Bilt. Hrvat. druš. med. inform. 2023:29(1)

# Razlika u znanju i ponašanju studenata zdravstvenih studija s obzirom na sigurnost na internetu

Ivana Hardi[1], Dubravka Matijašić-Bodalec[1], Mirko Pešić[1], Krešimir Šolić[1,2]

[1]*Medicinski fakultet Sveučilišta J. J. Strossmayera u Osijeku, Osijek, Hrvatska*

[2]*Fakultet elektrotehnike, računarstva i informacijskih tehnologija Sveučilišta J. J. Strossmayera u Osijeku, Osijek, Hrvatska*

e-pošta: kresimir@mefos.hr

*Sažetak:* Cilj ovog istraživanja bio je usporediti stvarno rizično online ponašanje sa samoprocjenom istog kod studenata zdravstvenih studija te korelirati njihovo ponašanje s njihovom razinom znanja o online rizicima. Ispitanici su studenti 3. godine Preddiplomskog studija medicinsko-laboratorijske dijagnostike te studenti 2. godine Integriranog preddiplomskog i diplomskog studija medicine. Istraživanje je, kao presječna studija, provedeno na Medicinskom fakultetu u Osijeku za potrebe diplomskog rada. U istraživanju je korištena online verzija validiranog Bihevioralno-kognitivnog upitnika internetske sigurnosti (BKUIS). Rezultati su pokazali da nema korelacije između rizičnosti stvarnog i samoprocijenjenog ponašanja studenata (uz koeficijent korelacije vrlo blizu nule). Naprotiv, dobivena je slaba povezanost između veće rizičnosti stvarnog ponašanja i većeg stupnja svjesnosti o postojanju online rizika, što potvrđuje ranije definirani paradoks da se dio svjesnijih online korisnika rizičnije ponaša. Čak tri od pet ispitanika unijelo je svoju lozinku na trik pitanje o njenoj kvaliteti. Generalno, visoka je razina znanja ali visok je i stupanj rizičnosti u njihovom online ponašanju.
Od velike je važnosti daljnji rad na podizanju svjesnosti o rizicima, a pogotovo među budućim zdravstvenim djelatnicima koji će pristupati osjetljivim podacima pacijenata unutar zdravstvenog informacijskog sustava.

*Ključne riječi:* internet; rizično ponašanje; sigurnost na internetu; zaštita osobnih podataka

## Uvod

U današnje vrijeme svakodnevni poslovi u različitim ustanovama prožeti su korištenjem interneta i elektroničkih sustava te su oni postali nezaobilazni dio svih zdravstvenih ustanova čemu nam svjedoče Bolnički informacijski sustav (BIS) i Laboratorijski informacijski sustav (LIS). U medicini je prisutna sve veća informatizacija, a digitalizacija i povezivanje medicinske dokumentacije uvelike je doprinijela kvaliteti i kvantiteti rada zdravstvenih djelatnika kao i većem povjerenju korisnika (1). No, istovremeno, informatizacija je uzrokovala probleme prilikom zaštite privatnosti pacijenata koji, za medicinske svrhe, povjeravaju mnogo svojih osobnih podataka. Stoga je nužno na adekvatan način zaštititi podatke kako ne bi došlo do njihove krađe ili zlouporabe. To podrazumijeva kvalitetnu edukaciju zdravstvenih radnika, ali i studenata zdravstvenih studija o opasnostima i sigurnom načinu korištenja interneta. Tu spada uporaba kvalitetno odabranih lozinki te valjane načine njihova memoriranja, korištenje antivirusne zaštite na računalima, izrade sigurnosnih kopija, izbjegavanje posjećivanja raznih ponuđenih reklamnih stranica, opreza pri otvaranju sumnjivih mailova i slično (2).

Činjenica da mlađa populacija odrasta uz suvremenu tehnologiju nije nužan preduvjet da znaju i koristiti internet na siguran način. Veći stupanj školske naobrazbe može omogućiti veće znanje i sposobnost za daljnju sigurnost i privatnost korištenja, pohranu osobnih podataka i općenito

obitavanja u online okruženju. Međutim, bez obzira na rasprostranjenu edukaciju u našem društvu, ne može se utjecati na svakog pojedinca kako bi samostalno kvalitetno i valjano koristio dostupna sredstva (3). Razni mediji primjerice mogu doprinijeti osvještavanju velikog broja ljudi, što je već znatan pomak u sigurnosti korištenja internetom.

U bolnicama je od iznimne važnosti kvalitetna logistička potpora, informacijska te komunikacijska povezanost radi lakšeg i kvalitetnijeg liječenja pacijenata. Stoga postoje informacijski sustavi koji upravo to i omogućavaju.

Određeni oblik bolničkog informacijskog sustava postoji otkad postoji bolnički način liječenja pacijenata, ali suvremeni bolnički informacijski sustav (BIS) obavezno uključuje korištenje elektroničkih računala te računalnih mreža (4). Glavni zadatci BIS-a su podrška djelotvornoj opskrbi pacijenata, racionalno korištenje potrošnog materijala i lijekova, automatizirano administriranje, smanjenje vremena potrebnog za pohranu informacija te uporabi informacija u upravne, stručne i znanstvene svrhe (5). Postojanje jedinstvenog informacijskog sustava u sklopu bolničke ustanove znatno olakšava komunikaciju među liječnicima i ostalim osobljem.

Laboratorijski informacijski sustav (LIS) je program koji omogućava unos te obradu i pohranu podataka koji su nastali kao rezultat laboratorijskih pretraga te obuhvaća i računalnu opremu koja je potrebna kako bi se svi ti procesi odvijali (4). On pruža cjelovitu potporu radu bolničkih laboratorija, pretežito laboratorija koji na dnevnoj bazi obrađuju veći broj uzoraka (npr. biokemijski i hematološki laboratorij) (6). LIS može djelovati unutar laboratorija, izoliran od ostatka bolnice ili pak može biti uklopljen u bolnički informacijski sustav te uvelike olakšati i ubrzati proces naručivanja pretraga, obavljanja pretraga te prikaza rezultata pretraga i samim time ubrzati proces dijagnosticiranja i liječenja.

Važnost zaštite osobnih podataka pacijenata prepoznata je još iz vremena prije Krista te je i sadržana u Hipokratovoj zakletvi: „Što po svojem poslu budem saznao ili vidio, pa i inače, u dodiru s ljudima, ukoliko se ne bude javno smjelo znati, prešutjet ću i zadržati tajnim“ (7). Pacijentu je zajamčena zaštita privatnosti medicinske dokumentacije pomoću BIS-a i LIS-a. Zahvaljujući tome liječnici gotovo odmah imaju uvid u pacijentove nalaze, čime se izbjegava mogućnost gubljenja prijašnjih papirnatih dokumenata, ali i mogućnost da neka druga, za to neovlaštena osoba vidi povjerljive podatke. Za pristup informacijskim sustavima medicinsko osoblje se mora prijaviti jedinstvenim korisničkim imenom i lozinkom koja se po pravilu mijenja svakih 90 dana, odnosno svaka 3 mjeseca. Liječnici i ostalo medicinsko osoblje s drugih odjela ne mogu imati uvid u pacijentovu medicinsku dokumentaciju, osim ako pacijent, zbog nastavka liječenja, nije upućen tim drugim liječnicima (5). Moderni LIS se u pravilu koristi mrežnim preglednicima kao klijentima. Na taj se način omogućava upis i dohvat podataka iz LIS-a na bilo kojem računalu s instaliranim mrežnim preglednikom. Pristup LIS-u je strogo ograničen upravo iz sigurnosnih razloga, kako bi se omogućila privatnost i tajnost podataka pacijenata (3).

Informatizacija i tehnološki napredak su uvelike doprinijeli olakšanoj i bržoj obradi, pohrani i pristupu podacima i informacijama, no istovremeno su nastale mnoge opasnosti, zbog kojih se poduzimaju mjere zaštite osobnih podataka. Zaštita podataka provodi se s ciljem sprječavanja krađe podataka ili zlonamjerne manipulacije podatcima (8). Pitanja privatnosti i zaštite osobnih podataka regulirana su međunarodnim konvencijama i obaveza je za sve članice Europske unije. Godine 1981. Vijeće Europe donijelo je Konvenciju za zaštitu osoba vezano za automatiziranu obradu osobnih podataka, poznatu i kao Konvencija 108 (po rednom broju donošenja). Konvencija je i danas podloga zaštite osobnih podataka, a njezina svrha je osiguravanje prava i poštovanje temeljnih sloboda svake osobe (9).

Povelja Europske unije o temeljnim pravima koja je stupila na snagu 1. prosinca 2009. godine regulira zaštitu osobnih podataka pojedinca i podizanje prava na privatnost na razinu temeljnih ljudskih prava. . Na razini Europske unije Povelja danas predstavlja svojevrsnu sigurnost zaštite osobnih podataka. Iz te Povelje je proizašla Opća uredba o zaštiti podataka (9).

Opća uredba o zaštiti podataka (NN, SL EU L119), poznata i kao GDPR - General Data Protection Regulation, stupila je na snagu 25. svibnja 2018. godine te se od tada primjenjuje na sve članice Europske unije, pa tako i na Republiku Hrvatsku. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka te je osigurana svakoj fizičkoj osobi bez obzira na njeno državljanstvo i prebivalište te neovisno o rasi, boji kože, jeziku, vjeri, spolu, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, rođenju, naobrazbi, imovini, društvenom položaju ili drugim osobinama (10). U Republici Hrvatskoj Zakonom o provedbi Opće uredbe o zaštiti podataka reguliran je nadzor nad prikupljanjem, obradom osobnih podataka i o slobodnom kretanju takvih podataka. Pod osobnim podatcima se smatraju oni iz kojih se s velikom vjerojatnošću može utvrditi identitet pojedinca. Podatci koji se GDPR-om štite su osnovni podatci (ime i prezime, broj osobne iskaznice te lokacijski podatci), zdravstveni karton, biometrijski podatci (npr. sken rožnice ili otisak prsta), podatci s kreditnih kartica, genetski podaci (npr. DNA), vjerska i filozofska uvjerenja, ekonomsko stanje, etnička pripadnost, seksualna orijentacija, spolni život, članstvo u sindikatu, IP adrese, kolačići u internet pregledniku, osobne poruke e-pošte te pseudonimizirani podaci. Ukoliko postoji potreba za obradom podataka, određuju se svrha i sredstva za obradu podataka te voditelj obrade. Oboje mora biti utvrđeno pravom Europske unije ili pravom državne članice. Pod voditeljem obrade smatra se svaka fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo pravno tijelo (11). U Republici Hrvatskoj Zakonom o zaštiti osobnih podataka osnovana je Agencija za zaštitu osobnih podataka kao samostalno i neovisno tijelo s temeljnom zadaćom provedbe nadzora nad obradom osobnih podataka (12).

Uz pretpostavku da postoji pozitivna povezanost između rizičnosti stvarnog i samoprocijenjenog ponašanja korisnika na internetu, cilj ovog istraživanja je ispitati stvarno rizično ponašanje studenata te ga usporediti s njihovom samoprocjenom rizičnog ponašanja. Dodatni cilj je ispitati razinu znanja studenata i razinu njihove svjesnosti o online rizicima te ispitati povezanost znanja i svjesnosti s rizičnošću ponašanja.

# Materijali i metode

Za ovo istraživanje korišten je online anonimni ranije validirani upitnik čiji su autori Tena Velki i Krešimir Šolić. Upitnik se sastoji od četiri samostajne subskale, a više o samome upitniku može se naći u literaturi (13). Prva subskala za simulaciju stvarnog rizičnog ponašanja stavlja ispitanike u potencijalne rizične situacije s kojima bi se oni mogli susrest pri korištenju računala i interneta (npr. „Ako želite primati obavijesti i naše besplatne promotivne materijale molim Vas upišite Vašu e-poštu“) na koje ispitanici mogu, ali i ne moraju dati odgovore te pitanja na koja odgovaraju sa da/ne. Preostale tri subskale ispitanici odgovaraju na pitanja koja se boduju po Likertovoj skali s 5 stupnjeva. Subskala samoprocjene rizičnog ponašanja se sastoji od 4 pitanja (primjer „Koliko često posuđujete pristupne podatke za Vašu e-poštu - korisničko ime i lozinka - prijateljima ili rođacima?“ ) s ponuđenih 5 stupnjeva odgovora od „nikad“ do „uvijek“. Iduća subskala se odnosi na važnost pravilnog i sigurnog korištenja računalnih sredstava s 4 pitanja (poput „Kako biste procijenili koliko je važno provjeravanje prijenosnih medija - npr. CD/DVD, USB memorija i sl. - od virusa prije upotrebe?“) gdje su stupnjevi odgovora od „nije važno“ do „jako važno“. Posljednja subskala se odnosi na rizično ponašanje ispitanika pri korištenju interneta koja uključuje 5 pitanja (primjer „Kako biste procijenili koliko je rizično hakiranje Vašeg osobnog računala, prijenosnog računala ili pametnog telefona?“) na skali Likertova tipa sa 5 stupnjeva od „nema rizika“ do „jako rizično“ (13).

Prije provođenja ovog istraživanja dobivena je suglasnost Etičkog povjerenstva Sveučilišta J. J. Strossmayera u Osijeku Medicinskog fakulteta Osijek (KLASA: 602-04/22-08/02; URBROJ:

2158-61-46-22-73; Osijek, 1. travnja 2022.)

Upitnik su ispunjavali studenti druge godine Integriranog preddiplomskog i diplomskog sveučilišnog studija medicine, njih 66 (72,5%) te studenti treće godine Preddiplomskog sveučilišnog studija medicinsko-laboratorijske dijagnostike, njih 25 (27,5%). Studenti su upitnik ispunjavali na svojim mobilnim uređajima (mobitelima) u učionici, na početku seminara kojemu je tema bila upravo informacijska i računalna sigurnost te zaštita privatnosti sa specifičnostima u zdravstvu. Studenti su upitnik popunjavali u tišini, bez dogovaranja, pod nadzorom predavača te je odaziv bio gotovo 100% ispitanika.

Kategorijski podaci su predstavljeni apsolutnim i relativnim frekvencijama. Numerički podatci su opisani aritmetičkom sredinom i standardnom devijacijom. Normalnost distribucije ispitana je Shapiro-Wilksovim testom.

Povezanost kategorijskih varijabli testirana je hi-kvadrat testom. Za ispitivanje korelacije simulacije i stvarnog ponašanja korišten je neparametrijski Spearmanov test korelacije. Statistička analiza je učinjena programskim sustavom MedCals (inačica 20.110., MedCale Software bvba). Sve p vrijednosti dobivene u statističkoj analizi smatraju se značajnim ako su manje od 0,05 te su dvostrane.

# Rezultati

U istraživanju je sudjelovao ukupno 91 ispitanik, student prosječne dobi od M = 20 (SD = 1,06) godina u rasponu od 18 do 25 godina. Značajno je više bilo studenata ženskog spola (Hi-kvadrat test, $p < 0,001$), njih 66 (72,5 %). Ispitanici su izjavili kako svakodnevno koriste internet - „barem pola svog života“, njih 62 (68,1 %) odnosno “otkad znaju za sebe“, njih 24 (26,4 %).

U prvoj subskali upitnika za simulaciju stvarnog rizičnog ponašanja koja stavlja ispitanike u potencijalne rizične situacije s kojima bi se oni mogli susresti pri korištenju računala i interneta, samo 3 ispitanika (3,3 %) je označilo da želi primati obavijesti na e-mailu, 21 ispitanik (23,1 %) je odabrao da želi putem e-pošte primiti besplatni antivirusni softver, te 18 ispitanika (19,8 %) upisalo svoju e-mail adresu ukoliko žele primati obavijesti i besplatne promotivne materijale. Na posljednje pitanje u upitniku, trik-pitanje kojim se traži upisivanje osobne lozinke (“poradi provjere njene kvalitete“), 55 ispitanika (60,4 %) je osobnu lozinku unijelo.

Iz prosječnih ocjena pojedine subskale proizlazi kako je samoprocjena ispitanika na izrazito visokoj razini (nula je najbolja ocjena), znatno višoj u odnosu na prosječnu ocjenu stvarnog ponašanja (Tablica 1).

*Tablica 1. Distribucija ocjena pojedinih subskala*

| Pojedina subskala | M (SD) | Me (25% - 75%) | min - maks |
|---|---|---|---|
| Subskala simulacije rizičnog ponašanja* | 1,07 (1,07) | 1,0 (0,0 - 1,0) | 0,0 - 4,0 |
| Subskala samoprocjene rizičnog ponašanja* | 0,17 (0,32) | 0,0 (0,0 - 0,25) | 0,0 - 1,25 |
| Subskala kognitivne važnosti zaštite† | 2,92 (0,73) | 3,0 (2,5 - 3,5) | 0,5 - 4,0 |
| Subskala svjesnosti postojanja rizika† | 2,82 (1,19) | 3,4 (1,8 - 3,8) | 0,0 - 4,0 |

**bolja je niža ocjena (ocjena nula znači najmanje rizično ponašanje)*
*†bolja je viša ocjena (najviše 4 znači izrazito visoku svjesnosti)*

Prema prosječnim ocjenama kognitivnih subskala kojima su ispitanici ocjenjivali važnost digitalne zaštite te svjesnost o online rizicima, gdje je većina ispitanika odgovarala sa „nisam siguran“, ocjene su gotovo pa vrlo dobre (bodovi su na skali od nula do četiri, pa stoga tri boda predstavljaju vrlo dobru ocjenu).

Spearmanov test korelacije pokazuje slabu, pozitivnu, statistički značajnu korelaciju između subskale simulacije (stvarno ponašanje) i subskale svjesnosti o postojanju rizika, te također između dvije kognitivne subskale, između svjesnosti o postojanju online rizika i svjesnosti o važnosti digitalne zaštite (Tablica 2).

*Tablica 2, Korelacije između pojedinih subskala*

| Parovi subskala | | rho | 95% CI | p* |
|---|---|---|---|---|
| Subskala simulacije rizičnog ponašanja† | Subskala samoprocjene rizičnog ponašanja† | 0,04 | -0,17 do 0,24 | 0,72 |
| | Subskala kognitivne važnosti zaštite‡ | 0,08 | -0,13 do 0,28 | 0,47 |
| | Subskala svjesnosti postojanja rizika‡ | 0,25 | 0,04 do 0,43 | *0,02* |
| Subskala samoprocjene rizičnog ponašanja† | Subskala kognitivne važnosti zaštite‡ | -0,19 | -0,38 do 0,02 | 0,08 |
| | Subskala svjesnosti postojanja rizika‡ | -0,03 | -0,23 do 0,18 | 0,79 |
| Subskala kognitivne važnosti zaštite‡ | Subskala svjesnosti postojanja rizika‡ | 0,32 | 0,12 do 0,49 | *0,002* |

**Spearmanov test korelacije*
*†bolja je niža ocjena (ocjena nula znači najmanje rizično ponašanje)*
*‡bolja je viša ocjena (najviše 4 znači izrazito visoku svjesnosti)*

Vrlo slaba, ali negativna povezanost, na granici statističke značajnosti dobivena je i između subskale samoprocjene rizičnog ponašanja i svjesnosti o važnosti zaštite, odnosno ispitanik manje rizično procjenjuje svoje ponašanje, ako ima višu razinu svjesnosti o važnosti digitalne zaštite. Korelacija vezana uz primarni cilj ovog istraživanja, povezanost rizičnosti stvarnog ponašanja simulacijskom subskalom i samoprocjene rizičnosti svoga ponašanja, praktički ne postoji (rho = 0,04, p = 0,72) (Tablica 2).

# Rasprava

Postavljeni glavni cilj istraživanja s pretpostavkom da postoji pozitivna povezanost između rizičnosti stvarnog i samoprocjenjenog ponašanja korisnika, nije potvrđena. Štoviše, rezultat pokazuje da nema niti blage povezanosti. Ovaj rezultat, dobiven na specifičnom uzorku, u skladu je s rezultatima ranijih istraživanja provedenih sa BKUIS upitnikom, a pokazuje kako prosječni korisnik interneta svoje online ponašanje procjenjuje puno bolje nego što ono stvarno jest (17). Još je „lošiji“ rezultat što postoji slaba, ali statistički značajna povezanost između veće rizičnosti stvarnog ponašanja procijenjenog simulacijskom subskalom i većeg stupnja svjesnosti o postojanju online rizika, što potvrđuje ranije definirani paradoks da se neki svjesniji online korisnici rizičnije ponašaju na internetu (18 - 21).

S obzirom na sekundarni cilj istraživanja, ispitana razina svjesnosti o online rizicima te važnosti

o zaštiti digitalnih podataka pokazuje indirektno vrlo dobru razinu znanja o pitanjima informacijske sigurnosti i zaštite privatnosti među ispitanicima. Ovaj rezultat pokazuje kako viša razina informacijske svjesnosti ne znači niže rizično ponašanje, odnosno ne dovodi do sigurnijeg ponašanja korisnika interneta.

Nasuprot vrlo dobre razine znanja među ispitanicima potvrda visokom stupnju rizika u stvarnom ponašanju je podatak da je čak 60,4 % ispitanika napisalo lozinku na trik-pitanje kojim je ona tražena radi procjene kvalitete, a s naglaskom na anonimnost, etičnost i znanstveni doprinos istraživanja u samome trik pitanju! Iako je točan odgovor ostavljanje praznog polja, svi odgovori poput „ne dam lozinku“ su izostavljeni, odnosno brojani kao točan odgovor. Ovaj podatak treba uzeti sa rezervom, što je pokazalo i nedavno istraživanje istom verzijom BKUIS upitnika na studentima zdravstvenih studija u susjednoj Sloveniji (16). No, čak i da je samo polovica napisanih lozinki stvarna lozinka sustava elektroničke pošte (a studenti su u 23,1 % slučajeva dali svoju adresu elektorničke pošte!) to nije zanemariva brojka.

Dosadašnja istraživanja su uglavnom ispitivala kvalitetu lozinke, no ovim upitnikom sa subskalom simulacije, odnosno trik-pitanjima, simuliran je proces tzv. pecanja (od engl. phishing) na internetu koji je pokazao koliko je prosječan korisnik tome podložan.

Budući da je prosječna ocjena na subskali samoprocjene rizičnog ponašanja niska, čak niža i od prijašnjih istraživanja (13, 16), a obje ocjene kognitivnih subskala svjesnosti i važnosti relativno vrlo dobre, proizlazi kako ispitanici imaju visok stupanj samopouzdanja u svoje znanje i vještine. Međutim, sam podatak o visokom postotku otkrivanja lozinke pokazuje kako je to samopouzdanje nerelano. Studenti očito shvaćaju kako postoji rizik pri korištenju interneta i računala te bi zbog te svjesnosti trebali ipak biti na većem oprezu pri korištenju raznih online usluga.

Prosječna ocjena subskale stvarnog rizičnog ponašanja je ipak nešto manja u odnosu na prijašnje istraživanje (13). Mlađe generacije se od malih nogu koriste računalima i internetom te je ovo vjerojatno pridonijelo činjenici da su mladi upoznati s rizicima i pravilima opreznog ponašanja na internetu, pa je sukladno tome i njihovo ponašanje manje rizično. Svi ispitanici koji su sudjelovali u istraživanju shvaćaju rizike prilikom korištenja računala i interneta, no nisu sigurni u veliku važnost pravilnog i sigurnog korištenja računalnih sredstava poput stalnog ažuriranja i mijenjanja starih lozinki te provjeravanja prijenosnih medija (npr. CD, DVD, USB memorija) od virusa. Ovo se vidi iz njihovih odgovora u trećoj subskali, gdje većina odgovara sa „nisam siguran“ na postavljena pitanja ove tematike.

Ovaj rezultat pokazuje kako bi možda kroz školovanje studentima trebalo dati više uputa te obratiti veću pozornosti na niz preventivnih mjera radi zaštite od zaraze računala poput korištenja antivirusnog softvera, potreba redovite nadogradnje i održavanja operacijskog sustava, korisnosti uključenog vatrozida (engl. firewall), korištenja skenera na virus te važnost redovite izrade rezervnih kopija vlastitih podataka (14).

Još jedna od stvari koja ima veliki utjecaj na zaštitu osobnih podataka je kvalitetna lozinka. Lozinke su često na meti hakiranja radi manipulacije, krađe identiteta i novčane ucjene, stoga je vrlo važno odabrati kvalitetnu lozinku. Ona mora biti dovoljno kratka da ju korisnik može zapamtiti, ali ipak dovoljno sigurna i duga radi bolje zaštite od hakiranja. Generalno, preporuka je koristiti kombinaciju velikih i malih slova, imati zasebne lozinke za svaki račun, ne zapisivati lozinke u datoteku koja je spremljena na računalo niti na dostupan papir te povremeno mijenjati lozinku (15).

Ipak, dobiveni rezultati su dijelom bolji nego u prethodnim istraživanjima (10, 13, 16), te se može zaključiti da postoji napredak posljednjih godina. Tome je, uz sve češća upozorenja institucija kroz medije, pridonijelo i poboljšanje edukacije. Uvođenje informatike kao obaveznog nastavnog predmeta već od prvog razreda osnovne škole svakako će dodatno pridonijeti sigurnijem ponašanju novih online generacija. U skladu s time, za očekivati je kako

će u bližoj budućnosti mladi postupati daleko sigurnije prilikom rada na računalu i korištenju interneta te će stoga buduća istraživanja biti daleko povoljnija u pogledu zaštite sigurnosti osobnih podataka no što su sadašnja.

# Zaključak

Temeljem provedenog istraživanja i dobivenih rezultata može se zaključiti kako je među ispitanicima visok stupanj rizičnosti u online ponašanju, dok je paradoksalno istovremeno i visoka razina znanja o nužnosti online zaštite, odnosno visoka je razina informacijske svijesti o rizicima i važnosti zaštite. Ovu kontradiktornost potvrđuje i nepostojanje korelacije između rizičnosti stvarnog i samoprocjenjenog online ponašanja, a dodatno potvrđuje obrnuta korelacija između svjesnosti o rizicima i rizičnosti stvarnog ponašanja.

Iako rezultati pokazuju kako samo znanje nije dovoljno, od velike je važnosti daljnji rad na podizanju svjesnost o mogućim online rizicima svih korisnika interneta. Kako su ispitanici budući zdravstveni djelatnici, to je još i bitnije jer se zbog naravi njihovog posla ne radi samo o sigurnosti njihovih osobnih podataka, nego o osobnim podatcima i zaštiti svih osoba koje koriste usluge zdravstvenog sustava, odnosno o pacijentima koji se sa povjerenjem oslanjaju na njih i na zajamčenost vlastite privatnosti.

# Literatura


1. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, i sur. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors 2021; 21(15):5119.
2. Aldawood H, Skinner G. Reviewing Cyber Security Social Engineering Training and Awareness Programs - Pitfalls and Ongoing Issues. Future Internet 2019; 11(3):73.
3. Alammari A, Sohaib O, Younes S. Developing and evaluating cybersecurity competencies for students in computing programs. PeerJ Comput Sci. 2022; 8:e827.
4. Kern J, Petrovečki M. Medicinska informatika. Zagreb: Medicinska naklada,2009.
5. Poje I, Braović M. Bolnički informacijski sustav - prednosti i nedostaci u radu. Bilten Hrvatskog društva za medicinsku informatiku 2019; 25(1):20-28.
6. "Laboratory Information System (LIS): Definition & Functions." Study.com, 23 January 2018. Dostupno na: http://study.com/academy/lesson/laboratory-informationsystem-lis-definition-functions.html, pristup 28.5.2022.
7. Borovečki A, Mustajbegović J, Jakšić Ž. Izborni predmet iz područja medicinske etike: Kako primijeniti Hipokratovu zakletvu? Zagreb: Medicinski fakultet, Škola narodnog zdravlja „Andrija Štampar“, 2013.
8. Varga M. Zaštita elektroničkih podataka. Tehnički glasnik 2011; 5(1):61-73.
9. Velki T, Šolić K, ur. Izazovi digitalnog svijeta. Osijek: Fakultet za odgojne i obrazovne znanosti Sveučilišta Josipa Jurja Strossmayera u Osijeku, 2019.
10. Velki T, Šolić K, Priručnik za informacijsku sigurnost i zaštitu privatnosti. Osijek: Fakultet za odgojne i obrazovne znanosti, Sveučilište Josipa Jurja Storssmayera u Osijeku; 2018.
11. Vodič kroz GDPR za početnike. GDPR informer. Dostupno na: https://gdprinformer.com/hr/vodic-kroz-gdpr, pristup 29.5.2022.
12. Agencija za zaštitu osobnih podataka. Dostupno na: https://azop.hr/, pristup 29.5.2022.
13. Velki T, Šolić K. Razvoj instrumenta za istraživanje socijalnog inženjeringa u populaciji

studenata: Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS). Policija i sigurnost 2020; 29(4/2020):341-355.

14. CERT - savjeti za zaštitu. Dostupno na: https://www.cert.hr/savjeti/, pristup 4.6.2022.
15. Sini.hr - Kako napraviti sigurnu lozinku. Dostupno na: https://sini.hr/2021/04/kako-napraviti-sigurnu-lozinku/, pristup 8.6.2022.
16. Velki T, Solic K, Zvanu B. Cross-cultural validation and psychometric testing of the Slovenian version of the Behavioral-Cognitive Internet Security Questionnaire (BCISQ), Elektrotehniški Vestnik 2022; 89(3):103-108.
17. Velki T, Solic K. Development and validation of a new measurement instrument: The Behavioral-Cognitive Internet Security Questionnaire (BCISQ). Int j electr comput eng syst 2019; 10(1):19-24.
18. Solic K, Plesa M, Velki T, Nenadic K. Awareness About Information Security and Privacy Among Healthcare Employees. SEEMEDJ 2019; 3(1):21-28.
19. Velki T, Romstein K. User risky behavior and security awareness through lifespan. Int j electr comput eng syst 2019; 9(2):53-63.
20. Gerber N, Gerber P, Volkamer M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Comput Secur 2018; 77:226-261.
21. Snyman DP, Kruger H, Kearney WD. I shall, we shall, and all others will: paradoxical information security behaviour. Inf Comput Secur 2018; 26(3):290-305.

# Difference in knowledge and behavior regarding Internet security among healthcare students

Ivana Hardi[1], Dubravka Matijašić-Bodalec[1], Mirko Pešić[1], Krešimir Šolić[1,2]

[1]*Faculty of Medicine, J.J. Strossmayer University of Osijek, Osijek, Croatia*

[2]*Faculty of Electrical Engineering, Computer Science and Information Technology, J.J. Strossmayer university of Osijek, Osijek, Croatia*

e-mail: kresimir@mefos.hr

*Abstract:* Aim of this research was to compare the actual risky online behavior with the self-assessment of it, among healthcare students and to correlate their behavior with their level of knowledge on online risks. The respondents were students of the 3rd year of the Undergraduate study of medical-laboratory diagnostics and students of the 2nd year of the Integrated undergraduate and graduate study of medicine. Research was conducted as a cross-sectional study at the Faculty of Medicine in Osijek for the purposes of a graduate thesis. The online version of the validated Behavioral-Cognitive Internet Security Questionnaire (BKUIS) was used in this research. The results showed that there is no correlation between the riskiness of real and self-assessed behavior among students with a correlation coefficient very close to zero. On the contrary, a weak connection was obtained between higher riskiness of actual behavior and a better degree of awareness regarding online risks, which confirms previously defined paradox that part of more aware online users behave riskier. As many as three out of five respondents entered their password to a trick question about its quality. In general, the level of knowledge is high, however, the level of riskiness in their online behavior is also high. Further work on raising awareness is of great importance, especially among future healthcare professionals who will have access to sensitive patient data within the healthcare information system.

*Keywords:* internet; risky behavior; internet security; personal data protection