Ана М. Славковић[1]
Академија техничких струковних студија Београд,
Одсек Београдска политехника
Београд (Србија)

Никола М. Славковић[2]
Академија техничких струковних студија Београд,
Одсек Компјутерско-машинско инжењерство
Београд (Србија)

Дане Р. Субошић[3]
Криминалистичко-полицијски универзитет,
Департман криминалистике, Катедра полицијских наука
Земун (Србија)

316.77: 004.738.5
305:316.472-053.6
Оригинални научни рад
Примљен 26/01/2023
Измењен 28/04/2023
Прихваћен 28/05/2023
doi: 10.5937/socpreg57-42454

АНАЛИЗА ПОНАШАЊА КОРИСНИКА ДРУШТВЕНИХ МРЕЖА У КОНТЕКСТУ СМАЊЕЊА РИЗИКА БЕЗБЕДНОСТИ У ДИГИТАЛНОМ ОКРУЖЕЊУ

Сажетак: Радом се проблематизује понашање корисника друштвених мрежа у контексту смањења ризика безбедности у дигиталном окружењу. С тим у вези, предмет рада је понашање корисника друштвених мрежа (претежно „миленијалаца" из студентске популације, безбедносне професионалне оријентације) у зависности од пола. Циљ истраживања је идентификација препорука за безбедније коришћење друштвених мрежа, па је зато реализовано истраживање које је базирано на анонимној анкети од 15 питања (3 демографског и 12 суштинског значаја), у којој је учествовало 333 студента основних и мастер студија оба пола, који студирају на факултету безбедносне програмске оријентације. Користећи *Mann-Whitney* тест, таблице контингенције, *Kruskal-Wallis* тест, као и *Spearman* тест, утврђено је да су модели понашања и мушкараца и жена на друштвеним мрежама веома слични, али и да постоје значајне статистичке разлике у неким сценаријима. Поред тога, показало се да испитана група, без обзира на пол, свесно улази у ризик од напада, остављајући своје податке уз неопрезно коришћење уређаја, заштитних лозинки и кодова. Поређењем наведених закључака са ставом опште хипотезе: „Постоје сличности и разлике између жена и мушкараца у погледу понашања на друштвеним мрежама и у сајбер простору уопште", долази се до закључка да је она верификована. Једно од решења идентификованих проблема понашања корисника друштвених мрежа јесте

[1] aslavkovic@atssb.edu.rs
[2] nslavkovic@atssb.edu.rs
[3] dane.subosic@kpu.edu.rs

подизање њихове свести о ризику пословања и/или забаве на друштвеним мрежама, као и њихова континуирана обука ради заштите сопствених података.

Кључне речи: сајбер безбедност, друштвене мреже, заштита података, пол, модели понашања

УВОД

Сајбер безбедност је тематика која се нарочито развила са појавом фреквентне употребе дигиталних ресурса. Друштвене мреже, е-пословање, мобилно банкарство, само су неки од мета нападача са крајњим циљем да се искористи туђ ресурс у сопствене сврхе и тако реализује материјална добит или формира неки други интерес стране која се тумачи као нападач или хакер. Један од важних фактора раста ризика безбедности у дигиталном окружењу је понашање људи, које се, између осталог, састоји у неопрезној и отвореној комуникацији на различитим мрежама, приликом које крајњи корисници омогућавају нападачима лакшу злоупотребу ресурса корисника.

Тренутно се у сајбер простору, у свету, налазе на располагању милијарде украдених комбинација корисничких имена и лозинки, спремних за лаку злоупотребу (Samtani, Kantarcioglu, Chen, 2021). Сви подаци које корисници депонују на веб-сајтовима могу бити осигурани криптософтверима, нарочито енкрипцијским софтвером, који омогућава да информације буду шифроване на начин да ниједна неауторизована особа не може реконструисати оригинални текст или бројке из кода (Menezes, Oorschot, Vanstone, 1997). Међутим и упркос овоме, инциденти цурења података постали су уобичајени у данашње време и носе огромне губитке. Укупно око 3,2 милијарде украдених података које чини комбинација корисничког имена и лозинке је данас доступно на веб-сајтовима (SpyCloud, 2021 Report). Поред овога, у свету се годишње краде око 133.000 лозинки највиших руководилаца многих компанија (Nordpass Research, 2022). Анализирајући проблем „цурења података", треба имати у виду да већина корисника има навику да стално користи исте комбинације корисничког имена и лозинке на више локација (Nordpass Research, 2022), како за своје приватне, тако и за своје радне налоге. Поновна употреба лозинке – „рециклирање лозинке", није једина лоша безбедносна навика у сајбер простору. Корисници су „криви" што су бирали сувише слабе лозинке за заштиту својих налога (SpyCloud, 2021 Report, Nordpass Research, 2022). Још један безбедносни проблем је тај што људи на друштвеним мрежама откривају превише података о свом личном животу, а познато је да сви своје лозинке праве од делова свог живота, имена вољених особа, града рођења, датума рођења или било ког другог личног важног догађаја (Kumar, Somani, 2018). Такође, људи воле да остављају коментаре на друштвеним мрежама, чиме се још више огољавају пред сајбер криминалцима. Недавно је доказано да испитаници у Србији најчешће сматрају коментарисање на друштвеним мрежама важним и утицајним (Necić, Milosavljević, 2022).

Фирма IBM је од јануара до децембра 2020. године прикупила велике количине података од својих клијената и јавних извора, како би анализирала типове сајбер напада, методе напада, глобална и индустријска поређења, и резултате свог истраживања

објавила у публикацији *ИБМ Секјурити ИКС-Форс* (*IBM Security X-Force Research Hub*, 2022). Резултати овог истраживања се односе на следеће:

- најпопуларнији метод сајбер напада у 2021. години био је *Рансомвер – Ransomware* (Federal Office for Information Security, Republic of France, 2021);
- процењена добит од врхунског *Рансомвера* је преко 100 милиона долара годишње. Процењује се да су само учесници *Содинокиби* (познатог и као *РЕвил*) *Рансомвера* остварили најмање 123 милиона долара профита у 2020. години и противправно отуђили око 21,6 терабајта података. Чак је и фирма *Apple* била њихова мета у априлу 2021. године, што указује на то да се овај тренд наставио и у 2022. години (IBM, Identity and access management solutions, 2022);
- што се тиче рањивости, сајбер нападачи су највише искористили слабост *Citrix* – ове мултинационалне *клауд* компаније, у смислу грешке у Јава програму који омогућава удаљену комуникацију сервера и корисника. Ова рањивост је искоришћена у 25% свих напада у првом кварталу 2020. године и у 8% укупних напада у целој 2020. години (IBM, *Zero Trust Security Strategy*, 2022);
- географски, Европа је била највише нападана у 2021. години. Доживела је 31% од свих напада, а за њом следе Северна Америка (27%) и Азија (25%). Латинска Америка, Блиски исток и Африка носе значајно мање од 10% напада (IBM Security, The Cost of Insider Threats 2021).

У комуникацијама преко платформе *Zoom*, хакери су успели у априлу 2021. године да великом провалом података открију око 500.000 корисничких лозинки (Zoom-Security-White-Paper, 2021). Просечан трошак цурења података у 2021. години, пријављених у свету, био је 3,86 милиона долара (World Development Report, 2021).

Како се употреба дигиталних алата повећава, тако се повећава и количина створених података. Светска банка је проценила да је до краја 2022. године, годишњи укупан интернет саобраћај порастао за око 50% у односу на ниво из 2021. године, достижући 4,8 зетабајта (The World Bank, World Development Report, 2021). Знатно шири простор за могућност сајбер напада и чини ову тематику још актуелнијом.

Наведеном проблему крађе података, тј. корисничких налога и лозинки, треба додати чињеницу да је потребно само 10 минута да се разбије лозинка са малим словима која има шест знакова (Avast antivirus, 2022), што заправо значи да у великом броју случајева није потребно ни украсти податке, већ су људи својом неопрезношћу и сопственим немаром себе учинили рањивима. У овим околностима, показало се да је сајбер криминалцима много лакше да „пробију" психолошки зид појединца, него технолошки систем заштите података који путују кроз рачунарске мреже.

Имајући у виду све до сада наведено, овим радом се проблематизује понашање корисника друштвених мрежа у контексту смањења ризика безбедности у дигиталном окружењу. Прецизније, предмет рада је анализа понашања „миленијалаца" из студентске популације, безбедносне професионалне оријентације, на друштвеним мрежама и то у зависности од пола. Циљ истраживања је дефинисање прецизних препорука за безбедније (мање ризично) коришћење друштвених мрежа.

Имајући у виду оно што се овим радом проблематизује, структуриран је његов главни део. Наиме, садржај рада обухвата: методологију и резултате истраживања, као и дискусију, чему следе: закључак, попис коришћене литературе и прилози. Дакле, рад има IMRAD структуру, што је последица његовог теоријско-емпиријског садржаја.

МЕТОДОЛОГИЈА ИСТРАЖИВАЊА

Истраживањем се верификује општа хипотеза која гласи: „Постоје сличности и разлике између жена и мушкараца у погледу понашања на друштвеним мрежама и сајбер простору уопште". Из ње су изведене посебне хипотезе које гласе:

1. постоје разлике у ризичности понашања на друштвеним мрежама између полова;
2. постоје разлике међу половима у времену проведеном на друштвеним мрежама;
3. сви млади људи олако остављају своје личне податке или фотографије на друштвеним мрежама, без обзира на пол;
4. постоји корелација између (не)обазривости у анализи туђих профила и прихватању непознатих људи за „пријатеље" на друштвеним мрежама;
5. постоји разлика између полова у креирању лозинки за приступ сајбер простору.

С тим у вези, реализовано је истраживање које је базирано на анонимној анкети, у којој је учествовало 333 студента, оба пола, који студирају на Факултету безбједносних наука Универзитета у Бања Луци, са свих година основних студија, као и студенти мастер студија.

Циљ истраживања је да се сагледају навике одраслих младих људи из студентске популације безбедносне оријентације при коришћењу друштвених мрежа, у зависности од којих ће бити формулисане препоруке, како би дошло до ублажавања или елиминисања идентификованих слабости њиховог понашања, али и понашања шире популације људи у наведеном контексту. Наведени узорак испитаника је изабран јер је претежно реч о „миленијалцима" (најфреквентнијим корисницима друштвених мрежа, због чега су изложенији ризичним догађајима који нарушавају сајбер безбедност од остатка популације) и студентима чија је професионална оријентација *безбедност*. Због тога се за њих може основано претпоставити да боље баратају дигиталним уређајима и информационо-комуникационим технологијама, као и да имају изграђенију безбедносну културу од остатка популације.

Истраживање има просторно и временско ограничење. Просторно, реч је о Факултету безбједносних наука Универзитета у Бања Луци, у ширем контексту о Републици Српској, а временски је ограничено на период 2017–2022. године. Наиме, Факултет је основан 2017. године, тако да реализује веома актуелан студијски програм *Безбједност и криминалистика* на основним, односно *Управљање безбједносним ризицима природних катастрофа* на мастер студијама, веома је популаран јер, уз студије психологије, има највећи број кандидата за упис на Универзитету у Бања Луци, што посредно указује на квалитет и мотивацију студената, односно испитаника. С друге стране, временско ограничење на период 2017–2022. године последица је обезбеђења узорка испитаника у стотинама, уз коришћење периода пандемије коронавируса, која је довела до експанзије коришћења интернета и дигиталних уређаја.

РЕЗУЛТАТИ ИСТРАЖИВАЊА

Од 333 испитаника, женског пола је било 150 (45%), а мушког пола 183 (55%). Испитивана група је била хомогена по полу, односно, заступљеност жена и мушкараца не показује статистички значајну разлику ($\chi 2 = 3{,}270$; $p = 0{,}071$ или $p > 0{,}05$). При томе, прва три питања су демографског карактера, тако да је анализа одговора испитаника урађена на питања од 4. до 15.

Питање 4: „Да ли користите исту лозинку за сваки веб-сајт и апликацију којој приступате?"

Код испитаника мушког и женског пола, дистрибуција одговора била је готово идентична, односно највећи број испитаника, на ово питање одговорио је: „Имам неколико које мењам." Одговори на питање 4 из упитника, не показују статистички значајну разлику између женског и мушког пола ($\chi^2 = 0{,}258$; $p = 0{,}879$ или $p > 0{,}05$). Такође, није нађена, статистички значајна, корелацијска повезаност (веза) између пола испитаника и понуђених одговора на питање ($r = 0{,}023$; $p > 0{,}05$).

Питање 5: „Колико често приступате друштвеним мрежама у току дана?"

Код испитаника мушког и женског пола, дистрибуција одговора је била готово идентична, односно највећи број испитаника ($N = 157$; 47,1%), на ово питање је одговорио: „Више од 5 пута дневно". Одговори на питање 5 из упитника не показују статистички значајну разлику између женског и мушког пола ($\chi^2 = 4{,}655$; $p = 0{,}325$ или $p > 0{,}05$). Даље, није нађена, статистички значајна, корелацијска повезаност између пола испитаника и понуђених одговора на питање 5 ($r = -0{,}038$; $p > 0{,}05$). Међутим, корелација је инверзног типа, што значи да су испитаници мушког пола склонији одговорима чешћег приступа друштвеним мрежама, што се може видети код најчешћег одговора „више од 5 пута дневно", где је од 157 испитаника њих 95 (60,5%) мушког пола.

Питање 6: „Колико времена дневно проводите на друштвеним мрежама?"

Код испитаника мушког и испитаника женског пола дистрибуција одговора је и код овог питања готово идентична, односно највећи број испитаника ($N = 186$; 55,9%), на ово је одговорио: „$60 \leq t \leq 240$". Одговори на питање 6 из упитника не показују статистички значајну разлику између женског и мушког пола ($\chi^2 = 1{,}423$; $p = 0{,}700$ или $p > 0{,}05$).

Није нађена статистички значајна разлика у времену проведеном на друштвеним мрежама између мушкараца и жена ($t = 0{,}395$; $p = 0{,}693$ или $p > 0{,}05$). На Слици 1 представљена је дистрибуција времена проведеног на друштвеним мрежама, за оба пола. Мушкарци су, на друштвеним мрежама, просечно проводили 186,51 минут, док су жене просечно проводиле 178,81 минут, и то укупно гледано од минималних 0 минута до максималних 1.080 минута (18 сати) дневно, а најучесталије (мод) 120 минута (Табела 4).

Посматрајући одговоре на питања 5 и 6, може се закључити да испитаници мушког пола више пута и дуже приступају друштвеним мрежама у односу на испитанике женског пола.

Питање 7: „На друштвеним мрежама остављам податке о себи као што су: датум рођења, место рођења, имејл, телефон, други лични подаци, као што су детаљи о пријатељима, неки део своје биографије, девојачко презиме мајке…"

Код испитаника мушког и испитаника женског пола дистрибуција одговора је различита, односно највећи број испитаника (N = 155; 46,5%), на ово питање је одговорио „Увек", тј. да на друштвеним мрежама оставља личне податке. Одговори на питање 7 из упитника не показују статистички значајну разлику између женског и мушког пола, ако користимо *Mann-Whitney* тест. Међутим, када се примени осетљивији *Kruskal Wallis* тест, нађена је статистички значајна разлика у дистрибуцији одговора на питање 7, између испитаника мушког и женског пола (χ^2 = 10,534; p = 0,005 или p < 0,01). Мање од 10% мушкараца никада не оставља своје личне податке на друштвеним мрежама, док је то случај код нешто мање од ¼ жена (22,7%), те се може рећи да мушкарци, статистички значајно, чешће остављају личне податке на друштвеним мрежама од жена (Табела 5).

Битно је закључити и да је остављање личних података, модел понашања на друштвеним мрежама ове целе испитиване групе, јер је статистички значајно најмање испитаника одговорило да никада на друштвеним мрежама не оставља своје податке (χ^2 = 50,829; p = 0,000 или p < 0,001).

Питање 8: „На свој профил на друштвеним мрежама постављам своје фотографије и фотографије чланова своје породице."

Код испитаника мушког и женског пола дистрибуција одговора је слична, односно највећи број испитаника (N = 155; 46,5%), на ово питање је одговорио: „Понекад", када је реч о учесталости постављања фотографија на свом профилу на друштвеној мрежи.

Одговори на питање 8 из упитника не показују статистички значајну разлику између женског и мушког пола, нити када је реч о *Mann-Whitney* нити *Kruskal Wallis* тесту (χ^2 = 4,082; p = 0,130 или p > 0,05). Међутим, постојање негативног предзнака испред Спирмановог коефицијента корелације указује на инверзан облик корелацијског односа, односно да су жене склоније постављању фотографија на друштвеним мрежама (r = -0,101; p > 0,05).

Питање 9: „Коментаришем догађаје који су објављени на друштвеним мрежама и пишем своје мишљење о стварима које су тамо објављене."

Код испитаника мушког и женског пола дистрибуција одговора била је готово идентична, односно највећи број испитаника (N = 172; 51,7%) на ово питање је одговорио: „Никада". Одговори на питање 9 из упитника не показују статистички значајну разлику између женског и мушког пола (χ^2 = 0,880; p = 0,644 или p > 0,05). Добијени резултати анкете показују да више од ½ мушкараца и више од ½ жена никада не коментаришу догађаје који су објављени на друштвеним мрежама.

Питање 10: „Увек детаљно проверавам профил некога ко жели да ми буде пријатељ на друштвеној мрежи."

Код испитаника мушког и испитаника женског пола дистрибуција одговора била је врло слична, односно највећи број испитаника (N = 204; 61,3%) на ово питање је одговорио: „Увек".

Одговори на питање 10 из упитника не показују статистички значајну разлику између женског и мушког пола ($\chi^2 = 1{,}922$; $p = 0{,}382$ или $p > 0{,}05$). Ипак, постојање негативног предзнака испред Спирмановог коефицијента корелације указује на инверзан облик корелацијског односа, односно да су жене склоније проверавању профила оног кога желе за пријатеља на друштвеним мрежама ($r = -0{,}075$; $p = 0{,}169$ или $p > 0{,}05$).

Питање 11: „На друштвеним мрежама прихватам као пријатеља искључиво некога кога лично познајем."

Код испитаника мушког и испитаника женског пола дистрибуција одговора била је врло слична, односно највећи број испитаника (N = 204; 61,3%) на ово питање је одговорио: „Увек". Одговори на питање 11 из упитника не показују статистички значајну разлику између женског и мушког пола ($\chi^2 = 2{,}282$; $p = 0{,}320$ или $p > 0{,}05$). Постојање негативног предзнака испред Спирмановог коефицијента корелације указује на инверзан облик корелацијског односа, односно да су жене склоније да за пријатеље прихватају само онога кога лично познају ($r = -0{,}005$; $p = 0{,}934$ или $p > 0{,}05$).

Питање 12: „Користим исти приступни уређај (рачунар или мобилни телефон) и за рад и за посету друштвеним мрежама."

Дистрибуција одговора је, у овом случају, различита између испитаника мушког и женског пола. Највећи број испитаника (N = 279; 83,8%) на ово питање је одговорио: „Увек". Одговори на питање 12 из упитника показују статистички значајну разлику између женског и мушког пола, када користимо *Mann-Whitney* тест. Такође, када се употреби осетљивији, *Kruskal Wallis* тест, коригован за таблицу контингенције типа 2×2, нађена је статистички значајна разлика у дистрибуцији одговора на питање 12, између испитаника мушког и женског пола ($\chi^2 = 5{,}968$; $p = 0{,}015$ или $p < 0{,}05$).

Одговор на питање 12 зависи од пола, што показује и постојање статистички значајне корелације између пола и одговора и на питање 12, односно да су жене склоније да користе различите приступне уређаје за рад, од оних које користе за посету друштвеним мрежама (Табела 6). Ова тврдња је поткрепљена и статистички значајном корелацијом ($r = 0{,}142$; $p = 0{,}009$ или $p < 0{,}01$). Може се такође закључити да је употреба истог уређаја и за рад и за посету друштвеним мрежама модел понашања у сајбер простору ове целе испитиване групе, јер је статистички значајно највише испитаника (N = 279; 83,8%) одговорило да увек користи исти приступни уређај, с тим што жене ређе користе исти приступни уређај од мушкараца, односно показују већи степен опрезности, тј. одговорности ($\chi^2 = 152{,}027$; $p = 0{,}000$ или $p < 0{,}001$).

Питање 13: „Да ли сте свесни да постоји опасност да Вам на основу података које остављате о себи на друштвеним мрежама неко сазна лозинку и злоупотреби је, или да може злоупотребити Ваше податке на неки други начин?"

Код испитаника мушког и испитаника женског пола дистрибуција одговора била је врло слична, односно највећи број испитаника (N = 325; 97,6%) на ово питање је одговорио: „Да". Одговори на питање 13 из упитника не показују статистички значајну разлику између женског и мушког пола ($\chi^2 = 0{,}006$; $p = 0{,}941$ или $p > 0{,}05$). Добијени резултати анкете показују да је 97,3% мушкараца и 98,0% жена свесно могућности „крађе" и злоупотребе лозинки и других података, те се може рећи да

одговор на питање 13 не зависи од пола, што показује и непостојање статистички значајне корелације између пола и одговора на питање 13, али постојање негативног предзнака испред Спирмановог коефицијента корелације указује на инверзан облик корелацијског односа, односно да су жене ипак свесније могућности „крађе" и злоупотребе лозинки и личних података ($r = -0{,}024$; $p = 0{,}665$ или $p > 0{,}05$).

Питање 14: „Ако сте свесни могућности злоупотребе, да ли и даље делите податке о себи на друштвеним мрежама?"

Код испитаника мушког и испитаника женског пола дистрибуција одговора је била врло слична, односно највећи број испитаника, тј. нешто више од 2/3 је на ово питање одговорио потврдно: „Да". Одговори на питање 14 из упитника не показују статистички значајну разлику између женског и мушког пола ($\chi^2 = 2{,}356$; $p = 0{,}125$ или $p > 0{,}05$). Добијени резултати анкете показују да 69,9% мушкараца и 61,3% жена, упркос чињеници да су свесни могућности злоупотребе, и даље „деле" податке о себи на друштвеним мрежама.

Питање 15: „Колико су Вам лозинке 'јаке'?"

Код испитаника мушког и испитаника женског пола дистрибуција одговора била је различита. Наиме, испитаници мушког (70,5%) и женског пола (70,7%), у готово идентичном проценту, користе лозинке које увек садрже 8–14 карактера, састављене од бројева и слова. Међутим, разлика између мушкараца и жена види се у употреби лозинки које садрже 14 и више карактера састављених од бројева и слова, коју жене (9,3%) ређе користе од мушкараца (17,5%), као и у чињеници да жене (12%) чешће не воде рачуна о „јачини" лозинке од мушкараца (5,5%) (Табела 7). Одговори на питање 15 из упитника показују статистички значајну разлику између женског и мушког пола, ако користимо *Mann-Whitney* тест. И када смо употребили осетљивији тест, *Kruskal Wallis* тест, нађена је статистички значајна разлика у дистрибуцији одговора на питање 15, између испитаника мушког и женског пола ($\chi^2 = 8{,}392$; $p = 0{,}039$ или $p < 0{,}05$). Добијени резултати анкете показују да мушкарци чешће користе лозинке које имају 14 и више карактера, састављене од бројева и слова, а да жене чешће не воде рачуна о „јачини" лозинке, што показује и постојање статистички значајне корелације између пола и одговора на питање 15 ($r = 0{,}151$; $p = 0{,}0006$ или $p < 0{,}001$).

Користећи *Mann-Whitney* тест, испитаници женског и мушког пола показују статистички значајну разлику само у одговорима на питања 12 и 15 (Табела 1). Прецизнија процентуална дистрибуција одговора, на сва питања из упитника, у зависности од пола испитаника, уочена је употребом Таблица контингенције, односно *Kruskal-Wallis* теста, где је уочена значајна статистичка разлика у питањима 7, 12 и 15 (Табела 2). Применом *Сйирмановоī* теста, утврђене су значајне вредности корелације код питања 7, 12 и 15 (Табела 3).

ДИСКУСИЈА

Одговори на питање 4 указују на то да нема статистички значајне разлике између испитаника мушког и женског пола када је реч о томе да ли користе исту лозинку за сваки веб-сајт и апликацију којој приступају. Најчешћи одговор на ово питање је

био: „Имам неколико које мењам", што указује на модел понашања на друштвеним мрежама испитиване групе.

Одговори на питање 5 указују на то да је приступање друштвеним мрежама више од пет пута дневно, модел понашања на друштвеним мрежама испитиване групе јер је, статистички значајно, најмање испитаника одговорило да никада не приступа друштвеним мрежама, односно да то чини једном дневно, као и да мушкарци показују већу склоност ка чешћем приступању друштвеним мрежама.

Одговори на питање 6 указују на то да је боравак на друштвеним мрежама у трајању од 60 до 240 минута, тачније од 60 до 180 минута, модел понашања на друштвеним мрежама ове испитиване групе, с тим што је најучесталије време проведено на друштвеним мрежама 120 минута. Млади мушкарци проводе више времена дневно на друштвеним мрежама од младих жена.

За питања 5 и 6 постоји статистички значајна директна, тј. позитивна, корелација времена проведеног на друштвеним мрежама и броја приступа друштвеним мрежама. То упућује на закључак да испитаници који чешће приступају друштвеним мрежама по правилу и више времена проведу на њима, те да су, мада не и статистички значајно, мушкарци склонији оваквом моделу понашања, тј. чешћем приступању и дужем боравку на друштвеним мрежама.

Одговори на питање 7 указују на то да је остављање личних података модел понашања на друштвеним мрежама ове испитиване групе јер је статистички значајно најмање испитаника одговорило да никада на друштвеним мрежама не оставља своје податке. Овакав модел понашања зависи од пола испитаника, односно, статистички значајно, овакав модел понашања чешћи је код мушкараца него код жена.

Одговори на питање 8 указују на то да је постављање личних фотографија модел понашања на друштвеним мрежама ове испитиване групе, те да су жене склоније да постављају своје фотографије на друштвеним мрежама.

Одговори на питање 9 указују на то да је некоментарисање догађаја и неписање сопствених ставова и мишљења модел понашања на друштвеним мрежама ове испитиване групе, која се састојала од студената. Овакав модел понашања је доминантан и код младих мушкараца и код младих жена, тј. не зависи од пола испитаника. Резултат потврђује раније спроведено истраживање (Necić, Milosavljević, 2022) где се у закључним разматрањима наводи да њихова испитивана група „коментарисање најчешће сматра важним и утицајним. Овакав став је нарочито присутан међу старијом популацијом".

Одговори на питање 10 указују на то да је проверавање профила оног кога жели да вам буде пријатељ на друштвеним мрежама, модел понашања ове испитиване групе, те да су жене склоније проверавању профила онога кога желе за пријатеља на друштвеним мрежама.

Одговори на питање 11 показују да је прихватање за пријатеља, на друштвеним мрежама, само онога кога лично познају, модел понашања ове испитиване групе, те да су жене склоније оваквом моделу понашања на друштвеним мрежама.

Одговори на питање 12 указују на то да је употреба истог приступног уређаја (рачунар или мобилни телефон) и за рад и за посету друштвеним мрежама модел понашања ове испитиване групе, те да је, статистички значајно, овакав модел понашања чешћи код мушкараца него код жена, и да је у директној корелацији са мушким полом.

Одговори на питање 13 показују да је познавање чињенице о могућности „крађе" и злоупотребе лозинки и других података на друштвеним мрежама важећи модел целе групе, те да је доминантан како код мушкараца тако и код жена, с тим што су жене свесније чињенице оваквих облика злоупотребе на друштвеним мрежама.

Одговори на питање 14 указују на то да без обзира на чињеницу да јесу свесни ризика таквог понашања, „дељење" података о себи на друштвеним мрежама јесте модел понашања целе групе. Овај модел понашања не зависи од пола, односно овакво понашање је карактеристично за испитанике ове групе, без обзира на пол.

Одговори на питање 15 указују на то да је употреба лозинки које увек садрже 8–14 карактера, састављених од бројева и слова, модел понашања ове групе, јер је статистички значајно највише испитаника (N = 235; 70,6%) одговорило да користи лозинке те „јачине", као и да „јачина" лозинки које користи ова испитивана група зависи од пола, односно жене ретко користе врло „јаке" лозинке и чешће о томе не воде рачуна.

ЗАКЉУЧАК

Истраживањем је потврђена хипотеза да код младе популације постоје разлике у ризичности понашања у сајбер простору између полова, у смислу да мушкарци, статистички значајно, чешће остављају личне податке на друштвеним мрежама у односу на жене. Уочено је да жене такође чешће постављају личне фотографије на друштвене мреже. Млади мушкарци проводе више времена на друштвеним мрежама од младих жена.

Млади мушкарци су, статистички значајно, склонији да користе исте приступне уређаје за рад и забаву, у односу на жене, тј. мање су обазриви од жена. То је додатно потврђено и постојањем статистички значајне корелације између пола и употребе истог приступног уређаја за рад и приступ друштвеним мрежама. Као потврда ове тврдње јесте и резултат да жене више проверавају профил онога ко жели да им буде пријатељ на друштвеној мрежи, пре прихватања „пријатељства". Жене су склоније да прихватају за пријатеља само онога кога лично познају.

Иако се мушкарци генерално ризичније понашају у сајбер окружењу, они ипак користе „јаче" лозинке, уочена је статистички значајна разлика у односу на жене. Чешће воде рачуна о томе какав је садржај лозинке, што потврђује и постојање статистички значајне корелације пола и „јачине" коришћених лозинки. Млади мушкарци своју сајбер безбедност првенствено базирају на јаким приступним лозинкама, док се у самом сајбер простору понашају опуштеније и ризичније од младих жена.

Верификацијом свих пет посебних хипотеза створили су се услови за верификацију опште хипотезе. Наиме, понашање на друштвеним мрежама зависи од пола у одређеним (не у свим) сценаријима. Поређењем тог закључка са ставом опште хипотезе: „Постоје сличности и разлике између жена и мушкараца у погледу понашања на друштвеним мрежама и сајбер простору уопште", долази се до закључка да је она верификована.

У овом раду потврђене су постојеће претпоставке о важности људског фактора за безбедност крајњих корисника друштвених мрежа. Истраживање је доказало да

постоје значајне статистичке разлике у приступу дигиталним ресурсима између мушког и женског пола у посматраној (студентској) популацији. С циљем превазилажења овог проблема, пожељан је развој препорука за коришћење друштвених мрежа и механизама контроле њихове примене. Такве препоруке треба да развијају радна тела влада намењена за информационе технологије и електронску управу, односно поједини органи државне управе (министарства, нпр. министарство за државну управу и локалну самоуправу и др.). Препоруке, као што су: 1) пожељно је коришћење различитих лозинки за сваки веб-сајт и апликацију којој се приступа, 2) на друштвеним мрежама се поставља минимум података о себи, 3) на свом профилу на друштвеним мрежама поставља се минимум сопствених фотографија и фотографија чланова породице, 4) увек се детаљно проверава профил некога ко жели да буде „пријатељ" кориснику на друштвеној мрежи, 5) на друштвеним мрежама прихвата се за „пријатеља" искључиво неко кога лично познаје корисник, 6) користе се увек „јаке" лозинке и др., треба да буду систематизоване у форми докумената каква су смернице или правила, а која су доступна на специјализованим платформама (нпр. Национална платформа за превенцију насиља које укључује децу „Чувам те"), до којих би корисници долазили ваљаним информисањем (маркетиншким кампањама у медијима, информисањем на радном месту или у образовној установи).

Најзад, правци будућих истраживања у овој области могу да се односе на долазак до сазнања о безбедности коришћења друштвених мрежа у зависности од старости и статуса корисника. Када је реч о статусу корисника, мисли се на њихов правни положај, нпр.: ученици, студенти, незапослени, запослени, пензионери и др. Тиме би се превазишла ограничења овог истраживања, јер је њиме истраживано само понашање корисника друштвених мрежа унутар дела студентске популације, у зависности од њиховог пола.

Ana M. Slavković[1]
Academy of Applied Technical Studies Belgrade,
Polytechnic Department, Belgrade Branch
Belgrade (Serbia)

Nikola M. Slavković[2]
Academy of Applied Technical Studies Belgrade,
Computer and Mechanical Engineering Department
Belgrade (Serbia)

Dane R. Subošić[3]
University of Criminal Investigation and Police Studies,
Criminal Investigation Department, Police Science Chair
Zemun (Serbia)

ANALYSIS OF THE BEHAVIOUR OF SOCIAL MEDIA USERS IN THE CONTEXT OF SECURITY RISK REDUCTION IN THE DIGITAL ENVIRONMENT

(Translation *In Extenso*)

Abstract: This paper deals with the issues of the analysis of the behaviour of social media users in the context of security risk reduction in the digital environment. In this respect, the subject of this paper is the behaviour of social media users (mainly millennials, from the population of university students, attending studies in the field of security) depending on the gender. The aim of the research is to identify recommendations for a safer use of social media. To this end, the research was conducted on the basis of an anonymous survey comprising 15 questions (3 of demographic and 12 questions of essential significance). The survey covered 333 university students (undergraduate and graduate students of both genders) attending study programmes in the field of security. With the use of the Mann-Whitney test, contingency tables, the Kruskal-Wallis test, as well as the Spearman's rank correlation test, it has been established that the behaviour patterns of men and women who use social media are very similar, but that there is a substantial statistical difference in certain scenarios. In addition to this, this survey has shown that, irrespective of the gender, risks of being attacked are consciously taken when sharing personal information, along with a reckless use of devices, passwords, and passcodes. By comparing the above-mentioned conclusions with the position of the general hypothesis: "There are similarities and differences between men and women in terms of the behaviour patterns on social media and in the cyberspace in general", so the conclusion is that it is verified. One of the solutions to

[1] aslavkovic@atssb.edu.rs
[2] nslavkovic@atssb.edu.rs
[3] dane.subosic@kpu.edu.rs

the identified problems in the behaviour of social media users is to raise their awareness regarding the risks of doing business and/or accessing entertainment content on social media, as well as their continuous training for the purpose of protecting their own data.

Keywords: cybersecurity, social media, data protection, gender, behaviour patterns

INTRODUCTION

Cybersecurity is the topic that has particularly developed with the emergence of frequent use of digital resources. Social media, e-business and m-banking are only some of the targets of attackers' choice, the ultimate goal of such attacks being to use someone's resources for one's own purposes and thus to acquire material gain or some other interest, by a party who is seen as the attacker or hacker. One of the important factors of increasing security risks in the digital environment is human behaviour, which, among other things, involves reckless and open communication on various social media, during which end users allow attackers to misuse more easily the social media users' resources.

Currently in the world there are myriads of available combinations of stolen usernames and passwords ready to be easily misused (Samtani, Kantarcioglu, Chen, 2021). All data that the users leave on web pages may be secured via cryptosoftware, especially the encryption software, which allows for information to be coded in a manner that prevents any unauthorised person from reconstructing the original text or digits from the code (Menezes, Oorschot, Vanstone, 1997). Nevertheless, data leak incidents have become common these days, as a result of which enormous losses are incurred. A total of 3.2 billion stolen data, which comprise a combination of username and relative password, are available today on web pages (SpyCloud, 2021 Report). Furthermore, approximately 133,000 passwords are stolen worldwide, these passwords belonging to top management of many companies (Nordpass Research, 2022). While analysing the issue of "data leaks", we should keep in mind that the majority of social media users are in the habit of always using same combinations of their usernames and passwords on multiple locations (Nordpass Research, 2022), both for their private and business accounts. Recycling passwords is not the only bad habit in the cyberspace. It is the users' fault that they decide to use passwords that are too weak to protect their accounts (SpyCloud, 2021 Report, Nordpass Research, 2022). Another security issue is that people disclose too much information about their personal lives on social media and it is a widely known fact that the passwords they create are related to their lives, such as the names of persons they love, year of birth, date of birth or any other personally important event (Kumar, Somani, 2018). Moreover, people tend to leave comments on social media, thus revealing themselves even further to cybercriminals. It has recently been proven that respondents in Serbia in the majority of cases think that posting comments on social media is important and influential (Necić, Milosavljević, 2022).

From January to December 2020, the IBM Company collected an abundance of data from their clients and public sources alike with the purpose of analysing various types and methods of cyberattacks, for the sake of making global and industrial comparisons. The results of this research were published in the IBM Security X-Force publication (*IBM Security X-Force Research Hub*, 2022). The results of this research refer to the following:

- the most widely used method of cyberattacks in 2021 was ransomware (Federal Office for Information Security, Republic of France, 2021);
- the estimated earnings generated from top-notch ransomware is in excess of USD 100 million annually. It is estimated that only the participants of the Sodinokibi ransomware (also known as Ransomware Evil or REvil) earned a profit of not less than USD 123 in 2020 and gained illegal access to approximately 21.6 TB of data. Even the Apple company was targeted in April 2021, which is indicative of the fact that this trend persisted in 2022 as well (IBM, Identity and access management solutions, 2022);
- as regards vulnerability, cyberattacks used mainly vulnerabilities of the Citrix Company - a multinational cloud company, this vulnerability being relative to a Java programme, which allows remote communication between servers and the users. This vulnerability was used in 25% of all attacks in Q1 of 2020 and 8% of the total number of attacks in the entire year of 2020 (IBM, *Zero Trust Security Strategy*, 2022);
- in geographical terms, Europe was the most targeted region in 2021. It suffered 31% of all global cyberattacks. Europe is followed by North America (27%) and Asia (25%). Latin America, Middle East, and Africa cumulatively account for almost 10% of cyberattacks (IBM Security, The Cost of Insider Threats 2021).

In communication via the Zoom platform, hackers cracked approximately 500,000 user passwords in a large-scale attack in April 2021 (Zoom-Security-White-Paper, 2021). The average cost of data leaks reported worldwide in 2021 amounted to USD 3.86 million (World Development Report, 2021).

With the use of digital tools being on the increase, the use of generated data increased accordingly. The World Bank estimated that by the end of 2022, the overall internet traffic had increased by 50% compared to the 2021 levels, having reached 4.8 zettabytes in 2020 (the World Bank, World Development Report, 2021). This makes substantially more room for cyberattacks and makes this topic even more interesting.

To the mentioned issue of data theft, i.e., user accounts and password theft, we should also add the fact that it takes only 10 minutes to crack a password that contains six characters in small caps (Avast antivirus, 2022), which in practical term means that in a large number of cases it is not even necessary to steal data because people make themselves vulnerable by being reckless and negligent. In such circumstances, it transpires that it is much easier for cybercriminals to "penetrate" the psychological wall of individuals than data protection firewalls that roam computer networks.

If we keep in mind all of that has been mentioned until now, this paper deals with the issues of the analysis of the behaviour of social media users in the context of security risk reduction in the digital environment. More specifically, the subject of this paper is to analyse the behaviour of millennials, from the university student population (attending security-oriented study programmes), on social networks, depending on the gender. The purpose of this research is to identify specific recommendations for a safer (less risky) use of social media.

Bearing in mind the issues dealt with in this paper, its main body has been structured accordingly. Namely, the content of this paper includes: research methodology and results, as well as relative discussion, which are followed by: conclusion, list of references

used, and appendices. Hence, this paper has the IMRAD structure, which is the result of its theoretical-empirical content.

RESEARCH METHODOLOGY

This research verifies the general hypothesis, which is the following: "There are similarities and differences between men and women in terms of the patterns of behaviour on social media and in the cyberspace in general". From this main hypothesis, others have been derived, as follows:

1. there are differences between the genders in terms of risk levels of behaviour on social media:
2. there are differences between the genders in terms of time spent on social media;
3. all young people do not think twice before leaving their personal information or photos on social media, regardless of the gender;
4. there is a correlation between caution (and lack thereof) in the analysis of other persons' profiles and accepting as connections on social media complete strangers;
5. there is a difference between the genders in terms of creating passwords for accessing various locations in the cyberspace.

In this respect, the research was on the basis of an anonymous survey, the participants of which were 333 university students of the Faculty of Security Studies of the University of Banjaluka (both genders), who attended all years of undergraduate studies, as well as the students of master's studies.

The aim of this research is to look into the habits of university student population (attending security-oriented study programmes) in terms of the use of social networks, depending on how recommendations will be worded, in order to mitigate or eliminate identified weaknesses in their behaviour patterns, but also in the behaviour patterns of a broader population in the said context. The mentioned sample was selected because the respondents were mainly millennials (the most frequent social media users, as a result of which, compared to other categories of population, they are more vulnerable to security risk events that violate cybersecurity). In addition, the respondents were selected because *security* is their professional orientation. Therefore, it is reasonable to expect that they are more skilled at using digital devices and information communication technologies, and also that their security culture is better structured than is the case with the rest of the population.

There are certain temporal and spatial limitations to this research. Location-wise, the research was conducted at the Faculty of Security Studies, the University of Banja Luka, in a broader context of Republika Srpska, while it is temporally limited to the period between 2017 and 2022. Namely, at this Faculty, established in 2017, there is a very sought-after study programme *Security and criminal investigation* taught as an undergraduate course, as well as the *Management of security risks of natural disasters*, which is taught within master's studies. These are very popular because, besides psychology, there is the largest number of applicants for these study programmes at the University of Banja Luka, which is indirectly indicative of the quality of said programmes and students', i.e., respondents', motivation. On the other hand, the temporal limitation to 2017-2022 period is a result of acquiring a respondent sample of several hundred students. The observed period partly coincided

with the COVID-19 pandemic, during which there was a strong growth of the use of the Internet and digital devices.

RESEARCH RESULTS

Among 333 respondents, there were 150 (45%) female and 183 (55%) male respondents. The respondent group was homogenous in terms of gender, i.e., there was no major statistical difference between female and male respondents ($\chi 2 = 3.270$; $p = 0.071$, or $p > 0.05$). It is worth noting that the first three questions are demographic in character, so the analysis was conducted relative to the answers provided to questions 4 to 15.

Question 4: "Do you use the same password for every webpage and application you access?"

The distribution of answers was almost identical both for male and female respondents. Namely, the majority of respondents answered this question as follows: "There are several passwords I change between". Answers to question 4 of the questionnaire do not show any major statistical difference between female and male respondents ($\chi 2 = 0.258$; $p = 0.879$, or $p > 0.05$). Furthermore, no statistically significant correlation link (connection) has been identified between the gender of respondents and multiple-choice answers provided for this question ($r = 0.023$; $p > 0.05$).

Question 5: "How often during the day do you access social media?"

The distribution of answers was almost identical both for male and female respondents. Namely, the majority of respondents (N=157; 47.1%) provided the following answer to this question: "More than 5 times a day". Answers to question 5 of the questionnaire do not show any statistically significant difference between female and male respondents ($\chi^2 = 4.655$; $p = 0.325$ or $p > 0.05$). Additionally, no statistically significant correlation link has been identified between the gender of respondents and multiple-choice answers provided for question 5 ($r = - 0.038$; $p > 0.05$). However, there is an inverse correlation, which means that male respondents are more inclined to answer that they access social media more frequently. This is confirmed by the most common answer "more than 5 times a day", whereas 95 (or 60.5%) out of 157 respondents who provided this answer were male.

Question 6: "How much time do you spend daily on social media?"

As for distribution in terms of male/female gender, it is almost the same for this question as well. Namely, the majority of respondents (N=186; 55.9%) answered this question as follows: „$60 \leq t \leq 240$". Answers to question 6 of the questionnaire do not show any statistically significant difference between female and male respondents ($\chi^2 = 1.423$; $p = 0.700$ or $p > 0.05$).

No statistically significant difference has been identified in terms of the time spent on social media between male and female respondents ($t = 0.395$; $p = 0.693$ or $p > 0.05$). Figure 1 shows the distribution of the time spent on social media per gender. The male respondents spent on average 186.51 minutes on social media, whereas the female respondents spent on average 178.81 minutes on social media, i.e., overall, from minimum 0 minutes up to

maximum 1.080 minutes (18 hours) a day, with 120 minutes being the most frequently stated amount of time (Table 4).

By observing answers to questions 5 and 6, it may be concluded that male respondents more frequently access and spend more time on social media than female respondents.

Question 7: "On social media, I leave personal information such as: date of birth, place of birth, email address, phone, some other personal information, e.g., information about friends, segments of my CV, mother's maiden name, etc."

The distribution of answers between male and female respondents varied. Namely, the majority of respondents (N=155; 46.5%) answered to this question "Always", i.e., that they leave personal information on social media. Answers to question 7 of the questionnaire do not show any statistically significant difference between female and male respondents, if the Mann-Whitney test is used. Nevertheless, when we used a more sensitive Kruskal-Wallis test, we identified a statistically significant difference between male and female respondents in the distribution of answers to question 7 ($\chi^2 = 10.534$; $p = 0.005$ or $p < 0.01$). Below 10% of male respondents never leave their personal information on social media, whereas this is the case with slightly below ¼ of female respondents (22.7%). Therefore, we may say that in terms of statistical significance, male respondents are more likely to leave personal information on social media than female respondents (Table 5).

It is also important to conclude that leaving personal information, the pattern of behaviour on social media for the entire observed group, because statistically important is the fact that the smallest number of respondents answered that they never left personal information on social media ($\chi^2 = 50.829$; $p = 0.000$ or $p < 0.001$).

Question 8: "I post the photos of me and my family members on my social media profiles."

The distribution of answers both for male and female respondents is similar. Namely, the majority of respondents (N=155; 46.5%) answered this question as follows: "Sometimes", this response being relative to posting photos on the respondents' social media profiles.

Answers to question 8 of the questionnaire do not show any statistically significant difference between female and male respondents, either for the Mann-Whitney or the Kruskal-Wallis test ($\chi^2 = 4.082$; $p = 0.130$ or $p > 0.05$). However, Spearman's rank correlation coefficient being negative is indicative of an inverse form of the correlation relationship, i.e., that female respondents are more inclined to post photos on social media ($r = -0.101$; $p > 0.05$).

Question 9: "I comment on events posted on social media and express my opinions on matters that are posted on social media."

The distribution of answers was almost identical both for male and female respondents. Namely, the majority of respondents (N=172; 51.7%) answered this question as follows: "Never". Answers to question 9 of the questionnaire do not show any statistically significant difference between female and male respondents ($\chi^2 = 0.880$; $p = 0.644$ or $p > 0.05$). The obtained survey results show that more than ½ of male respondents and more than ½ of female respondents never comment on events that are posted on social media.

Question 10: "I always thoroughly check the profiles of persons who want to connect with me on social media."

The distribution of answers of both male and female respondents was very similar. Namely, the majority of respondents (N=204; 61.3%) answered this question as follows: "Always". Answers to question 10 of the questionnaire do not show any statistically significant difference between female and male respondents ($\chi^2 = 1.922$; $p = 0.382$ or $p > 0.05$). However, Spearman's rank correlation coefficient being negative is indicative of an inverse form of the correlation relationship, i.e., that female respondents are more inclined to check the profiles of persons who wish to connect with them on social media ($r = -0.075$; $p = 0.169$ or $p > 0.05$).

Question 11: "On social media, I never accept connections whom I do not know personally."

The distribution of answers of both male and female respondents was very similar. Namely, the majority of respondents (N=204; 61.3%) answered this question as follows: "Always". Answers to question 11 of the questionnaire do not show any statistically significant difference between female and male respondents ($\chi^2 = 2.282$; $p = 0.320$ or $p > 0.05$). Spearman's rank correlation coefficient being negative is indicative of an inverse form of the correlation relationship, i.e., that female respondents are more inclined to accept as their connections on social media only persons whom they know personally ($r = -0.005$; $p = 0.934$ or $p > 0.05$).

Question 12: "I use the same device (computer or mobile phone) for work and for accessing social media."

In this case, the distribution of answers between female and male respondents varies. The majority of respondents (N=279; 83.8%) answered this question as follows: "Always". Answers to question 12 of the questionnaire show a statistically significant difference between female and male respondents if the Mann-Whitney test is used. Furthermore, when we used a more sensitive Kruskal-Wallis test, in which a correction was made with relation to the 2×2 contingency table, a statistically significant difference in the distribution of answers to question 12 of male and female respondents was identified ($\chi^2 = 5.968$; $p = 0.015$ or $p < 0.05$).

Answers to question 12 depend on the gender, which shows the existence of a statistically significant correlation between the gender and the answers to question 12, i.e., that women are more inclined to use different devices for work and devices they use for accessing social media (Table 6). This statement is substantiated by the statistically significant correlation ($r = 0.142$; $p = 0.009$ or $p < 0.01$). It can also be concluded that the use of the same device both for work and for accessing social media is a behaviour pattern in the cyberspace which is characteristic of the entire respondent group since it is statistically significant that the majority of respondents (N=279; 83.8%) answered that they always used the same device for access purposes. However, female respondents use the same device for access purposes less frequently than male respondents, i.e., women demonstrated a higher level of caution, responsibility as a matter of fact ($\chi^2 = 152.027$; $p = 0.000$ or $p < 0.001$).

Question 13: "Are you aware that there is danger that based on personal information you leave on social media someone may find out what your password is and misuse it, or that you your personal information may be abused in some other way?

The distribution of answers was quite similar both for male and female respondents. Namely, the majority of respondents (N=325; 97.6%) answered this question as follows: "Yes". Answers to question 13 of the questionnaire do not show any statistically significant difference between female and male respondents ($\chi^2 = 0.006$; $p = 0.941$ or $p > 0.05$). The obtained survey results show that 97.3% of male respondents and 98.0% of female respondents are aware of possible data "theft" and misuse of passwords and other data. Therefore, we may reasonably say that the answer to question 13 is not conditional upon gender, which shows the absence of a statistically significant correlation between the gender and answers to question 13. However, Spearman's rank correlation coefficient being negative is indicative of an inverse form of the correlation relationship, i.e., that female respondents are still more aware of possible data "theft" and misuse of passwords and personal information ($r = -0.24$; $p = 0{,}665$ or $p > 0.05$).

Question 14: "If you are aware of possible misuse, do you still share personal information on social media?"

The distribution of answers both for male and female respondents is similar. Namely, the majority of respondents, i.e., slightly more than 2/3 answered this question as follows: "Yes". Answers to question 14 of the questionnaire do not show any statistically significant difference between female and male respondents ($\chi^2 = 2.356$; $p = 0.125$ or $p > 0.05$). The obtained survey results show that 69.9% of male respondents and 61.3% of female respondents, despite being aware of possible misuse, still "shared" their personal information on social media.

Question 15: "How 'strong' are the passwords you use?"

The distribution of answers between male and female respondents varied. Namely, male respondents (70.5%) and female respondents (70.7%), i.e., with almost identical percentage, use alphanumeric passwords always comprising 8-14 characters. Nevertheless, the difference between male and female respondents can be seen in the use of passwords comprising 14+ alphanumeric characters, which female respondents (9.3%) use less frequently than male respondents (17.5%), as well as the fact that female respondents (12%) are more cautious when it comes to password "strength" than male respondents are (5.5%) (Table 7). Answers to question 15 of the questionnaire show a statistically significant difference between female and male respondents if the Mann-Whitney test is used. Nevertheless, when we used a more sensitive Kruskal-Wallis test, we identified a statistically significant difference between male and female respondents in the distribution of answers to question 15, ($\chi^2 = 8.392$; $p = 0.039$ or $p < 0.05$). The obtained survey results show that male respondents more frequently use 14+ character alphanumeric passwords, whereas female respondents are more frequently cautious when it comes to password "strength", which is also indicative of the existence of a significant correlation between the gender and answers to question 15 ($r = 0.151$; $p = 0.0006$ or $p < 0.001$).

If the Mann-Whitney test is used, only for answers to questions 12 and 15 of the questionnaire there is a statistically significant difference between female and male respondents (Table 1). A more precise distribution of answers to all questions contained in the questionnaire, depending on the respondents' gender, was identified with the use of the contingency tables, i.e., the Kruskal-Wallis test. A statistically significant difference was identified for questions 7, 12 and 15 (Table 2). Significant values of correlations were identified for questions 7, 12 and 15 with the use of the Spearman's rank correlation test (Table 3).

DISCUSSION

Answers to question 4 indicate that there is no statistically significant difference between male and female respondents with regard to the use of the same password for every webpage and application they access. The most common answer to this question was: "There are several I change between", which is indicative of the respondent group's behaviour pattern on social media.

Answers to question 5 indicate that accessing social media more than five times a day is the respondent group's behaviour model since it is statistically significant. The smallest number of respondents answered that they never accessed social media, or that they did this once a day. Moreover, male respondents are more inclined to access social media more frequently.

Answers to question 6 indicate that time spent on social media ranges between 60 and 240 minutes. More specifically, the length of time between 60 and 180 minutes is the respondent group's behaviour model. It should be noted that the most common length of time spent on social media is 120 minutes. Young male respondents spend more time daily on social media than young female respondents.

Regarding questions 5 and 6, there is a statistically significant direct, i.e., positive correlation of time spent on social media and the number of times social media are accessed. This leads to the conclusion that those respondents who access social media more frequently as a rule spend more time there and also, though this is not statistically significant, that male respondents are more inclined to behave in this manner, i.e., to access social media more frequently and spend more time there.

Answers to question 7 indicate that leaving personal information is a behaviour pattern on social media for this observed group, because it is statistically significant that the smallest number of respondents answered that they never left personal information on social media. Such a behaviour pattern depends on the gender of respondents, or what is significant in statistical terms is that this behaviour pattern is more common among male respondents than among female ones.

Answers to question 8 indicate that leaving personal photos is behaviour pattern on social media for this observed group, and also that female respondents are more inclined to post their photos on social media.

Answers to question 9 indicate that not leaving comments on events and not expressing one's own views and opinions is a behaviour pattern on social media for this observed group, which consisted of university students. Such a behaviour pattern is prevalent in young male respondents and young female respondents alike, i.e., it is not conditional upon the gender. The results confirm an earlier survey (Necić, Milosavljević, 2022), in whose final considerations it is noted that their observed group "consider that leaving comments is important and that it has an impact. Such a position is especially common among senior population".

Answers to question 10 indicate that checking profiles of persons who want to connect with you on social media is a behaviour pattern on social media for this observed group, and also that female respondents are more inclined to check the profiles of persons they wish to accept as connections on social media.

Answers to question 11 indicate that accepting as connections on social media only persons whom you personally know, is a behaviour pattern on social media for this observed

group, and also that female respondents are more inclined to this behaviour pattern on social media.

Answers to question 12 indicate that the use of the same device (computer or mobile phone) both for work and for accessing social media is a behaviour pattern on social media for this observed group, and that, what is of statistical significance, this behaviour pattern is more common among male respondents than among female ones, and also that it is in direct correlation with the male gender.

Answers to question 13 indicate that being aware of the fact of possible data "theft" and misuse of passwords and other data on social media is a behaviour pattern which is characteristic of the entire observed survey group and also that it is predominant both among male respondents and female ones. However, female respondents are more aware of such forms of misuse on social media.

Answers to question 14 indicate that regardless of whether they are aware of the risks inherent in such a behaviour, sharing personal information on social media is a behaviour patter for the entire observed group. This behaviour pattern is not dependent upon the gender, i.e., this behaviour is characteristic of the respondents of this survey group, regardless of the gender.

Answers to question 15 indicate that the use of passwords which comprise 8-14 alphanumeric characters is a behaviour pattern of this survey group, since it is statistically significant that the majority of respondents (N=235; 70.6%) responded that they used passwords that are this "strong", and also that the "strength" of passwords used by this survey group depended on the gender, i.e., that female respondents rarely used very "strong" passwords and were in more cases less cautious.

CONCLUSION

This research has confirmed the hypothesis that among younger populations there are differences in terms of risky behaviour in the cyberspace, these differences being dependent upon the gender. In this regard, male respondents, which is statistically significant, more frequently leave personal information on social media, as compared with female respondents. It has also been noted that women more commonly post personal photos on social media. Young male respondents spend more time on social media than young female respondents.

Statistically significant is the fact that young male respondents are more inclined to use the same devices for work and entertainment purposes, compared to female respondents, i.e., that the former are less cautious than the latter. It has additionally been confirmed that there is a statistically significant correlation between the gender and the use of the same device for work purposes and for accessing social media. To confirm this statement additionally, survey results have shown that prior to "connecting", female respondent check more thoroughly the profiles of persons who wish to connect with them on social media. Female respondents are more inclined to accept to connect only with persons whom they know personally.

Although generally speaking, men tend to behave more recklessly in the cyberspace, they nevertheless use "stronger" passwords, so a statistically significant difference compared with women has been identified. They are more mindful of the content of passwords, which

confirms the existence of a statistically significant correlation between the gender and the "strength" of used passwords. Young male respondents base their cybersecurity mainly on strong access passcodes, whereas they behaviour in the very cyberspace is more relaxed and reckless than is the case with young female respondents.

With all five hypotheses being verified, conditions have been fulfilled for the verification of the general hypothesis. Namely, behaviour on social media is dependent upon the gender in certain (however not all) scenarios. By comparing the mentioned conclusions with the position of the general hypothesis: "There are similarities and differences between men and women in terms of the patterns of behaviour on social media and in the cyberspace in general", it has been concluded that it is verified.

This paper confirms that existing assumptions regarding the importance of human factor with relation to the security of end users of social media. This research has proven that in terms of the approach to digital resources, there are significant statistical differences between men and women in the observed (university student) population. For the purpose of overcoming this issue, it is advisable to develop a set of recommendations for the use of social media and mechanisms that would control the application of said recommendations. These recommendations should be developed by competent state authorities which are in charge of information technologies and e-administration, or certain state authorities (ministries, e.g. The Ministry of Public Administration and Local Self-Government, etc.). Recommendations such as 1) it is advisable to use multiple passwords for every webpage and application that is accessed, 2) one should leave minimum required personal information on social media, 3) a minimum number of one's own and one's family photos should be posted on social media, 4) profiles of persons who want to "connect" with social media users should always be thoroughly checked, 5) accept on social media as your "connections" solely persons whom you know personally, 6) always use "strong" password, etc. These recommendations should be compiled in one document in the form of guidelines or rules, which should be available on specialised online platforms (e.g., *I'm Watching over You* – the national platform for the prevention of violence, which includes children as well. Social media users would become aware of these recommendations through proper PR, i.e., media campaigns, provision of information in workplaces or education institutions).

Finally, directions of future research in this area may refer to acquiring knowledge in terms of the safe use of social media, depending on the user's age and status. As regards social media users' status, what is meant by this is their legal standing, e.g.: pupils, students, unemployed persons, employed persons, retirees, etc. With this, limitations of this research would be overcome because in this research we only looked into behaviour patterns of social media users within one segment of the university student population, depending on respondents' gender.

REFERENCES / ЛИТЕРАТУРА

Akyazi U., van Eeten M., Gañán C. H. (2021). Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum, *WEIS 2021*, June 28–29, 2021, Online Conference https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-akyazi.pdf

Avast antivirus (2022). https://support.avast.com/en-my/article/use-antivirus-password-protection/#pc

Cost of Cybercrime Study in Financial Services: Report (2019). www.slideshare.net/accenture/cost-of-cybercrime-study-in-financial-services-2019-report

Cybersecurity Threats in the Banking Sector (2021). https://www.packetlabs.net/banking-and cybersecurity/

Federal Office for Information Security, Republic of France (2021). *Fourth edition of the Franco-German Common Situational Picture.* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F_Reports/Common_Situational_Picture_2021.pdf?_blob=publicationFile&v=3

IBM (2022). *Identity and access management (IAM) solutions*, https://www.ibm.com/security/identity-access-management/privileged-access-management

IBM (2022). Security X-Force Research Hub, IBM, https://www.ibm.com/security/xforce/research-hub

IBM Security (2021). *The Cost of Insider Threats 2021*, https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

IBM (2022). *X Force Threat Intelligence Index 2022*, https://www.ibm.com/security/data-breach/threat-intelligence

IBM (2022). *Zero Trust Security Strategy*, https://www.ibm.com/security/zero-trust

Kumar, S., Somani, V. (2018). Cyber Threats and Risks Prevention and Mitigation Techniques, *IJSART - Volume 4 Issue 4* – April 2018 ISSN [online]: 2395-1052:125, www.ijsart.com

Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. (1997). *Handbook of Applied Cryptography (1st ed.)*. CRC Press. https://doi.org/10.1201/9780429466335

Necić, N., Milosavljević I. (2022). Commenting on the Internet – Attitudes and Habits of Serbian Citizens. *Sociološki pregled*, 56 (2), 559–581. DOI: 10.5937/socpreg56-36652.

Nordpass Research (2022). *Top passwords used by business executives.* https://nordpass.com/business-executive-passwords/

Samtani, S., Kantarcioglu, M., Chen, H. (2021). A Multi-Disciplinary Perspective for Conducting Artificial Intelligence-enabled Privacy Analytics: Connecting Data, *Algorithms, and Systems. ACM Trans. Manage. Manage. Syst.* 12, 1, Article 1 (March 2021), https://doi.org/10.1145/3447507

SpyCloud Report (2021). *Breach Exposure of the Fortune 1000*, https://spycloud.com/2021-report-breach-exposure-of-the-fortune-1000/#:~:text=Across%20all%20industries%2C%20nearly%2026,%25%20increase%20from%20last%20year

Trend Micro, Exploits as a Service (2021). *Cybercrime-as-a-Service Series* https://documents.trendmicro.com/assets/guides/executive-brief-exploits-as-a-service.pdf

The World Bank (2021). *World Development Report.* https://wdr2021.worldbank.org/stories/crossing-borders/#:~:text=By%202022%2C%20yearly%20total%20internet,as%20dazzling%20as%20the%20volume.

World Bank Development Report (2021). *Data for Better Lives*, https://www.worldbank.org/en/publication/wdr2021

Zoom-Security-White-Paper (2021). *Security Guide*. https://explore.zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

APPENDIX / ПРИЛОГ

Табела 1. Mann-Whitney *тест испитиване групе* /
Table 1. Mann-Whitney *test of survey respondents*

	Mann-Whitney U	*Wilcoxon W*	*Z*	*p*
Питање / Question 4	13.411,500	30.247,500	-0,423	0,672
Питање / Question 5	13.165,000	24.490,000	-0,694	0,488
Питање / Question 6	13.503,500	30.339,500	-0,282	0,778
Питање / Question 7	12.247,000	29.083,000	-1,844	0,065
Питање / Question 8	12.267,000	23.592,000	-1,842	0,066
Питање / Question 9	13.500,500	30.336,500	-0,291	0,771
Питање / Question 10	12.689,500	24.014,500	-1,376	0,169
Питање / Question 11	13.663,500	24.988,500	-0,083	0,934
Питање / Question 12	12.280,500	29.116,500	-2,588	**0,010**
Питање / Question 13	13.624,500	24.949,500	-0,434	0,665
Питање / Question 14	12.543,000	29.379,000	-1,649	0,099
Питање / Question 15	11.789,000	28.625,000	-2,758	**0,006**

НАЗАД
BACK

Табела 2. Kruskal-Wallis *тест испитиване групе* /
Table 2. Kruskal-Wallis *test of survey respondents*

	χ^2	*p*=	*p*
Питање / Question 4	0,258	0,879	p > 0,05
Питање / Question 5	4,655	0,325	p > 0,05
Питање / Question 6	1,423	0,700	p > 0,05
Питање / Question 7	**10,534**	**0,005**	**p < 0,01**
Питање / Question 8	4,082	0,130	p > 0,05
Питање / Question 9	0,880	0,644	p > 0,05
Питање / Question 10	1,922	0,382	p > 0,05
Питање / Question 11	2,282	0,320	p > 0,05
Питање / Question 12	**5,968**	**0,015**	**p < 0,05**
Питање / Question 13	0,006	0,941	p > 0,05
Питање / Question 14	2,356	0,125	p > 0,05
Питање / Question 15	**8,392**	**0,039**	**p < 0,05**

НАЗАД
BACK

Табела 3. *Спирманов тест корелације испитиване групе* / Table 3. *Spearman's rank correlation test of survey respondents*

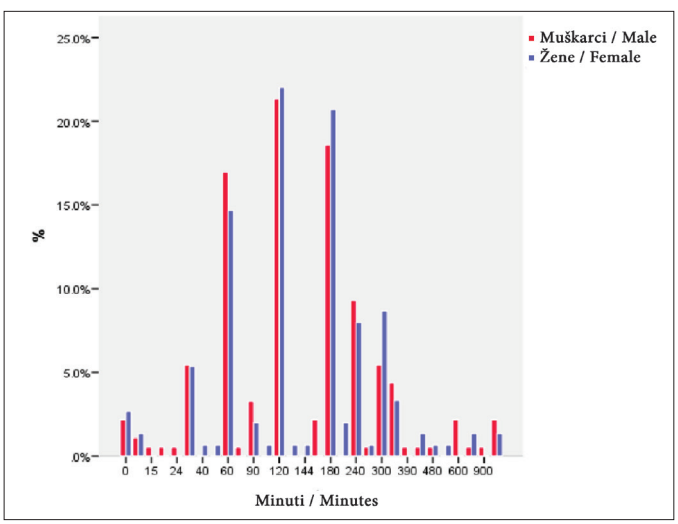
	r	*p*
Питање / Question 4	0,023	p > 0,05
Питање / Question 5	-0,038	p > 0,05
Питање / Question 6	0,016	p > 0,05
Питање / Question 7	**0,101**	**p > 0,05**
Питање / Question 8	-0,101	p > 0,05
Питање / Question 9	0,016	p > 0,05
Питање / Question 10	-0,075	p > 0,05
Питање / Question 11	-0,005	p > 0,05
Питање / Question 12	**0,142**	**p < 0,01**
Питање / Question 13	-0,024	p > 0,05
Питање / Question 14	0,090	p > 0,05
Питање / Question 15	**0,151**	**p < 0,001**

НАЗАД
BACK

Табела 4. *Преглед времена проведеног на друштвеним мрежама, по полу* / Table 4. *Distribution of time spent on social media, per gender*

Групна статистика / Cumulative statistical data			
	Пол / Gender	N	Средња вредност / Mean value
Питање / Question 6	Мушки / Male	183	186,51
	Женски / Female	150	178,81

НАЗАД
BACK



НАЗАД
BACK

Слика 1. *Хистограм дистрибуције времена које испитаници проводе на друштвеним мрежама* / Figure 1. *Histogram distribution of time that respondents spend on social media*

Табела 5. *Расподела остављања личних података на друштвеним мрежама по полу* / Table 5. *Distribution of time spent on social media per gender*

Пол / Gender * Питање / Question 7 – Унакрсна табела / Contingency table						
			Питање / Question 7			Укупно / Total
			Увек / Always	Понекад / Sometimes	Никад / Never	
Пол / Gender	Мушки / Male	Број / Count	89	76	18	183
		% пол / gender	48,6%	41,5%	**9,8%**	100,0%
		% питање / question 7	57,4%	60,3%	34,6%	55,0%
		% укупно / total	26,7%	22,8%	5,4%	55,0%
	Женски / Female	Број / Count	66	50	34	150
		% пол / gender	44,0%	33,3%	**22,7%**	100,0%
		% питање / question 7	42,6%	39,7%	65,4%	45,0%
		% укупно / total	19,8%	15,0%	10,2%	45,0%
Укупно / Total		Број / Count	155	126	52	333
		% пол / gender	46,5%	37,8%	15,6%	100,0%
		% питање / question 7	100,0%	100,0%	100,0%	100,0%
		% укупно / total	46,5%	37,8%	15,6%	100,0%

Табела 6. *Расподела употребе приступних уређаја по полу* / Table 6. *Distribution of devices used for accessing, per gender*

Пол / Gender * Питање / Question 12 – Унакрсна табела / Contingency table					
			Питање / Question 12		Укупно / Total
			Увек / Always	Никад / Never	
Пол / Gender	Мушки / Male	Број / Count	162	21	183
		% пол / gender	88,5%	11,5%	100,0%
		% питање / question 12	58,1%	38,9%	55,0%
		% укупно / total	48,6%	6,3%	55,0%
	Женски / Female	Број / Count	117	33	150
		% пол / gender	78,0%	22,0%	100,0%
		% питање / question 12	41,9%	61,1%	45,0%
		% укупно / total	35,1%	9,9%	45,0%
Укупно / Total		Број / Count	279	54	333
		% пол / gender	83,8%	16,2%	100,0%
		% питање / question 12	100,0%	100,0%	100,0%
		% укупно / total	83,8%	16,2%	100,0%

НАЗАД
BACK

Табела 7. *Расподела јачине коришћених лозинки по полу* /
Table 7. *Distribution of the strength of used passwords per gender*

Пол / Gender * Питање / Question 15 – Унакрсна табела / Contingency table							
			Питање / Question15				Укупно / Total
			Увек 14+ са БС / Always 14+ with BS	Увек 8-14 са БС / Always 8-14 with BS	Увек 8-14 без БС / Always 8-14 without BS	Не водим рачуна / I don't take care	
Пол / Gender	Мушки / Male	Број / Count	32	129	12	10	183
		% пол / gender	17,5%	70,5%	6,6%	5,5%	100,0%
		% питање / question 15	69,6%	54,9%	50,0%	35,7%	55,0%
		% укупно / total	9,6%	38,7%	3,6%	3,0%	55,0%
	Женски / Female	Број / Count	14	106	12	18	150
		% пол / gender	9,3%	70,7%	8,0%	12,0%	100,0%
		% питање / question 15	30,4%	45,1%	50,0%	64,3%	45,0%
		% укупно / total	4,2%	31,8%	3,6%	5,4%	45,0%
Укупно / Total		Број / Count	46	235	24	28	333
		% пол / gender	13,8%	70,6%	7,2%	8,4%	100,0%
		% питање / question 15	100,0%	100,0%	100,0%	100,0%	100,0%
		% укупно / total	13,8%	70,6%	7,2%	8,4%	100,0%

НАЗАД
ВАСК