SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

MEDICINSKI FAKULTET OSIJEK

Studij sestrinstva

Mateo Pleša

POTENCIJALNO RIZIČNO PONAŠANJE MEDICINSKIH SESTARA NA INTERNETU

Završni rad

Osijek, 2017.

Rad je ostvaren u: Klinički bolnički centar Osijek

Mentor rada: Krešimir Šolić, doc. dr. sc. ing.

Rad ima 22 lista, 6 tablica i 1 sliku.

Predgovor radu

Ovim putem, na kraju školovanja na preddiplomskom studiju sestrinstva, želio bih se zahvaliti svojim roditeljima, majci Vesni i ocu Ivanu, sestri Ivani i bratu Dariju koji su mi omogućili školovanje te mi uvijek bili podrška na putu koji je vodio do cilja na kojem sam sada. Isto tako, želio bih se zahvaliti gospodinu Krešimiru Šoliću, doc. dr. sc. ing., na mentorstvu i stručnom vođenju kroz proces izrade ovoga završnog rada te pomoći koju mi je pružio u ostvarenju istoga.

SADRŽAJ

Kratice:

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

ISDN – digitalna mreža integriranih usluga (engl. Integrated Services Digital Network)

DSL – digitalna pretplatnička petlja (engl. Digital Subscriber Line)

MIPRO - Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku

KBC – Klinički bolnički centar

PIN – osobni identifikacijski broj (engl. Personal Identification Number)

e-pošta – elektronska pošta (engl. electronic)

1. Uvod

1.1. Povijest nastanka interneta

Internet se nije odjednom pojavio kao globalna struktura kakva je danas. U vrijeme kasnih 50--ih i ranih 60-ih godina dvadesetog stoljeća dvije su neovisne teme bile u razvoju. Prva je tema bila istraživanje koje je s vremenom vodilo do razmjene informacija putem mreže to jest putem današnjeg interneta. U ovo su istraživanje bili uključeni Leonard Kleinrock, Paul Baran i Donald Davies koji su tražili odgovor na pitanje kako poboljšati arhitekturu, izvršavanje i teoriju umrežavanja podataka. Druga je tema, neovisna o prvoj, bila nastanak i razvoj Agencije za napredne istraživačke projekte. To je bila institucija koja je financirala projekt umrežavanja četiriju superračunala. Ova su se dva otkrića sredinom 60-ih godina spojila u jedno te napravila „prijelom“ u svjetskoj povijesti koji je vodio do razvijanja ARPANET-a. Nakon spajanja mogla je započeti faza izvršavanja i razvoja koja je uključivala nove ključne suradnike i uspješne faze razvoja u povijesti interneta. Nekoliko godina kasnije, točnije u listopadu 1972. godine, dogodila se prva javna demonstracija ARPANET tehnologije na Međunarodnoj konferenciji o računalnim komunikacijama (International Conference on Computer Communications) u Washingtonu. Reakcija je proizvođača tadašnjih računala na ARPANET-ovo otkriće bila stvaranje vlastite mrežne arhitekture temeljene na njihovim vrstama računala dok je pružatelj telefonskih usluga ignorirao ovu činjenicu. Uskoro su i ostale mreže bile pripojene ARPANET-u, ponajprije one koje su radile na razvoju bežičnog povezivanja. Tijekom 70-ih godina međusobno je povezivanje mreža nazvano „internetworking“ te je tako neologizam koji je ARPANET proširio s vremenom dobio stalan naziv kao današnji internet (1-3).

1.2. Internet danas

Internet je globalni informacijsko-komunikacijski sustav koji povezuje računalne mreže pojedinih zemalja i organizacija te omogućava posjednicima računala diljem svijeta da putem svojih lokalnih i telefonskih mreža međusobno komuniciraju, razmjenjuju informacije i koriste brojne druge usluge (4). To je mreža koja međusobno povezuje milijune računalnih uređaja diljem svijeta. U početku su to bila tradicionalna stolna računala, no danas se na internet povezuju prijenosna računala, mobilni uređaji, a u zadnje vrijeme sve više televizijskih uređaja, uređaja u automobilima, web kamera (od engl. web – mreža), sigurnosnih sustava (5).

1.3. Povezivanje na internet i korištenje interneta

Za korištenje je interneta potrebno računalo, modem (uređaj koji modulira i demodulira signale sa svrhom prilagođavanja prijenosa signala putem telefonske linije), davatelj internetskih usluga, komunikacijski program i komunikacijska veza. Ima više vrsta komunikacijskih veza: tradicionalna telefonska linija, ISDN linija, kabelska linija, DSL, optičko vlakno ili se kao komunikacijska veza može koristiti satetliti ili radiovalovi. Za svako računalo nije potreban modem, ako su računala dio jedne lokalne računalne mreže, već je potrebna mrežna kartica koja se ugrađuje u svako računalo u mreži, a to znači da je za sva računala potreban samo jedan modem (6).

1.4 Mrežne usluge

Kako se internet tehnologija razvijala, tako se povećavao broj usluga koje su bile dostupne putem različitih uslužnih programa: elektronička pošta, mreža (World Wide Web, WWW ili samo Web), servis za prijenos podataka, novinske skupine, poštanske liste i drugi oblici priopćavanja. Najpopularnije su usluge elektronička pošta i mreža (6).

1.5. Sigurnost na internetu

Budući da su u današnje vrijeme internetske usluge postale sastavni dio čovjekovog života, tako se stvara sve više mogućnosti, kako u pozitivnom smislu za napredak tehnologije i komunikaciju među ljudima, tako i u onom negativnom, a to je postojanje rizika za osobnu sigurnost i privatnost. Iz toga proizlazi i potreba za zaštitom osobnih podataka kako bi se smanjio rizik od otuđenja informacija o korisnicima koji su svih dobnih skupina, od najmlađih do najstarijih. Nove usluge na internetu (aplikacije, elektronički zdravstveni sustav, kupovina…), koje su sve potrebnije te zahvaćaju sve više korisnika, zahtijevaju od korisnika da otkriju dio svojih osobnih podataka. S time raste i potencijalni rizik, a budući da je čimbenik neznanja i neupućenosti u informacijsko-komunikacijski sustav prisutan kod brojnih korisnika, oni prihvaćaju i počinju upotrebljavati nove usluge čim se pojave na digitalnom tržištu. Kako su dosadašnja istraživanja pokazala da je čovjek kao korisnik informacijskog sustava možda i najkritičniji sigurnosni element u istom tom sustavu, najvjerojatnije se u potpunosti nikada ni neće moći riješiti pitanje privatnosti i zaštite korisnika iako su programske zaštite, sigurnosne procedure i automatizacija sigurnosnih kopija na visokoj razini. Naravno da to nije dovoljno kako bi u potpunosti zaštitilo samog korisnika.Potrebno je

i odgovorno i savjesno korištenje internetskih usluga od strane samog korisnika. Stoga je moguće smanjiti taj rizik, a jedan je od najboljih načina povećanje svijesti korisnika, odnosno edukacija, jer postoje razne vrste prijevara i gubljenja privatnosti na internetu pa tako, na primjer, instaliranje dodatne aplikacije ili odavanje manjeg dijela osobnih podataka može u konačnici završiti financijskim ili nekim drugim manje materijalnim gubitkom što nikako nije bio cilj korisnika koji je tu aplikaciju instalirao ili odao dio svojih podataka (7).

1.6. Lozinka

Lozinka je tajna riječ ili niz znakova koj se koristi za prepoznavanje korisnika kako bi dokazali identitet ili za odobrenje pristupa izvoru informacija. U današnje vrijeme korisnička imena i lozinke ljudi obično koriste tijekom procesa prijave koji kontrolira pristup zaštićenim računalnim operativnim sustavima, bankomatima, mobilnim i ostalim uređajima. Korisnici računala imaju lozinke za različite svrhe: prijava na korisničke račune i e-poštu, pristup aplikacijama, bazama podataka, mrežama, internetskim stranicama (8).

1.6.1. Izbor lozinke

Jedan je od savjeta za izradu lozinke nekorištenje osobnih podataka i pravih riječi koje mogu biti pronađene u raznim smjernicama. Dostupni su alati koji pomažu napadačima pogoditi lozinku korisnika. S današnjom računalnom snagom nije potrebno puno vremena da se isproba svaka riječ i nađe tražena lozinka pa je zato najbolje za lozinku ne koristiti gramatički točne riječi. Da bi se slijedile smjernice informacijske sigurnosti, preporučljivo je koristiti složene izraze u lozinci. Moguće je napraviti lozinku koja je sigurnija tako što se izmiješaju različite vrste znakova pokušavajući zapamtiti napravljenu lozinku koristeći se raznim dijelovima riječi ili pamteći prvih nekoliko slova riječi ili izraza (9,10).

1.7. Zaštita podataka na internetu

Općenito se zaštita podataka, ne samo na internetu, provodi s ciljem sprječavanja krađe podataka ili nedopuštenog manipuliranja podacima. Postoje dva razloga zaštite elektroničkih podataka: zbog mogućnosti gubitka istih te zbog mogućeg neovlaštenog korištenja podataka od strane nepouzdane osobe koja ima zlonamjerne ciljeve. Postoji više načina kako zaštiti podatke, a jedan je on najčešćih uporaba antivirusnih programa koji štite operacijski sustav računala i samo računalo od zlonamjernih programa virusa. Prije korištenja operacijskog sustava računala, radi sigurnosti osobnih podataka na računalu, poželjno je ažurirati

antivirusni program. Zlonamjerne osobe koje žele nanijeti štetu korisnicima računala i proizvođačima programa ili operacijskih sustava zapravo to rade s ciljem dokazivanja da proizvođači nisu izradili aplikaciju, program ili operacijski sustav na odgovarajući način sa zadovoljavajućim mehanizmima zaštite. Tako da zlonamjerne osobe nemaju prevelike koristi od razvijanja i proizvodnje virusa (5,11).

1.8. Informatika i informacijski sustav u sestrinstvu

Definiciju je informatike u sestrinstvu objavila 2006. godine Američka udruga sestara (engl. *American Nurses Association*) prema kojoj ona povezuje računalnu znanost, informatiku i sestrinstvo s ciljem administriranja i razmjene podataka, informacija i znanja iz sestrinske prakse. Informacijska se i komunikacijska tehnologija prvenstveno primjenjuje u procesu njege bolesnika i komunikaciji sa svrhom poboljšanja kvalitete zdravstvene skrbi o bolesniku koja doprinosi lakšoj organizaciji sestrinske službe, poboljšava kvalitetu obrazovanja medicinskih sestara i tehničara te se upotrebljava u istraživačkom radu u sestrinstvu (6).

Informacijski sustav u sestrinstvu treba u prvom redu osigurati prikupljanje kliničkih podataka i informacija koji čine temelj za provedbu sestrinske prakse. To znači da medicinske sestre i tehničari trebaju znati raditi s elektroničkim podacima, od prikupljanja i unosa podataka u elektronički zdravstveni zapis pacijenta, razmjene podataka pomoću računala do samostalnog odlučivanja u radu (6).

Budući da se u radu upotrebljavaju osobni podatci pacijenta, a kako je medicinsko osoblje dužno poštivati etička i moralna načela, potrebno je čuvati njihovu tajnost. Stoga medicinske sestre i tehničari prvo trebaju znati čuvati vlastite podatke na internetu, odnosno računalu, kako bi isto to mogli primjeniti i u sestrinskoj praksi.

1.9. Prethodna istraživanja

Kako je internet postao naša svakodnevica, ovakva se istraživanja već provode na općoj populaciji diljem svijeta i to s ciljem ispitivanja korisnikovog znanja i ponašanja na internetu. Mnoga su se empirijska istraživanja na ovu temu već provela (12-17), a zadnje je ovakvo istraživanje provedeno na 701 odraslom ispitaniku, od toga je sudjelovalo 269 muškaraca i 432 žene. Istraživanje je prezentirano na Međunarodnom skupu MIPRO 2017. godine u Rijeci, s kojim je ovo istraživanje i uspoređivano te koji ima zapravo identičan cilj, samo je ispitana skupina bila ciljana.

2. Cilj

Cilj je ovog istraživanja bio ispitati razinu znanja o pitanjima informacijske sigurnosti i privatnosti među medicinskim sestrama zaposlenim u KBC Osijek te ispitati koliko je njihovo ponašanje na internetu potencijalno rizično.

Specifični podciljevi su:

- usporediti znanje i ponašanje ispitanika prema demografskim obilježjima,
- usporediti znanje i ponašanje sa prosječnim vrijednostima po subskalama iz ranijeg istraživanja.

3. Ispitanici i metode

3.1 Ustroj studije

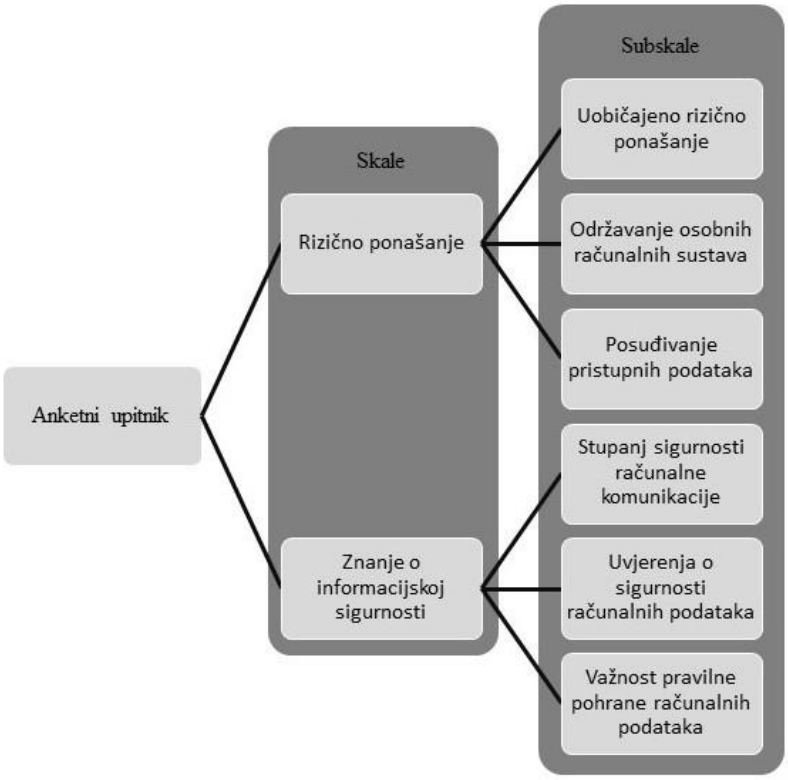
Ustroj je studije bilo presječno istraživanje.

3.2 Ispitanici

Podatci su prikupljeni tijekom srpnja 2017. godine. Ispitanici su bili medicinske sestre/tehničari zaposleni u KBC Osijek svih dobnih skupina. Najmlađi je ispitanik imao dvadeset a najstariji šezdest i jednu godinu. Riječ je osobama oba spola, a u istraživanju je sudjelovao 90 ispitanika.

3.3 Metode

Kao instrument istraživanja korišten je validirani znanstveni upitnik „Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava“ (UZPK) koji se sastoji od 33 pitanja koja se procjenjuju bodovima na Likertovoj skali od 1 do 5 pri čemu ponuđeni odgovori imaju različita značenja. Anketni upitnik dijeli se u dvije skale: Skala rizičnog ponašanja računalnih korisnika (k=17) sastoji se od tri subskale: Subskala uobičajenih rizičnih ponašanja korisnika računala (k=6), Subskala održavanja osobnih računalnih sustava (k=6) i Subskala posuđivanja pristupnih podataka (k=5)), a Skala znanja o informacijskoj sigurnosti (k=16) također se sastoji od tri subskale: Subskala stupnja sigurnosti računalne komunikacije (k=5), Subskala uvjerenja o sigurnosti računalnih podataka (k=5) i Subskala važnosti pravilne pohrane računalnih podataka (k=6)) (Slika 1) (5). Na kraju su anketnog upitnika dodana dva kontrolna pitanja koja su usmjerena na sigurnost osobnih podataka ispitanika. Autori navedenog upitnika su Krešimir Šolić, Tena Velki i Krešimir Nenadić, profesori sveučilišta u Osijeku. Za korištenje upitnika dobivena je dozvola autora te upute o načinu korištenja istoga. Primijenio se i anketni list s demografskim podacima koji se sastoji od 7 pitanja (dob, spol, bračno stanje, stručna sprema, radno mjesto, radni staž na trenutnom radilištu te cjelokupni radni staž u struci). Anketa je bila anonimna. Svi su ispitanici dobili Obavijest ispitanika o istraživanju te su svojim potpisom izrazili suglasnost o sudjelovanju u istraživanju.



Slika 1. Podjela anketnog upitnika na skale i subskale

3.4 Statističke metode

Prilikom statističke analize korišten je računalni program MedCalc, inačica 17.8. (MedCalc Software bvba, Mariakerke, Belgium). Rezultati su ispitivanja prikazani tabelarno i/ili grafički. Kategorijski su podaci predstavljeni aposlutnim i relativnim frekvencijama. Numerički su podatci 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 testiran je Hi-kvadrat testom. Razlike su numeričkih varijabli testirane Studentovim T-testom, a korelacije Spearmanovim testom. Vrijednosti dobivene u statističkoj analizi smatraju se značajnim ako su manje od $\alpha=0,05$.

3.5. Etička načela

Prije provođenja samog istraživanja dobivena je suglasnost etičkog povjerenstva KBC Osijek (broj odobrenja: R1-11681-5/2017., 07. srpnja 2017. godine).

4. Rezultati

4.1. Opća obilježja ispitanika

Distribucija po spolu, od ukupno 90 ispitanika, prikazana je u Tablici 1. gdje je statistički značajno manje medicinskih tehničara od medicinskih sestara (Hi-kvadrat test, P = 0,001). Također, u istoj je tablici prikazana distribucija po stručnoj spremi gdje je isto tako vidljiva statistički značajna razlika između srednje, više i visoke stručne spreme (Hi-kvadrat test, P = 0,001) (Tablica 1). Prosječna dob ispitanika je 40,7 godina sa standradnom devijacijom 10,8, najmlađi ima 20, a najstariji ispitanik 61 godinu. Istraživanje je provedeno na pet klinika/zavoda u KBC Osijek sa slijedećim brojem ispitanika po pojedinoj klinici/zavodu: 33 (36,7%) ispitanika, a ujedno i najviše njih, sudjelovalo je na Klinici za kirurgiju, na Klinici za anesteziologiju, reanimatologiju i intenzivno lječenje sudjelovalo je 23 (25,6 %) ispitanika, zatim slijedi Klinika za neurologiju s 20 (22,2 %) ispitanika, dok je na Klinici za neurokirurgiju sudjelovalo 8 (8,9 %) ispitanika, te na zadnjem mjestu je Klinika za ortopediju, gdje je sudjelovalo najmanji broj ispitanika, to jest njih 6 (6,7 %). Prosječna duljina radnog staža svih ispitanika je 20,2 godina sa standardnom devijacijom 11,2.

Tablica 1. Distribucija po spolu i stručnoj spremi ispitanika

	Broj (%)	P*
medicinski tehničari	16 (17,8)	**0,001**
medicinske sestre	74 (82,2)	
SSS	57 (63,3)	**0,001**
VŠS	27 (30,0)	
VSS	6 (6,7)	
Ukupno	90 (100,0)	

* Hi-kvadrat test

Sljedeća tablica prikazuje broj (%) odgovora na pojedino pitanje koja ispituju uobičajena ponašanja korisnika računalnih informacijsko-komunikacijskih sustava (Tablica 2).

Tablica 2. Frekvencija odgovora na pitanja koja ispituju ponašanje

Pitanje	Broj (%) odgovora					
	učestalost					
	nikad	rijetko	ponekad	često	uvijek	ukupno n (%)
1. Posuđivanje službenih podataka*	56 (62,2)	18 (20,0)	10 (11,1)	5 (5,6)	1 (1,1)	90 (100,0)
2. Posuđivanje privatnih podataka za pristup računalu*	73 (81,1)	12 (13,3)	4 (4,4)	0	1 (1,1)	90 (100,0)
3. Posuđivanje privatnih podataka za pristup e-pošti*	82 (90,0)	4 (4,4)	4 (4,4)	0	0	90 (100,0)
4. Posuđivanje privatne kreditne kartice*	80 (88,9)	9 (10,0)	1 (1,1)	0	0	90 (100,0)
5. Otkrivanje podataka prilikom plaćanja karticom*	84 (93,3)	5 (5,6)	1 (1,11)	0	0	90 (100,0)
6. Korištenje raznih zaporki	24 (26,7)	8 (8,9)	13(14,4)	3 (14,4)	32 (35,6)	90 (100,0)
7. Održavanje zaštite privatnog računala	16 (17,8)	25 (27,8)	17 (18,9)	12 (13,3)	20 (22,2)	90 (100,0)
8. Nadogradnja ostalih programa	19 (21,1)	23 (25,6)	25 (27,8)	7 (7,8)	16 (17,8)	90 (100,0)
9. Instaliranje programa nepoznatog proizvođača*	43 (47,8)	31 (34,4)	10 (11,1)	4 (4,4)	2 (2,2)	90 (100,0)
10. Ostavljanje podataka na društvenim mrežama*	70 (77,8)	12 (13,3)	2 (2,2)	3 (3,3)	3 (3,3)	90 (100,0)
11. Odgovaranje na mailove nepoznatih pošiljatelja*	84 (93,3)	5 (5,6)	0	0	1 (1,1)	90 (100,0)
12. Otvaranje priloga od nepoznatih pošiljatelja*	65 (72,2)	23 (25,6)	2 (2,2)	0	0	90 (100,0)
13. Prosljeđivanje lančanih mailova*	74 (82,2)	10 (11,1)	4 (4,4)	0	0	90 (100,0)
14. Korištenje više e-pošta adresa	43 (47,8)	10 (11,1)	9 (10,0)	9 (10,0)	19 (21,1)	90 (100,0)
15. Prijavljivanje na e-poštu na javnim mjestima*	43 (47,8)	22 (24,4)	15 (16,7)	8 (8,9)	2 (2,2)	90 (100,0)
16. Odjavljivanje nakon završetka rada	11 (12,2)	5 (5,6)	5 (5,6)	12 (13,3)	57 (63,3)	90 (100,0)
17. Zaključavanje službenog računala prilikom odlaska s radnog mjesta	43 (47,8)	15 (16,7)	12 (13,3)	7 (7,8)	13 (14,4)	90 (100,0)

* - obrnuto kodirano pitanje

Isto tako, tablica 3 prikazuje broj (%) odgovora na pojedino pitanje koja ispituju znanje i svjesnost korisnika pri korištenju internetskih usluga.

Tablica 3. Frekvencija odgovora na pitanja koja ispituju sigurnost, uvjerenje i važnost

Pitanje	**Broj (%) odgovora**					
	sigurnost					
	potpuno nesigurno	prilično nesigurno	ne znam	prilično sigurno	potpuno sigurno	ukupno n (%)
1. Dopisivanje putem električne pošte*	9 (10,0)	32 (35,6)	31 (34,4)	16 (17,8)	2 (2,2)	90 (100,0)
2. Komunikacija putem društvenih mreža*	23 (25,6)	38 (42,2)	20 (22,2)	7 (7,8)	2 (2,2)	90 (100,0)
3. Komunikacija mobitelom	11 (12,2)	30 (33,3)	22 (24,4)	22 (24,4)	5 (5,6)	90 (100,0)
4. Komunikacija žičnim telefonom*	14 (15,6)	29 (32,2)	20 (22,2)	22 (24,4)	5 (5,6)	90 (100,0)
5. Općenito komunikacija putem interneta*	20 (22,2)	33 (36,7)	22 (24,4)	12 (13,3)	3 (3,3)	90 (100,0)
	uvjerenje					
	nisam uvjeren/a	možda	ne znam	prilično	potpuno	ukupno n (%)
6. Krađa službenih podataka	10 (11,1)	42 (46,7)	25 (27,8)	12 (13,3)	1 (1,1)	90 (100,0)
7. Krađa privatnih podataka s računala	20 (22,2)	38 (42,2)	22 (24,4)	9 (10,0)	1 (1,1)	90 (100,0)
8. Krađa privatnih podataka s mobitela	11 (12,2)	42 (46,7)	26 (28,9)	11 (12,2)	0	90 (100,0)
9. Otuđenje novca s bankovnog računa	17 (18,9)	34 (37,8)	26 (28,9)	11 (12,2)	2 (2,2)	90 (100,0)
10. Krađa identiteta na internetu	12 (13,3)	36 (40,0)	28 (31,1)	12 (13,3)	2 (2,2)	90 (100,0)
	važnost					
	potpuno nevažno	prilično nevažno	ne znam	prilično važno	izrazito važno	ukupno n (%)
11. Kopiranje dokumenata na drugu lokaciju	4 (4,4)	5 (5,6)	15 (16,7)	38 (42,2)	28 (31,1)	90 (100,0)
12. Provjeriti tuđi memorijski štapić od virusa	4 (4,4)	3 (3,3)	13 (14,4)	37 (41,1)	33 (36,7)	90 (100,0)
13. Čuvanje tajnosti zaporke	3 (3,3)	2 (2,2)	10 (11,1)	31 (34,4)	44 (48,9)	90 (100,0)
14. Periodično mijenjati zaporke	3 (3,3)	7 (7,8)	16 (17,8)	32 (35,6)	32 (35,6)	90 (100,0)
15. Odvajanje poslovnih i privatnih računalnih resursa	3 (3,3)	4 (4,4)	18 (20,0)	31 (34,4)	34 (37,8)	90 (100,0)
16. Čuvati memorijski štapić od krađe	1 (1,1)	3 (3,3)	12 (13,3)	32 (35,6)	42 (46,7)	90 (100,0)

* - obrnuto kodirano pitanje

Na kraju su anketnog upitnika dodana dva kontrolna pitanja. Na prvo pitanje koje glasi „Kada ste posljednji put radili sigurnosnu kopiju (engl. backup) osobnih podataka i dokumenata?“ najviše ispitanika, odnosno njih 32 (35,6 %), odgovorilo je s *nikada* što je, može se reći, zabrinjavajuće dok je 28 (31,1 %) ispitanika odgovorilo s *ne sjećam se*. Drugo pitanje glasi „Koliko osoba zna zaporku za pristup Vašem sustavu elektroničke pošte?“ te je većina, to jest 42 (46,7 %) ispitanika, odgovorila sa *samo ja* što je i dobro, dok je njih 36 (40,0 %) odgovorilo s *ja i još jedna osoba*..

4.2. Usporedba prema spolu

Sljedeća tablica prikazuje usporedbu prema spolu po svim subskalama na koja su pitanja podijeljena (Tablica 4). Pronađena je statistički značajna razlika između muškog i ženskog spola u petoj subskali „Uvjerenje o sigurnosti računalnih sustava“ (Studentov T-test, P = 0,038).

Tablica 4. Usporedba prema spolu po subskalama

Subskale	aritmetička sredina (standardna devijacija)		P*
	medicinski tehničari n = 16	medicinske sestre n = 74	
Posuđivanje pristupnih podataka	4,71 (0,28)	4,76 (0,35)	0,599
Održavanje osobnih računalnih sustava	2,84 (1,25)	2,98 (0,96)	0,627
Uobičajeno rizično ponašanje	4,40 (0,53)	4,58 (0,48)	0,180
Stupanj sigurnosti računalne komunikacije	3,23 (1,25)	3,50 (0,80)	0,268
Uvjerenje o sigurnosti računalnih sustava	2,03 (0,75)	2,49 (0,82)	**0,038**
Važnost pravilne pohrane podataka	3,98 (0,93)	4,07 (0,84)	0,718

*Studentov T-test

4.3 Usporedba prema stručnoj spremi

Tablica 5 prikazuje usporedbu po svim subskalama prema stručnoj spremi ispitanika gdje se viša i visoka stručna sprema gleda kao jedna cjelina. Ovdje je također pronađena statistički značajna razlika (Studentov T-test, P = 0,038) ali u prvoj subskali koja govori o posuđivanju pristupnih podataka.

Tablica 5. Usporedba po subskalama prema stručnoj spremi

Subskale	aritmetička sredina (standardna devijacija)		P*
	SSS n = 57	VŠS i VSS n = 33	
Posuđivanje pristupnih podataka	4,82 (0,29)	4,64 (0,39)	**0,018**
Održavanje osobnih računalnih sustava	2,86 (1,04)	3,12 (0,94)	0,237
Uobičajeno rizično ponašanje	4,60 (0,46)	4,45 (0,54)	0,158
Stupanj sigurnosti računalne komunikacije	3,47 (0,97)	3,42 (0,76)	0,792
Uvjerenje o sigurnosti računalnih sustava	2,50 (0,90)	2,26 (0,67)	0,190
Važnost pravilne pohrane podataka	3,99 (0,98)	4,16 (0,60)	0,372

*Studentov T-test

4.4 Usporedba s prethodnim istraživanjem

Slijedeća tablica prikazuje usporedbu po subskalama s prosječnim vrijednostima iz prethodnog istraživanja gdje je broj ispitanika bio 701 (Tablica 6). Statistički su značajne razlike pronađene u dvije subskale. Prva je statistički značajna razlika vidljiva u drugoj subskali „Održavanje osobnih računalnih sustava“ (Studentov T-test, P = 0,03), dok je druga statistički značajna razlika vidljiva u petoj subskali „Uvjerenje o sigurnosti računalnih sustava“ (Studentov T-test, P = 0,001).

Tablica 6. Usporedba po subskalama na pitanja koja ispituju znanje i svjesnost s prosječnim vrijednostima iz prethodnog istraživanja (prosječne vrijednosti, n = 701)

Subskale	aritmetička sredina (standardna devijacija)		P*
	vrijednosti na cijelom uzorku n = 90	vrijednostima iz prethodnog istraživanja n = 701	
Posuđivanje pristupnih podataka	4,75 (0,34)	4.74 (0.39)	0,758
Održavanje osobnih računalnih sustava	2,96 (1,01)	3.18 (0.91)	**0,030**
Uobičajeno rizično ponašanje	4,55 (0,49)	4.52 (0.43)	0,493
Stupanj sigurnosti računalne komunikacije	3,45 (0,90)	3.48 (0.83)	0,758
Uvjerenje o sigurnosti računalnih sustava	2,41 (0,83)	2.06 (0.79)	**0,001**
Važnost pravilne pohrane podataka	4,05 (0,86)	4.18 (0.68)	0,099

*Studentov T-test

4.5 Usporedba sa starosnom dobi

Statistički značajna povezanost postoji između dobi ispitanika i treće subskale o Rizičnosti ponašanja (Tablica 7). Stupanj korelacije je mali i pozitivan (Spearmanov test korelacije, P = 0,016) što znači da što su stariji ispitanici imali bolju ocjenu iz ponašanja, što je u skladu s dosadašnjim zaključcima, jer su obično stariji i oprezniji (8).

Tablica 7. Usporedba po svim subskalama sa starosnom dobi

Subskale	Starosna dob ispitanika		
	r	95% CI od r	P*
Posuđivanje pristupnih podataka	0,104	od -0,105 do 0,305	0,327
Održavanje osobnih računalnih sustava	-0,033	od -0,239 do 0,175	0,757
Uobičajeno rizično ponašanje	0,253	od 0,048 do 0,437	**0,016**
Stupanj sigurnosti računalne komunikacije	0,081	od -0,128 do 0,284	0,447
Uvjerenje o sigurnosti računalnih sustava	-0,020	od -0,226 do 0,188	0,854
Važnost pravilne pohrane podataka	0,012	od -0,196 do 0,218	0,914

*Spearmanov test korelacije

5. Rasprava

U usporedbi s već spomenutim prethodnim istraživanjem izloženim u Rijeci ove godine, također su vidljive statistički značajne razlike u nekoliko subskala, koje su, može se reći, nešto zanimljivije nego od do sada izloženih rezultata. Naime, statističke značajne razlike nisu nađene u četiri subskale: „Posuđivanje pristupnih podataka“, „Uobičajeno rizično ponašanje“, „Stupanj sigurnosti računalne komunikacije“ te „Važnost pravilne pohrane podataka“ u kojima je P vrijednost bila veća od 0,05 što znači da uzorak od 90 ispitanika ne odstupa od referentnih vrijednosti iz prethodnog istraživanja, odnosno prosječnog internet korisnika. Analizirajući tablicu 6. prva je statistička značajna razlika vidljiva u drugoj subskali (P = 0,030) gdje ispitanici iz prethodnog istraživanja imaju veća učestalost održavanja zaštite svog privatnog računala, odnosno nadograđivanje antivirusnih programa, korištenja privatne i službene e-pošte, odjavljivanja s informacijskog sustava prilikom završetka rada te zaključavanja računala prilikom kraćeg odlaska s radnog mjesta. Ovdje je važno naglasiti da čak više od ¼ (26,7 %) ispitanika nikada ne koristi različite zaporke za različite sustave (pitanje 6, tablica 2) što nije po smjernicama informacijske sigurnosti. Isto tako, nešto malo manje od ½ (47,8 %) ispitanika nikada ne zaključava službeno računalo prilikom kraćeg odlaska s radnog mjesta što je u sestrinskoj struci iznimno važno radi održavanja tajnosti podataka pacijenta budući da se tu radi o radnim mjestima gdje su prisutni i drugi pacijenti (ambulante opće prakse, odjeli) i protok ljudi je velik. Sljedeća, i u ovom istraživanju ujedno i najveća statistički značajna razlika, vidi se u petoj subskali koja se odnosi na „Uvjerenje o sigurnosti računalnih sustava“ (Tablica 6). Ovo znači da su, u usporedbi s prosječnom populacijom iz prethodnog istraživanja, ispitanici manje uvjereni da će im netko ukrasti privatne ili službene podatke s privatnog ili službenog računala ili mobitela, otuđiti novac s bankovnog računa i ukrasti identitet na internetu. To može biti posljedica širokog spektra znanja na internetu kojeg pojedini ispitanik ima, ali isto tako i neznanja koje dovodi do krivog razmišljanja da se takve situacije ne događaju na internetu, stoga je to individualno. Čak 42 (46,7 %) ispitanika misli da će im netko možda ukrasti privatne podatke s mobilnog uređaja.

Uspoređujući odgovore muške i ženske populacije, nisu vidljive statističke značajne razlike u pet od šest subskala što znači da se oba spola slično ponašaju na internetu kada govorimo o posuđivanju osobnih podataka, održavanju osobnih računalnih sustava i rizičnom ponašanju. Također imaju podjednaku razinu znanja na internetu što se vidi iz četvrte i šeste subskale koja se odnose na stupanj sigurnosne računalne komunikacije i na važnost pravilne pohrane

podataka (Tablica 4). Međutim, statistički je značajna razlika vidljiva u subskali „Uvjerenje o sigurnosti računalnih sustava“ (P = 0,038) što znači da je ženski dio ispitane populacije skeptičniji u vezi sigurnosti na internetu i njegovim uslugama (elektronička pošta, internet bankarstvo...) na različitim uređajima (računala, mobilni uređaji) te da su žene više uvjerene da postoji mogućnost krađe identiteta na internetu (Tablica 4). Pogledamo li kojom su se brzinom u kratkom vremenu razvili informatika kao znanost i njezina tehnologija te da se i dalje nastavljaju razvijati, moramo priznati da su donekle u pravu. No, isto tako, razvojem tehnologija ravijaju se zaštitni i sigurnosni mehanizmi samo je pitanje znaju li korisnici tih tehnologija, u ovom slučaju internet tehnologije, da oni uopće postoje i, ako znaju, znaju li se služiti njima na pravilan i primjeren način. Iz ovog se isto tako može vidjeti da sestrinsku struku i dalje biraju više žene nego muškarci, iako je broj muškaraca u sestrinstvu u porastu (18).

Gledajući usporedbu prema stručnoj spremi, gdje postoje dvije grupe na koje su ispitanici podijeljeni (prva je srednja stručna sprema, a druga je grupa viša i visoka stručna sprema tj. završen preddiplomski i/ili diplomski studij sestrinstva), također je vidljivo da nema statistički značajnih razlika u pet od šest subskala (Tablica 5). Statistički je značajna razlika vidljiva samo u prvoj subskali koja govori o učestalosti posuđivanja pristupnih podataka (korisničko ime i zaporka), osobnih ili službenih, kolegama na poslu, prijateljima, rođacima ili poznanicima (P = 0,018) što pokazuje da je srednja stručna sprema odgovorila bolje u odnosu na višu i visoku stručnu spremu. To jest, srednja stručna sprema u odnosu na višu i visoku rjeđe posuđuje osobne ili službene pristupne podatke kako kolegama na poslu tako i prijateljima, rođacima ili poznanicima. Mnogi se s ovom tvrdnjom možda ne bi složili budući da većina ljudi vjerojatno misli kako su visokoobrazovani ljudi ujedno i odgovorniji, no dobiveni odgovori na ova pitanja ukazuju na suprotno. Na prvo pitanje „Koliko često posuđujete službene pristupne podatke (korisničko ime i zaporka) kolegama studentima ili kolegama na poslu koji se nađu u potrebi (npr. za vrijeme bolovanja, godišnjeg)?“, od ukupno 90 ispitanika njih 74 (82,2 %) odgovorilo je s *nikada* ili *rijetko (nekoliko puta godišnje)*. Na pitanje koliko često posuđuju svojim prijateljima, rođacima i poznanicima svoje privatne pristupne podatke za pristup kućnome računalu 73 (81,1 %) ispitanika odgovorilo je s nikada, a njih 12 (12,2 %) odgovorilo je rijetko (nekoliko puta godišnje). Pitanje koje se odnosi na učestalost posuđivanja svojih privatnih pristupnih podataka za pristup osobnoj ili privatnoj e-pošti bilježi 82 (90,0 %) odgovora *nikada*. Na pitanje „Koliko često posuđuju prijateljima, rođacima ili poznanicima svoje privatne kreditne kartice i pripadajuće im PIN-ove?“ 80 (88,9

%) je ispitanika odgovorilo s *nikada* , ali na to se pitanje i mogao očekivati ovakav broj odgovora. Međutim, titulu pobjednika u ovoj subskali o učestalosti nosi pitanje „Koliko često otkrivate svoj PIN (neskrivanjem, glasnim izgovaranjem prodavaču) kada plaćate karticom u trgovini?“ na koje je čak 84 (93,3 %) ispitanika odgovorilo s *nikada*. Na kraju, analizom je svakog pitanja pojedinačno vidljivo da su obje grupe odgovorile s visokim ocjenama (vidljivo po aritmetičkim sredinama obje grupe) to jest s odgovorom 4 – *rijetko (nekoliko puta godišnje)* ili 5 – *nikad* (na Likertovoj skali), no, kako je već spomenuto, vidljiva je statistički značajna razlika između te dvije grupe.

Zadnja je usporedba napravljena u ovom istraživanju usporedba po subskalama sa starosnom dobi (Tablica 7) u kojoj postoji statistički značajna razlika između dobi ispitanika i treće subskale o Rizičnosti ponašanja. Budući da je stupanj korelacije mali i pozitivan (P = 0,016) stariji su ispitanici imali bolju ocjenu iz ponašanja, što je u skladu s dosadašnjim zaključcima, jer su obično stariji i oprezniji (19). Isto takom, na kontolno je pitanje o otkrivanju lozinke e-pošte samo 16 (17,8 %) ispitanika napisalo odgovor, što zapravo također upućuje na to da su ispitanici svijesni potencijalnih problema koji se na internetu događaju.

Budući da u nekim dijelovima korištenja interneta i njegovih usluga, u ovom slučaju ne u znanju, već u ponašanju, postoji potencijalno rizično ponašanje medicinskih sestara i tehničara, bilo bi dobro provesti edukaciju u KBC Osijek s ciljem promicanja znanja i svjesnosti radi smanjenja broja mogućih posljedica.

6. Zaključak

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

- U usporedbi s referentnim vrijednostima iz prethodnog istraživanja, medicinske se sestre/tehničari KBC-a Osijek statistički ne razlikuju po znanju od prosjeka, u jednom segmenti su i iznadprosječni, ali ispitano ponašanje na internetu je potencijalno rizično.

- Medicinske sestre, u odnosu na medicinske tehničare, skeptičnije su kada je u pitanju krađa privatnih, službenih podataka, novca i identiteta na internetu,

- Medicinske sestre i tehničari sa završenom srednjom stručnom spremom, u odnosu na višu i visoku, opreznije se ponašaju na internetu u smislu rijeđeg posuđivanja privatnih i službenih podataka ostalim osobama,

- Ispitane medicinske sestre i tehničari, u odnosu na prethodno istraživanje, lošiji su u održavanju osobnih računalnih sustava, odnosno rijeđe to provode,

- Ispitane medicinske su sestre i tehničari, u odnosu na prethodno istraživanje, skeptičniji kada je u pitanju krađa privatnih, službenih podataka, novca i identiteta na internetu.

7. Sažetak

Cilj istraživanja: Ispitati nivo znanja o pitanjima informacijske sigurnosti i privatnosti među medicinskim sestrama i tehničarima zaposlenim u KBC Osijek s obzirom na spol i stručnu spremu te ispitati koliko je njihovo ponašanje na internetu potencijalno rizično u usporedbi s prethodnim istraživanjem.

Nacrt studije: Istraživanje je provedeno kao presječno.

Ispitanici i metode: U istraživanju je sudjelovalo 90 medicinskih sestara i tehničara koji su zaposleni u KBC Osijek sa završenom srednjom, višom i visokom stručnom spremom. Kao instrument istraživanja korišten je validirani znanstveni upitnik „Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava“ (UZPK) koji se sastoji od 33 pitanja koja se procjenjuju bodovima na Likertovoj skali od 1 do 5 pri čemu ponuđeni odgovori imaju različita značenja. Na kraju su anketnog upitnika dodana dva kontrolna pitanja. Primijenio se anketni list s demografskim podacima koji se sastoji od 7 pitanja.

Rezultati: Statističke su značajne razlike vidljive u usporedbi s prethodnim istraživanjem u dvije subskale, jedna govori o održavanju osobnih računalnih sustava, a druga o uvjerenju o sigurnosti računalnih sustava, u kojoj je također vidljiva statistički značajna razlika prilikom usporedbe prema spolu. U prvoj je subskali vidljiva statistički značajna razlika u usporedbi prema stručnoj spremi, a uspoređujući subskale sa starosnom dobi vidljiva je u trećoj.

Zaključak: U usporedbi s referentnim vrijednostima iz prethodnog istraživanja, medicinske se sestre/tehničari KBC-a Osijek statistički ne razlikuju po znanju od prosjeka, u jednom su segmenti i iznadprosječni, ali ispitano ponašanje na internetu je potencijalno rizično.

Ključne riječi: internet, rizično ponašanje na internetu, sigurnosti i privatnost na internetu

8. Summary

Potentially risky behaviour among nurses on the Internet

Research goal: Test the level of knowledge regarding information safety and privacy among the nurses and technicians employed at the Clinical Hospital Centre Osijek, considering their gender and completed education, and test the level of potential risk resulting from their behaviour online, when compared to the previous study.

Study plan: The conducted study was implemented as a cross-sectional study.

Research participants and methods: 90 nurses and technicians employed at the Clinical Hospital Centre Osijek participated in the study, their level of completed education was secondary school, college, and higher education. The validated scientific questionnaire "Questionnaire on the Knowledge and Risky Behaviour of the Information System Users" was used as a research instrument. The questionnaire contains 33 questions evaluated using points on the Likert scale of 1 to 5, where the offered responses have different meanings. Two control questions were added at the end of the survey questionnaire. A survey questionnaire containing demographic information and 7 questions was used.

Results: There is significant difference in two subscales, when compared to the previous study, first one is about personal computer maintenance, and the second one is about secured data, in which is significant difference regarding gender. Also, there is significant difference in first subscale regarding completed education and in third one regarding age.

Conclusion: The nurses and technicians employed at the Clinical Hospital Centre Osijek do not differ from the average concerning their knowledge, when compared to the previous study. In one segment they are even above the average, but their behaviour online is potentially risky.

Keywords: Internet, risky online behaviour, online safety and privacy

9. Literatura

1. Kleinrock L. An early history of the internet [History of Communications]. IEEE Communications Magazine. 2010;48;26-36.

2. Kleinrock L. Hstory of the Internet and Its Flexible Future. IEEE Wireless Communications. 2008;15;8-18.

3. Leiner B. The Past and Future History of the Internet. Commun, 1997;40;102-108.

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

5. James FK, Keith WR. Computer Networking: A Top-Down Approach. 5. izd. Addison Wesley: University of Massachusetts Amherst: 2007.

6. Josipa K., Mladen P. Medicinska informatika. Zagreb: Medicinska naklada; 2009.

7. Velki T, Šolić K, Nenandić K. Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). Psihologijske teme. 2015;24;401-424.

8. Šolić K., Očevčić H., Blažević D. Survey on Password Quality and Confidentality. 2015;56;69-75.

9. Williams M. Adventures in implementing a strong password policy. SANS Security Essentials. 2003.

10. Indiana university. Indiana university passphrase policy and strength estimation, Dostupno na adresi: http://kb.iu.edu/data/acpu.html. Datum pristupa: 28.8.2017.

11. Varga M. Zaštita elektroničkih podataka. Tehnički glasnik. 2011;5;61-73.

12. Tsohou A., Kokolakis S., Karyda M., Kiountouzis E. Process-variance models in information security awareness research. Information Management & Computer Security, 2008;16;271-287.

13. Williams S.,Akanmu S. Relationship between Information Security Awareness and Information Security Threats. IJRCM. 2013;3;115-119.

14. Puhakainen P., Siponen M. Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. MIS Quarterly. 2010;34;757-778

15. Šolić K. Ilakovac V. Security perception of a portable PC user (The difference between medical doctors and engineers): a pilot study. Medicinski glasnik Dobojsko-Tuzlanskog kantona. 2009;6;261-264

16. Crossler RE. Johnston AC. Lowry PB. Warkentin M. Baskerville R. Future directions for behavioral information security research. Computers&Security. 2013;32;90-101.

17. Keszthelyi A. About Passwords. Acta Polytechnica Hungarica. 2013;10;99-118.

18. Licul R. Sestrinstvo – ženska profesija? JAHR. 2014;4;183-192.

19. 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. MIPRO conference/ISS. 2017.

.

10. Životopis

Ime i prezime: Mateo Pleša

Datum i mjesto rođenja: 09.06.1995., Osijek

Adresa: Jana Žiške 24, Jelisavac, 31 000 Našice

Mobitel: 095 866 72 27

e-pošta: mateoplesa@gmail.com

Obrazovanje:

2002. - 2010. Osnovna škola Ivana Brnjika Slovaka Jelisavac

2010. - 2014. Srednja škola Isusovačka klasična gimnazija s pravom javnosti u Osijeku

2014. - 2017. Sveučilišni preddiplomski studij Sestrinstvo, Medicinski fakultet Osijek