IZVORNI ZNANSTVENI ČLANAK

UDK:159.9:004.056.53
159.9:316.77
Primljeno: travanj 2020.

TENA VELKI*, KREŠIMIR ŠOLIĆ**

Razvoj instrumenta za istraživanje socijalnog inženjeringa u populaciji studenata: Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS)

Sažetak

Ubrzani razvoj digitalne tehnologije doveo je i do specifičnih problema - posebice po pitanju informacijske sigurnosti. Socijalni inženjering, koji podrazumijeva manipuliranje ljudima u svrhu otkrivanja povjerljivih informacija, napada korisnike računalnih sustava kao najslabiji sigurnosni element. Korisnik svojim nepromišljenim i nesavjesnim ponašanjem uvelike doprinosi pojavi socijalnog inženjeringa. Podizanje razine svijesti korisnika o potencijalnim trikovima kojima se socijalni inženjeri koriste protiv njih pokazalo se kao jedna od najučinkovitijih sigurnosnih mjera. Kako bi se uopće mogli suprotstaviti socijalnom inženjeringu, potrebno je imati valjanu i pouzdanu metodu procjene rizičnog ponašanja i razine svjesnosti o informacijskoj sigurnosti kod tipičnog korisnika. Cilj istraživanja bio je razviti i validirati hrvatsku inačicu novog instrumenta za istraživanje socijalnog inženjeringa: Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS). U istraživanju su sudjelovali studenti Sveučilišta J. J. Strossmayera u Osijeku (N=287) koji su putem posebno dizajniranog softvera online popunili BKUIS. BKUIS se sastoji od četiri subskale, prve dvije ispituju bihevioralnu komponentu (samoprocjenu i simulaciju rizičnog online ponašanja), a druge dvije kognitivnu komponentu internetske sigurnosti (svjesnost o online rizicima i važnosti sigurnog korištenja računalnih sustava). Rezultati su pokazali kako stvarno rizično online ponašanje korisnika nije povezano s njihovim vlastitim procjenama, odnosno - jedno samoprocjenjuju, a drugačije se ponašaju u virtualnome svijetu. Štoviše, iako većina korisnika ima prilično visoku razinu svjesnosti o

* izv. prof. dr. sc. Tena Velki, psiholog, Fakultet za odgojne i obrazovne znanosti Sveučilišta J. J. Strossmayera u Osijeku, Republika Hrvatska.

** doc. dr. sc. Krešimir Šolić, inženjer računarstva, Medicinski fakultet Sveučilišta J. J. Strossmayera u Osijeku, Republika Hrvatska.

potencijalnim online rizicima - veliki broj spomenutih upisao je svoju e-adresu (20,9 %), a još je veći broj ostavio svoju lozinku za pristup e-adresi (61,7 %). BKUIS se pokazao kao pouzdan i valjan mjerni instrument zadovoljavajućih psihometrijskih karakteristika koji može poslužiti za pouzdanu procjenu online ponašanja i razine svjesnosti korisnika informacijsko-komunikacijskih sustava.

Ključne riječi: *internetska sigurnost, privatnost podataka, ponašanje korisnika, upitnik, BKUIS.*

1. UVOD

Današnje digitalno doba, unatoč svojim prednostima ponajprije u povezivanju ljudi i brzom prijenosu velike količine informacija, dovelo je i do razvoja specifičnih problema posebice vezano uz pitanja internetske sigurnosti. Transfer velikog broja aktivnosti iz realnog u virtualni svijet posljedično je doveo i od ubrzanog razvoja socijalnog inženjeringa (Haley, 2011; Selmar i Tibert, 2018). Procjenjuje se kako su napadi socijalnih inženjera trenutačno najveća prijetnja internetskoj sigurnosti (Arana, 2017; Chargo, 2018), a dodatni je problem što ih se jedino može detektirati, ali ne i zaustaviti (Libicki, 2018). Socijalni inženjering odnosi se na svaki oblik psihološke manipulacije s ciljem odavanja osobnih i povjerljivih podataka korisnika (Anderson, 2008). Socijalni se inženjeri usmjeravaju na lakovjernog i nesavjesnog korisnika kao najslabiju kariku informacijsko-komunikacijskog sustava (Lukasik, 2011; Sasse, Brostoffand i Weirich, 2001) koji svojim nepromišljenim i rizičnim ponašanjem mogu značajno ugroziti cijeli sustav informacijske sigurnosti. Početno odavanje manjeg broja osobnih informacija korisnika ili instaliranje dodatnih prividno bezazlenih aplikacija čije porijeklo nije provjereno, može rezultati financijskim gubitkom, ali i drugim vrstama zloporabe privatnih podataka (otuđenje identiteta, ucjene, razne prijevare i sl.). Pitanje sigurnosti na internetu postaje sve veći problem za suvremeno informacijsko društvo gdje razvoj brojnih novih aplikacija npr. za društvene mreže, kupnju putem interneta, ali posebice za digitalnu javnu upravu i elektronički zdravstveni sustav koji sadrže mnogobojne privatne i povjerljive informacije o korisniku - predstavljaju laku metu socijalnim inženjerima.

Ministarstvo pravosuđa SAD-a (2018) jasno navodi kako su napadi socijalnih inženjera jedna od najvećih prijetnji sigurnosti današnjice. Prema izvještaju IBM-a iz 2015. godine 55 % svih proboja sigurnosti bilo je povezano izravno s ponašanjem zaposlenika, a čak 95 % incidenata prouzročila je ljudska pogreška. Slično pokazuje i izvještaj Velike Britanije iz 2015. godine u kojem se navodi kako je u 31 % najtežih slučajeva proboja sigurnost kriva ljudska pogreška, a u čak 20 % slučajeva proboj sigurnosti nastao je zbog namjerne zlouporabe tehnologije od strane samih zaposlenika. Posljedice proboja sigurnosti su višestruke. Tako je npr. zloćudni program imena „wannacry“ 2016. godine zarazio tisuće računala u više od 150 država. Počinjena šteta nije bila samo materijalna već je bilo ugroženo i zdravlje pojedinaca jer su u nekim slučajevima zbog toga bili otkazani liječnički pregledi na temelju pogrešaka u sustavu prouzročenih ovim zloćudnim programom (Smart, 2018). Kazneni zakon RH ima cijelu glavu posvećenu kaznenim djelima protiv računalnih sustava, programa i podataka (čl. 266.-273.), pri čemu je jasno definirano koja se sve djela kažnjavaju, od neovlaštenog pristupa računalnom sustavu ili računalnim podacima pa sve do različitih vrsta zloporabe računalnih podataka iz čega je jasno vidljivo kako se u zakonu RH sankcioniraju napadi socijalnih inženjera.

Tijekom posljednjih godina postalo je jasno kako se sigurnosni incidenti ne mogu

ublažiti isključivo tehničkim rješenjima (Parsons, McCormac, Butavicius, Pattinson i Jerram, 2014; Parsons i sur., 2015). Korisnik, odnosno njegovo ponašanje, pokazalo se ključno za pitanje sigurnosti (ENISA, 2014). U početku se najučinkovitijom sigurnosnom mjerom protiv socijalnog inženjeringa smatralo povećanje svijesti korisnika o trikovima kojima se socijalni inženjeri koriste protiv njih (Wilcox, Bhattacharya i Islam, 2014). Stoga je svjesnost o informacijskoj sigurnosti, kao preduvjet za uvođenje prevencijskih programa, postala dio mnogih međunarodnih standarda. Ako organizacije žele dobiti međunarodno priznati certifikat o informacijskoj sigurnosti, nužno moraju usvojiti plan o povećanju svijesti o informacijskoj sigurnosti čiji je glavni cilj smanjenje broja sigurnosnih incidenata, usvajanje međunarodnih standarda ili najbolje moguće prakse informacijske sigurnosti, pokrivanje svih problema u sigurnosnom upravljanju informacijama i sustavima te usklađivanje rada sa zakonskim propisima vezanim uz zaštitu sigurnosti i privatnosti podataka (Bauer, Bernroider i Chudzikowski, 2013). Međutim, samo povećanje razine svijesti i znanja korisnika nije uvijek dovelo do smanjenja njihova online rizičnog ponašanja, čak ni među visokoobrazovanom populacijom kao što su sveučilišni profesori (Šolić i Ilakovac, 2009; Šolić, Ilakovac, Marušić i Marušić, 2009). Štoviše, neka su istraživanja pokazala kako veće znanje i viša razina svjesnosti o informacijskoj sigurnosti dovode i do rizičnijeg ponašanja korisnika pri uporabi informacijskih sustava (Velki i Romstein, 2019a, 2019b; Velki, Šolić, Gorjanac i Nenadić, 2017). Ova se pojava objašnjava paradoksom obrazovanja. Samo znanje i svijest o tome da osoba nešto zna stvara lažni osjećaj sigurnosti u računalnih korisnika koji pridonosi tome da ne paze i ne pridržavaju se naučenih pravila o informacijskoj sigurnosti.

Očito je da samo znanje, pa i svjesnost o informacijskoj sigurnosti, ne služe uvijek kao zaštitni čimbenici u rizičnom online ponašanju te da je potrebno dublje istražiti ovaj fenomen, odnosno dodatne čimbenike koji utječu na svijest o informacijskoj sigurnosti korisnika i njihovo ponašanje (Lebek, Uffen, Neumann, Hohler i Breitner, 2014) kao i stvarno ponašanje korisnika u virtualnome svijetu (Velki, Mayer i Norget, 2018). Pregled novije literature o informacijskoj sigurnosti naglašava istraživanja čiji je cilj upravo stremio razviti pouzdane mjere za procjenu rizičnog ponašanja računalnih korisnika i razine njihove informacijske svjesnosti (Crossler i sur., 2013; Fenz, Heurix, Neubauer i Pechstein, 2014; Sommestad, Hallberg, Lundholm i Bengtsson, 2014). Prije 6 godina u RH, ali i u svijetu, razvijen je prvi validirani mjerni instrument *Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava* (UZRPKIS; Velki, Šolić i Očevčić, 2014). U SAD-u je razvijen upitnik pod nazivom *Security Behavior Intentions Scale* (SeBIS; Egelman, Harbach i Peer, 2016), a u Turskoj nešto opširniji upitnik pod nazivom *Four Measurements Scales* (Öğütçü, Testik i Chouseinoglou, 2016). Najopširniji upitnik, *Human Aspects of Information Security* (HAIS-Q), razvili su znanstvenici iz Australije (Parsons i sur., 2017). Glavni nedostaci postojećih mjernih instrumenata mogu se sažeti u nekoliko točaka: 1) upitnici su predugački, sastoje se od previše pitanja što dovodi do zamora osobe koja ga popunjava; 2) temelje se isključivo na samoprocjeni koja može biti iskrivljena, posebice zbog davanja socijalno poželjnih odgovara; 3) ne mjere razinu stvarnog ponašanja; 4) zbog korištenja različite metodologije u raznim istraživanjima nemoguća je generalizacija dobivenih rezultata istraživanja, odnosno nije moguća usporedba podataka između različitih zemalja. Uzimajući u obzir navedene nedostatke razvijen je i validiran *Behavioral-Cognitive Internet Security Questionnaire* (BCISQ; Velki i Šolić, 2019b). Novi upitnik je najkraći dosad, sastoji se od samo 17 pitanja podijeljenih u 4 subskale, 2 kognitivne koje mjere informacijsku svjesnost i 2 bihevioralne koje mjere rizično ponašanje korisnika. Dodatna prednost nad postojećim upitnicima je to što se prvi put rabi i simulacijska skala

koja mjeri stvarnu razinu rizičnog ponašanja, a ne isključivo procjene korisnika. Međutim za potrebe međunarodnih istraživanja razvijena je i validirana prvotno samo engleska verzija ovoga novog upitnika. Postavlja se pitanje koliko je opravdano na prosječnom korisniku, čiji je materinji jezik hrvatski, primijeniti mjerni instrument na engleskome jeziku, odnosno koliko su pitanja na engleskome jeziku razumljiva korisniku i mogu li korisnici dati pouzdane podatke. Čak i većina studenata u RH, koji su budući visokoobrazovani građani[1], nastavu sluša na hrvatskom, a ne na engleskom jeziku, što dodatno predstavlja razlog za razvoj i primjenu paralelne inačice *Behavioral-Cognitive Internet Security Questionnaire* na hrvatskome jeziku.

Cilj istraživanja bio je razviti i validirati hrvatsku inačicu Bihevioralno-kognitivnog upitnika internetske sigurnosti (BKUIS) kao novog mjernog instrumenta za istraživanje problematike socijalnog inženjeringa. Upitnikom se želi ispitati sljedeće: 1) stvarno online ponašanje (simulacijska subskala) što prijašnji mjerni instrumenti ne ispituju, 2) samoprocjena rizičnog online ponašanja (subskala samoprocjene rizičnog ponašanja korisnika) kao kratke skale koja daje brzu i pouzdanu procjenu, te 3) razina svjesnosti korisnika o informacijskoj sigurnosti koja mjeri dva aspekta informacijske sigurnosti (subskala samoprocjene razine svjesnosti o potencijalnim online rizicima te subskala samoprocjene razine svjesnosti o važnosti sigurnog korištenja računalnih sustava i interneta) što je preduvjet za uvođenje prevencijskih programa.

2. METODA

2.1. Sudionici

U istraživanju je sudjelovalo 287 studenata Sveučilišta J. J. Strossmayera u Osijeku, od toga 17,4 % (N=50) muških i 82,6 % (N=237) ženskih sudionika, pretežno iz područja društvenih znanosti (N=129, 44,9 %) te biomedicine i zdravstva (N=107, 37,3 %). Raspon godina kretao se od 19 do 38, a prosječna dob bila je M=22,44 (SD=2,36); najviše sudionika pripadalo je kategoriji od 21. do 25. godine starosti (61 %).

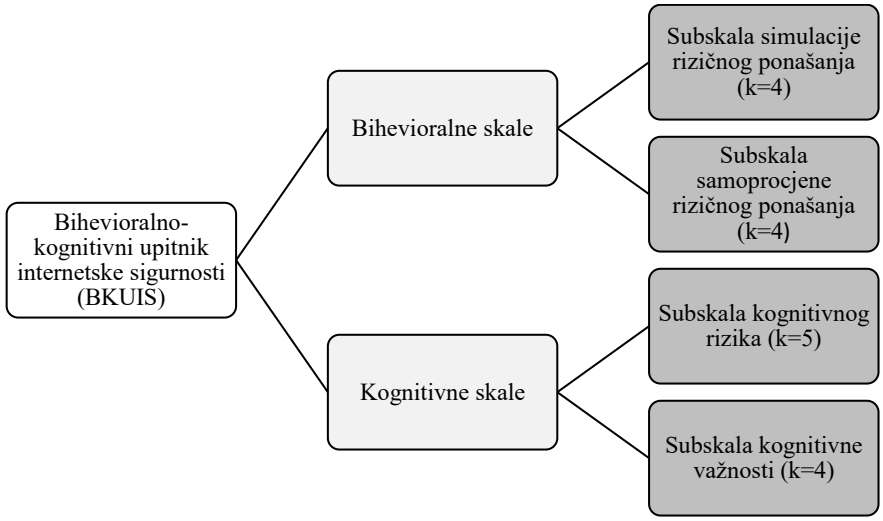
2.2. Mjerni instrument

2.2.1. Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS)

BKUIS je novi instrument za mjerenje internetske sigurnosti, odnosno rizičnog ponašanja računalnih korisnika te njihove razine svjesnosti o potencijalnim online rizicima. Prvotno je razvijen i validiran na engleskome jeziku (Velki i Šolić, 2019). Sastoji se od 4 subskale, 2 bihevioralne i 2 kognitivne (k=17). Bihevioralne skale mjere razinu rizičnog ponašanja računalnih korisnika, pri čemu subskala samoprocjene rizičnog ponašanja (k=4) mjeri samoprocijenjenu razinu rizičnog ponašanja računalnih korisnika (primjer čestice *Koliko često dajete lozinku Vaše e-pošte drugima?*) na skali Likertova tipa sa 5 stupnjeva (od „nikad“ što je označeno brojem 0 do „uvijek“ što je označeno brojem 4), dok subskala simulacije rizičnog

[1] Prema podacima Državnog zavoda za statistiku, popis stanovništva iz 2011. pokazuju kako u Hrvatskoj ima svega 10,26 % visokoobrazovanih građana.

ponašanja (k=4) simulira potencijalna rizična ponašanja s kojima se korisnici tijekom rada mogu susresti (primjer čestice *Ako želite primati obavijesti i naše besplatne promotivne materijale, molim Vas upišite Vašu e-poštu*), a korisnik može ili ne mora dati odgovor. Kognitivne skale mjere razinu svjesnosti o pitanjima informacijske sigurnosti, pri čemu subskala kognitivnog rizika (k=5) mjeri samoprocijenjenu razinu svjesnosti potencijalnih rizika pri korištenju interneta [primjer čestice *Kako biste procijenili koliko je rizič*na: *krađa Vašeg identiteta na internetu (npr. putem internetskog bankarstva, Facebooka, e-pošte?)*] na skali Likertova tipa sa 5 stupnjeva (od „nije rizično" što je označeno brojem 0 do „jako rizično" što je označeno brojem 4), dok subskala kognitivne važnosti (k=4) mjeri samoprocijenjenu razinu svjesnosti o važnosti sigurnog korištenja računalnih sustava i interneta (primjer čestice *Kako biste procijenili koliko je važno: povremeno mijenjanje starih lozinki, barem za usluge, programe i sustave koje učestalo koristite?*) na skali Likertova tipa sa 5 stupnjeva (od „nije važno" što je označeno brojem 0 do „jako važno" što je označeno brojem 4). Za subskalu simulacije rizičnog ponašanja rezultat se kreira kao zbroj odgovora koje su korisnici dali na simulacijska pitanja, a teoretski se kreće od 0 (nisu odgovorili ni na jedno simulacijsko pitanje što predstavlja potpuno sigurno online ponašanje) do 4 (na sva 4 simulacijska pitanja odgovorili su što predstavlja maksimalno rizično online ponašanje). Za sve ostale subskale rezultat se kreira kao aritmetička sredina odabranih čestica i teoretski se kreće od 0 (nema rizičnih online ponašanja te ne postoji svjesnost o potencijalnim rizicima i važnosti sigurnog korištenja računalnih sustava) do 4 (maksimalna rizična online ponašanja te visoka svjesnost o potencijalnim rizicima i važnosti sigurnog korištenja računalnih sustava).



Slika 1: Prikaz skala i subskala Bihevioralno-kognitivnog upitnika internetske sigurnosti (BKUIS) s pripadajućim brojem pitanja

2.3. Postupak

Istraživanje je provedeno online, primjenjujući posebno dizajniran softver za prikupljanje podataka putem BKUIS (http://security.o-i.hr/). Tijekom ljetnog semestra 2019./2020. studente su njihovi nastavnici zamolili da izdvoje desetak minuta za popunjavanje online upitnika. Istraživanje je bilo u potpunosti dobrovoljno i anonimno.

3. REZULTATI I RASPRAVA

U skladu s pretpostavljenim ciljem istraživanja (razvoj i validacija BKUIS-a) provjerena je sadržajna i konstruktna valjanost novoga upitnika, pouzdanost njegovih subskala te mogućnost generalizacije odnosno njegove daljnje primjene u populaciji (vanjska valjanost). Prije odabira odgovarajućih statističkih postupaka napravljene su pred analize (tablica 1) te je zaključeno da se na temelju deskriptivnih pokazatelja može primijeniti parametrijska statistika.

Tablica 1: Prikaz deskriptivnih pokazatelja za sve 4 subskale BKUIS-a

Subskale BKUIS-a	N	Min	Max	M	SD	Indeks asimetričnosti	Indeks zaobljenosti
Subskala simulacije rizičnog ponašanja	287	0,00	4,00	1,209	1,176	1,003	0,062
Subskala samoprocjene rizičnog ponašanja	287	0,00	2,75	0,198	0,402	3,505	11,574
Subskala kognitivne važnosti	287	0,50	4,00	3,011	0,713	-0,789	0,565
Subskala kognitivnog rizika	287	0,00	4,00	2,871	1,118	-0,734	-0,678

Indeks asimetričnosti ukazuje na odstupanje rezultata od normalne distribucije, pri čemu se kod vrijednosti do -/+ 4 smatra da nema značajnijih odstupanja od normalnosti (Field, 2013) te se može primijeniti parametrijska statistika kao u prikazanom slučaju. Indeks zaobljenosti također je mjera odstupanja normalnosti distribucije. Za subskalu samoprocjena rizičnog ponašanja – uočeno je da na ovoj mjeri dolazi do značajnijeg odstupanja od normalnosti, u smjeru da većina sudionika procjenjuje kako se nikada ne ponaša rizično za vrijeme korištenja interneta. Ovi su podaci očekivani te u skladu s nekim prijašnjim istraživanjima koja jasno pokazuju da ono što sudionici izvještavaju o svojem ponašanju nije u skladu s onim što u stvarnosti i čine (Velki i Šolić, 2019a; 2019b; Velki, Šolić i Nenadić, 2015).

3.1. Provjera sadržajne i konstruktne valjanosti BKUIS-a

Sadržajna valjanost upitnika odnosi se na stručni odabir odgovarajućih čestica koje najbolje zahvaćaju konstrukt koji upitnik namjerava mjeriti (Taherdoost, 2016; Yébenes Prous, Salvanés i Ortells, 2009). S obzirom na to da su Velki i Šolić (2019b) razvili i validirali englesku verziju BKUIS-a (Behavioral-Cognitive Internet Security Questionnaire, BCISQ) - bilo je potrebno napraviti njezin prijevod i uskladiti s duhom hrvatskoga jezika. Prijevod su neovisno napravili stručnjak iz područja psihologije i stručnjak iz područja računarstva, a profesor hrvatskoga jezika napravio je jezične prilagodbe. Ova verzija upitnika testirana je na psiholozima u sklopu 27. godišnje konferencije hrvatskih psihologa čija je tema bila Psihologija i digitalni svijet (Velki, 2019). Sustručnjaci u ovome području složili su se da su odabrane čestice prilagođene duhu hrvatskog jezika te sadržajno dobro opisuju pretpostavljeni mjereni konstrukt.

Za provjeru konstruktne valjanosti primijenjena je konfirmatorna faktorska analiza (CFA) putem strukturalnog modeliranja (SEM) na uzorku studenata Sveučilišta J. J. Strossmayera u Osijeku (N=278). Pretpostavljen je 4-faktorski model, identičan onome iz engleske inačice upitnika (Velki i Šolić, 2019b), koji se dijeli na 4 subskale, dvije bihevioralne (simulacija i samoprocjena rizičnog online ponašanja) te dvije kognitivne (informacijska svjesnost o online rizicima i važnosti sigurnog korištenja računala i interneta). U tablici 2 prikazani su rezultati pristajanja modela pri čemu možemo vidjeti da na svim mjerama model pokazuje dobro pristajanje, odnosno - možemo zaključiti da je dobivena dobra konstruktna valjanost 4-faktorskog modela. U budućoj primjeni BKUIS-a opravdano je koristiti sve četiri subskale koje mjere različite aspekte istoga konstrukta, informacijske sigurnosti, te nam njihova primjena daje uvid u cjelokupnu situaciju.

Tablica 2: Prikaz statistike pristajanja modela za konfirmatornu faktorsku analizu

Indeksi pristajanja modela	**Studenti N=287**	**Referentne vrijednosti***	
	Model (ss=111)	**Dobro pristajanje modela**	**Zadovoljavjuće pristajanje modela**
$\chi 2$	198,691/111=1,79	$p > 0,01$ (n.s.)	$\chi^2 / df \leq 2$
CFI	0,96	$\geq 0,95$	$\geq 0,90$
TLI	0,95	$\geq 0,95$	$\geq 0,90$
RMSEA	0,05	$\leq 0,06$	$\leq 0,08$
SRMR	0,04	$\leq 0,08$	$\leq 0,10$

* http://davidakenny.net/cm/fit.hm

3.2. Testiranje pouzdanosti

Pouzdanost se odnosi na stupanj u kojem mjerenje odabranog konstrukta daje stabilne i konzistentne rezultate. Za provjeru unutarnje konzistencije, tj. pouzdanosti, izračunati su koeficijenti pouzdanosti tipa Cronbach alpha (tablica 3).

Tablica 3: Prikaz pouzdanosti za subskale BKUIS-a

Subskale BKUIS-a	Cronbach α
Subskala samoprocjene rizičnog ponašanja (k=4)	0,68
Subskala simulacije rizičnog ponašanja (k=4)	0,66
Subskala kognitivne važnosti (k=4)	0,71
Subskala kognitivnog rizika (k=5)	0,93

Dobivena je umjerena do visoka pouzdanost (Hinton, Brownlow, Mcmurray i Cozens, 2004) za sve subskale BKUIS-a. Prema tome pouzdan će upitnik pri ponovljenom mjerenju iste pojave, pod uvjetom da se ona u međuvremenu nije promijenila, dati isti rezultat. Ako primijenimo BKUIS na drugim sudionicima - dobit ćemo pouzdane procjene za mjerene konstrukte internetske sigurnosti (rizičnog online ponašanja i informacijske svjesnosti).

3.3. Provjera vanjske valjanosti BKUIS-a

Testiranje vanjske valjanosti omogućuje nam provjeru generalizacije dobivenih rezultata i u drugim situacijama te na drugim populacijama (Field, 2013; King i He, 2005; Taherdoost, 2016; Yébenes Prous, Salvanés i Ortells, 2009). U tu svrhu prvo su provjerene spolne razlike (tablica 4). Rezultati istraživanja pokazali su kako studentice pokazuju nešto veću razinu informacijske svjesnosti, odnosno svjesnije su potencijalnih online rizika za razliku od studenata.

Tablica 4: Spolne razlike na subskalama BKUIS-a

Subskale BKUIS-a	spol	N	M	SD	t-test
Subskala simulacije rizičnog ponašanja	muško	50	1,220	1,166	0,073
	žensko	237	1,207	1,180	
Subskala samoprocjene rizičnog ponašanja	muško	50	0,155	0,298	-1,030
	žensko	237	0,207	0,421	
Subskala kognitivne važnosti	muško	50	2,995	0,741	-0,163
	žensko	237	3,014	0,709	
Subskala kognitivnog rizika	muško	50	2,448	1,207	-2,776*
	žensko	237	2,960	1,080	

* $p<0,01$

Dobiveni su rezultati u skladu s prijašnjim istraživanjima koja su sustavno pokazivala kako su žene (studentice, ali i odrasle zaposlene ženske osobe) ipak malo opreznije u otkrivanju osobnih podatka putem interneta (Helsper, 2010; Šolić, Velki i Galba, 2015), a isto je potvrđeno i na srednjoškolskoj populaciji (Velki i sur., 2017). Žene procjenjuju važnijim pravilno održavanje i pohranu podataka te rizičnijom online komunikaciju (Velki i Šolić, 2018; Velki, Šolić i Nenadić, 2015). Dobivene spolne razlike u istome smjeru kao i u prijašnjim istraživanjima govore nam kako je novi upitnik primjenjiv na sudionicima obaju spolova.

Prednost BKUIS-a nad ostalim postojećim upitnicima jest i nova simulacijska skala koja mjeri stvarno rizično ponašanje korisnika, a ne samo procjenu korisnika. Istraživanja su jasno pokazala kako se ljudi zapravo u stvarnosti ne ponašaju onako kako izjavljuju i procjenjuju da se ponašaju, stoga je korelacijskom analizom (tablica 5) provjereno ima li potrebe za uvođenjem simulacijske skale za procjenu ponašanja, odnosno dobivamo li time dodatne i smislene podatke.

Tablica 5: Pearsonovi koeficijenti korelacije između subskala BKUIS-a

Subskale BKUIS-a	Subskala simulacije rizičnog ponašanja	Subskala samoprocjene rizičnog ponašanja	Subskala kognitivne važnosti	Subskala kognitivnog rizika
Subskala simulacije rizičnog ponašanja	1	-0,021	0,062	0,052
Subskala samoprocjene rizičnog ponašanja	-0,021	1	0,039	0,005
Subskala kognitivne važnosti	0,062	0,039	1	0,178**
Subskala kognitivnog rizika	0,052	0,005	0,178**	1

** p<0,01

Rezultati korelacijske analize pokazuju dvije bitne stvari. Prvo, dobivena je statistički pozitivna, relativno niska korelacija između dviju kognitivnih, odnosno između procjena informacijske svjesnosti o online rizicima i procjena važnosti sigurnog korištenja računala i interneta. Kako obje subskale mjere isti konstrukt, informacijsku svjesnost, dobiveni su rezultati očekivani. Osobe koje procjenjuju da postoji veća razina online rizika ujedno procjenjuju da im je važnije sigurno korištenje računala i interneta. Štoviše, kako ove dvije subskale mjere različite aspekte informacijske svjesnosti očekivano je da ne budu u prevelikim korelacijama (jer bi to inače značilo da mjere iste aspekte jednog konstrukta). Iz navedenog možemo zaključiti da su obje kognitivne subskale važne pri procjeni razine informacijske svjesnosti, odnosno da nam daju različite podatke koji se međusobno dopunjuju. Drugo, rezultati nam pokazuju da nije dobivena statistički značajna povezanost između samoprocjena rizičnog ponašanja korisnika i simulacije njihova online rizičnog ponašanja. Ovi su podaci u skladu i s prijašnjim istraživanjima (Velki i Šolić, 2019a; 2019b; Velki, Mayer i Norget, 2019) koja su jasno pokazala da ono što osobe govore i čine nije uvijek povezano. Time je dodatno

opravdano uvođenje simulacijske skale, koja mjeri stvarno ponašanje računalnih korisnika, te nam daje bolje procjene rizičnog online ponašanja nego što nam daju sami korisnici. U prilog ovim rezultatima govori i izrazito niska samoprocjena rizičnog ponašanja korisnika (M=0,198, SD=0,402, tablica 1) gdje studenti procjenjuju da se gotovo nikada ne ponašaju rizično („0" znači nikad, a „1" rijetko); međutim pri simulaciji rizičnog ponašanja njih je 20,9 % (N=60) ostavilo svoju e-adresu, a čak ih je 61,7 % (N=177) napisalo svoju zaporku koju najčešće upotrebljavaju.

Provjera vanjske valjanosti testirana je i u odnosu na vanjske varijable, koje nisu dio upitnika. Prvo je provjeren odnos između samoprocjene znanja korisnika o informacijskoj sigurnosti i privatnosti te općeg tehničkog znanja o računalima i internetu s korisnikovom samoprocjenom rizičnog ponašanja i njegovim stvarnim rizičnim ponašanjem (simulacijska skala). Dobiveni su zanimljivi rezultati. Samoprocijenjeno online rizično ponašanje statistički je značajno negativno povezano s općim tehničkim znanjem o računalima i internetu ($r=-0,119$, $p<0,05$) no nije statistički značajno povezano sa znanjem o informacijskoj sigurnosti i privatnosti ($r=-0,015$, n.s.). Veća procijenjena razina općeg tehničkog znanja ujedno znači da korisnici procjenjuju i sigurnije svoje online ponašanje. Simulirano online rizično ponašanje statistički je značajno negativno povezano sa znanjem o informacijskoj sigurnosti i privatnosti ($r=-0,120$, $p<0,05$), ali nije povezano s općim tehničkim znanjem o računalima i internetu ($r=-0,047$, n.s.). Korisnici koji procjenjuju veću razinu znanja o informacijskoj sigurnosti i privatnosti ujedno se u stvarnosti ponašaju i manje online rizično. Dobiveni rezultati u skladu su s prijašnjim istraživanjima koja su pokazala da su podizanje razine znanja i svijesti ključni u prevenciji socijalnog inženjeringa, odnosno smanjenja rizičnog online ponašanja korisnika (Wilcox, Bhattacharya i Islam, 2014). Međutim još je važniji podatak da za smanjenje stvarnog rizičnog ponašanja nisu dovoljna opća znanja, već specifična o informacijskoj sigurnosti i privatnosti što različiti autori naglašavaju kao glavni nedostatak prijašnjih istraživanja i prevencija usmjerenih općenito na informatička znanja korisnika (Lebek i sur., 2014.; Wilcox, Bhattacharya i Islam, 2014).

Konačno su uspoređeni i rezultati hrvatske i engleske verzije BKUIS-a. Kako je prvotno BKUIS razvijen na engleskome jeziku i testiran na studentima Sveučilišta J. J. Strossmayera u Osijeku (Velki i Šolić, 2019b) postavlja se pitanje je li potrebno razviti i validirati i hrvatsku inačicu istoga upitnika. Engleska, verzija validirana je na 165 studenata (23,5 % muških i 76,5 % ženskih), koji su pretežno iz područja društvenih znanosti (N=69, 41,8 %), a najviše sudionika pripadalo je kategoriji od 21 do 25 godina starosti (61,2 %). S obzirom na sličnosti uzorka u odnosu na demografske karakteristike, uzroci su usporedivi i očekivano je da se procjene na BKUIS-a ne razlikuju između ovih dviju skupina studenata. Međutim, dobiveni rezultati ukazuju na statistički značajne razlike (tablica 6).

Tablica 6: Razlike u procjenama na subskalama BKUIS-a pri korištenju engleske i hrvatske inačice upitnika

Subskale BKUIS-a	Grupa studenata	N	M	SD	t-test
Subskala simulacije rizičnog ponašanja	testirani na engleskom	165	0,782	1,127	-3,820*
	testirani na hrvatskom	287	1,209	1,176	
Subskala samoprocjene rizičnog ponašanja	testirani na engleskom	165	0,270	0,492	1,686
	testirani na hrvatskom	287	0,198	0,402	
Subskala kognitivne važnosti	testirani na engleskom	165	2,806	0,816	-2,682*
	testirani na hrvatskom	287	3,011	0,713	
Subskala kognitivnog rizika	testirani na engleskom	165	2,475	1,163	-3,534*
	testirani na hrvatskom	287	2,871	1,118	

* $p<0,01$

Dobivene su statistički značajne razlike na 3 subskale BKUIS-a. Studenti koji su procjene radili na hrvatskome jeziku (N=287) procijenili su, statistički značajno, veći stupanj stvarnog rizičnog ponašanja (simulacijska skala) te veći stupanj informacijske svjesnosti za oba aspekta (informacijska svjesnost o online rizicima i važnosti sigurnog korištenja računala i interneta). Rezultati govore u prilog tome da studenti, kao budući visokoobrazovani građani koji se koriste engleskim jezikom pri studiranju, nisu na zadovoljavajućem stupnju znanja engleskog jezika da bi dali jednake procjene kao kada to čine na materinjem jeziku. Iako su karakteristike ovih dviju skupina studenata usporedive po dobi, spolu i znanstvenom usmjerenju - ipak su dobivene statističke značajne razlike u procjenama na hrvatskome i engleskom jeziku što je dodatni razlog potrebe za razvojem i validacijom hrvatske inačice Bihevioralno-kognitivnog upitnika internetske sigurnosti.

Općenito gledano, dobiveni rezultati govore u prilog dobroj vanjskoj valjanosti, odnosno mogućnosti primjene upitnika na populaciji u Republici Hrvatskoj te opravdanosti uvođenja simulacijske skale i inačice upitnika na hrvatskome jeziku. Treba naglasiti da su validacijski rezultati dobiveni na studentskoj populaciji, što predstavlja populaciju mladih odraslih i visokoobrazovnih osoba, ali ne i opću populaciju odraslih korisnika informacijsko-komunikacijskih sustava, što bi bilo poželjno provjeriti u budućnosti.

3.4. Praktične implikacije

Novi mjerni instrument za istraživanje socijalnog inženjeringa ima višestruku primjenu. Ponajprije služi kao pouzdan instrument koji u kratkom vremenu može ispitati razinu rizičnog online ponašanja kao i razinu svjesnosti o informacijskoj sigurnosti na bilo kojoj skupini korisnika [počevši od srednjoškolaca za koje su prijašnja istraživanja pokazala da su najrizičnija skupina korisnika (Velki i sur., 2017), odnosno od 15 godina naviše]. Kako je za svaku prevenciju ključna dobra procjena situacije, BKUIS-a predstavlja prvi korak pri prevenciji različitih oblika socijalnog inženjeringa. Nadalje, pri edukaciji, koja se pokazala da treba biti

specifično usmjerena na tehnička znanja i konkretne trikove koje socijalni inženjeri koriste, BKUIS može posložiti i za mjerenje učinka preventivnih programa. Procjena sigurnosti bitna je u mnogim privatnim sektorima (npr. banke, telekomunikacijske tvrtke i dr.), ali i javnim državnim sektorima posebice onima koji barataju s velikom količinom privatnih podataka korisnika (npr. bolnice, MUP, sudovi i dr.) - stoga je velika potencijalna primjena BKUIS-a kao pokazatelja trenutačnog stanja po pitanju informacijske sigurnosti i privatnosti podataka kojima svakodnevno upravljaju zaposlenici.

4. ZAKLJUČAK

Novi instrument za istraživanje socijalnog inženjeringa, Bihevioralno-kognitivni upitnik internetske sigurnosti, pokazao se kao pouzdan mjerni instrument dobrih psihometrijskih karakteristika pri testiranju na populaciji studenata. Četiri subskale mjere različite aspekte internetske sigurnosti, bihevioralne - koje se odnose na rizična online ponašanja korisnika te kognitivne - koje se odnose na svjesnost o informacijskoj sigurnosti. U odnosu na postojeće mjerne instrumente (Egelman, Harbach i Peer, 2016; Parsons i sur., 2017; Oğutcu, Testik i Chouseinoglou, 2016; Velki, Šolić i Nenadić, 2015) BKUIS daje brzu i pouzdanu procjenu internetske sigurnosti u kratkome vremenskom razdoblju, a dodatna mu je prednost simulacijska skala koja mjeri stvarno rizično ponašanje za razliku od prijašnjih upitnika koji daju samo grube procjene korisnika koje se nisu pokazale povezane s njihovim stvarnim online ponašanjem. Također, uz hrvatsku verziju postoji i paralelna inačica na engleskome jeziku (BCISQ; Velki i Šolić, 2019b) što omogućuje široku međunarodnu primjenu s mogućnošću usporedbe i generalizacije dobivenih rezultata.

LITERATURA

1. Anderson, R. J. (2008). *Security engineering: a guide to building dependable distributed systems*. Indianapolis, IN: Wiley.
2. Arana, M. (2017). *How much does a cyberattack cost companies*? Open Data Security, 1-4.
3. Bauer, S., Bernroider, E. i Chudzikowski, K. (2013). *End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study*. Proceeding from Eighth Workshop on Information Security & Privacy, 1-16.
4. Chargo, M. (2018). *You've been hacked: How to better incentivize corporations to protect consumers' data*. Transactions: The Tennessee Journal of Business Law, 20, 115-143.
5. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. i Baskerville, R. (2013). *Future directions for behavioral information security research*. Computers & Security, 32, 90-101.
6. Egelman, S., Harbach, M. i Péer, E. (2016). *Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS)*. Proceedings of Annual ACM Conference on Human Factors in Computing Systems, 7-12.
7. ENISA (2014). *Roadmap for NS education programs in Europe.* Madrid: ENISA.
8. Fenz, S., Heurix, J., Neubauer, T. i Pechstein, F. (2014). *Current challenges in information security risk management.* Information Management & Computer Security, 22(5), 410-430.

9. Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics And Sex and Drugs and Rock "N" Roll*. Los Angeles, London, New Delhi: Sage.
10. Haley, K. (2011). *Information robbery - The 2011 Internet security threat report. InfoSecToday.* Preuzeto s *http://www.infosectoday.com/Articles/Information_ Robbery.htm*, 3. 5. 2018.
11. Helsper, E. (2010). *Gendered internet use across generations and life stages*. Communication Research, 37, 352-374.
12. Hinton, P. R., Brownlow, C., Mcmurray, I. i Cozens, B. (2004). *SPSS explained*. East Sussex, England: Routledge Inc.
13. IBM (2015). *Cyber Security Intelligence Index*. Preuzeto s *https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf*, 12. 12. 2017.
14. Kazneni zakon. *Narodne novine* 56/2015., 61/2015., 101/2017., 118/2018., 126/2019.
15. King, W.R. i He, J. (2005). *External Validity in IS Survey Research.* Communications of the Association for Information Systems, 16, 880-894.
16. Lebek, B., Uffen, J., Neumann, M., Hohler, B. i Breitner, M. H. (2014). *Information security awareness and behavior: a theory-based literature review.* Management Research Review, 37(12), 1049-1092.
17. Libicki, M. (2018). *Could the issue of DPRK hacking benefit from benign neglect?* Georgetown Journal of International Affairs, 19, 83-89.
18. Lukasik, S. J. (2011). *Protecting Users of the Cyber Common*. Communications of the ACM, 54, 54-61.
19. Ögütçü, G., Testik, Ö. M. i Chouseinoglou, O. (2016). *Analysis of personal information security behavior and awareness.* Computers & Security, 56, 83-93.
20. Parsons, K., Calic, D., Pattinson, M. R., Butavicius, M. A., McCormac, A. i Zwaans, T. (2017). *The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies.* Computers & Security, 66, 40-51.
21. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. i Jerram, C. (2014). *A study of information security awareness in Australian government organizations.* Information Management & Computer Security, 22(4), 334-345.
22. Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M. i Jerram, C. (2015). *The Influence of Organisational Information Security Culture on Cybersecurity Decision Making.* Journal of Cognitive Engineering and Decision Making: Special Issue on Cybersecurity Decision Making, 9(2), 117-129.
23. Sasse, M. A., Brostoffand, S. i Weirich, D. (2001). *Transforming the 'weakest link'- a human/computer interaction approach to usable and effective security*. BT Technology Journal, 19, 122.-131.
24. Selmar, M. i Tibert, V. (2018). *Reducing consumer risk in electronic marketplaces*. Computer in Human Behavior, 86, 205-217.
25. Smart, W. (2018). *Lessons learned review of the WannaCry ransomware cyber attack*. Preuzeto s *https://www.england.nhs.uk/wp-content/uploads/2018/02/06_pb_08_02_18-lessons-learned-review-wannacry-ransomware-cyber-attack.pdf,* 15. 3. 2019.
26. Sommestad, T., Hallberg, J., Lundholm, K. i Bengtsson, J. (2014). *Variables influencing information security policy compliance: A systematic review of quantitative studies*. Information Management & Computer Security, 22(1), 42-75.
27. Šolić, K. i Ilakovac, V. (2009). *Security perception of a portable PC user (The difference between medical doctors and engineers): a pilot study.* Medicinski Glasnik Ljekarske komore Zeničko-dobojskog kantona, 2, 261-264.

28. Šolić, K., Ilakovac, V., Marušić, A. i Marušić, M. (2009). *Trends in using insecure e-mail services in communication with journal editors*. Proceedings PRC, 50.
29. UK Government (2015). *Information Security Breaches Survey*. Preuzeto s *https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf*, 12. 12. 2017.
30. United States Department of Justice (2018). *Report of the Attorney General's Cyber Digital Task Force.* Preuzeto s *https://www.justice.gov/cyberreport*, 22. 4. 2020.
31. Taherdoost, H. (2016). *Validity and Reliability of the Research Instrument: How to Test the Validation of a Questionnaire/Survey in a Research*. International Journal of Academic Research in Management, 5 (3), 28-36.
32. Velki, T. (2019). *Rizična ponašanja računalnih korisnika u digitalnom svijetu*. Pozvano predavanje u sklopu 27. godišnje konferencije hrvatskih psihologa: Psihologija i digitalni svijet.
33. Velki, T., Mayer, A. i Norget, J. (2019). *Development of a New International Behavioral-Cognitive Internet Security Questionnaire: Preliminary Results from Croatian and German samples*. Proceedings from 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1410-1413.
34. Velki, T. i Romstein, K. (2019a). *User Risky Behavior and Security Awareness through Lifespan.* International journal of electrical and computer engineering systems, 9(2), 9-16.
35. Velki, T. i Romstein, K. (2019b). Nacionalno istraživanje rizičnog ponašanja i znanja računalnih korisnika. U: T. Velki i K. Šolić (urednici). Izazovi digitalnog svijeta. Osijek: Sveučilište J. J. Strossmayera u Osijeku, Fakultet za odgojne i obrazovne znanosti, 41-59.
36. Velki, T. i Šolić, K. (2019a). *Izazovi digitalnog svijeta*. Osijek: Fakultet za odgojne i obrazovne znanosti Sveučilišta J. J. Strossmayera u Osijeku.
37. Velki, T. i Šolić, K. (2019b). *Development and Validation of a New Measurement Instrument: The Behavioral-Cognitive Internet Security Questionnaire (BCISQ)*. International Journal of Electrical and Computer Engineering Systems, 10(1), 19-24.
38. Velki, T. i Šolić, K. (2018). *Priručnik za informacijsku sigurnost i zaštitu privatnosti.* Osijek: Fakultet za odgojne i obrazovne znanosti Sveučilišta J. J. Strossmayera u Osijeku.
39. Velki, T., Šolić, K., Gorjanac, V., i Nenadić, K. (2017). *Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results.* Proceedings from 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1280-1284.
40. Velki, T., Šolić, K. i Nenadić, K. (2015). *Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS).* Psihologijske teme, 24(3), 401-424.
41. Velki, T., Šolić, K. i Očevčić, H. (2014). *Development of Users' Information Security Awareness Questionaire (UISAQ): Ongoing Work*. Proceedings from 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1417-1421.
42. Wilcox, H., Bhattacharya, M. i Islam, R. (2014). *Social Engineering through Social Media: An Investigation on Enterprise Security*. U: L. Batten, G. Li, W. Niu i M. Warren (urednici). Communications in Computer and Information Science. Berlin: Heidelberg Springer, 243-255.
43. Yébenes Prous, M. J. G., Salvanés, R. F., Ortells, C. L. (2009). *Validation of questionnaires*. Reumatologia Clínica, 5(4), 171-177.

Summary

Tena Velki, Krešimir Šolić

Development of Social Engineering Research Tool on College Student Population: Behavioural Cognitive Internet Security Questionnaire (BCISQ)

The rapid development of digital technology has led to specific problems, especially in the information security area. Social engineering, which involves manipulating people to disclose confidential information, attacks computer system users as the weakest security link. The user contributes greatly to this phenomenon through his reckless and conscienceless behaviour. Raising users' awareness of social engineers' potential tricks against them has proven to be one of the most effective security measures. In order to be able to oppose social engineering at all, it is necessary to have a valid and reliable method of assessing the risky behaviour and level of information security awareness of the typical user. The research aimed to develop and validate a new Croatian version of a measurement instrument for social engineering research: the Behavioural-Cognitive Internet Security Questionnaire (BCISQ). Students of the J. J. Strossmayer University in Osijek (N=287) participated in this study. They have completed the BCISQ online through specially designed software. The BCISQ consists of 4 subscales, the first two examining the behavioural component (self-assessment and simulation of risky online behaviour) and the other two measuring the cognitive component of cybersecurity (awareness of online risks and the importance of safe computer systems use). The results showed that real (simulated) risky online behaviour of users is not related to their own assessments; that is, their self-assessments differ from their actual behaviour in the virtual world. Moreover, although most users have a quite high level of awareness of the potential online risks, a large number of them have entered their email address (20.9 %), and an even greater number have left their password to access the same (61.7 %). The BCISQ has proven to be a reliable and valid measurement instrument with good psychometric characteristics. It can be used for reliable assessment of the online behaviour and the security awareness level of information-communication system's users.

Keywords: internet security, data privacy, user behaviour, questionnaire, BCISQ.