Ispitivanje znanja i ponašanja studenata o pitanjima zaštite privatnosti na internetu metodom socijalnog inženjeringa

Horvat, Enis

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

MEDICINSKI FAKULTET OSIJEK

DIPLOMSKI SVEUČILIŠNI STUDIJ MEDICINSKO LABORATORIJSKA DIJAGNOSTIKA

Enis Horvat

ISPITIVANJE ZNANJA I PONAŠANJA STUDENATA O PITANJIMA ZAŠTITE PRIVATNOSTI NA INTERNETU METODOM SOCIJALNOG INŽENJERINGA

Diplomski rad

Osijek, 2020.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

MEDICINSKI FAKULTET OSIJEK

DIPLOMSKI SVEUČILIŠNI STUDIJ MEDICINSKO LABORATORIJSKA DIJAGNOSTIKA

Enis Horvat

ISPITIVANJE ZNANJA I PONAŠANJA STUDENATA O PITANJIMA ZAŠTITE PRIVATNOSTI NA INTERNETU METODOM SOCIJALNOG INŽENJERINGA

Diplomski rad

Osijek, 2020.

Rad je ostvaren na Medicinskom fakultetu Osijek.

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

Rad ima 25 list, 11 tablica i 1 sliku.

Zahvala

Zahvaljujem se svojim roditeljima, braći i sestri na neizmjernoj podršci i razumijevanju koje su mi pružali tijekom cijelog školovanja i bez kojih danas ne bi bio ovdje.

Veliko hvala mentoru Doc. dr. sc. Krešimiru Šoliću, dipl. ing. el. na stručnom vodstvu u pisanju diplomskog rada. Hvala Vam na strpljenju, razumijevanju i uloženom trudu.

Isto tako, zahvaljujem se svim svojim prijateljima koji su mi uljepšali studentske dane.

Sadržaj

1. Uvod

Nikad nije bio veći protok i dostupnost informacijama nego što je to danas. Razlog tome je razvoj tehnologije i sveprisutnost interneta što kao posljedicu ima mnogo pozitivnih i mnogo negativnih strana. Možemo reći da je internet promijenio način života ljudi bez obzira na dob i spol. Internet nam je olakšao komunikaciju s ljudima pojavom društvenih mreža i raznih aplikacija koje služe za komunikaciju, lakšu i bržu dostupnost mnogim informacijama, olakšava mnogim poduzetnicima i tvrtkama komunikaciju i njihovom radu, olakšava razmjenu znanja, iskustava i materijala među znanstvenicima, liječnicima, profesorima i studentima što omogućava bolji i brži napredak i samim time olakšava i podiže standard života. Uz spomenutih ima i mnogo drugih pozitivnih strana interneta, upravo zbog toga mnogi ne vide i nisu svjesni negativnih strana korištenja i sveprisutnosti interneta (1).

Internet je za većinu ljudi postao svakodnevnica i nešto neophodno, isprepleten je gotovo u svakom aspektu ljudskog života. Poznat je svim ljudima bez obzira na njihovu dob, spol i zanimanje. Razlog tome je širok raspon sadržaja i usluga koje nudi i što cjelokupan proces ekspanzije interneta još uvijek traje i raste svakim danom.

Kada bismo htjeli definirati što je to internet rekli bismo da je internet javno globalna podatkovna mreža koja povezuje računala i računalne mreže korištenjem istoimenog protokola (IP-Internet protokol).

Godine 1968. u SAD-u je nastala globalna podatkovna mreža - ARPANET (Advanced Research Project Agency Network), Internet, koja je povezivala svega nekoliko računala koja su se koristila kao vojna mreža američkog Ministarstva obrane, a internet koji mi danas koristimo (World Wide Web servis) osmišljen je 1989. godine u Švicarskoj.

Kada govorimo o informacijskoj sigurnosti, socijalni inženjering bismo definirali kao psihološku manipulaciju ljudi kako bi otkrili svoje povjerljive podatke (1). Ovaj pojam se često koristi za široki spektar zlonamjernih aktivnosti, tj. interakcija s ljudima kako bi manipulacijom zavarali korisnike u činjenju sigurnosnih pogrešaka i odavanja informacija koje bi se mogle zloupotrijebiti. Samim time narušava se i privatnost što je jedno od osnovnih ljudskih prava. Informacijska sigurnost podrazumijeva podatke pojedinca o njegovom materijalnom, intelektualnom, kulturnom i duhovnom smislu, tj. podatke o svim sferama života jednog čovjeka. S obzirom na ovo moderno doba u kojem se nalazimo i tehnologiju kojom se svakodnevno koristimo, čuvanje vlastite privatnosti je postalo puno teže.

Velik broj ljudi svjesno ili nesvjesno dijeli svoje osobne podatke putem društvenih mreža, ne znajući da se ti podaci mogu iskoristiti i da dijeljenjem svojih osobnih podataka mogu nastati brojne i ozbiljne posljedice koje se često teško daju ispraviti.

S obzirom da živimo u digitaliziranom svijetu u kojem broj prijevara putem društvenih mreža raste, važno je podići razinu svjesnosti o rizicima koji se javljaju kod korištenja interneta te opreznije upravljati i dijeliti informacije putem društvenih mreža kako bi se ti rizici sveli na minimum.

Kako nema dobnih granica korištenja interneta, najranjivija skupina ljudi koji su često žrtve korištenja interneta su djeca (2). Djeca najviše koriste internet za zabavu i komunikaciju, znatno manje za učenje i informiranje. Korištenjem društvenih mreža i raznih aplikacija koje zahtijevaju razne informacije o osobi koja ih koristi, odaju se osobni podaci koji se lako mogu zloupotrebljavati i samim time ugroziti sigurnost ljudi te oni gube privatnost što rezultira brojnim štetnim posljedicama. Djeca su najranjivija skupina zbog slabog poznavanja pravila sigurnosti upotrebe interneta, svoje naivnosti i svoje slabo razvijene vještine donošenja odluka (3).

Osim odavanja osobnih podataka, korištenjem interneta, djeca su izložena mnogim neprimjerenim sadržajima koji ostavljaju ozbiljne posljedice na djecu.

Djeca koja su izložena nasilnom sadržaju, a posljedično tome u skorijoj budućnosti ta djeca budu i sama verbalno i fizički agresivnija jer imaju tendenciju oponašati modele koji im se čine privlačnima bez obzira je li ta vrsta ponašanja prihvatljiva ili ne (1). Dugotrajnom izloženosti takvoj vrsti sadržaja dijete ima iskrivljenu sliku dobrog i normalnog društvenog ponašanja te stvara vjerovanja i stavove koji utječu na ponašanje pojedinca. Razlog toga je što djeca u najranijoj fazi svog života uče prosuđivati, promišljati, razlikovati dobrog od lošeg, opažati i reagirati na situacije i događaje u svojoj okolini. Najveći utjecaj osim filmova i YouTubea na kojem djeca vole provode većinu svojeg vremena imaju i video igrice koje uz već spomenute negativne posljedice imaju za posljedicu i asocijalno ponašanje djece i mladih.

Uz to prekomjerno i nekontrolirano korištenje interneta može uzrokovati i nisko samopoštovanje, depresiju i tjeskobu, a nerijetko dolazi i do zanemarivanja školskih obaveza.

Važno je istaknuti i rizik tzv. „cyberbullyinga“ i pedofilije s kojim se djeca susreću kod korištenja interneta. Isto tako postoji rizik i opasnost od izlaganja neprimjerenim porukama koje sadržavaju seksualno eksplicitne tekstualne poruke, videozapise ili slike putem

društvenih mreža. Takve poruke često potiču da i sami dijele i šalju takve neprimjerene sadržaje drugim ljudima putem društvenih mreža. Te osobe nerijetko ranije počinju stupati u seksualne odnose, gdje se javlja i rizik od neželjenih trudnoća, čestog mijenjanja seksualnih partnera i spolno prenosivih bolesti koje na sebe nadovezuju brojne druge probleme.

Kako bi izbjegli sve spomenute negativne strane i posljedice nekontroliranog korištenja interneta postoje nekoliko roditeljskih strategija (1):

1. Aktivno posredovanje - usmjeravanje djece prema medijskim sadržajima kako bi smanjili vjerojatnost negativnih posljedica
2. Zajedničko korištenje interneta i medija
3. Ograničavanje korištenja interneta i medija
4. Naučiti odgovornosti i svjesnom ponašanju
5. Pronalaženje alternative tehnologiji.

Odrasli isto tako mnogo vremena provode koristeći internet i medije za zabavu i komunikaciju. Za razliku od djece i mladih, velik broj ljudi koristi internet neizbježno zbog prirode posla kojeg obavljaju (4). Oni isto tako snose posljedice korištenja interneta zbog slabe upućenosti, neosviještenosti i neinformiranosti, neshvaćajući opasnosti kojoj su izloženi korištenjem interneta (5).

Važna je visoka razina svijesti o rizicima korištenja interneta kako kod djece i mladih, tako i kod odraslih ljudi, a osobito kod ljudi kojima je u opisu posla rad s ljudima i njihovim privatnim podacima (6). Svako rizično ponašanje, nepažnja i otkrivanje podataka (ime i prezime, bankovni računi, adrese, lozinke i sl.) mogu se zloupotrijebiti i dovesti do financijskih šteta, krađa identiteta, problema u privatnom i poslovnom životu.

1.1 Zaštita privatnosti

Zaštita privatnosti je postao važan i velik problem naše današnjice. Prvi korak kao oblik prevencije i zaštite privatnosti bio bi ograničavanje podataka koje dijelimo na internetu, tj. društvenim medijima (1). Na taj način sprječavamo i smanjujemo mogućnost ugroze naših podataka i informacija koje bi se mogle zloupotrijebiti. Nažalost, velik broj ljudi, najčešće mladi, imaju naviku dijeliti informacije putem društvenih mreža (Facebook, Instagram,

Twitter...) te tako postaju potencijalne žrtve (7). Uz to trebalo bi izbjegavati praksu čuvanja i pohranjivanja osobnih i povjerljivih podataka na svojim računalima, mobitelima i ostalim uređajima kao jednu od mjera prevencije.

Postavljanje lozinke je jedan od važnijih oblika samozaštite i sprječavanja neovlaštenih pristupa našim podacima uljezima. Kao najsigurniji oblici lozinke su one koje sadržavaju kombinaciju velikih i malih slova, brojeve i različite znakove (8). Važno je napomenuti da se ne smije koristiti jedna lozinka za dva ili više uređaja i izrađenih računa jer se otkrivanje lozinke ugrožava privatnost i povjerljivost svih podatka i informacija koji postoje na tim uređajima i izrađenim računima.

Jedna od vrsta samozaštite je i korištenje virtualne privatne mreže (VPN) koja pruža privatnost tako što onemogućava davateljima internetskih usluga praćenje naših podataka i povijest našeg preglednika te samim time nas štiti od drugih ljudi koji žele pristupiti našim osobnim podacima i informacijama koje bi njima bile korisne (9). Isto tako su kao mjere samozaštite izbjegavanje otvaranja i odgovaranja na sumnjive i nepoznate poruke (10; 11), povezivanje na nepoznatim bežičnim mrežama, otvaranje poveznica iz nepoznatih izvora te skidanje i instaliranje različitih aplikacija nepoznatih i sumnjivih tvrtki. Ono što je isto tako važno, a velik broj ljudi to ne radi je da treba pročitati svako dopuštenje koju dajemo prilikom preuzimanja i instaliranja aplikacije.

Osim mjera samozaštite, postoje i brojne aplikacije koje nam služe kao zaštita, tj. programi koji štite našu privatnost i naše uređaje od zlonamjernih napada. Da bi svaki uređaj normalno funkcionirao, potrebno je instalirati aplikaciju za zaštitu. Aplikacije rade na principu da traže pogreške i slabe točke koje popravljaju da bi spriječile ranjivost same aplikacije i uređaja. Da bi aplikacija za zaštitu što učinkovitije služila svojoj svrsi, potrebno ju je održavati i ažurirati kako bi se nadogradila i preuzela najnoviji popis zloćudnih programa.

Gledajući pravne aspekte o zaštiti osobnih podataka koja je temeljno pravo svakog čovjeka, ona je potkrijepljena međunarodnim i nacionalnim pravnim dokumentima. U Republici Hrvatskoj, 12. lipnja 2003. godine je donesen Zakon o zaštiti osobnih podataka u svrhu zaštite privatnog života te ostalih ljudskih prava i temeljnih sloboda u prikupljanju osobnih podataka, obradi i korištenju tih podataka. Osobni podaci se smiju prikupljati uz informirani pristanak osobe, u slučajevima određenim zakonom i u svrhu zaštite ili tjelesnog integriteta ispitanika.

1.2 Zaštita privatnosti u zdravstvu

Razvojem tehnologije došlo je do razvoja informacijskog sustava u zdravstvu. Zahvaljujući tome je došlo do brže i lakše komunikacije ljudi u zdravstvu, bolje izmjene i dostupnosti informacijama te značajne uštede vremena (12). Uz nabrojane prednosti javlja se problem zaštite informacija i privatnosti pacijenata. Zaštita podataka o zdravstvenom stanju spada u posebnu skupinu osobnih podataka koju zbog svoje osjetljive prirode zdravstveni djelatnici moraju štititi te oprezno koristiti podatke i informacije o svojim pacijentima (1).

Posebno valja istaknuti Bolnički informacijski sustav-BIS i Laboratorijski informacijski sustav-LIS koji su uvelike pomogli i olakšali rad zdravstvenih djelatnika. Spomenutim sustavima ne bi smjele pristupiti neovlaštene osobe zbog osjetljivosti i važnosti informacija i podataka koje se nalaze u tim sustavima, a koje bi mogle ugroziti privatnost pacijenata (1).

2. Cilj istraživanja

Cilj ovog istraživanja je ispitati stupanj rizičnog ponašanja te razinu znanja o pitanjima zaštite privatnosti na internetu među studentima Medicinsko-laboratorijske dijagnostike.

Podciljevi istraživanja su:

1. Usporediti znanje i ponašanje s obzirom na demografska obilježja (dob, spol), stupanj predznanja o pitanjima zaštite privatnosti, dnevnoj učestalosti korištenja interneta te godini studija.
2. Ispitati postoji li razlika u znanju i ponašanju između studenata Medicinsko-laboratorijske dijagnostike i studenata drugih studija Sveučilišta J. J. Strossmayer u Osijeku iz prethodno provedenog istraživanja.

3. Ispitanici i metode

3.1 Ustroj studije

Ustroj studije je presječno istraživanje.

3.2 Ispitanici

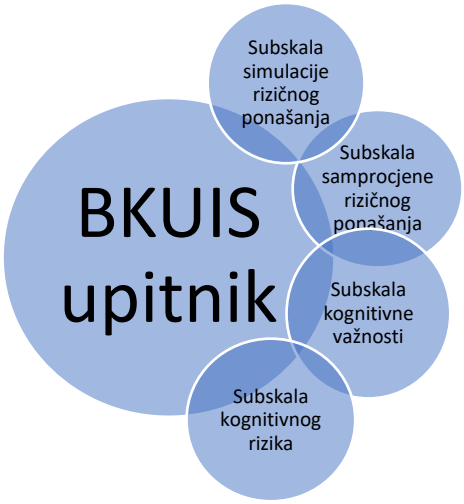
Ispitanici su bili studenti 3. i 5. godine medicinsko laboratorijske dijagnostike Medicinskog fakulteta Osijek, njih ukupno 35. U ovome istraživanju koristili su se i izvorni, još neobjavljeni podaci, prikupljeni u prethodnom istraživanju na 278 studenata Sveučilišta J. J. Strossmayer.

3.3 Etička načela

Prije same provedbe istraživanja zatražena je i dobivena suglasnost od Etičkog povjerenstva Medicinskog fakulteta Osijek za provedbu istraživanja. Broj odobrenja Etičkog povjerenstva: 2158-61-07-20-109, 20. lipnja 2020.

3.4 Metode

Za prikupljanje podataka i kao mjerni instrument koristio se znanstveno validirani upitnik: Bihevioralno kognitivni upitnik za internetsku sigurnost (BKUIS) autora Tene Velki i Krešimira Šolića. Upitnik se sastojao od četiri subskale. Prva subskala simulacijom ispituje stvarno ponašanje ispitanika uz potvrdne odgovore ili (o)davanje traženog podatka (mail adresa i lozinka). Druge tri subskale sa po četiri do pet pitanja uz ponuđene odgovore stupnjevane Likert skalom mjere stupanj rizičnosti ponašanja te stupanj znanja i svjesnosti ispitanika o pitanjima informacijske sigurnosti i zaštite privatnosti.



Slika 1. Shematski prikaz subskala BKUIS upitnika

Upitniku prethodi informacija o istraživanju te anketna pitanja kojima su se prikupili demografski podaci, stupanj predznanja o pitanjima zaštite privatnosti, dnevnoj učestalosti korištenja interneta te godini studija. Ispitivanje je bilo anonimno, a na kraju upitnika su uz zahvalu navedeni savjeti za sigurnije ponašanje na internetu.

Podaci su se prikupljali online u drugom semestru akademske godine 2019./2020. Studente treće godine je zamolio profesor da ispune upitnik nakon predavanja predmeta koji je srodan s temom koja se ispituje upitnikom. Prije ispunjavanja upitnika je naglašeno da se upitnik ispunjava dobrovoljno i da je anoniman te da je u svrhu pisanja diplomskog rada. Student koji provodi istraživanje zamolio svoje kolege pete godine da ispune upitnik u svrhu pisanja diplomskog rada te im je prije online ispune upitnika naglasio kako je upitnik anoniman te da se ispunjava dobrovoljno.

3.5 Statističke metode

Kategorijski podaci su predstavljeni apsolutnim i relativnim frekvencijama. Numerički podatci su opisani aritmetičkom sredinom i standardnom devijacijom u slučaju raspodjela koje slijede normalu, odnosno medijanom i interkvartilnim rasponom u slučaju kada ne slijede normalnu raspodjelu.

Povezanost kategorijskih varijabli testirana je Hi-kvadrat testom te po potrebi Fisherovim egzaktnim testom. Razlike numeričkih varijabli su testirane Studentovim T testom te po potrebi neparametrijskim analogonom Mann-Whitney U-testom i Kruskal-Wallis testom. Vrijednosti dobivene u statističkoj analizi smatraju se značajnim ako su manje od $\alpha = 0,05$.

4. Rezultati

4.1 Demografska obilježja ispitanika

U ovom istraživanju je sudjelovalo 35 ispitanika, od toga je značajno više (Hi-kvadrat test, P = 0,009) bilo žena, njih 28 (80,0 %). Svi ispitanici su bili studenti medicinsko laboratorijske dijagnostike, 16 ispitanika 3. godine preddiplomskog studija i 19 ispitanika 5. godine diplomskog studija. Među 35 ispitanika najveći broj ispitanika (Hi-kvadrat test, P < 0,001) je bilo između 21. i 25. godine starosne dobi (65,7 %), (tablica 1).

Tablica 1. Distribucija demografskih karakteristika ispitanika

	Kategorije	Broj (%) ispitanika	P*
Godina studija	3.	16 (45,7)	0,72
	5.	19 (54,3)	
Spol	Muški	7 (20,0)	0,009
	Ženski	28 (80,0)	
Starosna dob	Od 18 do 20	1(2,9)	< 0,001
	Od 21 do 25	30 (85,7)	
	Od 26 do 30	4 (11,4)	
Procjena znanja o informacijskoj sigurnosti i privatnosti	Slabo	3 (8,6)	< 0,001
	Dobro	29 (82,6)	
	Izvrsno	3 (8,6)	
Procjena općeg tehničkog znanja o računalima i internetu	Slabo	4 (11,4)	0,001
	Dobro	27 (77,1)	
	Izvrsno	4 (11,4)	
Sudjelovanje u edukaciji o sigurnosti i privatnosti na internetu	Da	27 (77,1)	0,02
	Ne	8 (22,9)	
Koliko dugo se služe internetom	Nekoliko godina	4 (11,4)	0,01
	Pola života	24 (68,6)	
	Otkad znam za sebe	7(20,0)	
Koliko dnevno koriste internetom	2 - 3 h	10(27,6)	0,56
	4 - 5 h	16(45,7)	
	6 - 10 h	9(25,7)	

* Hi-kvadrat test

† Fisherov egzaktni test
Na otvorena pitanja u upitniku značajna većina ispitanika (Hi kvadrat test, P < 0,001) svoje znanje o informacijskoj sigurnosti te svoje opće tehničko znanje procjenjuje kao dobro. Također većina studenata (Hi kvadrat test, P = 0,02) je sudjelovala u nekoj vrsti edukacije o sigurnosti i zaštiti privatnosti na internetu te se većinom (Hi kvadrat test, P = 0,01) internetom služe već pola svog života (tablica 1).

4.2 Rezultati prema subskalama BKUIS-a

Prema distribuciji vrijednosti subskala BKUIS upitnika nije nađena statistički značajna razlika (tablica 2).

Tablica 2. Distribucija vrijednosti/pokazatelja subskala BKUIS-a

Subskale BKUIS-a	Min	Max	Aritmetička sredina	SD
Subskala simulacije rizičnog ponašanja	0	4,00	1,17	1,40
Subskala samprocjene rizičnog ponašanja	0	1,00	0,16	0,29
Subskala kognitivne važnosti	1,00	3,75	3,13	0,67
Subskala kognitivnog rizika	0,80	3,80	2,63	1,10

S obzirom na godinu studija ispitanika nije nađena statistički značajna razlika prema subskalama BKUIS upitnika (tablica 3).

Tablica 3. Razlike po subskalama BKUIS-a s obzirom na godinu studija

Subskale BKUIS-a	Aritmetička sredina (SD)		P*
	3. god.	5. god.	
Subskala simulacije rizičnog ponašanja	1,5 (1,41)	0,89 (1,33)	0,20
Subskala samoprocjene rizičnog ponašanja	0,13 (0,25)	0,18 (0,32)	0,79
Subskala kognitivne važnosti	3,09 (0,61)	3,16 (0,71)	0,53
Subskala kognitivnog rizika	2,93 (1,08)	2,39 (1,06)	0,15

* Mann-Whitney test

Prema BKUIS upitniku uočili smo kako postoji statistički značajna razlika u sbuskali kognitivnog rizika (Mann-Whitney test, P = 0,02) koji nam pokazuje razliku s obzirom na spol ispitanika (tablica 4). Dobiveni rezultati ukazuju kako žene imaju bolji rezultat od muškaraca prema subskali kognitivne važnosti BKUIS upitnika.

Tablica 4. Razlike po subskalama BKUIS-a s obzirom na spol

Subskale BKUIS-a	Aritmetička sredina (SD)		P*
	Muško	Žensko	
Subskala simulacije rizičnog ponašanja	1,14 (1,55)	1,07 (1,36)	0,81
Subskala samoprocjene rizičnog ponašanja	0,11 (0,26)	0,17 (0,30)	0,50
Subskala kognitivne važnosti	3,14 (0,65)	3,13 (0,67)	0,85
Subskala kognitivnog rizika	1,43 (0,69)	2,94 (0,97)	**0,02**

* Mann-Whitney test

Nije nađena statistički značajna razlika u subskalama prema BKUIS upitniku s obzirom na starosnu dob ispitanika (tablica 5).

Tablica 5. Razlike po subskalama BKUIS-a s obzirom na starosnu dob

Subskale BKUIS-a	Aritmetička sredina (SD)			P*
	18 - 20 g.	21 - 25 g.	26 - 30 g.	
Subskala simulacije rizičnog ponašanja	2,00 (0,00)	1,07 (1,39)	1,75 (1,48)	0,43
Subskala samoprocjene rizičnog ponašanja	0 (0,00)	0,16 (0,29)	0,19 (0,32)	0,84
Subskala kognitivne važnosti	3,25 (0,00)	3,13 (0,72)	3,13 (0,38)	0,88
Subskala kognitivnog rizika	2,00 (0,00)	2,55 (1,13)	3,45 (0,46)	0,31

* Kruskal-Wallis test

Ispitujući razlike po subskalama BKUIS upitnika s obzirom na znanje o informacijskoj sigurnosti dobivena je statistički značajna razlika (Kruskal-Wallis test, P = 0,003), dok kod preostalih tri subskala nema statistički značajnih razlika. Značajno najveću ocjenu dobili su ispitanici sa slabim znanjem o informacijskoj sigurnosti koji su se značajno najlošije procijenili (tablica 6).

Tablica 6. Razlike po subskalama BKUIS-a s obzirom na znanje o informacijskoj sigurnosti

Subskale BKUIS-a	Aritmetička sredina (SD)			P*
	Slabo	Dobro	Izvrsno	
Subskala simulacije rizičnog ponašanja	1,00 (1,30)	1,28 (1,42)	0,33 (1,22)	0,56
Subskala samoprocjene rizičnog ponašanja	0,75 (0,32)	0,09 (0,30)	0,17 (0,22)	**0,003**
Subskala kognitivne važnosti	3,17 (1,18)	3,16 (0,53)	2,75 (0,78)	0,51
Subskala kognitivnog rizika	2,73 (1,19)	2,70 (1,13)	1,93 (0,75)	0,60

* Kruskal-Wallis test

Prema razini općeg tehničkog znanja ispitanika prema BKUIS subskalama nema statističkih značajnih razlika (tablica 7).

Tablica 7. Razlike po subskalama BKUIS-a s obzirom na opće tehničko znanje

Subskale BKUIS-a	Aritmetička sredina (SD)			P*
	Slabo	Dobro	Izvrsno	
Subskala simulacije rizičnog ponašanja	1,75 (1,41)	1,11 (1,44)	1 (0,47)	0,64
Subskala samoprocjene rizičnog ponašanja	0,19 (0,00)	0,16 (0,24)	0,3 (0,24)	0,99
Subskala kognitivne važnosti	2,94 (0,42)	3,15 (0,67)	3,19 (0,74)	0,94
Subskala kognitivnog rizika	2,95 (0,77)	2,59 (1,11)	2,6 (1,05)	0,80

* Kruskal-Wallis test

Dobiveni rezultati ukazuju kako nema statističkih značajnih razlika po skalama BKUIS upitnika (tablica 8).

Tablica 8. Razlike po subskalama BKUIS-a s obzirom na sudjelovanje u edukacijama o sigurnosti i privatnosti na Internetu

Subskale BKUIS-a	Aritmetička sredina (SD)		P*
	Nisu imali edukaciju	Imali neku edukaciju	
Subskala simulacije rizičnog ponašanja	1,00 (1,32)	1,22 (1,41)	0,54
Subskala samoprocjene rizičnog ponašanja	0,13 (0,18)	0,17 (0,32)	0,68
Subskala kognitivne važnosti	3,22 (0,40)	3,10 (0,73)	0,63
Subskala kognitivnog rizika	3,03 (1,05)	2,52 (1,09)	0,19

* Mann-Whitney test

Kod ispitivanja razlika po subskalama BKUIS upitnika ispitanika s obzirom na „koliko dugo koriste internet“ (tablica 9), te razlike s obzirom na „koliko dnevno koriste internet“ (Tablica 10), nije pronađena statistički značajna razlika.

Tablica 9. Razlike po subskalama BKUIS-a s obzirom na „to koliko dugo koriste internet“

Subskale BKUIS-a	Aritmetička sredina (SD)			P*
	Nekoliko godina	Pola života	Otkad znam za sebe	
Subskala simulacije rizičnog ponašanja	2,00 (1,58)	1,08 (1,32)	1,00 (1,41)	0,48
Subskala samoprocjene rizičnog ponašanja	0,25 (0,31)	0,14 (0,29)	0,18 (0,29)	0,56
Subskala kognitivne važnosti	2,63 (0,96)	3,22 (0,49)	3,11 (0,84)	0,64
Subskala kognitivnog rizika	2,75 (1,05)	2,66 (1,14)	2,49 (0,98)	0,89

* Kruskal-Wallis test

Tablica 10. Razlike po subskalama BKUIS-a s obzirom na „to koliko dnevno koriste internet“

Subskale BKUIS-a	Aritmetička sredina (SD)			P*
	2 - 3 h	4 - 5 h	6 - 10 h	
Subskala simulacije rizičnog ponašanja	1,6 (1,78)	1,13 (1,27)	0,78 (0,93)	0,76
Subskala samoprocjene rizičnog ponašanja	0,25 (0,34)	0,19 (0,30)	0 (0,00)	0,12
Subskala kognitivne važnosti	3,18 (0,82)	3,17 (0,54)	3 (0,66)	0,61
Subskala kognitivnog rizika	2,96 (1,10)	2,61 (1,01)	2,13 (1,10)	0,23

* Kruskal-Wallis test

4.3 Usporedba rezultata s prethodnim istraživanjem

Usporedbom rezultata ovog istraživanja u kojem je sudjelovalo 35 studenata Medicinske laboratorijske dijagnostike (MLD) Medicinskog fakulteta s prethodnim istraživanjem u kojem je sudjelovalo 287 studenata drugih sastavnica Sveučilišta J.J. Strossmayera u Osijeku nije pronađena statistički značajna razlika u rezultatima po subskalama BKUIS upitnika (tablica 11).

Tablica 11. Razlike rezultata po subskalama BKUIS-a upitnika s prethodnim istraživanjem

Subskale BKUIS-a	Aritmetička sredina (SD)		P*
	MLD studenti	Studenti drugih fakulteta Sveučilišta	
Subskala simulacije rizičnog ponašanja	1,17 (1,42)	1,21 (1,18)	0,85
Subskala samoprocjene rizičnog ponašanja	0,16 (0,30)	0,20 (0,40)	0,57
Subskala kognitivne važnosti	3,13 (0,68)	3,01 (0,71)	0,34
Subskala kognitivnog rizika	2,63 (1,12)	2,87 (1,12)	0,23

* Studentov T test

5. Rasprava

U ovom istraživanju je sudjelovalo 35 studenata Medicinsko laboratorijske dijagnostike 3. i 5. godine Medicinskog fakulteta u Osijeku. Istraživanje je provedeno korištenjem Bihevioralno-kognitivnog upitnika internetske sigurnosti (BKUIS) koji je podijeljen na 4 skupine pitanja, tj. subskale: subskala rizičnog ponašanja, subskala procjene rizičnog ponašanja, subskala kognitivne važnosti i subskala kognitivnog rizika.

Istraživanje je provedeno kako bi se među studentima Medicinske laboratorijske dijagnostike ispitao stupanj rizičnog ponašanja te njihovo znanje o zaštiti privatnosti na internetu. Osim toga, istraživanje se provelo kako bi se prema subskalama BKUIS upitnika usporedilo njihovo znanje i ponašanje s obzirom na njihova demografska obilježja te ispitala razlika ovog istraživanja i prijašnjeg provedenog istraživanja drugih studenata ostalih studija Sveučilišta J.J. Strossmayera u Osijeku prema subskalama BKUIS upitnika.

Najveći broj ispitanika je bio između 21. i 25. godina starosne dobi, njih 30 (85,7 %). U procjeni svog znanja o informacijskoj sigurnosti i privatnosti, 29 (82,6 %) ispitanika je procijenilo kako imaju dobro znanje, a u procjeni općeg tehničkog znanja o računalima i internetu 27 (77,1 %) ispitanika je procijenilo dobro opće tehničko znanje. Rezultati su bili očekivani s obzirom da smo okruženi raznim uređajima, aplikacijama i modernom tehnologijom kojom se služimo gotovo u svim segmentima života. Od 35 ispitanika njih 27 je sudjelovalo u edukacijama o sigurnosti i privatnosti u korištenju interneta, što je jako važno s obzirom da se većina ispitanika dnevno koristi internetom 4 do 5 sati. Na pitanje koliko se dugo koriste internetom, više od pola ispitanika, njih 24 (68,6%) je odgovorilo kako se koriste internetom „pola života“.

Prema rezultatima se može reći kako je većina ispitanika sama sebe procijenila kako dobro poznaju rizike i opasnosti koje su prisutne u korištenju interneta te da imaju dobro opće znanje o računalima i internetu, dok je stimulacijom dobivena veća rizičnost u usporedbi sa samoprocjenom što se slaže s prethodnim provedenim istraživanjem (13).

Prema subskalama BKUIS upitnika u dobivenim rezultatima nema značajne statističke razlike među studentima 3. i 5. godine (tablica 3), što nam ukazuje da studenti 3. i 5. godine imaju podjednako znanje o zaštiti i sigurnosti na internetu te podjednaku svjesnost o opasnostima i rizicima kojim se izlažu korištenjem interneta. Daljnjom statističkom obradom dobivenih

podataka i usporedbom rezultata prema spolu ispitanika (tablica 4), pokazalo se da nema statistički značajnih razlika prve tri već spomenute subskale, dok se kod četvrte subskale, tj. subskale kognitivnog rizika, javlja značajnija statistička razlika (Mann-Whitney test, P = 0,02) koja se može interpretirati kako žene imaju višu razinu svjesnosti potencijalnih rizika pri korištenju interneta od muškaraca. S obzirom da su i u prijašnjem istraživanju bili slični rezultati koji su ukazivali kako su žene opreznije od muškaraca, dobiveni su očekivani rezultati.

Prema subskalama BKUIS upitnika i statistički obrađenih podataka nema statistički značajnih razlika u rezultatima uspoređujući ih prema starosnoj dobi ispitanika (Kruskal-Wallis test, P > 0,05), no možemo zamijetiti nešto više vrijednosti aritmetičkih sredina ispitanika koji su starosne dobi između 26. i 30. godina što ukazuje kako su oprezniji i imaju nešto više znanja o informatičkoj sigurnosti i rizicima koji se javljaju pri korištenju interneta, ali ipak nisu dovoljne visoke vrijednosti kako bi bile statistički značajne (tablica 5). Ispitujući razlike po subskalama BKUIS-a s obzirom na znanje o informacijskoj sigurnosti (tablica 6) jedina statistički značajna razlika je prisutna kod subskale samoprocjene rizičnog ponašanja (Kruskal-Wallis test, P = 0,003) što govori kako razina znanja o informacijskoj sigurnosti utječe na rezultate prema subskalama BKUIS upitnika, dok kod preostale 3 subskale nema statističkih značajnih razlika, što su isto tako očekivani rezultati uspoređujući ih sa prijašnjim istraživanjima. Kod ispitivanja razlika po skalama BKUIS-a u odnosu na njihovo opće tehničko znanje nema statistički značajnijih razlika (tablica 7) što ukazuje kako razina znanja o informacijskoj sigurnosti ima veći utjecaj na rezultate prema subskalama BKUIS upitnika. Isto tako nema statističkih značajnih razlika ni kod usporedbi osoba koje su imale neku vrstu edukacija vezano o sigurnosti i privatnosti na internetu i osoba koja nisu imale nikakvu edukaciju (tablica 8) što odstupa od očekivanih rezultata jer su očekivanja bila da će osobe koje su imale neku vrstu edukacije na tu temu imati znatno bolje rezultate prema subskalama BKUIS upitnika. Važno je istaknuti kako nema statističkih značajnih razlika prema subskalama BKUIS upitnika neovisno o vremenu i koliko često ispitanici koriste internet što su zanimljivi rezultati jer su očekivanja bila kako će osobe koje provode više i duže vremena koristeći internet, imati više znanja i višu razinu svjesnosti o rizicima i opasnostima koje se javljaju pri korištenju interneta.

Usporedbom ovog istraživanja gdje su ispitanici bili studenti treće i pete godine smjera: Medicinsko laboratorijske dijagnostike Medicinskog fakulteta u Osijeku s već spomenutim prijašnjim provedenim istraživanjem u kojem je sudjelovalo 287 studenata Sveučilišta J.J.

Strossmayera u Osijeku (tablica 11), uočavamo kako nema statistički značajnih razlika te kako je razlika u dobivenim rezultatima gotovo nezamjetljiva. Možemo uočiti kako su vrijednosti aritmetičkih vrijednosti u prijašnjem istraživanju nešto više u svim subskalama osim kod subskale kognitivne važnosti. No ipak, razlika između ovog i prijašnjeg istraživanja nije velika ni statistički značajna. Razina znanja i razina svjesnosti o važnosti zaštite privatnosti na internetu čini se podjednaka kod ispitanika u oba istraživanja. Dobiveni rezultati u ovom istraživanju u usporedbi s prethodnim već provedenim istraživanjem su očekivani rezultati s obzirom da se radi o mladoj populaciji u oba provedena istraživanja.

U ovom istraživanju sudjelovao je relativno mali broj ispitanika te bi trebalo ponoviti isto ovakvo istraživanje s većim brojem ispitanika. No, bez obzira na broj ispitanika istraživanje je uspješno provedeno te pokazuje relativno dobro znanje ispitanika o pitanjima zaštite privatnosti i rizicima koji se javljaju pri korištenju interneta.

6. Zaključak

Na osnovi dobivenih rezultata možemo zaključiti sljedeće:

- U ovom istraživanju nema statistički značajnih razlika po subskalama BKUIS upitnika s obzirom na godinu studija ispitanika.
- S obzirom na spol ispitanika postoji statistički značajna razlika prema subskali kognitivnog rizika BKUIS upitnika koja nam govori kako su žene opreznije i imaju višu razinu svjesnosti o potencijalnim rizicima pri korištenju interneta.
- Nema statistički značajnih razlika prema subskalama BKUIS upitnika s obzirom na dob ispitanika.
- Razina znanja o informacijskoj sigurnosti prema subskalama BKUIS upitnika ima statistički značajnu razliku u samoprocjeni rizičnog ponašanju pri korištenju interneta, najlošije su se samoprocijenile osobe sa slabim predznanjem.
- S obzirom na razinu tehničkog znanja prema subskalama BKUIS upitnika nema statistički značajnih razlika.
- S obzirom na to jesu li ispitanici sudjelovali u nekoj vrsti edukacije o sigurnosti i privatnosti na internetu i ispitanika koji nisu sudjelovali u takvim edukacijama, nema statističkih značajnih razlika prema subskalama BKUIS upitnika.
- Prema subskalama BKUIS upitnika nema statističkih značajnih razlika s obzirom koliko se dugo i često ispitanici koriste internetom.
- U usporedbi ispitanika ovog istraživanja s ispitanicima prijašnjeg istraživanja na ostalim fakultetima sveučilišta, zaključujemo kako se ispitanici statistički ne razlikuju po znanju i svjesnosti o opasnostima i rizicima pri korištenju interneta prema subskalama BKUIS upitnika.

Kako je internet postao sastavni dio života većine ljudi i s obzirom na rezultate ovog istraživanja, vidi se kako postoji potreba za dodatnom edukacijom kojom bi se podigla razina svjesnosti o rizicima i opasnostima koji se javljaju pri korištenju interneta i kako bi se sveo rizik ponašanja na minimum.

7. Sažetak

Cilj istraživanja: ispitati stupanj rizičnog ponašanja te razinu znanja o pitanjima zaštite privatnosti na internetu među studentima Medicinsko laboratorijske dijagnostike Medicinskog fakulteta u Osijeku te usporediti sa studentima drugih studija Sveučilišta J. J. Strossmayer u Osijeku iz prethodno provedenog istraživanja.

Nacrt studije: Istraživanje je provedeno kao presječno.

Ispitanici i metode: U istraživanju je sudjelovalo 35 studenata treće i pete godine Medicinsko laboratorijske dijagnostike. Istraživanje je provedeno na Medicinskom fakultetu u Osijeku. Kao instrument istraživanja je korišten validirani upitnik: „Bihevioralno kognitivni upitnik za internetsku sigurnost“ (BKUIS).

Rezultati: U usporedbi rezultata treće i pete godine Medicinsko laboratorijske dijagnostike nema statističkih značajnih razlika u dobivenim rezultatima. Usporedivši ovo istraživanje s prijašnjim istraživanjem koje se provelo na studentima drugih Sveučilišta J.J. Strossmayera u Osijeku također nema statističkih značajnih razlika te se potvrđuju očekivani rezultati.

Zaključak: Prema dobivenim i statistički obrađenim rezultatima možemo zaključiti kako nema značajnih statističkih razlika među studentima treće i pete godine Medicinsko laboratorijske dijagnostike u znanju i razini svjesnosti o opasnosti i rizicima koji se javljaju pri korištenju interneta. Isto tako nema statističkih značajnih razlika u rezultatima i usporedbi s prijašnjim istraživanjem.

Ključne riječi: internet, studenti Medicinsko laboratorijske dijagnostike, opasnost i rizici

8. Summary

Examining students' knowledge and behavior on the Internet privacy issues usnig social engineering method

Research goal: To examine the degree of risky behavior and the level of knowledge on issues of privacy protection on the Internet among students from the Medical Laboratory Diagnostics program at the Faculty of Medicine in Osijek, and make a comparison with students from other study programs at the J.J. Strossmayer University of Osijek from previously conducted research.

Study plan: The research was conducted as a cross-section.

Subjects and methods: The study involved 35 third- and fifth-year students from the Medical Laboratory Diagnostics program. The research was conducted at the Faculty of Medicine in Osijek. A validated questionnaire titled "Behavioral Cognitive Questionnaire for Internet Security" (BKUIS) was used as a research instrument.

Results: In comparison with results from the third and fifth year of the Medical Laboratory Diagnostics program, there are no statistically significant differences in the obtained results. Comparing this research with previous research involving students from other J.J. Strossmayer Universities in Osijek also showed no statistically significant differences and confirms the expected results.

Conclusion: According to the obtained and statistically processed results, we can conclude that there are no significant statistical differences among third and fifth year students in the Medical Laboratory Diagnostics program in terms of knowledge and level of awareness as to the dangers and risks that occur when using the Internet. There are also no statistically significant differences in the results and comparison with the previous study.

Keywords: Internet, Medical Laboratory Diagnostics students, danger and risks.

9. Literatura

1. Borić Letica I., Borovac T., Duvnjak I. i sur., „Izazovi digitalnog svijeta“, 1. izd., Osijek: Fakultet za odgojne i obrazovne znanosti Sveučilišta J.J. Strossmayera u Osijeku; 2019.
2. Dinleyici M., Carman K. B., Ozturk E., Sahin-Dagli F., “Media Use by Children, and Parents’ Views on Children’s Media Usage”, Interactive Journal of Medical Research,2016; 5 (2), 18.
3. Velki T., Šolić K., Gorjanac, V., Nenadić K., „Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results“, Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, 2017; 2, 1496-1500.
4. Lebek B., Uffen J., Neumann M., Hohler, B. i Breitner, M. H., “Information security awareness and behavior: a theory-based literature review”, Management Research Review, 2014; 37 (12), 1049-1092.
5. Velki T., Romstein K., „User Risky Behavior and Security Awareness through Lifespan“, International Journal of Electrical and Computer Engineering Systems, 2018; 9 (2), 53-60.
6. Sasse M. A., Brostoffand S., Weirich D., „Transforming the ‘weakest link’ - a human/ computer interaction approach to usable and effective security”, BT Technology Journal, 2001; 19 (3), 122-131.
7. Öğütçü G., Testik Ö.M., Chouseinoglou O., „Analysis of personal information security behavior and awareness”, Computers & Security, 2016; 56, 83-93.
8. Egelman S., Harbach M., Péer E., „Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS)”, Proceedings of Annual ACM Conference on Human Factors in Computing Systems, 2016; 16, 5257–5261.

9. Rathore S., Sharma K. P., Loia V., Jeong Y. S., Park J. H., „Social network security: Issues, challenges, threats, and solutions“, Information Sciences, 2017; 421, 43-69.

10. Šolić K., Jović F., Blažević D., „An Approach to the Assessment of Potentially Risky Behavior of ICT System's Users“, Tehnički vjesnik, 2013; 20 (2), 335-342.
11. Šolić K., Nenadić K., Galić D., „Empirical Study on the Correlation between User Awareness and Information Security", International Journal of Electrical and Computer Engineering Systems, 2012; 3 (2), 47-51.
12. Šolić K., Ilakovac V., „Security perception of a portable PC user (The difference between medical doctors and engineers): a pilot study“, Medicinski glasnik Dubojsko-tuzlanskog kantona, 2009; 6 (2), 261-264 .
13. Velki T., Šolić K., Nenadić K., „Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS)“, Psihologijske teme, 2015; 24 (3), 401-424.

10. Životopis

Ime i prezime: Enis Horvat

Datum i mjesto rođenja: 31.01.1995., Koprivnica

Adresa: Trg kralja Tomislava 24, 48327 Molve

Mobitel: 099 766 1377

E-pošta: ehorvat.enis@gmail.com

Obrazovanje:

2001. - 2009. Osnovna škola Molve

2011. - 2015. Srednja škola Koprivnica, Medicinska sestra/tehničar opće njege

2015. - 2018. Zdravstveno Veleučilište Zagreb, Preddiplomski stručni studij Medicinsko laboratorijske dijagnostike

2018. - 2020. Medicinski fakultet Osijek, Diplomski studij Medicinsko laboratorijske dijagnostike