, to ne znači i da su ispitanici pokazali dovoljno dobre rezultate. Važno je često i kontinuirano raditi na poboljšanju svjesnosti među korisnicima interneta. U današnjem se svijetu nekontrolirano brzo razvijaju *software*-i kojima je cilj krađa informacija, a najslabija su karika u sustavu zaštite ljudi. Posebno je važno da zdravstveni djelatnici budu dobro upućeni u opasnosti koje ih okružuju te da svjesno postupaju s informacijama na internetu ili svojim privatnim podacima. Budući da je u poslu zdravstvenih djelatnika prisutno mnogo povjerljivih medicinskih informacija, važno je znati sačuvati ih od neželjenih krađa i manipulacija kako bi očuvali svoju, ali i privatnost drugih sudionika na internetu.

6. Zaključak

Na temelju provedenog istraživanja i dobivenih rezultata mogu se izvesti sljedeći zaključci:

- Većina ispitanika u svim je skalama dala visoke ocjene
- Najviše su ocjene u skali koja ispituje rizično ponašanje, što znači da se ispitanici ne ponašaju previše rizično, dok su najniže ocjene u skali koja ispituje svjesnost o postojećim rizicima
- Na „trik“ pitanju samo je troje ispitanika odalo svoju lozinku
- Uvjete korištenja prihvatilo je 83 % ispitanika, ali je samo oko 15 % njih pristalo prihvaćati obavijesti ili su podijelili privatni e-mail
- Studentice ženskog spola značajno su svjesnije rizika nego njihovi kolege
- Ispitanici mlađe skupine pokazali su da su svjesniji rizika nego ispitanici starije skupine

Dobiveni rezultati odgovaraju očekivanjima s obzirom na dosad provedena istraživanja na većim skupinama. Ispitivana skupina studenata Medicinsko laboratorijske dijagnostike pokazala je očekivane rezultate s obzirom na njihov trenutni stadij obrazovanja. Potrebno je poraditi na edukaciji studenata o mogućim opasnostima i rizicima koji prijete privatnosti na internetu, a takav bi program trebalo uvesti već u niže razrede osnovne škole te ga konstantno nadograđivati prateći napredak informacijskih znanosti.

7. Sažetak

Ciljevi istraživanja: Ispitati razinu zaštite privatnosti, svjesnosti i rizičnosti ponašanja na internetu među studentima preddiplomskog studija Medicinsko laboratorijske dijagnostike.

Nacrt studije: Studija je dizajnirana kao presječna studija.

Ispitanici i metode: U istraživanju je sudjelovalo 59 studenata preddiplomskog studija. Istraživanje je provedeno na Medicinskom fakultetu u Osijeku tijekom svibnja 2019. godine. Za istraživanje se koristio validirani upitnik čiji su autori Krešimir Šolić i Tena Velki. Statistička obrada učinjena je u računalnom programu MedCalc.

Rezultati: Na opća pitanja o poznavanju sigurnosti na internetu te njegovu korištenju, većina ispitanika odgovorila je prosječnom ocjenom „dobro“. Čak 25,4 % ispitanika odgovorilo je da dosad nisu imali nikakvu edukaciju po pitanju zaštite na internetu. Ispitanici su pokazali relativno visoke ocjene u svim mjernim skalama. Osobe ženskog spola pokazale su se značajno svjesnije rizika koji vladaju internetom. Mlađa skupina ispitanika, od 18 do 21 godine starosti, pokazala se značajno svjesnija rizika nego starija skupina, od 22 do 25 godina starosti. U skalama ponašanja i znanja nisu pronađene statistički velike razlike između spolova ili dobi. Tek 5,1% ispitanika odalo je svoju pravu lozinku na „trik“ pitanju.

Zaključak: Iako je većina ispitanika pokazala visoke rezultate na svim skalama, to ne znači da su rezultati zadovoljavajući. Najviše ocjene dobivene su u skali rizičnog ponašanja i ukazuju na to da su ispitanici ipak oprezni u svojim postupcima. S druge su strane najniže ocjene na skali svjesnosti, što ukazuje na manjak edukacije. Dobiveni rezultati nisu iznenađujući u usporedbi s prijašnjim istraživanjima, no uočena je velika potreba za dodatnom edukacijom i povećanjem svijesti među korisnicima interneta.

Ključne riječi: internet, privatnost, sigurnost, rizično ponašanje

8. Summary

Testing the Level of Privacy among the Students of Medical Laboratory Diagnostics

Objectives: To test the level of protection of privacy, awareness and risk behavior on the Internet among undergraduate students of Medical Laboratory Diagnostics considering their gender and age.

Study Design: Study was conducted as a cross-sectional study.

Participants and Methods: 59 undergraduate students participated in this study. The study was conducted at the Faculty of Medicine in Osijek during May 2019. The validated questionnaire was authored by Krešimir Šolić and Tena Velki. Statistical data was processed in the MedCalc computer program.

Results: The majority of participants answered the general questions about safety and knowledge about the Internet, with an average grade being "good". As many as 25.4% of respondents stated that they had not had any education on online security issues up until then. Respondents showed relatively high scores on all scales measured. Women have proven to be significantly more aware of the risks that are present on the Internet. The younger group of respondents, between 18 and 21 years old, showed a significant difference in risk awareness than the older group, between 22 and 25 years old. No statistically significant differences between genders or age were found in the behavioral and knowledge scales. Only 5.1% of respondents revealed their real password to trick question.

Conclusion: Although most respondents showed high scores on all scales, this does not mean that the results are satisfactory. The highest scores were given on the behavioral scale, indicating that respondents are cautious in their actions. On the other hand, the lowest scores are on the awareness scale indicating a lack of education. The results obtained are not surprising compared to previous research, but there is a great need for additional education and awareness among Internet users.

Keywords: Internet, privacy, safety, risky behaviour

9. Literatura

1. Cohen-Almagor R. Internet History. Int J Technoethics. 2011;2:45-64.
2. Kleinrock L, Schwartz M. An early history of the Internet (History of communications). IEEE Commun Mag. 2010;48:26-36.
3. Kern J, Petrovečki M. Medicinska informatika. Medicinska naklada. Zagreb; 2009.
4. Velki T, Šolić K, Nenadić K. Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). Psihologijske teme [Internet]. 2015; 24(3):401-424.
5. Varga M. Zaštita elektroničkih podataka. TG-TJ. 2011; 5(1):61-73.
6. Velki T, Šolić K. Priručnik za informacijsku sigurnost i zaštitu privatnosti. Osijek: Fakultet za odgojne i obrazovne znanosti, Sveučilište Josipa Jurja Strossmayera u Osijeku 2018.
7. Šolić K, Očevčić H, Blažević D. Survey on Password Quality and Confidentiality. Automatika [Internet]. 2015; 56(1):69-75.
8. Indiana university. Indiana university passphrase policy and strength estimation, Dostupno na adresi: http://kb.iu.edu/data/acpu.html. Datum pristupa: 19.6.2019.
9. Bošnjak Z. Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja [Undergraduate thesis]. Zagreb: University of Zagreb, Faculty of Transport and Traffic Sciences; 2016.
10. Šolić, K., Velki, T., & Galba, T. Empirical study on ICT system's users' risky behavior and security awareness. 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2015, pp. 1356-1359.
11. CERT. Upute za laike "Sigurnije na Internetu". 2010. Preuzeto s: http://www.cert.hr/dokumenti/sigurnije_na_internetu.

10. Životopis

Ime i prezime: Marina Martinović

Datum i mjesto rođenja: 21. 9. 1997., Slavonski Brod

Adresa: Šetalište braće Radić 20, 35000 Slavonski Brod

Mobitel: 0917615354

e-pošta: mmartinovic1@gmail.com

Obrazovanje:

2004 – 2012. Osnovna škola „Ivan Goran Kovačić“, Slavonski Brod

2012 – 2016. Klasična gimnazija fra Marijana Lanosovića s pravom javnosti, Slavonski Brod

2016 – 2019. Preddiplomski sveučilišni studij Medicinsko laboratorijske dijagnostike, Medicinski fakultet Osijek