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

Enis Horvat i Krešimir Šolić
Medicinski fakultet Osijek, Katedra za medicinsku statistiku i medicinsku informatiku, Osijek, Hrvatska
e-pošta: ehorvat.enis@gmail.com, kresimir@mefos.hr

Cilj ovog diplomskog rada je bio 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. Diplomski je koncipiran kao presječno istraživanje, u kojem su sudjelovali studenti treće i pete godine Medicinsko laboratorijske dijagnostike. Instrument za prikupljanje podataka je bio validirani upitnik „Bihevioralno kognitivni upitnik za internetsku sigurnost“ (BKUIS). Rezultati su pokazali kako nema značajne razlike između studenata različitih studijskih godina niti različitih sastavnica Sveučilišta J.J. Strossmayera u Osijeku. Razlika je nađena jedino prema spolu, gdje su očekivano ispitanice pažljivije i opreznije od ispitanika. Usporedbom sa ranijim istraživanjima dobija se opći zaključak kako su novije generacije svijesnije o rizicima na internetu te se ponašaju sigurnije, iako bi prosječne ocjene po svim ispitivanim subskalama trebale biti znatno bolje.
Ključne riječi: informacijska sigurnost; zaštita privatnosti; rizično ponašanje; Internet; BKUIS

Uvod

Zbog razvoja tehnologije i sveprisutnosti interneta danas imamo veliki protok informacija te visoku dostupnost informacijama, što za posljedicu ima mnogo pozitivnih, ali i puno negativnih elemenata. Internet je za većinu ljudi postao svakodnevnica i nešto neophodno, isprepleten je gotovo u svakom aspektu ljudskog života. Razlog tome je širok raspon sadržaja i usluga koje nudi te zato što cjelokupan proces ekspanzije interneta još uvijek traje i raste svakim danom.

Međutim, zbog ubrzanog načina života i neznanja, korisnici Interenta u velikoj mjeri nisu svjesni svjesni negativnih strana korištenja i sveprisutnosti interneta. Danas se većina prevara na internetu zasniva na socijalnom inženjeringu koji bismo mogli definirati kao psihološku manipulaciju ljudi u svrhu otkrivanja vlastitih povjerljivih podataka, a s ciljem ostvarivanja materijalne koristi (1).

Kako nema dobnih granica korištenja interneta, najranjivija skupina korisnika interneta su djeca. Iako su djeca, pa zatim tinejđeri, detektirni kao najranjivije skupine, svi korisnici interneta, bez obzira na dob, zbog slabog poznavanja pravila sigurnosti, zbog svoje naivnosti i neiskustva su potencijalne žrtve online prevara (2, 3).

Za razliku od djece i mladih, velik broj ljudi koristi internet neizbježno zbog prirode posla kojeg obavljaju, a upravo su poslovni subjekti zanimljiviji online lopovima, jer takve prevare mogu biti znatno financijski izdašnije nego uspješne prevare nad privatnim osobama (4, 5).

Stoga je od velike važnosti edukacijom utjecati na svijest 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 (7, 8).

Razvojem tehnologije došlo je do razvoja i informacijskog sustava u zdravstvu, što je omogućilo brže i lakše komuniciranje ljudi u zdravstvu, bolje izmjene i dostupnost informacijama, organizacijska poboljšanja te značajne uštede vremena (9). Uz nabrojane prednosti javlja se problem zaštite informacija i privatnosti kako pacijenata tako i zdravstvenih djelatnika. Zaštita podataka o zdravstvenom stanju pacijenata, uz neophodnu tajnost, stavlja ove podatke u posebnu skupinu osobnih podataka koju zbog svoje osjetljive prirode zdravstveni djelatnici moraju oprezno koristiti (1). Informacijko-komunikacijska zaštita BIS i LIS sustava treba biti na izrazito visokom nivou, a korisnici sustava trebaju imati dovoljno znanja da ne bi bili sigurnosno slabiji element sustava od tehničke i programske zaštite. 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).

Cilj ovog istraživanja bio je ispitati stupanj rizičnog ponašanja te razinu znanja o pitanjima zaštite privatnosti na internetu među studentima Medicinsko-laboratorijske dijagnostike te ih usporediti sa studentima drugih sastavnica Sveučilišta J. J. Strossmayer u Osijeku.

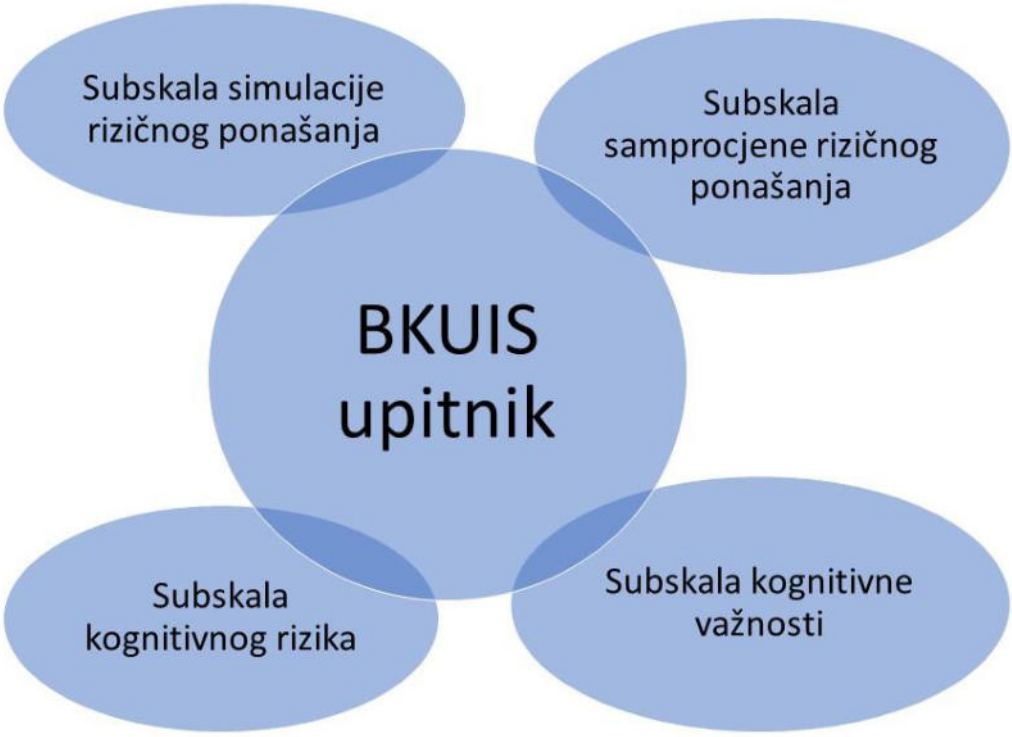
Ispitanici i metode

U ovoj presječnoj studiji ispitanici su bili studenti treće i pete godine Medicinsko-laboratorijske dijagnostike Medicinskog fakulteta u Osijeku te su se koristili podaci prikupljeni u prethodnom istraživanju na studenatima drugih sastavnica Sveučilišta J. J. Strossmayer.

Za prikupljanje podataka korišten je znanstveno validirani upitnik: Bihevioralno kognitivni upitnik za internetsku sigurnost (BKUIS) autora Velki i Šolić (10). 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. Veća ocjena u prve dvije subskale znači rizičnije ponašanje, dok veća ocjena u druge dvije skale znači veće znanje i svijesnost ispitanika (Slika 1).

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. Prije ispunjavanja upitnika je naglašeno da se upitnik ispunjava dobrovoljno i da je anoniman te da je u svrhu pisanja diplomskog rada.

Za statističku obradu prikupljenih podataka korištene su standardne metode: za analizu kategorijskih podataka korišteni su Hi-kvadrat test te po potrebi Fisherov egzaktni test, dok su za analizu numeričkih podataka korišteni Studentov T test te Mann-Whitney U-test i Kruskal-Wallis test. Vrijednosti dobivene u statističkoj analizi smatraju se značajnim ako su manje od $\alpha = 0,05$.



Slika 1. *Shematski prikaz subskala BKUIS upitnika*

Rezultati

U 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 s treće godine preddiplomskog studija i 19 ispitanika s pete godine diplomskog studija. Među ispitanicima značajno najveći broj (Hi-kvadrat test, P < 0,001) je bilo između 21. i 25. godine starosne dobi (65,7 %). 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.

Nije nađena statistički značajna razlika prema subskalama BKUIS upitnika niti s obzirom na godinu studija ispitanika, ni prema većini drugih promatranih parametara, ni usporedbom sa ostalim studentima Sveučilišta (Tablica 1).

Značajna razlika dobivena je u subskali kognitivnog rizika (Mann-Whitney test, P = 0,02) s obzirom na spol ispitanika, gdje su žene postigle bolji rezultat od muškaraca. Također je nađena značajna razlika između ispitanika s obzirom na stupanj znanja o informacijskoj sigurnosti (Kruskal-Wallis test, P = 0,003), odnosno najvećom ocjenom (najrizičnije ponašanje) su ocjenjeni ispitanici sa slabim znanjem (Tablica 1).

***Tablica 1**. Razlike rezultata po subskalama BKUIS-a upitnika s s obzirom na različite podjele*

Vrsta podjele		**Subskale BKUIS-a** /Aritmetička sredina (SD)							
		Simulacija rizičnog ponašanja	P	Samoprocjena rizičnog ponašanja	P	Kognitivne važnosti	P	Kognitivni rizik	P
Godina studija	treća	1,5 (1,41)	0,20*	0,13 (0,25)	0,79*	3,09 (0,61)	0,53*	2,93 (1,08)	0,15*
	peta	0,89 (1,33)		0,18 (0,32)		3,16 (0,71)		2,39 (1,06)	
Spol	Muško	1,14 (1,55)	0,81*	0,11 (0,26)	0,50*	3,14 (0,65)	0,85*	1,43 (0,69)	***0,02****
	Žensko	1,07 (1,36)		0,17 (0,30)		3,13 (0,67)		2,94 (0,97)	
Dob	18 - 20	2,00 (0,00)	0,43†	0 (0,00)	0,84†	3,25 (0,00)	0,88†	2,00 (0,00)	0,31†
	21 - 25	1,07 (1,39)		0,16 (0,29)		3,13 (0,72)		2,55 (1,13)	
	26 - 30	1,75 (1,48)		0,19 (0,32)		3,13 (0,38)		3,45 (0,46)	
Stupanj znanja	Slabo	1,00 (1,30)	0,56†	0,75 (0,32)	***0,003†***	3,17 (1,18)	0,51†	2,73 (1,19)	0,60†
	Dobro	1,28 (1,42)		0,09 (0,30)		3,16 (0,53)		2,70 (1,13)	
	Izvrsno	0,33 (1,22)		0,17 (0,22)		2,75 (0,78)		1,93 (0,75)	
Opće tehničko znanje	Slabo	1,75 (1,41)	0,64†	0,19 (0,00)	0,99†	2,94 (0,42)	0,94†	2,95 (0,77)	0,80†
	Dobro	1,11 (1,44)		0,16 (0,24)		3,15 (0,67)		2,59 (1,11)	
	Izvrsno	1 (0,47)		0,3 (0,24)		3,19 (0,74)		2,6 (1,05)	
Prethodna edukacija	Ne	1,00 (1,32)	0,54*	0,13 (0,18)	0,68*	3,22 (0,40)	0,63*	3,03 (1,05)	0,19*
	Imali su	1,22 (1,41)		0,17 (0,32)		3,10 (0,73)		2,52 (1,09)	
Korištenje interneta	Nekoliko godina	2,00 (1,58)	0,48†	0,25 (0,31)	0,56†	2,63 (0,96)	0,64†	2,75 (1,05)	0,89†
	Pola života	1,08 (1,32)		0,14 (0,29)		3,22 (0,49)		2,66 (1,14)	
	Oduvjek	1,00 (1,41)		0,18 (0,29)		3,11 (0,84)		2,49 (0,98	
Internet na dnevnoj bazi	2 - 3 h	1,6 (1,78)	0,76†	0,25 (0,34)	0,12†	3,18 (0,82)	0,61†	2,96 (1,10)	0,23†
	4 - 5 h	1,13 (1,27)		0,19 (0,30)		3,17 (0,54)		2,61 (1,01)	
	6 - 10 h	0,78 (0,93)		0 (0,00)		3 (0,66)		2,13 (1,10)	
Usporedba sa drugim studentima	MLD	1,17 (1,42)	0,85‡	0,16 (0,30)	0,57‡	3,13 (0,68)	0,34‡	2,63 (1,12)	0,23‡
	Ostali	1,21 (1,18)		0,20 (0,40)		3,01 (0,71)		2,87 (1,12)	

*Mann-Whitney test
†Kruskal-Wallis test
‡Studentov T test

Rasprava i zaključak

Istraživanje je pokazalo kako su ocjene prema svim subskalama relativno slabe, odnosno ni ponašanje niti znanje studenata na temu informacijske sigurnosti te zaštite privatnosti na internetu nije na visokoj razini, iako je većina studenata sudjelovala u nekoj vrsti edukacije. Štoviše 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 ipak dobivena veća rizičnost u usporedbi sa samoprocjenom. Korelacija između ispitivanog i samoprocjenjenog stupnja rizičnosti ponašanja na internetu nije postojala niti u ranijem istraživanju, što je na neki način i očekivano obzirom da se radi o mladoj populaciji sličnih godina i predznanja u oba provedena istraživanja (11).

Podjelom ispitanika na skupine dobivena je značajna razlika samo po jednoj subskali za spol, odnosno studentice su opreznije i ekspričnije po ponašanju, te po jednoj subskali za stupanj znanja gdje se pokazalo da slaba razina znanja dovodi do visoke ocjene rizičnosti samoprocjenjenog ponašanja. Obja rezultata su očekivana, jer se žene inače u životu opreznije ponašaju, a utjecaj edukacije na nivo znanja ne treba isticati.

Nije nađena značajna razlika niti s obzirom na starosnu dob, niti s obzirom na godinu studija, iako je ispitivanje provedeno prije edukacije na temu sigurnosti na internetu, niti s obzirom na opće tehničko znanje, niti s obzirom na eventualnu prethodnu edukaciju na temu sigurnosti. Ovi rezultati nisu očekivani, no mogu se djelomično objasniti vrlo malim uzorkom ispitanika. Također nije nađena razlika u ocjenama po subskalama niti s obzirom na učestalost korištenja interneta, niti u usporedbi sa drugim studentima Sveučilišta J.J. Strossmayer u Osijeku, što nije neočekivano. Iako nisu statistički značajni, rezultati ipak ukazuju kako su očekivano stariji ispitanici, odnosno studenti više godine studija, manje rizično ponašaju te su svijesniji rizika koji postoje pri korištenju interneta.

U ovom istraživanju sudjelovao je relativno mali broj ispitanika te bi bilo dobro ponoviti isto ovakvo istraživanje s većim brojem ispitanika. 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 te kako bi se sveo rizik ponašanja na minimum.

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 KB, 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 MH. 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 MA, 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 ÖM, 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. 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.
10. Velki T, Šolić K. Development and Validation of a New Measurement Instrument: The Behavioral-Cognitive Internet Security Questionnaire (BCISQ). International Journal of Electrical and Computer Engineering Systems 2019; 10 (1):19-24.
11. Velki T, Šolić K, Nenadić K. Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS). Psihologijske teme 2015; 24 (3): 401-42.