Sigurnost društvenih mreža i zaštita osobnih podataka

Beriša, Janet

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Diplomski sveučilišni studij

Janet Beriša

Sigurnost društvenih mreža i zaštita osobnih podataka

Social media security and personal data protection

Diplomski rad

Opatija, 2023.

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Diplomski sveučilišni studij
Marketing u turizmu

Sigurnost društvenih mreža i zaštita osobnih podataka

Social media security and personal data protection

Diplomski rad

Kolegij:	**Inovativne tehnologije**	Student:	**Janet Beriša**
Mentor:	Izv. prof. dr. sc. **Ljubica Pilepić Stifanich**	Matični broj:	**ds3708/22**

Opatija, kolovoz 2023.

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG DIPLOMSKOG RADA

Janet Beriša	**Ds3708**
(ime i prezime studenta)	(matični broj studenta)

Sigurnost društvenih mreža i zaštita osobnih podataka
(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor diplomskog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa diplomskim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog diplomskog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/liceses/.

U Opatiji, kolovoz, 2023.

Janet Beriša
Potpis studenta

Sažetak

Ovaj diplomski rad temelji se na istraživanju sigurnosti i zaštite podataka na društvenim mrežama. Fokus istraživanja proširuje se na raznoliko područje društvenih mreža, uključujući poznate platforme poput Facebooka, Twittera, Instagrama, LinkedIna, TikToka i drugih. Svaka od ovih platformi nudi specifične karakteristike i funkcionalnosti koje će biti detaljno analizirane u radu. Također, rad se bavi pojašnjenjem ključnih pojmova kao što su Malware, Phishing i Ransomware, koji predstavljaju prijetnje korisnicima interneta. Ovi napadi ciljaju kako pojedince, tako i organizacije, iskorištavajući ranjivosti digitalnog okoliša, što često dovodi do ozbiljnih posljedica kao što su gubitak podataka, financijske štete i ugrožena privatnost. Primarni cilj istraživanja jest pažljivo analizirati aspekte sigurnosti i privatnosti koji se odnose na osobne podatke korisnika unutar društvenih mreža. Kroz korištenje empirijskog istraživačkog pristupa te metode anketiranja provedene na uzorku od 104 ispitanika, istraživanje nastoji razotkriti različite perspektive i stavove o sigurnosnim mjerama društvenih mreža te praksama ponašanja prema osobnim podacima korisnika. Rezultati ovog istraživanja ukazuju na visoku razinu osjetljivosti i izloženosti podataka na društvenim mrežama, ističući nužnost unaprjeđenja sigurnosnih aspekata. Posebno se naglašava važnost edukacije kao ključnog faktora u podizanju razine sigurnosti pri korištenju društvenih mreža.

Ključne riječi: Internet; društvene mreže; sigurnost podataka.

Sadržaj

UVOD 1

1. DRUŠTVENE MREŽE 4

1.1. Povijest društvenih mreža 5

1.2. Svrha i razvoj društvenih mreža 7

1.3. Usporedba društvenih mreža 10

1.3.1. Meta 12

1.3.2. Twitter 13

1.3.3. Tik Tok 15

1.3.4. Youtube 17

2. RIZIK I OPASNOST DRUŠTVENIH MREŽA 19

2.1. Malware 20

2.2. Ransomware 22

2.3. Phishing 24

2.4. Najveći napadi i krađe podataka 25

3. SIGURNOST I ZAŠTITA OSOBNIH PODATAKA 27

3.1. Obrada osobnih podataka 28

3.2. Zloupotreba privatnih informacija 31

4. PREGLED DOSADAŠNJIH ISTRAŽIVANJA 33

5. ISTRAŽIVANJE STAVOVA ISPITANIKA O SIGURNOSTI DRUŠTVENIH MREŽA 36

5.1. Sadržaj i ciljevi istraživanja 36

5.2. Metodologija 37

5.3. Analiza rezultata 39

5.4. Rasprava 51

5.5. Ograničenja i preporuka za buduća istraživanja 53

ZAKLJUČAK 54

BIBLIOGRAFIJA 56

POPIS ILUSTRACIJA 61

ANKETNI UPITNIK 62

Uvod

Društvene mreže su postale nezaobilazni dio našeg svakodnevnog života. Korištenje društvenih mreža promijenilo je naš način komunikacije, druženja, dijeljenja informacija i podataka. Postoji više različitih društvenih mreža, poput Facebooka, Twittera, Instagrama, LinkedIna, TikToka i mnogih drugih, a svaka od njih ima svoje jedinstvene značajke i funkcionalnosti.

Društvene mreže su nastale kao platforme za druženje i povezivanje ljudi, no s vremenom su postale i ključni alat za marketinške kampanje, istraživanja tržišta, razmjenu informacija i stvaranje zajednica oko zajedničkih interesa. Na društvenim mrežama korisnici stvaraju profile kroz koje mogu dijeliti svoje misli, fotografije i videozapise, razgovarati s ostalim korisnicima, održavati odnose s prijateljima i obitelji te upoznavati nove ljude. Također, na društvenim mrežama korisnici mogu konzumirati sadržaj koji su na njima objavili drugi, kako privatni, tako i korporativni profili. Sadržaj koji se konzumira na društvenim mrežama često utječe na ponašanje korisnika, među ostalim na njihove odluke u vezi kupovine i trošenja novca.

Paralelno s porastom intenziteta korištenja društvenih mreža, rasla je i zabrinutost za zaštitu osobnih podataka korisnika i općenito sigurnosti društvenih mreža. Zbog toga je izrazito važno da korisnici budu svjesni u kojoj mjeri postoji sigurnosni rizik na društvenim mrežama i pronađu način na koji će primijeniti odgovarajuće mjere opreza kako bi zaštitili svoju privatnost i sigurnost.

Predmet diplomskog rada je istraživanje stanja sigurnosti na društvenim mrežama te načina zaštite osobnih podataka korisnika kroz pravnu regulativu. Shodno predmetu rada, osnovni ciljevi istraživanja su sljedeći:

- Identificirati vrste sigurnosnih prijetnji i napada na društvenim mrežama;
- Istražiti stavove korisnika društvenih mreža o percipiranoj sigurnosti;
- Istražiti stavove korisnika društvenih mreža o dijeljenju podataka:
- Istražiti stavove korisnika društvenih mreža o potrebi za edukacijom o sigurnosti.

Temeljem navedenih ciljeva formulirana su sljedeća istraživačka pitanja:

IP1: Koje su najčešće vrste prijetnji i napada na društvenim mrežama?

IP2: Kakvi su stavovi korisnika društvenih mreža o sigurnosti?

IP3: Kakvi su stavovi korisnika društvenih mreža o dijeljenju podataka?

IP4: Kakvi su stavovi korisnika društvenih mreža o potrebi za edukacijom o sigurnosti?

Svrha istraživanja je ustanoviti u kojoj mjeri korisnici vjeruju društvenim mrežama i osjećaju li se sigurno dijeliti svoje osobne podatke putem interneta.

Struktura rada se, osim uvoda i zaključka, sastoji od pet poglavlja, od kojih svaki doprinosi boljem razumijevanju društvenih mreža i problema sigurnosti osobnih podataka.

U uvodnom dijelu rada iznosi se problem i predmet istraživanja, navode se ciljevi i istraživačka pitanja te ukratko opisuje struktura rada.

U prvom poglavlju provodi se istraživanje povijesti, svrhe i evolucije društvenih mreža. Najpoznatije i najutjecajnije platforme za društveno umrežavanje, kao što su Facebook, Twitter, Instagram, LinkedIn, TikTok, između ostalih, navedene su i analizirane. Ovaj povijesni segment postavlja okvir za razumijevanje dubokog utjecaja koje ove platforme imaju na modernu komunikaciju, društvenu interakciju i širenje informacija.

Prelaskom na drugi dio, fokus se pomiče na kritičnu temu rizika i opasnosti ugrađenih u područje društvenih mreža. U ovoj kritičkoj analizi, rad naglašava neke od najopasnijih prijetnji sigurnosti koje se mogu pojaviti u kontekstu ovih platformi. Objašnjene su zlonamjerne sile krađe identiteta, ransomware-a i zlonamjernog softvera koji iskorištavaju ranjivosti unutar društvenih mreža. Nadalje, poglavlje identificira slučajeve poznatih napada i povreda podataka koji su obilježili online okruženje. Poglavlje ne naglašava samo veličinu ovih prijetnji, već također naglašava važnost snažnih sigurnosnih mjera.

Treće poglavlje bavi se složenim postupcima obrade osobnih podataka i potencijalne zlouporabe osobnih podataka korisnika. Budući da privatnost korisnika zauzima središnje mjesto u digitalnom dobu, ovo poglavlje pruža pojašnjenje načina na koje se postupa s osobnim podacima u kontekstu društvenih mreža. Također, dotiče se zakonodavnog okvira koji oblikuje zaštitu podataka. Uvrštavanje relevantnih zakona i propisa u ovu raspravu naglašava ozbiljnost problema i mjere koje se primjenjuju za zaštitu podataka o korisnicima.

Četvrto poglavlje navodi prethodna istraživanja povezanih radova te se iznose zaključci, rezultati i način na koji su istraživanja provedena.

Peti dio rada spaja teoriju i praksu kroz prikaz rezultata provedenog istraživanja. Prikupljeni podaci daju uvid u kompleksne osjećaje i stavove koje pojedinci imaju prema društvenim mrežama te ukazuju na način na koji se ti osjećaji i stavovi isprepliću s njihovim razumijevanjem digitalne sigurnosti.

U zaključku se opisuju razmatranja cjelokupnog istraživanja i odgovara se na istraživačka pitanja.

Ovaj rad predstavlja sveobuhvatan mozaik povijesti, rizika, kompleksnosti podataka i korisničkih percepcija koje zajedno definiraju suvremeni pregled društvenog umrežavanja. Ovo istraživanje služi kao podloga za korisnike i istraživače kojima je pružena detaljna analiza spoja tehnologije, privatnosti i ljudske interakcije

1. Društvene mreže

Od skromnih početaka sa SixDegrees.com, preko Friendstera, i MySpacea pa sve do i Facebooka i Twittera i svih onih koje su se u međuvremenu pojavile i nestajale sa globalne komunikacijske scene i društvenog prostora, društvene mreže postale su globalni komunikacijski fenomen.[1] Od 1967. godine, društvene mreže postale su jedno od istraživačkih područja u kojem znanstvenici iz različita disciplina traže inspiraciju.[2]

U današnje doba život bez društvenih mreža je gotovo nezamisliv. Pomalo je zastrašujuće u kojoj smo se mjeri naviknuli da u svakom trenutku budemo povezani s drugima preko društvenih mreža, kako direktnom komunikacijom, tako konzumiranjem objavljenog. Neki se oslanjaju na društvene mreže čak i za obavljanje posla - rastom društvenih mreža došlo je do stvaranja novih radnih mjesta. Pojam „influencer“, koji označava osobu koja sadržajem koji objavljuje na društvenim mrežama utječe na stavove i ponašanja ostalih korisnika, postao je uobičajen u zadnjih par godina. Osobito tijekom Covid pandemije porastao je broj influencera diljem svijeta.

Ono što društvene mreže čini jedinstvenima nije to što dopuštaju pojedincima da se upoznaju i druže za strancima, već to što korisnicima omogućuju da budu povezani sa određenim temama, interesima, aktualnim događanjima te da, ukoliko to žele, podjele svoja mišljenja te dijelove svojeg života. To može rezultirati vezama između pojedinaca kojih inače ne bi bilo, bržim povezivanjem korisnika koji djele zajedničke interese, lakšim pronalaženjem određenih proizvoda te bržim povezivanja kolega u svrhu poslovnih odabira.

Način na koji ljudi komuniciraju promijenio se kao rezultat društvenih medija. Više društvenih interakcija i poslovnih operacija odvija se online. Ali, kako se te tehnologije

[1] Grbavac, J. i Grbavac, V. (2014). Pojava društvenih mreža kao globalnog komunikacijskog fenomena., Media, culture and public relations, 5 (2), str. 206.
[2] Musiał, K., & Kazienko, P. (2012). Social networks on the Internet. World Wide Web, str. 42.

razvijaju, pojedinci su izloženiji riziku od invazije na privatnost. Za sigurnost korisnika potrebni su regulatorni okviri i zakonodavni instrumenti koji još uvijek nemaju snažnu online prisutnost.

Ovaj rad bavi se istraživanjem dubokog utjecaja platformi društvenih medija na naše svakodnevne živote te načinom na koji su one informirale našu komunikaciju, interakciju i dijeljenje informacija.

1.1. Povijest društvenih mreža

Prva prepoznatljiva društvena mreža pokrenuta 1997. godine kada je *SixDegrees.com* svojim korisnicima omogućio stvaranje profila, popis svojih prijatelja te, počevši od 1998. godine, surfanje listama prijatelja.[3] Svaka od ovih značajki postojala je u nekom obliku prije SixDegreesa. Profili su postojali na većini glavnih stranica za upoznavanje i mnogim stranicama zajednice.

Classmates.com omogućio je ljudima da se povežu sa svojom srednjom školom ili fakultetom, ali korisnici nisu mogli stvarati profile ili popisati prijatelje sve godinama kasnije. SixDegrees bio je prvi koji je kombinirao te značajke, no kasnije, 1999. godine, kupljen je od strane YouthStream Media Networks za 125 milijuna dolara.

Friendster je društvena mreža koju je 2002. godine osnovao bivši zaposlenik Netscapea Jonathan Abrams. Stranica je dizajnirana tako da korisnicima omogućuje kreiranje profila koji sadrže osobne podatke i nudi mogućnost povezivanja s prijateljima s kojima nije tako lako stupiti u kontakt.

Jorn Barger izumio je pojam "weblog" 1997. Web-log je u biti web-stranica koja 'bilježi' hiperveze na web-mjesta koja su web-surferu zanimljiva. Pojam weblog kasnije je skraćen u "blog".[4] Prva stranica za objavljivanje blogova bila je „LiveJournal“ 1999. godine. To se

[3] Boyd, D. M., Ellison, N. B. (2007). Social Network Sites: Definition, History and Scholarship, Journal of Computer-Mediated Communication, 13(1), str 214.
[4] Merholz, P. (2002). Play with your words., peterme.com, http://www.peterme.com/archives/00000205.html.

poklopilo s lansiranjem druge platforme za objavljivanje blogova „Blogger“ od strane tehnološke tvrtke Pyra Labs, koju je Google kasnije kupio 2003. godine.

LinkedIn je 2002. godine osnovan kao mrežno mjesto za profesionalce orijentirane na karijeru. I dalje je popularan među tražiteljima posla, kao i za menadžere ljudskih potencijala koji traže kvalificirane kandidate. Druga dva velika pohoda na društvene medije propala su nakon niza početnih uspjeha.

MySpace je stranica za društveno umrežavanje osnovana 2003. Glazba je od početka bila središnja komponenta ove stranice koja je nekoć bila najpopularnija stranica te vrste, no nakon raznih debakla srušili su je novi online konkurenti, poput Facebooka.[5] Godine 2011. Myspace je kupio glazbenik Justin Timberlake za 35 milijuna dolara, ali nije uspio doseći ni približnu popularnost Instagram.

Reddit je pokrenut 2005. godine od strane 20-godišnjaka iz Massachusettsa, Steve Huffmana i Alexis Ohaniana, kao platforma za dijeljenje vijesti. Njezinih 300 milijuna korisnika transformiralo je Reddit u jednu od najaktivnijih platformi za prikupljanje vijesti i društvenih komentara. Redditova popularnost temelji se na mogućnosti "glasanja za" i "glasanja protiv" korisničkih objava.

Twitter su 2026 osnovali Jack Dorsey, Evan Williams, Biz Stone i drugi kao stranicu za mikroblogiranje, a do 2020. godine, 22% odraslih Amerikanaca bili su korisnici Twittera, prema Pew Researchu.[6]

Mark Zuckerberg, tada student na Harvardu, odlučio je osnovati online stranicu na kojoj će samo studenti Harvardskog sveučilišta biti u mogućnosti međusobno komunicirati te dijeliti informacije. Vrlo brzo, doduše, broj korisnika je porastao te je došlo do početka Facebook-a 2008. godine.

Osnovan 2010. godine od strane diplomanta Stanforda Kevina Systroma kao mjesto za dijeljenje fotografija, Instagram ima više od milijardu korisnika diljem svijeta. Kupio ga je Facebook 2012. godine.

[5] Danowitz, E. S. (2018). The SAGE International Encyclopedia of Travel and Tourism, Reference Reviews, 32(3), str. 29.
[6] Twitter Revenue and Usage Statistics (2023) - *Business of Apps*

Ekspanzijom interneta i sve većom popularnošću društvenog i kolaborativnog računalstva, koje se od nedavno obično naziva društveno računalstvo, društvene mreže su se pojavile kao značajno i obećavajuće područje studija unutar računalnih znanosti. Društveno računalstvo uključuje takve aktivnosti kao što su prikupljanje, izdvajanje, pristup, obrada, računanje i vizualizacija svih vrsta društvenih informacija.

Glavni cilj društvenih mreža je stvaranje, održavanje i predstavljanje društvenih odnosa svojim korisnicima, kao i međusobno povezivanje istih. Kako bi postigli te ciljeve, potrebno je uvesti neke dodatne komunikacijske usluge kao što su e-pošta, chatovi, instant slanje poruka. Glavne značajke društvenih mreža su: samoizražavanje (održavanje osobnih profila), uključujući predstavljanje osobnih postignuća, uspostavljanje odnosa s drugima i međusobnu komunikaciju. Načini komunikacije između korisnika unutar ovih mrežnih mrežnih stranica razlikuju se ovisno o funkcionalnosti portala: e-pošta, chat, forum, blog, komentari, svjedočanstva, album fotografija/filmova itd. Sve u svemu, što je više komunikacijskih kanala na mreži, to bolje, jer pruža veću priliku za stvaranje novih i održavanje postojećih odnosa unutar sustava.[7]

Društvene mreže promijenile su način na koji ljudi komuniciraju. Poslovni procesi i društvene interakcije sve se više odvijaju u kibernetičkom prostoru. Međutim, kako cyber tehnologije napreduju, korisnici postaju izloženiji prijetnjama privatnosti. Regulatorni i pravni okviri potrebni su instrumenti kojima trenutno nedostaje snažna kibernetička prisutnost radi zaštite korisnika.

1.2. Svrha i razvoj društvenih mreža

U početku su društveni mediji postojali kako bi pomogli krajnjim korisnicima da se digitalno povežu s prijateljima, kolegama, članovima obitelji i istomišljenicima koje možda nikad nisu

[7] Musiał, K., & Kazienko, P. (2012). Social networks on the Internet, World Wide Web, str. 59.

osobno sreli. Pristup uslugama oglasne ploče s računala olakšao je razvoj besplatnih online zajednica bez napuštanja kuće uz minimalan trošak oglašavanja i marketinških kampanja.

Sadržaj Weba 2.0 većinom stvaraju korisnici, a vlasnici i operateri stranica nisu u potpunosti uključeni kontrolu nad sadržajem koji prikazuju njihove stranice.[8] Nažalost, korisnik generirani sadržaj može koristiti na načine za koje nije izvorno namijenjen. Važno je imati na umu kako društveni mediji stvaraju mnogo osobnih informacija na pojedinačnim profilima.

Izum pametnog telefona oslobodio je društvene medije stolnih i prijenosnih računala. Appleov prvi iPhone, koji je pokrenuo Steve Jobs 2007., pomogao je prebaciti fokus izgradnje online zajednice na mobilni uređaj. Facebook, Twitter, Snapchat, Instagram, TikTok i druge usluge društvenih medija napredovale su u okruženju mobilnih aplikacija.

Web 2.0 je evolucija weba prema većoj jednostavnosti (ne zahtijeva nikakvo tehničko znanje ili računalo za korisnike) i interaktivnosti (omogućuje svima, pojedinačno ili kolektivno, da doprinose, dijele i surađuju u različitim oblicima).[9] Pojava Weba 2.0 pridonijela je transformaciji prosječnog korisnika iz pasivnog čitatelja u kreatora sadržaja. Korisnici sada mogu komunicirati s drugima ljudima, stvarati, redistribuirati ili razmjenjivati informacije i mišljenja te izražava sebe u virtualnim zajednicama.[10]

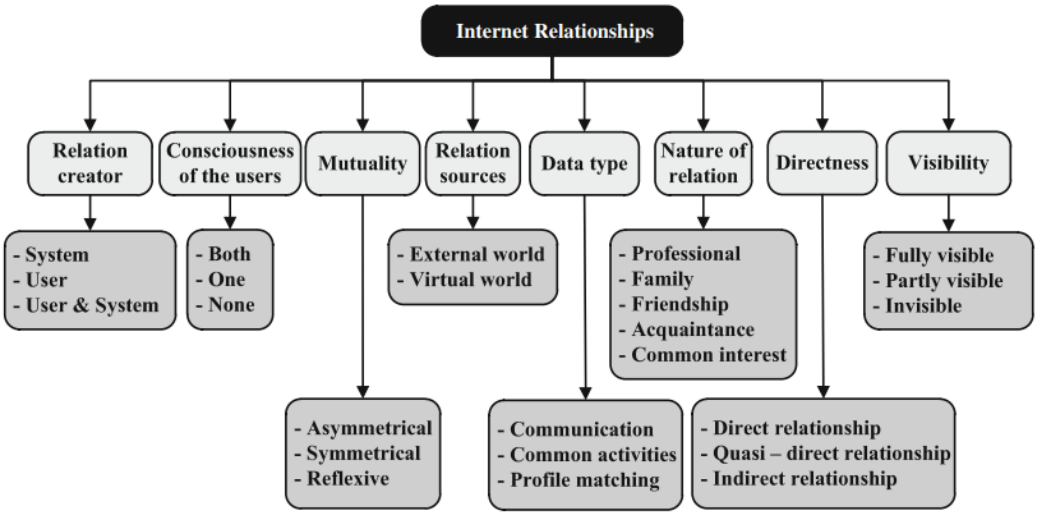
Društvene mreže također pružaju bogate izvore prirodnih podataka o ponašanju. Podaci profila s društvenih mreža mogu se prikupiti korištenjem automatiziranih tehnika prikupljanja ili putem skupova podataka kojima raspolaže vlasnička tvrtka, omogućavanjem istraživanja mrežne analize obrasca prijateljstva, korištenja i drugih vidljivih pokazatelja, te nastavakom analize trenda koji je započeo ispitivanjem blogova i drugih web stranica.[11] Kako su ove mreže evoluirale iz društvenih alata u oruđe za ključne marketinške kampanje, razmjenu informacija i središte zajedničkih interesa, fokus je sada usmjeren na zaštitu privatnosti i podataka korisnika.

[8] Mansfield-Devine, S. (2008). Anti-social networking: Exploiting the trusting environment of Web 2.0, Network Security 11, str. 2.
[9] Sfetcu, N. (2014). Small Business Management for Online Business – Web Development, Internet Marketing, Social Networks, str. 2.
[10] Podobnik, Vedran i drugi. (2013). Web 2.0 as a Foundation for Social Media Marketing: Global Perspectives and the Local Case of Croatia. Str. 1.
[11] Boyd, D. M., Ellison, N. B. (2007). Social Network Sites: Definition, History and Scholarship, Journal of Computer-Mediated Communication, 13(1), str. 220.

Vrste internetskih odnosa mogu se klasificirati na mnogo različitih načina i temeljiti se na različitim karakteristikama:

1. Aktivni subjekt koji je odgovoran za stvaranje novih odnosa (korisnik, sustav, korisnik i sustav)
2. Svijest korisnika da su uključeni u odnose i uzajamnost povezanosti između korisnika (asimetrična, simetrična, refleksivna) te opći izvori odnosa (vanjski ili virtualni svijet)
3. Vrsta podataka koji sustav koristi za stvaranje odnosa (izravna interakcija, zajednička aktivnost, korisnički profili, bez korištenja podataka ako je odnos kreirao korisnik),
4. Priroda odnosa (profesionalni, obiteljski, prijateljski, poznanstvo, zajednički interes, itd.),
5. Vidljivost odnosa za korisnike (potpuno ili djelomično vidljivi, nevidljivi).
6. Izravnost temelja odnosa (izravno, kvazi izravno, neizravno).

Slika 1. Taksonomija internetskih odnosa



Izvor: Musiał, K., & Kazienko, P. (2012). Social networks on the Internet, World Wide Web, 16(1), str. 47.

1.3. Usporedba društvenih mreža

Mnogi ljudi misle kako su sve društvene mreže jednake, ali nisu. Sve oni imaju svoju specifičnu svrhu i ulogu u društvenom umrežavanju. Razumijevanje njihove svrhe i za što koristiti svaki kanal omogućuje bolje poslovno korištenje kroz razumijevanje koja će društvena mreža najbolje funkcionirati za interakciju s klijentima.[12] Brz razvoj brzih internetskih veza uzrokovao je to da se online mogu jednostavno prenijeti ne samo tekstualne poruke, nego i glasovni i video zapisi.

Jedna od klasifikacija društvenih mreža može se napraviti prema vrsti pristupa društvenoj mreži. Mreže mogu imati otvorene, tj. imati javni ili ograničeni pristup. Otvorenim mrežama svatko se može pridružiti, i tu su najpoznatije mreže kao Facebook, MySpace, ICQ itd. dok se u mrežama s ograničenim pristupom može pristupiti jedino uz pozivnicu nekoga tko je već član, kao npr. Raya. Neke mreže s ograničenim pristupom ograničene su samo na ljude koji pripadaju određenoj skupini ili tvrtki.

Istraživanje provedeno 2020. godine tvrdi kako više od 3.96 milijardi korisnika provodi aktivno vrijeme na društvenim mrežama. To u teoriji znači da svaki drugi stanovnik na planeti ima otvoren račun na društvenoj mreži. Zanimljivost je da 99% korisnika pristupa društvenim mrežama s mobilnog uređaja. Najviše korisnika ima Facebook i to čak 2.6 milijardi, dok Youtube i Whatsapp dijele drugo mjesto s 2 milijarde korisnika. Instagram je na 6. mjestu dok je Tik Tok odmah iza njega. Američki portal TechCrunch iznio je podatke o najpopularnijim aplikacijama u prošloj godini, a na prvo je mjesto ponovno zasjeo Tik Tok s ukupno 672 milijuna preuzimanja dok ga prati Instagram s 548 milijuna preuzimanja.[13]

Vodeće trgovine mobilnih aplikacija su Google Play i Apple Store. Google Play zauzima prvo mjesto i to za jedan milijun više preuzimanja. Najčešća kategorija preuzimanja aplikacije na obje platforme su mobilne igre. Dok je na Google Playu druga kategorija edukacija, na Apple

[12] Petrauskas, K. (2019). What Are The Differences Between Social Media Platforms, KJP Creative, https://kjpcreative.com/what-are-the-differences-between-the-big-social-media-platforms/

[13] Mujanović, A. (2023). *TikTok u 2022. ostvario najviše preuzimanja, Metine platforme zauzele čak tri mjesta među top 10.*

Storeu su to poslovne aplikacije. Prema statističkim podacima, prosječno vrijeme provedeno na mobilnom uređaju diljem svijeta iznosi 2 sata i 55 minuta.

S porastom društvenih mreža nastupila je nova era stvaranja sadržaja kojima pojedinci mogu lako razmjenjivati iskustva i informacije s drugim korisnicima.[14] Ono što je započelo kao iskustvo stolnog ili prijenosnog računala prešlo je na mobilne telefone i tablete kako su se mobilne usluge širile. Proširile su se mogućnosti mobilnih telefona, pretvarajući ih u "pametne telefone“, a brzi, bežični internet postao je lakše dostupan u domovima, tvrtkama i javnim prostorima.

S pojavom aplikacija za društvene medije koje se mogu pokretati na pametnim telefonima, krajnji korisnici mogu povesti svoje zajednice sa sobom kamo god krenu. Tvrtke su iskoristile ovu novu mobilnost potrošača služeći svojim kupcima nove, jednostavnije metode interakcije i nove načine kupnje dobara i usluga.

Facebook je počeo postavljati oglase na svoju platformu još 2006, dok je Twitter omogućio oglase 2010. godine. LinkedIn, Instagram, Pinterest, Snapchat i Tik Tok su svi pokušali unovčiti svoje usluge kroz razne oblike sponzoriranog oglašavanja. Osim postavljanja oglasa na platforme društvenih medija, tvrtke su otkrile potencijalnu korisnost njegovanja aktivne, angažirane prisutnosti na društvenim medijima.

Dok se oglašavanje na društvenim mrežama mora platiti, čin stvaranja i dijeljenja informativnog ili zabavnog sadržaja na Facebooku, Instagramu, Twitteru i drugim platformama pokušaj je brendova da organski povećaju publiku, drugim riječima, bez izravnog plaćanja. Društvene mreže su sada mjesto za razmjenu informacija i stjecanje znanja o proizvodima i uslugama.[15]

[14] Chen, J., Xu, H. & Whinston, A.B. (2011). Moderated online communities and quality of user-generated content, Journal of Management Information Systems, 28(2), str. 238.

[15] Chen, J., Xu, H. & Whinston, A.B. (2011). Moderated online communities and quality of user-generated content, Journal of Management Information System, 28(2), str. 237.

1.3.1. Meta

Meta je tvrtka koja je osnovana 2004. godine pod imenom Facebook, a nedavno je promijenila ime u Meta kako bi odrazila svoju viziju fokusiranu na virtualnu i proširenu stvarnost.

Tvrtka upravlja s nekoliko popularnih društvenih mreža, uključujući Facebook, Instagram i WhatsApp. Prilikom stvaranja profila na Facebooku, Instagramu i WhatsAppu, korisnici se moraju pridržavati određenih pravila. Na primjer, korisnici ne smiju stvarati lažne profile ili koristiti tuđe identitete, ne smiju objavljivati sadržaj koji krši autorska prava ili koji je uvredljiv prema drugim korisnicima. Također, korisnici moraju pažljivo upravljati svojim osobnim podacima i biti svjesni mogućnosti krađe podataka. Postotak krađe podataka na društvenim mrežama prilično je visok, pogotovo ako korisnici ne prate svoje sigurnosne postavke ili ako ne znaju prepoznati i izbjeći prijevare.

U ovakvim situacijama najčešće nastradaju starije populacije koje dolaze na internet s velikim povjerenjem i ne znaju prepoznati sumnjive aktivnosti. Ukradeni podaci mogu biti zlouporabljeni u razne svrhe, poput krađe identiteta ili Phishing napada. Phishing napad je pokušaj prevare nekoga da putem interneta ili putem e-pošte oda podatke koji bi omogućili nekom drugom da od njega uzme novac, na primjer skidanjem novca s njegovog bankovnog računa.[16]

Studija otkriva kao se korisnici ne odlučuju uvijek postaviti svoje profile kao privatne kada se prvi put registriraju na Facebooku. To je zato što korisnici nisu dovoljno upućeni u mogućnosti profilnih postavki, a također postoji nedostatak svijesti o važnosti takve zaštite. Većina korisničkih podataka djelomično je dostupna na korisničkim profilima, a to je idealna situacija koju kriminalni elementi mogu iskoristiti. Bilo tko maskiran kao jedan od korisnikovih prijatelja može pristupiti ovim osjetljivim informacijama prijavom i pretraživanjem tih podataka.[17]

[16] Phishing (2023). PHISHING | English Meaning – Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/phishing.

[17] Nyoni, P., & Velempini, M. (2015). Data protection laws and privacy on Facebook, SA Journal of Information Management, 17(1). Str. 8.

Instagram je aplikacija popularna među korisnicima društvenih medija koje zanimaju putovanja, zabava, moda i druge vizualno orijentirane teme. Iako je platforma popularna diljem svijeta, Instagram se nedavno pronašao u središtu jednog od najvećih skandala vezanih uz krađu podataka korisnika. U svibnju 2021. godine, izvješće The Guardiana otkrilo je da tvrtka koja je zadužena za prikupljanje podataka iz Mumbaija, Chtrbox, prikupila i izložila podatke korisnika Instagrama.[18] Ti podaci su uključivali privatne poruke, lozinke i druge osjetljive informacije. Podaci korisnika bili su izloženi u nezaštićenoj bazi podataka, što je rezultiralo time da su podaci milijuna korisnika postali meta za krađu identiteta i ostale vrste cyber napada.

Kada se prijavi kršenje tuđih podataka na Instagramu, platforma poduzima određene mjere kako bi zaštitila privatnost korisnika. Instagram ima opcije za prijavu prijevara i kršenje pravila u bilo kojem obliku: neprimjereno ponašanje, novčane prijevare, kršenje autorskih prava itd.

Facebookova matična tvrtka, Meta, pogođena je velikom kaznom od 265 milijuna eura (277 milijuna dolara) od strane Irske komisije za zaštitu podataka (DPC), vodećeg regulatora tehnološkog diva za Opću uredbu o zaštiti podataka Europske unije (GDPR).[19] Meta je kažnjena jer nije uspjela zaustaviti širenje osjetljivih informacija milijuna korisnika Facebooka. U to je vrijeme Meta pokušala umanjiti značaj incidenta tvrdeći da su otkrivene informacije zastarjele i da su ih vjerojatno dobili "zlonamjerni akteri" koristeći značajku uvoznika kontakata koju je pružala do rujna 2019., prije nego što je uvrstila promjene kako bi spriječila zlouporabu podataka.[20]

1.3.2. Twitter

Najpoznatija platforma društvene mreže za mikroblogiranje je Twitter. Posebnost Twittera je što korisnik može slijediti bilo koji profil bez dopuštenja drugog korisnika. Biti pratitelj na Twitteru znači da korisnik prima sve poruke zvane „tweetovi“ od korisnika koje prati.

---

[18] Milmo, D. (2021). *Facebook and Instagram gathering browsing data from under-18s, study says. The Guardian.*

[19] Eberechukwu, E. (2022). Meta fined €265 million over Facebook data breach and scraping, Technex https://technext24.com/2022/11/28/meta-fined-e265-million-over-facebook-data/

[20] Eberechukwu, E. (2022). Meta fined €265 million over Facebook data breach and scraping, Technex https://technext24.com/2022/11/28/meta-fined-e265-million-over-facebook-data/

Twitter je široko korišten besplatni alat za društveno umrežavanje koji ljudima omogućuje razmjenu informacija u stvarnom vremenu putem objavljivanja kratkih poruka o svojim iskustvima i razmišljanjima.[21] „Tweetovi“ su ograničeni na najviše 140 znakova i mogu sadržavati poveznice na blogove, web stranice, slike, videozapise i sve druge materijale na mreži.[22] Osnovan je 2006. godine, a danas ima preko 300 milijuna aktivnih korisnika. Korisnici prate aktualne teme te su u toku s događanjima, a Twitter im je savršena platforma za dijeljenje svojeg mišljenja i ideja s drugima.

Prilikom registracije na Twitter račun, korisnici moraju pružiti osnovne osobne podatke, uključujući svoje ime, e-mail adresu i lozinku. Uz te podatke, Twitter može prikupiti i druge informacije o korisnicima, poput informacija o njihovim interesima koja su popratili i aktivnostima na platformi.

Jedan od najvećih Twitterovih skandala dogodio se 2018. godine kada su se pojavile tvrdnje da je tvrtka Cambridge Analytica (koja je također bila uključena u skandal vezan uz Facebook) koristila podatke korisnika Twittera kako bi izravno utjecala na američke izbore 2016. godine. Kao rezultat, ljudi su postali svjesni da su osobni podaci 87 milijuna korisnika Facebooka bili izloženi bez njihovog pristanka i da ih je Cambridge Analytica koristila za podršku političkim kampanjama. Tisuće ljudi iz različitih dijelova svijeta izrazilo je na društvenim medijima svoje reakcije i razmišljanja o skandalu, odnos prema privatnosti podataka i njegove šire implikacije.[23]

Osim podataka koji otkrivaju identitet, dijeljenje drugih vrsta osobnih podataka na Twitteru može dovesti ljude u opasnost da ih se iskoristi. Primjerice, u lipnju 2009. Izrael Hyman, videopodcaster sa sjedištem u Arizoni, objavio je na Twitteru da se raduje svojoj obitelji i odmoru u Saint Louisu gdje će tjedan dana biti u posjetu obiteljskim prijateljima. Objavio je i „tweet“ kad je s obitelji uspješno stigao u Missouri. Dok ih nije bilo, provaljeno im je u kuću i ukradeno nekoliko tisuća dolara računalne i video opreme. Iako ovo je možda bio izolirani

[21] Maclean, F., Jones, D., Carin-Levy, G., & Hunter, H. (2013). Understanding Twitter, British Journal of Occupational Therapy, 76(6), str. 295.
[22] Maclean, F., Jones, D., Carin-Levy, G., & Hunter, H. (2013). Understanding Twitter, British Journal of Occupational Therapy, 76(6), str. 295.
[23] González-Pizarro, F., Figueroa, A., López, C., & Aragon, C. (2022). Regional Differences in Information Privacy Concerns After the Facebook-Cambridge Analytica Data Scandal, Computer Supported Cooperative Work, 31(1), str. 9.

događaj, postavlja se pitanje o tome tko ima pristup osobnim informacijama i kako to može dovesti ljude u opasnost.[24]

1.3.3. Tik Tok

Tik Tok je društvena mreža koja omogućuje korisnicima dijeljenje kratkih videozapisa, popularnih plesova, šaljivih izazova i drugih zanimljivih sadržaja. Tik tok je predstavljen u rujnu 2016. i brzo je preuzeo vodeću ulogu u svijetu društvenog dijeljenja.[25] Uspon Tik Toka do globalnog fenomena bio je nevjerojatno brz. Udvostručio je svoju svjetsku bazu korisnika između 2019. i 2021. (291,4 milijuna na 655,9 milijuna). Do 2025. godine približit će se broju od 1 milijarde korisnika.[26]

Ciljna skupina Tik Toka su uglavnom mlađe generacije, posebno tinejdžeri i mladi. Tik Tok je popularan zbog svoje jednostavnosti i zabave te omogućuje korisnicima da stvore i podijele kreativne i zanimljive sadržaje s drugima. Video mogućnosti uključuju glazbene uzorke, filtre, brze rezove, naljepnice i druge dodatke.

U 2021. Tik Tok bio je najpopularnija aplikacija među američkim tinejdžerima i mladim odraslim osobama, ali to više nije samo aplikacija za tinejdžere. U SAD-u je 2022. dobna skupina od 25 do 34 godine činila 25,4% korisnika Tik Toka. U kombinaciji s demografijom 18-24 (23,9%), odrasli u demografiji 18-34 činili su 49,3% korisnika Tik Toka u Sjedinjenim Državama.[27]

Prema podacima iz Sensor Towera, Tik Tokov angažman po zemlji raste iz godine u godinu. U 2022. korisnici Tik Toka u prosjeku su koristili aplikaciju 95 minuta dnevno, u usporedbi sa 62 minute u 2020. Od 2022. godine, 20,83% korisnika interneta u svijetu (4,8 milijardi) koristilo

[24] Humphreys, L., Phillipa, G., i Krishnamurthy, B. (2012). How much is too much? Privacy issues on Twitter, In: Conference of international communication association, Singapore 2010 Jun 21, str. 4.
[25] Tiktok, "About tiktok", https://www.tiktok.com/about?lang=en
[26] Intelligence, I. (n.d.). TikTok users worldwide & growth forecast https://www.insiderintelligence.com/charts/tiktok-users-worldwide-forecast/
[27] Grossman, M. M. (2023). 15 TikTok Facts and Stats to Know in 2023, yellowHEAD. https://www.yellowhead.com/blog/tiktok-facts-and-stats/

je Tik Tok. Povećanje je to od 2020., kada je Tik Tok koristilo 18% svih korisnika interneta diljem svijeta.

Postotak krađe podataka korisnika i osobnih podataka na Tik Toku nije poznat, ali društvena mreža prikuplja velike količine podataka o svojim korisnicima, uključujući informacije o njihovim interesima, lokaciji i uređajima koje koriste. Također, Tik Tok je bio pod prismotrom zbog navodnog prikupljanja osobnih podataka korisnika bez njihovog pristanka.[28]

Kako bi se netko registrirao na Tik Tok, potrebno je stvoriti korisnički račun pomoću e-mail adrese, telefonskog broja ili postojećeg računa na drugoj društvenoj mreži poput Facebooka ili Instagrama. Tik Tok također može zatražiti druge informacije o korisnicima, kao što su njihova imena, datum rođenja i spol. Ako netko prekrši pravila Tik Toka ili krši privatnost drugih korisnika, Tik Tok može poduzeti različite mjere, uključujući brisanje korisničkog računa ili ograničavanje pristupa određenim značajkama.

Tik Tok se također suočio s nekoliko situacija u kojima su se pojavile sigurnosne prijetnje i pitanja privatnosti korisnika. Primjerice, 2020. godine, Tik Tok je bio pod pritiskom američke vlade zbog navodne veze s kineskom vladom i mogućnosti da se podaci korisnika prikupljaju i dijele s kineskim vlastima.[29] Tik Tok je također bio pod istragom Europske unije zbog navodnog kršenja prava korisnika na privatnost i zaštite podataka.[30]

Od trećeg tromjesečja 2022. Tik Tok je koristilo više od 1,5 milijardi aktivnih mjesečnih korisnika diljem svijeta. U kombinaciji s 600 milijuna korisnika Douyina, kineske verzije Tik Toka, korisnička baza iznosi više od 2 milijarde. Aplikacija Tik Tok preuzeta je više od 3,5 milijardi puta otkad je lansirana. Samo od Q1-Q3 2022, aplikacija je preuzeta više od 571 milijun puta, prema Business of Apps.[31]

---

[28] Juničić, K., (2021). TikTok optužen da je ilegalno prikupljao podatke milijuna maloljetnika. Tvrtki prijeti golema kazna. https://www.jutarnji.hr/life/tehnologija/tiktok-optuzen-da-je-ilegalno-prikupljao-podatke-milijuna-maloljetnika-tvrtki-prijeti-golema-kazna-15067204

[29] Shepardson, D., (2023.). TikTok CEO: App has never shared US data with Chinese government, Reuters. https://www.reuters.com/technology/tiktok-ceo-app-has-never-shared-us-data-with-chinese-goverment-2023-03-22/

[30] Reuters. TikTok's lead EU regulator opens two data privacy probes. https://www.reuters.com/technology/ireland-regulator-opens-data-privacy-probes-into-tiktok-2021-09-14/

[31] Grossman, M. M. (2023). 15 TikTok Facts and Stats to Know in 2023, yellowHEAD. https://www.yellowhead.com/blog/tiktok-facts-and-stats/

1.3.4. Youtube

YouTube, osnovan 2005. godine, najpopularnija je internetska video zajednica u svijetu gdje milijuni ljudi mogu otkriti, gledati i dijeliti izvorno stvorene videozapise. Web stranica je naglo rasla, a u srpnju 2006. tvrtka je objavila da se svakodnevno prenosi više od 65 000 novih videozapisa te da je web-lokacija dnevno imala 100 milijuna video pregleda (YouTube, 2005). Ljudi provode u prosjeku 23 minute na YouTubeu svaki put kad ga posjete (Hootsuite, 2020). YouTube je druga najposjećenija web stranica na svijetu, nakon Googlea.[32]

Počevši od 2005. godine, YouTube se razvio u istaknuto online odredište za dijeljenje videa. Milijuni video isječaka na YouTubeu predstavljaju široki spektar interesa korisnika, uključujući interese nastavnika, znanstvenika i istraživača.[33] U Sjedinjenim Američkim Državama najviše korisnika (81%) ima od 15 do 25 godina.

YouTube je izvor video sadržaja na globalnoj razini.[34] Iako je YouTube uspio utjeloviti obje funkcije, tražilicu i društveno umrežavanje dvije su izrazito različite usluge. Unatoč činjenici da platforma-pružatelj ima za cilj biti sve za svakoga, različiti segmenti kupaca koriste platformu za različiti potrebe. Stoga YouTube također koriste različite skupine korisnika za svoje različite potrebe.[35]

Google i njegova podružnica YouTube, platit će 170 milijuna dolara kako bi se riješili optužbi Savezne komisije za trgovinu i državnog odvjetnika New Yorka da je YouTube usluga za dijeljenje video zapisa nezakonito prikupljala osobne podatke od djece bez pristanka njihovih roditelja.[36] Platforma YouTube omogućuje vlasnicima Google računa, uključujući velike komercijalne subjekte, stvaranje "kanala" za prikazivanje njihovog sadržaja. Prema optužbi,

---

[32] Global top websites by monthly visits 2022 | Statista. (n.d.). Statista. https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/

[33] Alias, N., Razak, S. H. A., elHadad, G., Kunjambu, N. R. M. N. K. & Muniandy, P. (2013). A Content Analysis in the Studies of YouTube in Selected Journals, Procedia - Social and Behavioral Sciences, 103, 12.

[34] Topic: YouTube. (n.d.). Statista. https://www.statista.com/topics/2019/youtube/

[35] Bowler, J. (2019). YouTube Community Posts: The new tool for creators, Printsome Insights https://blog.printsome.com/youtube-community-posts/

[36] Federal Trade Commission., Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (2019). https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.

vlasnici kanala koji ispunjavaju uvjete mogu odlučiti unovčiti svoj kanal dopuštajući YouTubeu da poslužuje bihevioralno ciljane oglase, što generira prihod i za vlasnike kanala i za YouTube.[37] YouTube se reklamirao kao glavno odredište za djecu u prezentacijama proizvođačima popularnih dječjih proizvoda i marki.

Nekoliko vlasnika kanala reklo je YouTubeu i Googleu da je sadržaj njihovih kanala bio usmjeren na djecu, a u drugim je slučajevima YouTubeov vlastiti sustav ocjenjivanja sadržaja identificirao sadržaj kao usmjeren na djecu. Osim toga, prema optužbi, YouTube je ručno pregledavao dječji sadržaj sa svoje YouTube platforme kako bi ga prikazao u svojoj aplikaciji YouTube Kids. Unatoč činjenici da je prepoznao sadržaj namijenjenih djeci, YouTube je posluživao ciljane oglase na tim kanalima. Prema optužbi, istovremeno je rekao jednoj tvrtki za oglašavanje da nema korisnike mlađe od 13 godina na svojoj platformi i stoga kanali na njezinoj platformi ne moraju biti u skladu sa COPPA-om.

[37] Federal Trade Commission., Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (2019). https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.

2. Rizik i opasnost društvenih mreža

Postotak sigurnosti podataka na društvenim mrežama ovisi o mnogim čimbenicima, a neki uključuju sigurnosne postavke korisnika i politike privatnosti platforme. Međutim, unatoč naporima da se osigura sigurnost podataka, društvene mreže su bile uključene u nekoliko kriza vezane uz privatnost i napade na osobne informacije korisnika.

Facebook je bio uključen u skandal Cambridge Analytica, gdje su podaci korisnika bili zlouporabljeni u političke svrhe. Ovakve krize su uvelike pridonijele potrebi za poboljšanjem sigurnosti podataka na društvenim mrežama. Velika prijetnja pravima na privatnost proizlazi iz činjenice da metode profiliranja mogu generirati osjetljive informacije "iz naizgled trivijalnih i/ili čak anonimnih podataka".[38]

Razni napadi na društvenim mrežama:[39]

1. Krađa identiteta – odnosi se na lažno predstavljanje prilikom kojeg napadač ilegalno preuzima kontrolu nad ciljanim profilom te zlorabi profil, najčešće radi stjecanja materijalne koristi.
2. Spam napadi – nakon što dođu do podataka o kanalima preko kojih mogu komunicirati s njihovim korisnicima, napadači im šalju neželjene podatke ili poruke, tvz. „spam“, najčešće kako bi isprovocirali reakciju određene vrste i naveli korisnika na radnje koje pogoduju napadaču.
3. Malware – vrlo česti problem među društvenim mrežama, Malware je software koji napadači šalju s namjerom infiltriranja na korisnikov uređaj kako bi ukrali podatke ili onemogućili daljnji rad uređaja;
4. Sybil napadi – lažni profili temelj su napada na Sybil, koji mogu naštetiti ispravnom funkcioniranju platforme društvenih medija, mogu se koristiti za distribuciju neželjenih informacija ili čak i Malware-a preko mreže. Kako bi se spriječili ovi napadi koriste se

[38] Hildebrandt, M. (2009). Who is profiling who? Invisible visibility, in: Protection, S. Gutwirth, Y. Poullet, P. De Hert, S. Nouwt, C. De Terwangne (eds), Reinventing Data Protection, Springer, Dordrecht, str. 250.
[39] Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction, Future Generation Computer Systems, 86, str. 916.

mehanizmi autentifikacije, s idejom da bi registracija korisnika na taj način postala sigurnija;

5. Lažni zahtjevi – napadač otvara profil na društvenoj mreži te s tog profila šalje zahtjeve a povezivanjem korisnicima s kojima nema interesa biti u iskrenom odnosu, već kako bi dobio pristup većoj količini podataka. Ako korisnici prihvate lažni zahtjev, napadač stječe više privilegija i na taj način može otkriti više informacija iz profila žrtava. Prevencija od lažnih zahtjeva nije moguća, stoga bi korisnik trebao biti odgovoran za svoj profil na društvenim mrežama.

2.1. Malware

Zlonamjerni softver je opći izraz za sve vrste malicioznog softvera, što u kontekstu računalne sigurnosti znači softver koji se koristi s ciljem pokušaja kršenja sigurnosne politike računalnog sustava s obzirom na povjerljivost, integritet ili dostupnost. Izraz softver ovdje treba shvatiti u najširem smislu, budući da se zlonamjerni učinak može koristiti izvršnim kodom, interpretiranim kodom, skriptama itd.

Računalni sustav čija je sigurnosna politika probijena obično je poznat kao meta za zlonamjerni softver. Napad može biti usmjeren na jednu ili više meta.

Klasifikacija Malware-a:[40]

Virus: Zlonamjerni softver koji se širi s jednog računala na drugo ugrađujući svoje kopije u datoteke, i na taj se način prenosi do cilja. Medij prijenosa poznat je i kao vektor virusa. Prijenos može pokrenuti sam virus (na primjer, može poslati zaraženu datoteku kao privitak e-pošte) ili se oslanjati ljudskog korisnika (koji na primjer prenosi CD-ROM koji sadrži zaraženu datoteku).

[40] Denning, P., & Lewis, T. (2019). Intelligence May Not Be Computable, American Scientist, https://www.americanscientist.org/article/intelligence-may-not-be-computable.

Crv: Zlonamjerni softver koji se širi s jednog računala na drugo tako što šalje svoje kopije putem mreže koja povezuje računala, bez upotrebe zaraženih datoteka.

Trojanhorse: Zlonamjerni softver koji je ugrađen u dio softvera koji ima naizgled koristan učinak. Koristan učinak je poznat i kao prekomjerni učinak, jer je primatelju očit, dok je učinak zlonamjernog softvera, poznat kao skriveni učinak, skriven od primatelja.

Logicbomb: Zlonamjerni softver koji je pokrenut nekim vanjskim događajem, kao što je određeni datum ili vrijeme. Može biti stvaranje ili brisanje određene stavke podataka, kao što je datoteka ili unos baze podataka.

Rabbit: (tkzv.Bacterium) Zlonamjerni softver koji koristi mnogo određenih klasa resursa, kao što su među spremnici poruka, prostor datoteka ili blokovi kontrole procesa na računalnom sustavu.

Stražnja vrata: Zlonamjerni softver koji, nakon što dosegne cilj, omogućuje inicijatoru pristup cilju bez prolaska kroz bilo koji od regularnih postupaka prijave i autentifikacije.

U posljednjem desetljeću napadači su rado pakirali zlonamjerni softver u Microsoft Office formate datoteka, posebice Word i Excel. Zapravo, u prvom tromjesečju 2022. gotovo polovica (45%) zlonamjernog softvera koji je zaustavio HP Wolf Security koristila je formate sustava Office. Razlozi su jasni: korisnici su upoznati s ovim vrstama datoteka, aplikacije koje se koriste za njihovo otvaranje su sveprisutne i prikladan su mamac za društveni inženjering.[41]

Posljedice[42]:

1. Gubitak podataka - Mnogi virusi i Trojanci pokušat će obrisati datoteke ili tvrde diskove kada se aktiviraju. Čak i ako rano uhvatite infekciju, možda ćete morati izbrisati zaražene datoteke.
2. Krađa računa - Mnoge vrste zlonamjernog softvera uključuju funkcije keyloggera, dizajnirane za krađu računa i lozinki od svojih meta. Ovo može dati autoru zlonamjernog

[41] Schläpfer, P. (2022). PDF Malware Is Not Yet Dead, HP Wolf Security. https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/

[42] Mohd, H. (2023). CSCA0101 – Computer Basics, FTMS College https://ftms.edu.my/v2/current-student/foundation-student/csca0101-computing-basics/

softvera pristup bilo kojem korisnikovom online računu, uključujući poslužitelje e-pošte s kojih haker može pokrenuti nove napade.

3. Botneti - Mnoge vrste zlonamjernog softvera također potkopavaju kontrolu nad korisničkim računalom, pretvarajući ga u "bota" ili "zombija". Hakeri grade mreže od ovih preuzetih računala, koristeći njihovu kombiniranu procesorsku snagu za zadatke poput razbijanja datoteka s lozinkama ili masovnog slanja e-pošte.
4. Financijski gubici - Ako haker dobije pristup kreditnoj kartici ili bankovnom računu putem keyloggera, on tada može upotrijebiti te podatke za naplatu ili pražnjenje računa. S obzirom na popularnost internetskog bankarstva i usluga plaćanja računa, haker koji uspije skriti keylogger na korisnikov sustav cijeli mjesec može dobiti pristup cjelokupnom korisnikovom financijskom portfelju, omogućujući mu da napravi što je više moguće štete u jednom napad.

Kako zaštiti svoje računalo?[43]

1. Instalirajte zaštitni softver.
2. Budite oprezni kada radite s datotekama iz nepoznatih ili upitnih izvora.
3. Ne otvarajte e-mail ako ne prepoznajete pošiljatelja.
4. Preuzimajte datoteke samo s pouzdanih internetskih stranica.
5. Instalirajte vatrozid (firewall).
6. Mjesečno skenirajte svoj tvrdi disk na viruse.

2.2. Ransomware

Ransomware je jedan od najrazornijih oblika digitalnog kriminala. Nije neuobičajeno da napadači uspješno iznude goleme svote novca od svojih žrtava. Ponekad iznuđuju žrtve za

[43] Dangerous Email Attachments: What You Need To Know To Stay Safe | Phriendly Phishing Blog. (2023). Phriendly Phishing. https://www.phriendlyphishing.com/blog/dangerous-email-attachments

milijune dolara, pri čemu su neke žrtve spremne platiti umjesto da ignoriraju prijetnju gubitka ili otkrivanja podataka.[44]

U svibnju 2021. milijun Amerikanaca iskusili su iz prve ruke štetu koju kibernetički napadi mogu prouzročiti, nakon što je dobavljač goriva Colonial Pipeline bio pogođen napadom ransomwarea. Organizacija je bila prisiljena zaustaviti rad nakon što su njezina poslovna mreža i sustav naplate bili ugroženi. Iako je ransomware odgovoran za velik dio štete, napadači su mogli podmetnuti zlonamjerni softver tek nakon što su dobili pristup lozinci zaposlenika. Najvjerojatniji način da to učinite je putem phishing e-pošte. Kao što je napomenula američka vlada, grupa odgovorna za napad zvana DarkSide koristila je takve metode.

Koliko je napad uzrokovao štete, nemoguće je točno utvrditi. Colonial Pipeline je napadačima platio 4,4 milijuna dolara (oko 3,75 milijuna eura) za ključ za dešifriranje, no to je bio mali dio posljedica. Organizacija, koja osigurava gotovo polovicu opskrbe naftom za istočnu obalu SAD-a, morala se zatvoriti na tjedan dana, što je rezultiralo ne isporukom oko 20 milijardi galona nafte, koja je na tržištu vrijedila približno 3,4 milijarde eura. Cijene benzina su skočile, što znači da su neki od troškova proslijeđeni javnosti. U međuvremenu, više od 10.000 benzinskih postaja ostalo je bez nafte čak tjedan dana nakon što su se sustavi Colonial Pipelinea vratili u normalu. Izvršni direktor Joseph Blount priznao je troškove šireg američkog gospodarstva u intervjuu za The Wall Street Journal, u kojem je objasnio svoju odluku da plati ransomware.[45]

U drugom tromjesečju 2021. količina napada ransomwareom dosegla je vrhunac sa 188,9 milijuna napada.[46] Od 2021. Sjedinjene Države i dalje su vodeća svjetska meta napada ransomwarea, što predstavlja više od 51% incidenata. Ostale zemlje uključuju[47]:

1. UK — 10%
2. Kanada — 5%

---

[44] What Is Ransomware and How Do You Prevent It? (2023). What Is Ransomware and How Do You Prevent It? https://www.antivirusguide.com/cybersecurity/ransomware/

[45] Irwin, L. (2022). The 5 Biggest Phishing Scams of All Time - IT Governance Blog En, IT Governance Blog En., https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time

[46] What Is Ransomware and How Do You Prevent It? (2023). What Is Ransomware and How Do You Prevent It? https://www.antivirusguide.com/cybersecurity/ransomware/

[47] What Is Ransomware and How Do You Prevent It? (2023). What Is Ransomware and How Do You Prevent It? https://www.antivirusguide.com/cybersecurity/ransomware/

3. Francuska — 3%
4. Australija — 3%

2.3. Phishing

Phishing se odnosi na pokušaj iznuđivanja informacija kao što su korisničko ime, lozinka i podaci o kreditnoj kartici od subjekata u elektroničkoj komunikaciji. Komunikacija koja je oblikovna tako da izgleda kao da dolazi s popularnih društvenih web stranica, aukcijskih stranica, procesa online plaćanja ili IT administratora uobičajena je taktika za phishing napade. Krađa e-pošte može sadrže poveznice na web stranice koje su zaražene zlonamjernim softverom.[48]

Od 2019. do 2020. dramatično se povećao broj zlonamjernih PDF datoteka, za čak 1160%, te je broj zlonamjernih datoteka porastao sa 411.800 na 5.224.056. PDF datoteke su primamljivi vektor za krađu identiteta budući da su višeplatformske i omogućuju napadačima da stupe u kontakt s korisnicima, čineći njihove sheme vjerodostojnijima od tekstualne e-pošte sa samo običnom vezom.[49]

Krađa identiteta objašnjena je korak po korak[50]:

1. Napadač šalje e-mail žrtvi.
2. Žrtva klikne na e-poštu i ode na phishing web stranica.
3. Napadač prikuplja osjetljive podatke žrtve.
4. Napadač koristi osjetljive podatke žrtve za pristup web stranici.

U siječnju 2016., zaposlenik u austrijskom proizvođaču zrakoplovnih dijelova FACC primio je e-poruku u kojoj se od organizacije traži prijenos 42 milijuna eura na drugi račun u sklopu "projekta akvizicije". Činilo se kako je poruka došla od izvršnog direktora organizacije,

[48] Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks, International Journal of Computer Applications, 182(33), str. 27.
[49] Ashutosh Chitwadgi, A. H., Hosseini, A., & Chitwadgi, A. (2021). Phishing Trends With PDF Files, Unit 42. https://unit42.paloaltonetworks.com/phishing-trends-with-pdf-files/
[50] Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks, International Journal of Computer Applications, 182(33), str. 27.

Waltera Stephana, ali zapravo je to bila prijevara. Budući da nije mogao uočiti pravi izvor e-pošte, zaposlenik je udovoljio zahtjevu. Malo je detalja otkriveno o tome što je točno pošlo po zlu, ali postoji razlog za vjerovanje da je Stephan bio barem djelomično kriv. FACC ga je otpustio nakon interne istrage, tvrdeći da je "teško prekršio svoje dužnosti". Također je otpustio svog glavnog financijskog direktora. FACC je tražio 10 milijuna Eura odštete od rukovoditelja, ali su austrijski sudovi odbacili tužbu.[51]

2.4. Najveći napadi i krađe podataka

Najveće curenje podataka u povijesti izazivaju hakeri koji koriste slabu sigurnost zaštite podataka tvrtke ili određene platforme. Većina prijavljenih kršenja je u Sjevernoj Americi, barem dijelom zbog relativno strogih zakona o otkrivanju podataka u sjevernoameričkim zemljama. Procjenjuje se da će prosječni trošak povrede podataka biti preko 150 milijuna dolara do 2020. godine, s predviđanjem da će globalni godišnji trošak iznositi 2,1 trilijuna dolara.[52]

U 2021. podaci više od 700 milijuna korisnika LinkedIna objavljeni su na prodaju na mračnom webu (Deep Web), uključujući e-mailove, korisnička imena, telefonske brojeve, račune na društvenim mrežama i druge detalje vezane uz posao. LinkedIn poriče da su radnje predstavljale kršenje, tvrdeći da je to samo rezultat previše javno dostupnih informacija. Od tada su hakeri stavili na prodaju druge zbirke podataka iz LinkedIn baza podataka na mračnom webu. Stručnjaci upozoravaju da akteri prijetnji mogu ciljati korisnike LinkedIna putem phishing napada, spama i napada "brutalnog prisiljavanja", što uključuje isprobavanje različitih varijacija lozinki dok ne pogode onu točnu.[53]

Korisnik na hakerskom forumu niske razine objavio je osobne podatke više od 530 milijuna korisnika Facebooka iz 106 zemalja 2021. godine. Iako su podaci bili stari nekoliko godina

[51] Irwin, L. (2022). The 5 Biggest Phishing Scams of All Time - IT Governance Blog En, IT Governance Blog En., https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time
[52] List of data breaches - Wikipedia. (2019), List of Data Breaches – Wikipedia https://en.wikipedia.org/wiki/List_of_data_breaches
[53] Biggest Data Breaches in History, Top 6 Breaches in U.S. (n.d.). Consumer Notice, LLC. https://www.consumernotice.org/data-protection/breaches/biggest-in-history/

zbog ranjivosti zakrpane 2019., to je bila vrsta podataka koje su kriminalci koristili za izvođenje društvenog inženjeringa ili pokušaja hakiranja. Irska komisija za zaštitu podataka izrekla je kaznu od 265 milijuna eura (276 milijuna dolara) i korektivne mjere u vezi s kršenjem.[54] Facebook je morao jasno izraziti da ne može dati nikakva jamstva u pogledu svoje privatnosti informacije, te da ukoliko klijenti otvore svoje profile, svi podaci koji se u njima nalaze postaju javno dostupni.

Grupa Starwood Hotels, koju je Marriott kupio 2016., napadnuta je 2014. godine. Imena, podaci za kontakt, podaci o putovnicama i brojevi programa vjernosti evidencije gostiju klijenata u Ujedinjenom Kraljevstvu bili su kompromitirani. Napad se nastavio do 2018., kada je Marriott prvi put primijetio problem i brzo djelovao kako bi poboljšao svoje sustave.[55]

[54] List of data breaches - Wikipedia. (2019), List of Data Breaches – Wikipedia https://en.wikipedia.org/wiki/List_of_data_breaches

[55] List of data breaches - Wikipedia. (2019), List of Data Breaches – Wikipedia https://en.wikipedia.org/wiki/List_of_data_breaches

3. Sigurnost i zaštita osobnih podataka

Zakon o zaštiti podataka promijenjen je od 25. svibnja 2018. Opća uredba o zaštiti podataka (GDPR) novi je, europski zakon koji zamjenjuje Zakon o zaštiti podataka iz 1998. u Ujedinjenom Kraljevstvu i nadzire Zakon o zaštiti podataka Ujedinjenog Kraljevstva iz 1998. To je dio šireg paketa reformi područja zaštite podataka koji uključuje Zakon o zaštiti podataka iz 2018. GDPR postavlja zahtjev i upute u vezi načina na koji organizacije trebaju postupati s osobnim podacima od 25. svibnja 2018.

Uz druge promjene, poboljšat će prava osoba čiji se podaci drže (poznatih kao subjekti podataka u Zakonu o zaštiti podataka) i dati im više kontrolu nad onim što se događa s njihovim podacima. Također dopušta izricanje financijskih kazni bilo kojoj organizaciji koja krši ta prava ili se ne pridržava načela odgovornosti, što u osnovi znači da voditelji obrade podataka i obrađivači podataka, tj. organizacije i određeni pojedinci, uključujući vijeća, moraju staviti tehničke i uspostavljene organizacijske mjere za zaštitu podataka koje posjeduju s ciljem izbjegavanja od gubitka, neovlaštenog pristupa itd. te kako bi se osigurala zaštita prava ispitanika.

Na sigurnost i privatnost korisničkih podataka utječu različiti poslovni modeli koje koriste platforme društvenih medija, kao što su ciljano oglašavanje i opsežni postupci prikupljanja podataka. Različite platforme društvenih medija imaju različite tehnike za prikupljanje, korištenje i dijeljenje osobnih podataka korisnika, što predstavlja različite opasnosti po sigurnost i privatnost za svaku bazu korisnika. S obzirom na nove platforme, nove odnose i nove primjene unutar ekosustava društvenih medija, uočeni su problemi koji se odnose na sigurnosnu kontrolu mehanizam, zaštitu privatnosti pojedinca i digitalno autorsko pravo.[56]

Glavni kriteriji za stranice društvenih mreža su sigurnost i privatnost. Međutim, još uvijek postoje teški napadi na sve te stranice društvenih mreža, a zaštita potencijalnih korisnika od ovih kriminalnih radnji pokazala se kao teški izazov za mnoge društvene analitičare i inženjere.

[56] Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. Future Generation Computer Systems, 86. Str. 917.

Zaštitom osobnih podataka smatra se poduzimanje mjera u svrhu zaštite osobne privatnosti i sigurnosti podataka. Republika Hrvatska je propisala mjere koje su regulirane skupom pravnih akata. Primjerice, jedan od najbitnijih pravnih akata je GDPR (General Data Protection Regulation) koji je počeo s regulacijom u cijeloj Europi 2018. godine. Taj pravni akt, preveden kao „Opća uredba u zaštiti podataka“, služi za regulaciju zaštite osobnih podataka. Njime je Hrvatska usklađena sa zakonodavstvom Europske unije.

I na nacionalnoj i na međunarodnoj razini, brojni zakonodavni i regulatorni okviri pojavili su se kao odgovor na rastuću zabrinutost oko privatnosti i sigurnosti podataka. Također je ispravno istaknuto da je privatnost pojam koji je teško definirati. Aludira na odsutnost imenovanja, spominjanja, ali također može uključivati pravo odlučivanja u kojoj se mjeri osobni podaci otkrivaju te kada se, kako i koji podaci mogu dijeliti s drugima.

Zaštita je preduvjet za internetsko samootkrivanje, ali samo otkrivanje dodatno umanjuje privatnost. Čini se da veze između ovih odnosa mogu biti pod utjecajem kritičnih varijabli, na primjer, povjerenja i kontrole. Povjerenje se definira kao uvjerenje da se ljudima, tvrtkama ili ustanovama može vjerovati i ima povoljan učinak na online samoizlaganje no često je u suprotnosti sa zaštitom.

Postoje dva pravna akta povezana s internetom i krađom osobnih podataka. Prvi je „Kazneni zakon“ te se on veže uz povredu privatnosti i zaštite osobnih podataka te definira jasno kaznene postupke. Drugi je „Zakon o elektroničkoj trgovini“ koji služi za reguliranje procesa prikupljanja podataka, obradu i korištenje privatnih podataka unutar elektroničke trgovine.

3.1. Obrada osobnih podataka

Prikupljanje, snimanje, organiziranje, pohranjivanje, prilagodba, korištenje, objavljivanje, prijenos, brisanje ili uništavanje podataka smatraju se dijelom obrade osobnih podataka.

Korištenje tuđih osobnih podatke nije legalno koristiti osim u svrhu koju se navede kada se prikupljaju. Ako ih se želi koristiti u drugu svrhu, trebali bi se vratiti osobi i zatražiti njezin pristanak za ovu dodatnu obradu. Ako se prikupljaju posebne kategorije podataka, osoba mora

dati izričit pristanak za obradu tih podataka. To znači da bi se za takve slučajeve trebao dobiti osobni potpis i voditi evidenciju da je osoba dala privolu.

Svako kršenje sigurnosti izravno ometa ekonomski rast organizacije. Društveni mediji mogu analizirati proučavanjem ponašanja svojih korisnika, što bi mogli biti pojedinac ili grupa.[57]

Učestalost sigurnosnih proboja na platformama društvenih medija postala je velika briga za poduzeća diljem svijeta u trenutnoj digitalnoj eri. Tvrtke su bile prisiljene usvojiti jake sigurnosne mjere kao rezultat stalnog niza ovih upada. Moguće posljedice proboja sigurnosti mogu izravno naštetiti robnoj marki i gospodarskom rastu pogođenog poslovanja, daleko nadilazeći brigu o privatnosti pojedinca. Razumijevanje ponašanja korisnika društvenih medija, bilo da se radi o pojedincima ili organizacijama, ključno je za ispravno rješavanje ovih sigurnosnih problema. Navike, ponašanje i interakcije korisnika na platformama društvenih medija mogu se analizirati kako bi se dobili važni uvidi koji mogu pomoći tvrtkama da ojačaju svoje sigurnosne protokole i zaštite kritične podatke.

Društvene mreže samo su jedan od primjera brojnih tvrtki i organizacija koje ljudima nude usluge ili proizvode u digitalnom svijetu. Ovi sustavi često obrađuju goleme količine osobnih podataka, što zahtijeva poštivanje strogih pravila. Agencija za zaštitu osobnih podataka nadležna je za nadzor nad obradom osobnih podataka i osigurava usklađenost iste sa zakonodavstvom o zaštiti podataka.

Većinu vremena tvrtke i organizacije koje korisnicima nude usluge ili proizvode, uključujući društvene mreže, obrađuju osobne podatke. Agencija za zaštitu osobnih podataka odgovorna je za nadzor nad obradom osobnih podataka i osiguravanje da se ona odvija u skladu sa zakonima o zaštiti podataka. Osobnim podacima smatraju se svi podaci koji se mogu koristiti za identifikaciju osobe čiji se podaci obrađuju, kao što su ime, adresa, datum rođenja, telefonski broj, e-mail adresa i sl.

Zakon o zaštiti podataka iz 1998. (DPA) temelji se na osam načela "dobrog rukovanja informacijama". Oni ljudima daju određena prava u vezi s njihovim osobnim podacima i

[57] Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. Future Generation Computer Systems, str. 918.

postavljaju obveze organizacijama koje su odgovorne za njihovu obradu. Ove smjernice objašnjavaju kako utvrditi jesu li informacije "osobni podaci" za potrebe DPA-a. Osmišljen je kako bi pomogao stručnjacima za zaštitu podataka da odluče spadaju li podaci u definiciju osobnih podataka u okolnostima u kojima to nije očito.[58]

U širem kontekstu rudarenja podataka, može se pronaći značajna mjera produktivnog analiziranja u svrhu učenja i napredne evidencije ljudskog ponašanja u međuljudskim odnosima, bez narušavanja privatnosti korisnika. Takve informacije trebaju biti dostupne, a da se istovremeno privatnost čuva s visokom razinom zaštite. S druge strane, malo je vjerojatno da se svaki autsajder koji je zaintrigiran da razbije informacije može smatrati pouzdanim, jer je činjenica da korištenje svih informacija, uključujući one prepoznatljive i delikatne, može omogućiti zloupotrebu.

Korisnici društvenih mreža često moraju otkriti osobne podatke kako bi se registrirali online, uključujući podatke koji nisu potrebni za korištenje same usluge. Društvene mreže često prikupljaju ove podatke za marketing i kako bi korisnicima ponudile personaliziranije iskustvo. Korisnici trebaju biti svjesni da se dijeljenjem osobnih podataka na društvenim mrežama izlažu opasnosti da ti podaci budu ukradeni ili neprikladno iskorišteni. Osobni podaci uključuju sve informacije koje se mogu koristiti za identifikaciju određene osobe, kao što su njihovo ime, adresa, datum rođenja, broj telefona ili adresa e-pošte.

Korisnici često nisu upoznati s novim zakonodavstvom, PoPI, koji nastoji braniti njihova prava na privatnost. Razlog tome mogao bi biti široka nezainteresiranost ili nemogućnost razumijevanja onoga što zakon podrazumijeva te način na koji je napisan.

Međutim, korisnici bi trebali biti oprezni kada otkrivaju osobne podatke na društvanim mrežama jer time svoje podatke izlažu opasnosti od krađe ili nepravilne upotrebe. Potrebna je viša razina svijesti kako bi se osiguralo da ljudi razumiju potencijalnije prijetnje i da bi poduzeli potrebne mjere opreza za očuvanje svoje privatnosti na internetu.

[58] Essential guide to the General Data Protection Regulation (GDPR). (2017). The Pharmaceutical Journal, https://pharmaceutical-journal.com/article/news/essential-guide-to-the-general-data-protection-regulation-gdpr

3.2. Zloupotreba privatnih informacija

Krađa osobnih podataka drugih korisnika na društvenim mrežama može donijeti ozbiljne posljedice, a kazne za ovakvo ponašanje ovise od zemlje do zemlje. U nekim zemljama, kazne za krađu podataka mogu biti vrlo stroge i uključuju visoke novčane kazne pa čak i zatvorske kazne. U Republici Hrvatskoj se kazne reguliraju prema propisanom zakonu te uključuju novčane kazne i ponekad kazneni progon. Prekršiteljima zakona može se pripisati novčana kazna od nekoliko tisuća kuna pa do nekoliko milijuna ovisno o težini prekršaja.

Očuvanje privatnosti korisnika registra središnja je uloga nadležnih tijela i svako odstupanje od propisanog potpuno bi uništilo upravljanje organizacijskom politikom, što zauzvrat dovodi do ozbiljnog ugrožavanja temeljnih prava društva.[59]

Ukradene informacije, uključi osobne podatke s društvenih mreža, često se iskorištavaju za različite vrste štetnog ponašanja. Najčešće se takvi podaci koriste za otvaranje novih računa na društvenim mrežama, bankama ili drugim platformama pomoću ukradenih podataka. Osim toga, hakeri mogu iskoristiti ove informacije kako bi naveli pojedince da im pošalju novac pretvarajući se da su vlasnici računa. Također, izrada prilagođenih marketinških kampanja korištenjem korisničkih preferencija i podataka o aktivnostima još je jedna česta primjena ukradenih podataka u ciljanom oglašavanju. Iako ovo može biti korisno za oglašivače, može smetati korisnicima i činiti se nametljivim.

Jedan od načina na koji hakeri mogu ukrasti osobne podatke je putem javnih WiFi mreža. Ove mreže koje se često nalaze u kafićima, restoranima brze hrane i hotelima koristi širok raspon ljudi. Prilikom korištenja javne mreže, svi podaci uglavnom se šalju putem radio valova i mogu se presresti.[60] Ovo se kazneno djelo definira kao krađa osobnih podataka od druge osobe i njihovo korištenje za vlastitu dobit. Kradljivci identiteta koriste se brojevima socijalnog osiguranja, datumima rođenja, brojevima kreditnih kartica, lozinkama, brojevima bankovnih računa, brojevima državnih osobnih iskaznica i drugim informacijama kako bi izvršili prijevaru

[59] Senthil Kumar N, Saravanakumar K, & Deepa K. (2016). On Privacy and Security in Social Media – A Comprehensive Study, Procedia Computer Science, str. 115.
[60] Wallin, P. (2014). Punishment for Stealing Personal Information through Public WiFi. https://www.wklaw.com/stealing-personal-information-public-wifi/

dok varaju nekog drugog.[61] Prekršajne kazne mogu premašiti 1000 USD. Kazne za kaznena djela mogu premašiti 500.

Osim toga, postoje slučajevi u kojima se ukradeni korisnički podaci prodaju na crnom tržištu i koriste za razne opasne i kriminalne aktivnosti, poput krađe identiteta, financijske prijevare ili distribucije zlonamjernog softvera.

Na individualni proces odlučivanja u vezi privatnosti utječu brojni čimbenici. Među njima, nepotpune informacije, ograničena racionalnost i sustavna psihološka odstupanja od racionalnosti sugeriraju da pretpostavka o savršenoj racionalnosti pojedinaca možda neće na odgovarajući način uzeti u obzir nijanse ponašanja pojedinca osjetljivog na privatnost.

Prednosti i troškovi povezani s napadima na privatnost i zaštitom su složeni, višestrani i specifični za kontekst. Često su u paketu s drugim proizvodima i uslugama (npr. upit tražilice može potaknuti željeni rezultat, ali također može dati promatračima informacije o interesima pretražitelja), a često se prepoznaju tek nakon što dođe do kršenja privatnosti.

[61] What Legally Constitutes Identity Theft? (2020), Newman & Allen
https://www.newmanallen.com/blog/2020/october/what-legally-constitutes-identity-theft-/

4. Pregled dosadašnjih istraživanja

U istraživanju iz 2019. godine, autori Dharmawan, Kasih i Stiawan[62] objašnjavaju zakonski okviri za elektroničke transakcije i odgovornosti pružatelja elektroničkih sustava u zaštiti osobnih podataka korisnika. Naglašavaju ugovorne obveze davatelja internetskih usluga i važnost pružatelja usluga računarstva u oblaku koji osiguravaju privatnost podataka i predlažu primjenu mjera iz propisa SAD-a i EU za poboljšanu zaštitu osobnih podataka u Indoneziji. Tekst također preporučuje razmatranje napredne tehnologije i regulacije Big Data za sveobuhvatne sigurnosne mjere.

U istraživanju iz 2020. godine, Romansky i Noninska[63] istražuju utjecaj digitalnih tehnologija poput virtualnih okruženja, strojnog učenja i sustava temeljenih na znanju na društvo i pojedinca. Članak naglašava važnost zaštite osobnih podataka u digitalnom dobu. Cilj je članka utvrditi neke posebnosti zaštite informacija i osobnih podataka te sažeti glavne izazove digitalnog doba u pogledu sigurnosti i privatnosti korisnika.

Također iste godine, autorica Mateeva[64] u svom istraživanju govori o donošenju novog pravnog okvira za zaštitu osobnih podataka u EU. Naglašava kako taj okvir modernizira načela uvođenjem zahtjeva transparentnosti, pristupa, brisanja i odgovornosti. istraživanje naglašava važnost poštivanja ovih načela kako bi se zaštitila osobna prava i spriječilo nekontrolirano prikupljanje podataka. U istraživanju se ističe važnost edukacije svih sudionika u postupcima zaštite podataka kako bi se osigurala učinkovita provedba i procijenila potencijalna kršenja. Istraživanje također naglašava kako ova načela uspostavljaju granice za obradu podataka, rješavaju sporove između konkurentskih prava i olakšavaju siguran protok podataka unutar država članica EU-a.

[62] Dharmawan, N. K. S., Kasih, D. P. D., i Stiawan, D. (2019). Personal data protection and liability of internet service provider: a comparative approach. International Journal of Electrical and Computer Engineering (IJECE), 9(4), str. 3183.
[63] Romansky, P. R., i Noninska, S.I. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), str. 5288.
[64] Mateeva, Z. (2020). Principles of personal data protection. 28. str. 103.

Grupa autora Fan, Wu, Yan i drugi[65] proveli su istraživanje s namjerom otkrivanja čimbenika koi utječu na namjeru otkrivanja osobnih podataka na društvenim mrežama u Kini. Istraživanje pokazuje kako percipirani rizik ne utječe značajno na spremnost korisnika da otkriju osobne podatke na društvenim mrežama. Korisnici često smatraju da moraju dati osobne podatke za korištenje društvenih medija, bez obzira na percipirane rizike. To može biti zbog toga što korisnici sebe smatraju pasivnim promatračima ili vjeruju robnim markama društvenih medija. Istraživanje sugerira da bi platforme društvenih medija trebale poboljšati postavke privatnosti, poboljšati zaštitu privatnosti, pružati vrijedne usluge korisnicima i zaštititi osjetljive informacije dok brinu o personaliziranim uslugama i pristupu podacima.

Istraživanje autora Marune i Hartanto[66] iz 2021. godine, naglašava potrebu da Indonezija ojača svoje sposobnosti u digitalnom području zbog sve većih cyber prijetnji. Ističe važnost donošenja sveobuhvatnih zakona, poput "Prijedloga zakona o zaštiti osobnih podataka", i osnivanja neovisne nadzorne agencije. Istraživanje također naglašava važnost promjene u vladi, obrazovanju i zajednicama u svrhu podizanja svijesti i izgradnje otporne cyber obrane. Osim toga, zalaže se za izradu i donošenje Zakona o kibernetičkoj sigurnosti i otpornosti. Suci se potiču da pažljivo razmotre slučajeve koji se odnose na sigurnost podataka i privatnost dok čekaju nove zakone.

Istraživanje autora Marín, Carpenter i dr.[67] iz 2022. godine nudi vrijedne uvide u problematiku sigurnosti, naglašavajući utjecaj pravnih okvira, digitalne kompetencije i kulturnih vrijednosti. Također je naglašena potreba da budući programi obuke nastavnika uključe elemente pismenosti o osobnim i kritičnim podacima, uzimajući u obzir čimbenike kao što su ovlaštenje nad osobnim podacima, institucionalna kontrola podataka i platforme društvenih medija u nastajanju.

[65] Fan, A., Wu, Q., Yan, X., i drugi., (2021). Research on Influencing Factors of Personal Information Disclosure Intention of Social Media in China. Data and Information Management, 5(1), str. 203.

[66] Marune, A. E. M. S., i Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. International Journal of Business, Economics, and Social Development, 2(4), str. 151.

[67] Marín, V. I., Carpenter, J. P., Tur, G., i drugi., (2022). Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers. Journal of Computers in Education. str 27.

Manipulacija ljudskim ponašanjem radi profita kodirana je u tvrtkama makijavelističkom preciznošću. Promicanje sadržaja koji nametljivo promovira korištenje društvenih medija drži korisnike stalno angažiranima, dok personalizirane preporuke koriste podatke ne samo za predviđanje, već i za utjecaj na naše radnje, pretvarajući korisnike u lak plijen za oglašivače i propagandiste.[68]

Veliki kreatori na društvenim mrežama slažu se oko jedne stvari - kada su započeli sa radom na društvenim mrežama, nisu ni sami znali kakav će utjecaj imati na ljude i koliko je zapravo ozbiljno to što stvaraju. Hoće li se trenutna situacija sa društvenim mrežama i prevelikim utjecajem koje imaju na svijet ikada promijeniti i hoćemo li možda u budućnosti biti bliži rješenju koje naglašava pozitivne strane interneta, a negativne stavlja u drugi plan?[69]

[68] The New York Times. "The Social Dilemma' Review: Unplug and Run, https://www.nytimes.com/2020/09/09/movies/the-social-dilemma-review.html
[69] Recenzija filma „The Social Dilemma" (2020). Kišobran. https://kisobran.uniri.hr/2020/12/08/recenzija-filma-the-social-dilemma/

5. Istraživanje stavova ispitanika o sigurnosti društvenih mreža

U ovom dijelu rada provesti će se empirijsko istraživanje stavova ispitanika o sigurnosti na društvenim mrežama. Empirijsko istraživanje se temelji na teoretskim postavkama iz prethodnih dijelova rada. U ovom poglavlju navode se sadržaj i ciljevi istraživanja, objašnjena je metodologija istraživanja te se prikazuju rezultati dobiveni istraživanjem. Nakon toga, navedena su ograničenja koja su nastala prilikom istraživanja te će se predložiti preporuke za buduća istraživanja. Poglavlje završava raspravom u kojoj se iznose osnovni zaključci provedenog istraživanja.

5.1. Sadržaj i ciljevi istraživanja

Brzo širenje platformi društvenih medija u današnjem digitalnom okruženju zasigurno je promijenilo način na koji ljudi komuniciraju jedni s drugima i dijele informacije sa svojim okruženjem. Međutim, u društvu koje postaje sve povezanije i sve više vođeno podacima, ova tehnološka inovacija istaknula je problematiku sigurnosti i zaštite osobnih podataka. Delikatan odnos društvenih medija s osobnim podacima narušio je problem sigurnosti, gdje povrede, neželjeni pristup i zlouporaba rutinski dovode u pitanje sigurnost osobnih podataka ljudi.

Predmet istraživanja jest prikazati odnos korisnika i društvenih mreža, ispitati koliko se osjećaju sigurno na društvenim mrežama te koliko su oprezni dok ih koriste. Ciljevi istraživanja jest utvrditi koliko zapravo društvene mreže utječu na sigurnost korisnika, osjećaju li se sigurno i shvaćaju li potencijalne posljedice dijeljenja svojih podataka na internetu. Također će se ispitivati prosječno korištenje društvenih mreža te koje mreže korisnici najviše koriste i u koju svrhu.

Stoga su osnovni ciljevi istraživanja sljedeći:

- Identificirati vrste sigurnosnih prijetnji i napada na društvenim mrežama;
- Istražiti stavove korisnika društvenih mreža o percipiranoj sigurnosti;
- Istražiti stavove korisnika društvenih mreža o dijeljenju podataka;

- Analizirati stavove korisnika društvenih mreža o potrebi za edukacijom o sigurnosti.

Istraživačka pitanja glase:

IP1: Koje su najčešće vrste prijetnji i napada na društvenim mrežama?

IP2: Kakvi su stavovi korisnika društvenih mreža o sigurnosti?

IP3: Kakvi su stavovi korisnika društvenim mreža o dijeljenju podataka?

IP4: Kakvi su stavovi korisnika društvenih mreža o potrebi za edukacijom o sigurnosti?

Ovo istraživanje također nastoji odrediti i analizirati slabosti i potencijalne opasnosti s kojima se ljudi suočavaju dok objavljuju svoje osobne podatke na velikom broju društvenih medija. Podloga istraživanja zahtijeva temeljitu analizu kako prošlih tako i modernih primjera povreda podataka, krađe identiteta, narušavanja privatnosti i nemarnog ili zlonamjernog iskorištavanja dijeljenih informacija.

5.2. Metodologija

Provedeno empirijsko istraživanje za prikupljanje podataka koristi metodu ispitivanja, a kao instrument istraživanja koristi anketni upitnik. Anketa je napravljena u obliku „Google forms-a“ te je proslijeđena ispitanicima putem aplikacije WhatsApp, Facebook i Instagram. Istraživanje je provedeno na prigodnom uzorku od 104 ispitanika, prilikom čega su svi valjano ispunjeni i uzeti u obradi rezultata.

Prikupljanje anketa je trajalo u periodu od 25.5.2023. do 5.6.2023. Anketni upitnik je sadržavao ukupno 28 pitanja, dok su pitanja bila raspoređena u pet skupina te su različitog tipa: pitanjima na koja se odgovara sa „da“ ili „ne“, pitanja otvorenog tipa gdje su ispitanici mogli upisivati vlastite odgovore, pitanja sa višestrukim izborom te pitanja kojim se mjere stavovi ispitanika pomoću Likertove ljestvice od 1 do 5, pri čemu 1 znači „u potpunosti se ne slažem“, dok ocjena 5 sugerira „u potpunosti se slažem“.

Prva skupina pitanja fokusirala se na učestalost korištenja društvenih mreža te na svrhu korištenja. Pitanja su preuzeta iz prethodnog istraživanja autora Gupta i Dhami (2015)[70]. Također se istraživalo kada koriste društvene mreže te na kojim uređajima ih najčešće koriste.

Druga skupina pitanja fokusirala se na percepciju opasnosti na društvenim mrežama. Istražuje se znaju li ispitanici prepoznati opasnost, jesu li ikada bili u situaciji napada na osobne podatke itd. Pitanja za ovu skupinu su preuzeta od prethodnog istraživanja autora Ishak, Sidi, Jabar, Mohd i dr. (2012).[71]

Treća skupina pitanja fokusira se na osjećaj sigurnosti na društvenim mrežama. Tu se otkriva jesu li ispitanicima jasne postavke privatnosti i sigurnosti, mogućnosti kontroliranja osobnih podataka te osjećaju li se ispitanici sigurnije ukoliko im se pruža veća opcija zaštite podataka. Pitanja iz ove skupine su preuzeta iz prethodnog istraživanja autora Wang, Liu, Zhou i dr. (2022).[72]

Četvrta skupina pitanja odnosi se na procjenu rizika. Postavljaju se pitanja poput „Mislim da su moji podaci zaštićeni dok dijelim osobne podatke na društvenim mrežama?“ ili „Smatram da sam dovoljno informiran/a o sigurnosnim prijetnjama na društvenim mrežama“ itd. Pitanja za ovu skupinu su preuzeta iz prethodnog istraživanja autora van Schaik, Jansen, Onibokun, Camp i Kusev (2018)[73].

Peta skupina pitanja se odnosi na edukaciju o sigurnosti. Svrha je saznati smatraju li ispitanici da je trenutna edukacija dovoljna ili bi li trebala biti dostupna svima i besplatna. Pitanja za ovu skupinu su preuzeta iz prethodnog istraživanja autora Marín, Carpenter, Tur i dr. (2022)[74].

[70] Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites, Journal of Direct, Data and Digital Marketing Practice, 17, str. 46.
[71] Ishak, I., Sidi, F., Jabar, M. A., Mohd Sani, N. F., Mustapha, A., & Supian, S. R. (2012). A Survey on Security Awareness among Social Networking Users in Malaysia, Australian Journal of Basic and Applied Sciences, 6(12), str. 24.
[72] Wang, Z., Liu, H., Zhou, L., i dr. (2022). Does Internet Use Affect Citizens' Perception of Social Safety? A Cross-Sectional Survey in China, Systems, 10(6), str. 11.
[73] Van Schaik, P., Jansen, J., Onibokun, J., i dr. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour, Computers in Human Behavior, 78, str. 80.
[74] Marín, V. I., Carpenter, J. P., Tur, G., i dr. (2022). Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers, Journal of Computers in Education, 28, str. 17.

5.3. Analiza rezultata

U nastavku slijedi prikaz rezultata istraživanja grafički i tabelarno.

Grafikon 1. prikazuje odgovor na pitanje "Jeste li korisnik društvenih mreža?". Prvo pitanje je ujedno i eliminacijsko pitanje jer onemogućava ispunjavanje daljnje ankete ukoliko je odgovor na postavljeno pitanje bio "NE".

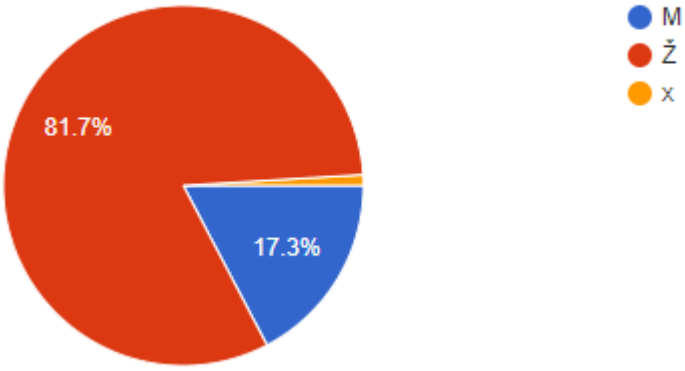
Grafikon 1. Korisnika sam društvenih mreža

Izvor: Vlastita izrada autora

Na postavljeno pitanje svi su ispitanici odgovorili potvrdno, tako da su sve ankete uzete u obzir prilikom obrade rezultata. Ukupno je obrađeno 104 anketna upitnika.

U slijedećem grafikonu prikazuje se spolna struktura ispitanika.

Grafikon 2. Spol ispitanika

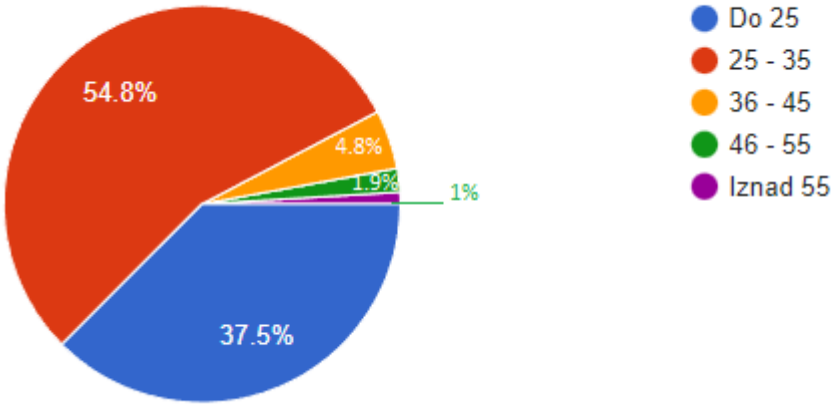


Izvor: Vlastita izrada autora

Iz grafikona 2 je vidljivo kako veliki broj ispitanika, odnosno 81,7%, čine žene, a 17,3% muškarci. Mali postotak od 0,9% ispitanika nije se izjasnio na ovo pitanje. Zaključak je da je većina ispitanika bila ženske populacije.

U sljedećem grafikonu prikazana je dob ispitanika po skupinama.

Grafikon 3. Dobna skupina ispitanika

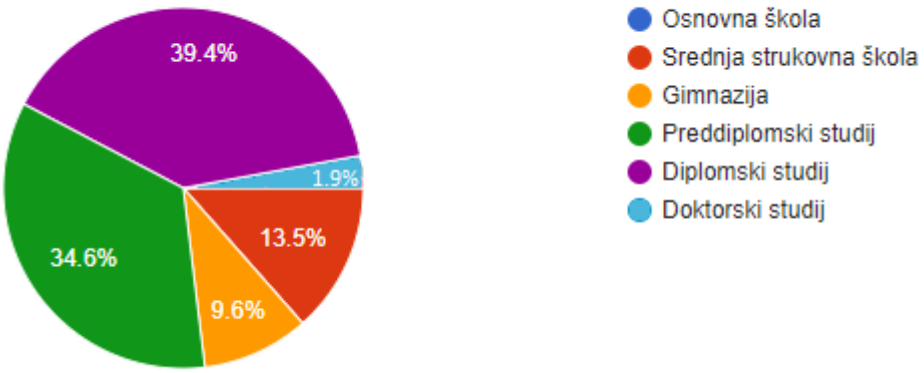


Izvor: Vlastita izrada autora

Iz grafikona 3 vidljivo je kako najveći broj ispitanika anketnog upitnika čine ispitanici u dobi od 25-35 godina, njih 54,8%, ispitanika u dobi do 25 godina je 37,5% te potom 4,8% ispitanika u dobi od 36-45 godina. Ispitanika u dobi od 46-55 godina je 1,9%. Najmanje ispitanika je u dobi iznad 55 godina, svega 0,9%.

U nastavku je prikazan stupanj obrazovanja ispitanika.

Grafikon 4. Stupanj obrazovanja

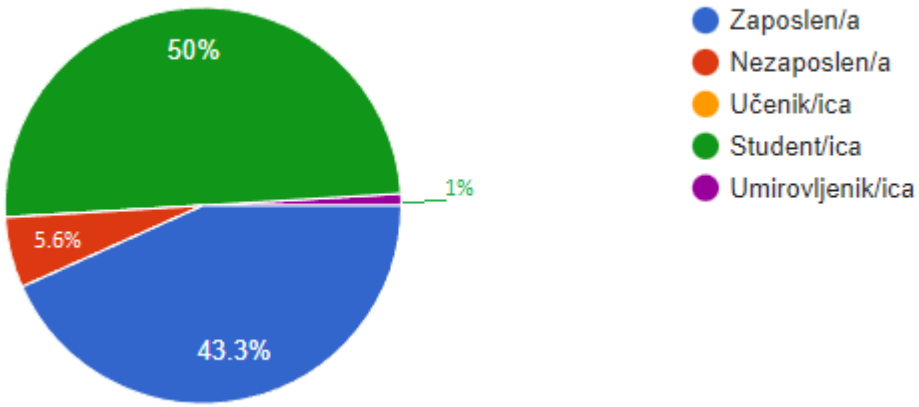


Izvor: Vlastita izrada autora

Iz grafikona 4 vidljivo je kako je najveći broj ispitanika završilo diplomski studij, njih 39.4% zatim njih 34.6% završilo je preddiplomski studij, 13.5% ispitanika završilo je srednju strukovnu školu, 9.6% ispitanika završilo je gimnaziju, a najmanje je onih ispitanika s završenim doktorskim studijem, njih 1.9%. Niti jedan ispitanik nije završio samo osnovnu školu.

Slijedi grafikon 5 koji prikazuje radni status ispitanika.

Grafikon 5. Stupanj obrazovanja

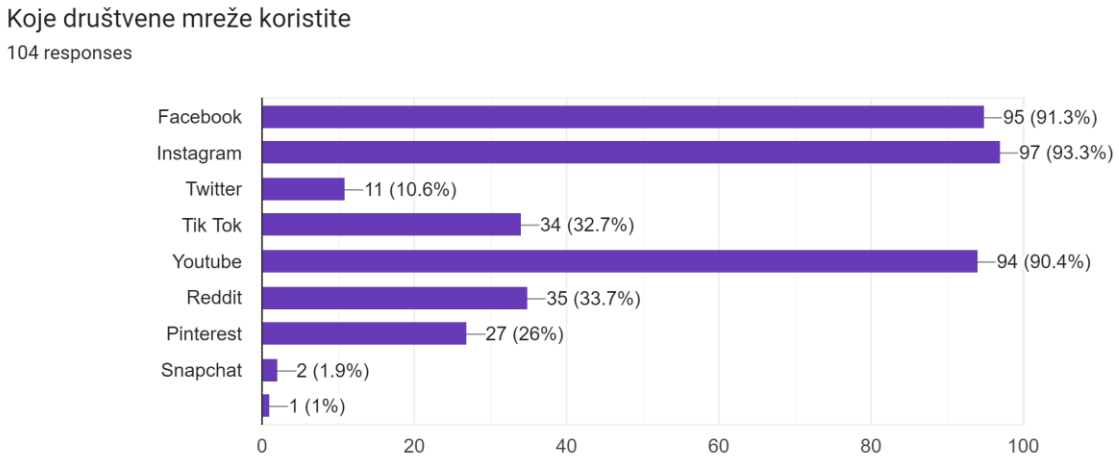


Izvor: Vlastita izrada autora

Iz prethodnog grafikona vidljivo je kako je najveći broj ispitanika studentske populacije, njih 50 %, 43,3% ispitanika je zaposleno, dok je 5.6% ispitanika izjavilo da su nezaposleni. Najmanje ispitanika, njih 1%, čine umirovljenici, dok učenika nije bilo u ispitivanju.

U nastavku su prikazane vrste društvenih mreža koje ispitanici koriste.

Grafikon 6. Koje društvene mreže koristite

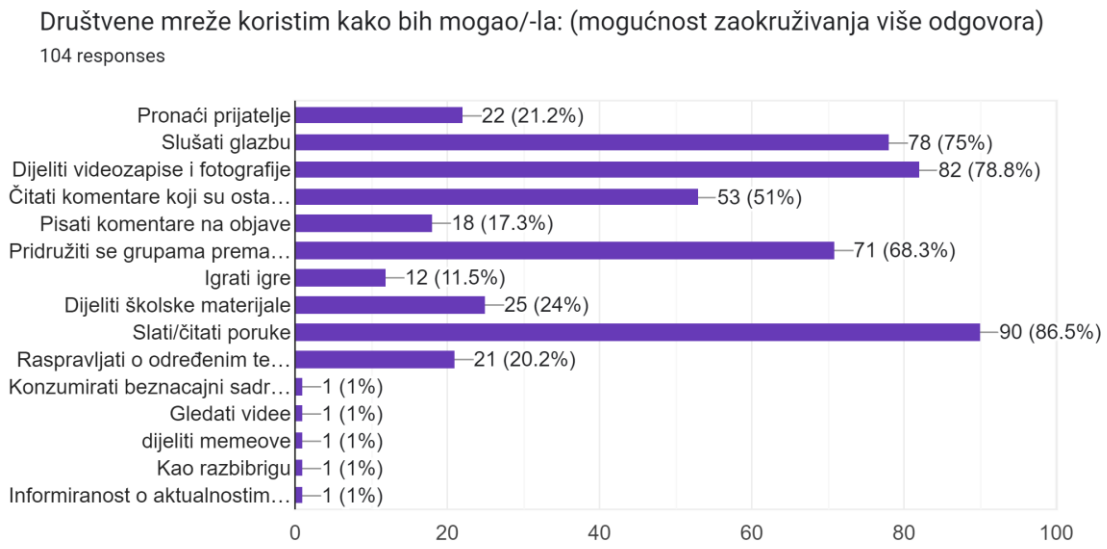


Izvor: Vlastita izrada autora

Grafikon 6 prikazuje pitanje „Koje društvene mreže koristite“ te su ponuđeni odgovori: Facebook, Instagram, Twitter, Tik Tok, YouTube, Reddit, Pinterest, Snapchat i pod ostalo je jedan ispitanik napisao odgovor LinkedIn. Možemo zaključiti kako većina ispitanika koristi Instagram (čak 93.3% korištenja). Drugo mjesto zauzima Facebook koji koristi 91.3% ispitanika, nakon njega YouTube sa 90.4% učestalosti. U ovom pitanju najčešća kombinacija odgovora bila je Facebook, Instagram i YouTube koje je odabralo čak 25 ispitanika. Druga kombinacija, sa 12 ispitanika, bila je Facebook, Instagram, YouTube i Reddit što ukazuje na veće korištenje Reddit-a koji je četvrti po učestalosti korištenja. Posljednje mjesto ima društvena mreža Snapchat koju koristi svega 1.9% ispitanika.

U nastavku su prikazani razlozi korištenja društvenih mreža.

Grafikon 7. Društvene mreže koristim kako bih mogao/-la



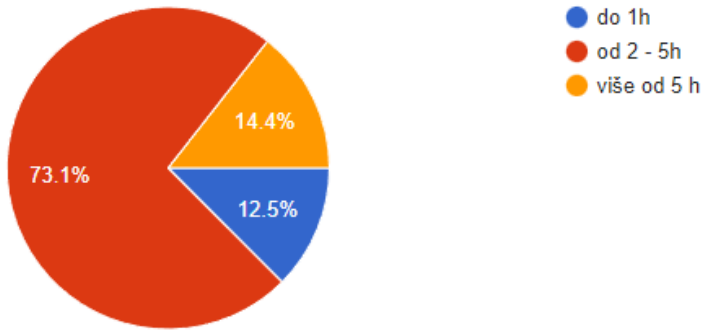
Izvor: Vlastita izrada autora

Na pitanje „Društvene mreže koristim kako bih mogao/la...“ ispitanici su odgovorili navođenjem razloga zbog kojih najčešće koriste društvene mreže. Neki od odgovora su: pronaći prijatelje, dijeliti videozapise i fotografije, slati/čitati poruke, slušati glazbu itd. Najčešći odgovor kojeg su ispitanici odabrali je „Slati/čitati poruke“ (86.5%). Navedeno objašnjava glavni razlog korištenja društvenih mreža, a to je komunikacija s drugima. Drugi najčešći razlog je „Dijeliti videozapise i fotografije“ (78.8%) dok je treći razlog „Slušati glazbu“ (75,0%).

Četvrti razlog je također čest „Pridružiti se grupama prema interesu“ (68,3%). Također, 51,0% ispitanika koristi društvene mreže za čitanje komentara, dok 24,0% ispitanika na taj način dijeli nastavne materijale. Otvoreni odgovori korištenja društvenih mreža su: informiranje o aktualnim temama (1,0%), gledanje video zapisa (1,0%), dijeljenje memova (1,0%), konzumiranje beznačajnog sadržaja (1,0%) i korištenje društvenih mreža za razbibrigu (1,0%).

U sljedećem pitanju „Koliko vremenski provedete sati u danu na društvenim mrežama“ ponuđeni odgovori su bili: provode li ispitanici manje od jedan sat, između dva i pet sati ili više od pet sati u danu na društvenim mrežama.

Grafikon 8. Koliko vremenski provedete sati u danu na društvenim mrežama?

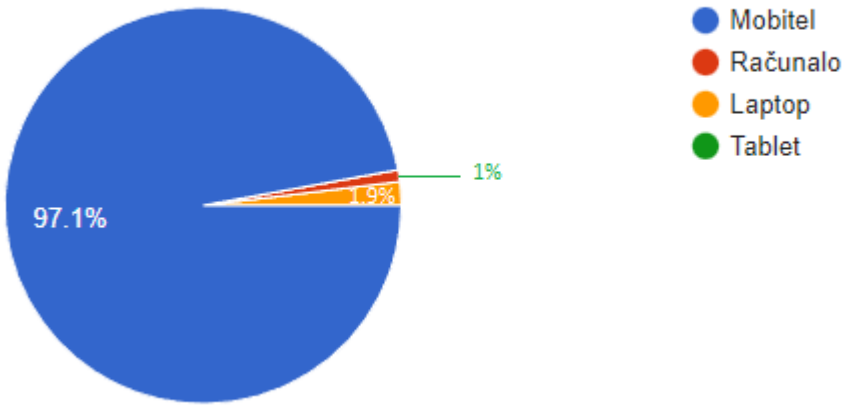


Izvor: Vlastita izrada autora

Iz grafikona 8 može se zaključiti kako većina ispitanika koristi društvene mreže između dva i pet sati dnevno (73,1%), dok je 14,4% ispitanika odgovorilo da koriste društvene mreže više od pet sati dnevno. Najmanji broj ispitanika (12,5%) koristi društvene mreže do jednog sata dnevno.

Slijedeći grafikon prikazuje koji uređaj ispitanici koriste za povezivanje na društvene mreže.

Grafikon 9. Za korištenje društvenih mreža najčešće koristim

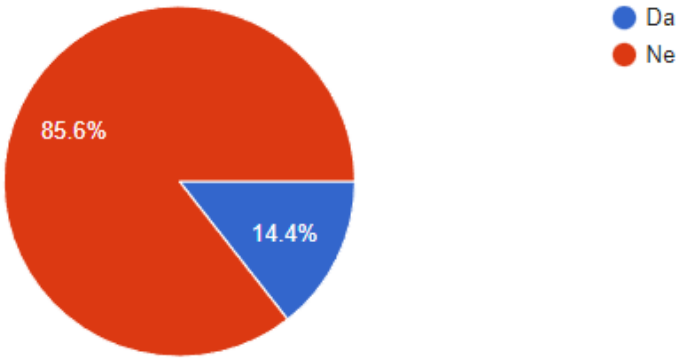


Izvor: Vlastita izrada autora

Grafikon 9 prikazuje odgovore na pitanje „Za korištenje društvenih mreža najčešće koristim...?“ te su ponuđeni odgovori: Mobitel, Računalo, Laptop i Tablet. Najveći broj ispitanika je odgovorio kako za korištenje društvenih mreža upotrebljava mobitel (97.1%). Neznatan broj ispitanika za korištenje društvenih mreža koristi stolno računalo (1%) i laptop (1.9%), a nitko od ispitanika ne upotrebljava tablet kako bi pristupio društvenim mrežama.

Sljedeći grafikon prikazuje odgovore na pitanje jesu li ispitanici doživjeli krađu identiteta ili bilo kakvu zloupotrebu osobnih podataka na društvenim mrežama.

Grafikon 10. Doživio sam krađu identiteta ili zloupotrebu osobnih podataka na društvenim mrežama.

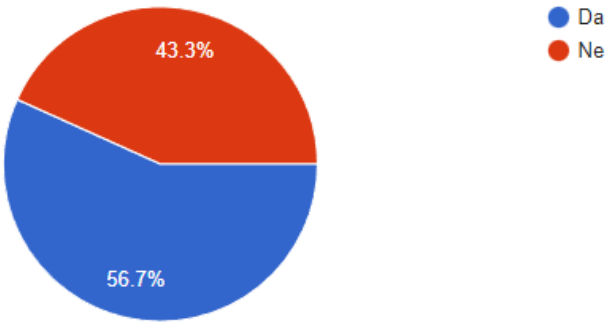


Izvor: Vlastita izrada autora

Na ovo pitanje je 85,6% ispitanika odgovorilo pozitivno, što znači da su doživjeli krađu identiteta ili zloupotrebu osobnih podataka na društvenim mrežama. Svega 14.4% ispitanika nikada nije doživljelo ovu vrstu zloupotrebe na društvenim mrežama.

Na sljedećem grafikonu prikazani su odgovori na pitanje jesu li su ispitanici upoznati sa praksama zaštite osobnih podataka na društvenim mrežama.

Grafikon 11. Upoznat/a s praksama zaštite osobnih podataka na društvenim mrežama.

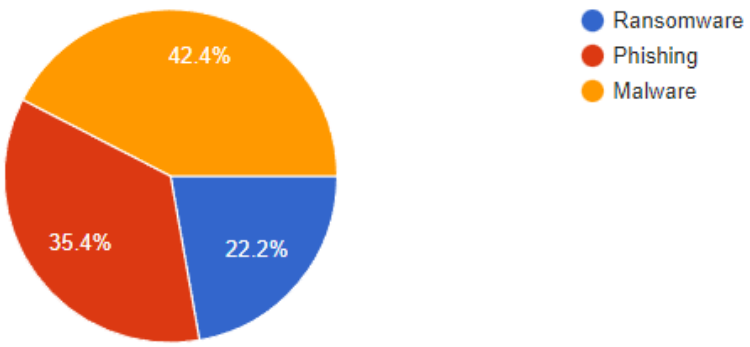


Izvor: Vlastita izrada autora

Iz gore prikazanog grafikona vidljivo je kako veći broj ispitanika (56,7%) na izjavu „Upoznat/a s praksama zaštite osobnih podataka na društvenim mrežama.“ odgovara potvrdno. 43,3% ispitanika odgovorilo je negativno, odnosno da nije upoznato s praksama zaštite osobnih podataka na društvenim mrežama.

Slijedi pitanje „Koje vrste prijetnji sigurnosti smatrate najvećim rizikom na društvenim mrežama?“ u kojemu ispitanici imaju mogućnost odgovora: Ransomware, Phishing ili Malware.

Grafikon 12. Koje vrste prijetnji sigurnosti smatrate najvećim rizikom na društvenim mrežama?



Izvor: Vlastita izrada autora

S obzirom na prikazane podatke u grafikonu 12, može se zaključiti kako ispitanici smatraju da je Malware najveća prijetnja sigurnosti tj. da je najveći rizik na društvenim mrežama (42,4%). Phishing kao vrstu prijetnje odabralo je 35,4% ispitanika, dok je najmanji broj ispitanika (22,2%) odabralo Ransomware kao najopasniju prijetnju na društvenim mrežama.

Ovaj grafikon prikazuje odgovor da istraživačko pitanje **IP1:** „Koje su najčešće vrste prijetnji i napada na društvenim mrežama?“, stoga se može zaključiti kako ispitanici smatraju da je najveća prijetnja Malware potom Phishing te na kraju Ransomware. Istovremeno, niti jedna prijetnja se ne ističe kao dominantna, stoga se može zaključiti kako su sve tri prijetnje učestale i prepoznatljive.

U nastavku su prikazani stavovi ispitanika mjereni tvrdnjama na koje su ispitanici odgovarali putem Likertove ljestvice za mjerenje stavova gdje je 1 označavao “u potpunosti se ne slažem”, a 5 “u potpunosti se slažem”. Prikazani rezultati izračunati su aritmetičkom sredinom i standardnom devijacijom za svaku tvrdnju u anketnom upitniku.

U sljedećem pitanju fokus je na sigurnosti dijeljenja osobnih podataka na društvenim mrežama.

Tablica 1. Društvene mreže

Društvene mreže	AS	SD
Osjećam se sigurno pri dijeljenju osobnih podataka na društvenim mrežama	2.63	1.14
Svoje osobne podatke smatram osjetljivim sadržajem na društvenim mrežama.	3.92	1.10
Ukupna prosječna oscjena	**3.28**	**1.29**

Izvor: Vlastita izrada autora

Prema tablici 1 vidljivo je kako se prosječna vrijednost slaganja ispitanika s tvrdnjama vezanim za percipiranje društvenih mreža kreće od 2.63 do 3.92. Tvrdnja s kojom se ispitanici najviše slažu jest tvrdnja da su osobni podaci osjetljivi sadržaj na društvenim mrežama (3.92) dok je manje slaganje s tvrdnjom o osjećaju sigurnosti pri dijeljenju osobnih podataka na društvenim mrežama (2.63). Vrijednosti standardne devijacije za sve tvrdnje su veće od 1, što pokazuje veću raspršenost od aritmetičke sredine.

U idućoj tablici prikazani su stavovi ispitanika o percipiranoj sigurnosti na društvenim mrežama

Tablica 2. Stavovi ispitanika o sigurnosti na društvenim mrežama

Sigurnost na društvenim mrežama	AS	SD
Jasne su mi postavke privatnosti i sigurnosti na društvenim mrežama.	3.22	1.06
Važna mi je mogućnost kontroliranja pristupa svojim osobnim podacima na društvenim mrežama.	4.47	0.81
Osjećam se sigurnije na društvenim mrežama koje pružaju više opcija zaštite osobnih podataka.	4.28	0.87
Bitna mi je transparentnost društvenih mreža u vezi s njihovim postupanjem s mojim osobnim podacima.	2.70	0.79
Ukupna prosječna ocjena	4.10	1.02

Izvor: Vlastita izrada autora

Temeljem tablice 2 vidljivo je kako se prosječna vrijednost slaganja ispitanika s tvrdnjama vezanim za percipiranu sigurnost na društvenim mrežama kreće u rasponu između 2,70 do 4,47. Tvrdnje s kojima se ispitanici najviše slažu jesu tvrdnja o mogućnosti kontroliranja pristupa osobnim podacima na društvenim mrežama (4,47) te tvrdnja o postojanju više opcija zaštite osobnih podataka na društvenim mrežama (4.28). Najniže slaganje ispitanika je s tvrdnjom o osjećaju sigurnosti kada je riječ transparentnosti društvenim mreža u vezi s njihovim postupanjem s osobnim podacima i iznosi 2,70. Vrijednosti standardne devijacije za tri varijable su manje od 1, te pokazuju manju raspršenost od aritmetičke sredine, dok je jedna varijabla veća od jedan te ukazuje na veću raspršenost od aritmetičke sredine.

Ova tablica također donosi odgovor na istraživačko pitanje **IP2.** "Kakvi su stavovi korisnika društvenih mreža o sigurnosti?" prema kojoj se zaključuje kako su stavovi ispitanika u skladu s brigom o svojoj sigurnosti na društvenim mrežama, no nije im toliko bitna transparentnost društvenih mreža prilikom korištenja njihovih podataka.

U sljedećoj tablici prikazani su stavovi ispitanika o dijeljenju podataka na društvenim mrežama

Tablica 3. Stavovi ispitanika o djeljenju podataka na društvenim mrežama

Djeljenje podataka	**AS**	**SD**
Mislim da su moji podaci zaštićeni dok dijelim osobne podatke na društvenim mrežama?	2.48	1.00
Smatram da sam dovoljno informiran/a o sigurnosnim prijetnjama na društvenim mrežama	2.87	1.07
Vjerujem vlastitim sposobnostima procjene rizika od sigurnosnih prijetnji na društvenim mrežama.	3.40	0.85
Dostupna su mi sredstva ili resursi za poboljšanje sigurnosti pri dijeljenju osobnih podataka na društvenim mrežama.	3.01	1.01
Osjećam se samopouzdano u vezi s odlukama koje donosim o dijeljenju osobnih podataka na društvenim mrežama.	3.49	0.89
Ukupna prosječna ocjena	3.05	1.04

Izvor: Vlastita izrada autora

Temeljem tablice 3 vidljivo je kako se prosječna vrijednost slaganja ispitanika s tvrdnjama vezanim za dijeljenje podataka na društvenim mrežama kreće u rasponu od 2.48 do 3.49. Tvrdnje s kojima se ispitanici najviše slažu jesu tvrdnja o samopouzdanju u vezi s odlukama koje donose o dijeljenju osobnih podataka na društvenim mrežama (3.49) te tvrdnja o sposobnostima procjene rizika od sigurnosnih prijetnji na društvenim mrežama (3.40). Najmanje slaganje ispitanika s tvrdnjama su tvrdnja o zaštićenim podacima (2.48) te tvrdnja o dovoljnom informiranju o sigurnosnim prijetnjama na društvenim mrežama (2.87). Vrijednost standardne devijacije za četiri varijable iznosi više od jedan te ukazuje na veću raspršenost od aritmetičke sredine, dok dvije varijable imaju manje od jedan što označava manju raspršenost od aritmetičke sredine.

Ova tablica odgovara na istraživačko pitanje **IP3**, „Kakvi su stavovi korisnika društvenim mreža o dijeljenju podataka?“ u kojem se saznaje kako su stavovi korisnika prilično snažni te se većina osjeća samopouzdano u vezi odluka koje donose dok dijele svoje podatke. Također, ispitanici vjeruju vlastitim sposobnostima prilikom procjene rizika na društvenim mrežama.

U sljedećoj tablici prikazani su stavovi o educiranju korisnika na društvenim mrežama.

Tablica 4. Educiranje korisnika

Educiranje korisnika	**AS**	**SD**
Smatram kako bi svaki korisnik društvene mreže trebao proći edukaciju o sigurnosti.	4.20	0.89
Smatram da je trenutna edukacija o sigurnosti na društvenim mrežama dovoljna.	2.42	0.88
Smatram da bi korisnici pažljivije koristili svoje podatke nakon edukacije o sigurnosti.	4.21	0.80
Smatram kako bi edukacija o sigurnosti trebala biti besplatna i obavezna svima.	4.52	0.71
Ukupna prosječna ocjena	3.79	1.22

Izvor: Vlastita izrada autora

Na temelju tablice 4, može se uočiti kako se prosječne vrijednosti odgovora ispitanika na tvrdnje vezane uz edukaciju korisnika o sigurnosti na društvenim mrežama kreću u rasponu od 2.42 do 4.52. Ispitanici se najviše slažu s tvrdnjom da bi svaki korisnik društvene mreže trebao proći edukaciju o sigurnosti (4.20) te da edukacija o sigurnosti treba biti besplatna i obavezna za sve (4.52). S druge strane, najmanje slaganje ispitanika zabilježeno je kod tvrdnje da je trenutna edukacija o sigurnosti na društvenim mrežama dovoljna (2.42).

Sve varijable standardne devijacije imaju manju vrijednost od jedan što znači da imaju manju raspršenost od aritmetičke sredine.

Prema ovoj tablici, kao odgovor na istraživačko pitanje **IP4**: „Kakvi su stavovi korisnika društvenih mreža o potrebi za edukacijom o sigurnosti?“ zaključuje se kako su stavovi ispitanika prema educiranju korisnika društvenih mreža izrazito pozitivno usmjereni. Ispitanici smatraju kako bi trebali biti educirani te da trenutna edukacija nije dovoljno snažna. Također smatraju kako bi edukacija trebala biti besplatna i obavezna svima.

5.4. Rasprava

Ovo istraživanje iznašlo je odgovore na sva istraživačka pitanja koja su prethodno postavljena. U nastavku slijedi detaljnija rasprava.

Ispitanici najčešće koriste društvene mreže kako bi komunicirali, najviše koriste društvene mreže poput Facebooka, Instagrama i YouTubea. Vremenski period koji provedu na društvenim mrežama obuhvaća najčešće od 2 do 5 sati dnevno te im je gotovo uvijek mobitel glavni uređaj na kojem koriste društvene mreže. U prosjeku se osjećaju sigurno dok dijele osobne podatke na društvenim mrežama te smatraju svoje osobne podatke osjetljivim sadržajem. Većina ispitanika doživjela je krađu identiteta ili zloupotrebu osobnih podataka na društvenim mrežama, dok je broj ispitanika upoznat s praksama zaštite osobnih podataka na društvenim mrežama gotovo jednak broju onih koji s istima nisu upoznati. Ispitanici u podjednakoj mjeri procjenjuju veličinu rizika Ransomware-a, Phishing-a i Malware-a na društvenim mrežama, iako je malo veći

postotak ipak naglasio Malware kao najveću prijetnju. Nadalje, ispitanicima su jasne postavke privatnosti i sigurnosti na društvenim mrežama.

Većina korisnika zabrinuta je za svoju privatnost, za koju smatraju da je ugrožena više nego ikad napretkom tehnologije. Zanimljivo je da korisnici nemaju saznanja o postojanju višestrukih pohrana njihovih osobnih podataka, ne znaju tko im može pristupiti te kako se takve informacije koriste. Nedostatak svijesti o tome koje se informacije o korisnicima pohranjuju, i na koji način, navela je mnoge korisnike da preispitaju Facebookov pristup privatnosti.[75]

Svima je važna mogućnost kontroliranja pristupa svojim osobnim podacima na društvenim mrežama te se svi osjećaju sigurnije na društvenim mrežama koje pružaju više opcija zaštite osobnih podataka. Također je svima bitna transparentnost društvenih mreža u vezi s njihovim postupanjem osobnih podataka. Ispitanici se malo manje poistovjećuju sa izjavom da su im podaci zaštićeni dok ih dijele na društvenim mrežama te također ocjenom 3 označuju kako su prosječno informirani o sigurnosnim prijetnjama na društvenim mrežama. Većina vjeruje vlastitim sposobnostima procjene rizika od sigurnosnih prijetnji na društvenim mrežama. Niti se ne slažu niti se slažu sa izjavom da su im dostupna sredstva ili resursi za poboljšanje sigurnosti pri dijeljenju osobnih podataka. Ispitanici se većinom osjećaju samopouzdano u vezi s odlukama koje donose o dijeljenju osobnih podataka. Većina ispitanika također smatra kako bi svi korisnici društvenih mreža trebali proći edukaciju o sigurnosti te smatraju kako trenutna edukacija nije dovoljna.

Većina ispitanika smatra kako bi korisnici pažljivije koristiti svoje podatke nakon edukacije o sigurnosti te smatraju kako bi edukacija o sigurnosti trebala biti besplatna i obavezna svima.

Također, zanimljivo dodatno pitanje koje je bilo postavljeno glasilo je „Od kojeg razreda osnovne škole bi trebali uvesti edukaciju o sigurnosti?“. Prosječni odgovor na ovo pitanje bio je od petog razreda osnovne škole.

[75] Nyoni, P., & Velempini, M. (2015, July 10). Data protection laws and privacy on Facebook. SA Journal of Information Management, 17(1).

5.5. Ograničenja i preporuka za buduća istraživanja

Važno je prepoznati kako ova studija može imati neka ograničenja. Prvo, istraživanje je primarno usredotočeno na popularne platforme društvenih medija, kao što su Facebook, Twitter, TikTok i YouTube, ali postoje brojne druge platforme koje mogu predstavljati jedinstvene sigurnosne rizike. Buduće studije mogle bi istražiti širi raspon platformi kako bi se dobila sveobuhvatnija perspektiva. Drugo, istraživanje je prvenstveno ispitivalo tehničke aspekte sigurnosti i privatnosti podataka, zanemarujući društvene i psihološke čimbenike koji mogu utjecati na ponašanje i donošenje odluka korisnika. Uključivanje multidisciplinarnog pristupa koji uzima u obzir ljudski element omogućilo bi dragocjene uvide u stavove, percepcije i ponašanja korisnika u vezi s privatnošću podataka.

Za buduća istraživanja preporuča se dublje proučavanje novih prijetnji i ranjivosti koje su specifične za platforme društvenih medija. To bi moglo uključivati istraživanje utjecaja tehnologija u razvoju, kao što su umjetna inteligencija, blockchain ili decentralizirane platforme na sigurnost i privatnost podataka.

Nadalje, istraživanje učinkovitosti postojećih regulatornih okvira i politika u zaštiti korisničkih podataka na platformama društvenih medija pružilo bi vrijedne uvide kreatorima politika i dionicima. Osim toga, istraživanje bi se trebalo usredotočiti na razvoj i procjenu intervencija usmjerenih na korisnika te na obrazovne programe s ciljem poboljšanja svijesti korisnika, njihovog znanje i ponašanja u vezi s privatnošću i sigurnošću. Na kraju, istraživanja koje prate razvoj sigurnosti i privatnosti podataka na društvenim medijima kroz duža vremenska razdoblja, s vremenom bi ponudile nijansiranije razumijevanje izazova i omogućile procjenu učinkovitosti provedenih mjera. Rješavanjem ovih ograničenja i slijedeći ove preporuke, buduća istraživanja mogu doprinijeti razvoju robusnijih i učinkovitijih strategija za osiguranje sigurnosti i privatnosti podataka na platformama društvenih medija.

Zaključak

Društvene mreže ukorijenile su se u svakodnevni život. Počevši od dijeljenja teksta, slika i poruka, mnogi su ljudi napredovali do dijeljenja šala, glazbe i videa u domeni zabave, upitnika, zadataka i radionica u domeni obrazovanja, kao i dijeljenja najnovijih vijesti i slika u medijskoj domeni. Pri korištenju društvenih mreže za razmjenu informacija, potrebno je pripaziti na sigurnost i privatnost osobnih podataka. Podaci o korisnicima trebaju biti privatni i ne smiju se dijeliti. Platforme društvenih medija i dalje se suočavaju s istim problemima kao i internetske platforme općenito, u smislu izazova prilikom osiguravanja integriteta podataka, povjerljivosti i pristupačnosti. Temeljni problemi sa zaštitom osobnih podataka - kao što su osiguravanje privatnosti, sprječavanje neželjenog pristupa i održavanje integriteta podataka - nisu adekvatno riješeni unatoč usponu platformi društvenih medija. Korisnici društvenih medija još uvijek nemaju dovoljno znanja i razumijevanja prijetnji njihovoj privatnosti i bitnih sigurnosnih mjera opreza za zaštitu svojih osobnih podataka.

Ovaj rad je istražio temu sigurnosti i privatnosti podataka u kontekstu platformi društvenih mreža. Kroz ispitivanje različitih platformi kao što su Facebook, Twitter, TikTok i YouTube, postalo je očito da izazovi povezani sa zaštitom osobnih podataka i dalje postoje. Proliferacija zlonamjernih aktivnosti, poput krađe identiteta i napada Ransomwarea, dodatno pogoršava rizike s kojima se suočavaju korisnici društvenih medija. Poglavlje o krađama na internetu služi kao oštri podsjetnik na moguće posljedice koje proizlaze iz iskorištavanja i zlouporabe osobnih podataka. Krađa identiteta, financijska prijevara, narušavanje nečijeg ugleda i drugi negativni učinci rezultat su nezakonitog pristupa i zlonamjerne upotrebe tuđih podataka.

Sudionici ispitivanja uglavnom koriste društvene mreže za komunikaciju, a najčešće se koriste Facebook, Instagram i YouTube. Na društvenim mrežama provodi se u prosjeku 2-5 sati dnevno, prvenstveno koristeći mobitele. Ispitanici se osjećaju umjereno sigurnima kada dijele osobne podatke na društvenim mrežama i smatraju ih osjetljivim sadržajem. Većina ispitanika je doživjela krađu identiteta ili zlouporabu osobnih podataka na društvenim mrežama, dok je otprilike polovica ispitanika upoznata s praksama zaštite podataka, a ostali nisu. Svi ispitanici podjednako percipiraju Ransomware, Phishing i Malware kao najveće rizike na društvenim mrežama, iako nešto veći postotak odabire Malware. Većina korisnika zabrinuta je za svoju

privatnost, smatrajući da je zbog napretka tehnologije ugroženija više nego ikad. Većina sudionika smatra da bi korisnici nakon sigurnosne edukacije bili oprezniji sa svojim podacima te smatraju da bi sigurnosna edukacija trebala biti besplatna i obvezna za sve. Zanimljivo je dopunsko pitanje u kojem bi razredu trebalo uvesti sigurnosno obrazovanje, a prosječni odgovor bio je peti razred osnovne škole.

Očito je da postoje brojni i složeni problemi sa sigurnošću i privatnošću podataka na društvenih medija. Problemi se ne mogu riješiti oslanjajući se isključivo na važeće zakone ili inicijative za edukaciju korisnika. Zanimljivo je da korisnici nemaju svijest o višestrukim pohranama podataka, tko im može pristupiti te kako se informacije koriste. Oni također nemaju kontrolu nad tim pohranama podataka. Kontrola nad pristupom osobnim podacima na društvenim mrežama svima je važna, a osjećaju se sigurnije na platformama koje nude više mogućnosti zaštite podataka. Transparentnost u pogledu načina na koji društvene mreže postupaju s osobnim podacima vrlo je važna. Ispitanici su manje sigurni u sigurnost svojih dijeljenih podataka i svoje znanje o sigurnosnim prijetnjama na društvenim mrežama ocjenjuju prosječnom razinom. Većina vjeruje u svoju sposobnost procjene sigurnosnih rizika na društvenim mrežama. Ispitanici se niti slažu niti ne slažu s tvrdnjom da imaju sredstva ili resurse za poboljšanje sigurnosti podataka. Sudionici se općenito osjećaju sigurnima u odluke o dijeljenju osobnih podataka. Također smatraju da bi svi korisnici društvenih mreža trebali proći sigurnosnu edukaciju i smatraju da je trenutna edukacija nedovoljna.

Korisnici, direktori platforma i zakonodavstvo moraju zajedno raditi na osmišljavanju temeljitih rješenja za uklanjanje ovih problema. Da bi se to postiglo, moraju se uspostaviti jake sigurnosne mjere, pravila o privatnosti moraju biti često ažurirana, mora se promicati svijest i edukacija korisnika te se mora njegovati kultura odgovornog rukovanja i dijeljenja podataka.

Bibliografija

Alias, N., Razak, S. H. A., elHadad, G., Kunjambu, N. R. M. N. K. & Muniandy, P. (2013). A Content Analysis in the Studies of YouTube in Selected Journals, Procedia - Social and Behavioral Sciences, 103, 10-18.

Ashutosh Chitwadgi, A. H., Hosseini, A., & Chitwadgi, A. (2021). Phishing Trends With PDF Files, Unit 42. https://unit42.paloaltonetworks.com/phishing-trends-with-pdf-files/ (Pristupljeno: 15.6.2023.)

Biggest Data Breaches in History, Top 6 Breaches in U.S. (n.d.). Consumer Notice, LLC. https://www.consumernotice.org/data-protection/breaches/biggest-in-history/

(Pristupljeno: 15.6.2023.)

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks, International Journal of Computer Applications, 182(33), 27-29.

Boyd, D. M., Ellison, N. B. (2007). Social Network Sites: Definition, History and Scholarship, Journal of Computer-Mediated Communication, 13(1), 210-230.

Bowler, J. (2019). YouTube Community Posts: The new tool for creators, Printsome Insights https://blog.printsome.com/youtube-community-posts/ (Pristupljeno: 26.5.2023.)

Chen, J., Xu, H. & Whinston, A.B. (2011). Moderated online communities and quality of user-generated content, Journal of Management Information Systems, 28(2), 237-268.

Dangerous Email Attachments: *What You Need To Know To Stay Safe* (2023). | *Phriendly Phishing Blog.* Phriendly Phishing. https://www.phriendlyphishing.com/blog/dangerous-email-attachments (Pristupljeno: 16.6.2023)

Danowitz, E. S. (2018). The SAGE International Encyclopedia of Travel and Tourism, Reference Reviews, 32(3), 29-30.

Denning, P., & Lewis, T. (2019). Intelligence May Not Be Computable, American Scientist, https://www.americanscientist.org/article/intelligence-may-not-be-computable (Pristupljeno: 25.5.2023.)

Dharmawan, N. K. S., Kasih, D. P. D., i Stiawan, D. (2019). Personal data protection and liability of internet service provider: a comparative approach, International Journal of Electrical and Computer Engineering (IJECE), 9(4), 3175-3184.

Eberechukwu, E. (2022). Meta fined €265 million over Facebook data breach and scraping, Technex https://technext24.com/2022/11/28/meta-fined-e265-million-over-facebook-data/ Pristupljeno: (18.6.2023.)

Essential guide to the General Data Protection Regulation (GDPR). (2017). The Pharmaceutical Journal, https://pharmaceutical-journal.com/article/news/essential-guide-to-the-general-data-protection-regulation-gdpr (Pristupljeno: 20.5.2023.)

Fan, A., Wu, Q., Yan, X., i drugi., (2021). Research on Influencing Factors of Personal Information Disclosure Intention of Social Media in China. Data and Information Management, 5(1), 195-207.

Federal Trade Commission., Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (2019). https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law (Pristupljeno: 25.5.2023.)

Global top websites by monthly visits 2022 | Statista. (n.d.). Statista. https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/ (Pristupljeno: 10.6.2023.)

González-Pizarro, F., Figueroa, A., López, C., & Aragon, C. (2022). Regional Differences in Information Privacy Concerns After the Facebook-Cambridge Analytica Data Scandal, Computer Supported Cooperative Work, 31(1).

Grbavac, J. i Grbavac, V. (2014). Pojava društvenih mreža kao globalnog komunikacijskog fenomena, Media, culture and public relations, 5 (2), 206-219.

Grossman, M. M. (2023). 15 TikTok Facts and Stats to Know in 2023. yellowHEAD. https://www.yellowhead.com/blog/tiktok-facts-and-stats/ (Pristupljeno: 25.5.2023.)

Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites, Journal of Direct, Data and Digital Marketing Practice, 17, 43-53.

Hildebrandt, M. (2009). Who is profiling who? Invisible visibility, in: Protection, S. Gutwirth, Y. Poullet, P. De Hert, S. Nouwt, C. De Terwangne (eds), Reinventing Data Protection, Springer, Dordrecht, 239-252.

Humphreys, L., Phillipa, G., i Krishnamurthy, B. (2012). How much is too much? Privacy issues on Twitter, In: Conference of international communication association, Singapore 2010 Jun 21.

Intelligence, I. (n.d.). TikTok users worldwide & growth forecast https://www.insiderintelligence.com/charts/tiktok-users-worldwide-forecast/ (Pristupljeno: 29.4.2023)

Irwin, L. (2022). The 5 Biggest Phishing Scams of All Time - IT Governance Blog En, IT Governance Blog En., https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time (Pristupljeno: 13.6.2023.)

Ishak, I., Sidi, F., Jabar, M. A., Mohd Sani, N. F., Mustapha, A., & Supian, S. R. (2012). A Survey on Security Awareness among Social Networking Users in Malaysia, Australian Journal of Basic and Applied Sciences, 6(12), 23-29.

Juničić, K., (2021). *TikTok optužen da je ilegalno prikupljao podatke milijuna maloljetnika. Tvrtki prijeti golema kazna.* https://www.jutarnji.hr/life/tehnologija/tiktok-optuzen-da-je-ilegalno-prikupljao-podatke-milijuna-maloljetnika-tvrtki-prijeti-golema-kazna-15067204 (Pristupljeno: 1.9.2023)

List of data breaches - Wikipedia. (2019), List of Data Breaches – Wikipedia https://en.wikipedia.org/wiki/List_of_data_breaches (Pristupljeno: 14.6.2023.)

Maclean, F., Jones, D., Carin-Levy, G., & Hunter, H. (2013). Understanding Twitter, British Journal of Occupational Therapy, 76(6), 295-298.

Mansfield-Devine, S. (2008). Anti-social networking: Exploiting the trusting environment of Web 2.0, Network Security 11, 2-7.

Marín, V. I., Carpenter, J. P., Tur, G., i dr. (2022). Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers, Journal of Computers in Education, 28, 1-27.

Marune, A. E. M. S., i Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. International Journal of Business, Economics, and Social Development, 2(4), 143-152.

Mateeva, Z. (2020). Principles of personal data protection, Audit 2, 28. 95-104.

Merholz, P. (2002). Play with your words., peterme.com, http://www.peterme.com/archives/00000205.html (Pristupljeno: 25.4.2023)

Milmo, D. (2021). *Facebook and Instagram gathering browsing data from under-18s, study says. The Guardian.* https://www.theguardian.com/technology/2021/nov/16/facebook-and-instagram-gathering-browsing-data-from-under-18s-study-says (Pristupljeno: 26.8.2023.)

Mohd, H. (2023). CSCA0101 – Computer Basics, FTMS College https://ftms.edu.my/v2/current-student/foundation-student/csca0101-computing-basics/ (Pristupljeno: 15.6.2023)

Musiał, K., & Kazienko, P. (2012). Social networks on the Internet, World Wide Web, 16(1), 31-72.

Mujanović, A. (2023). *TikTok u 2022. ostvario najviše preuzimanja, Metine platforme zauzele čak tri mjesta među top 10.* https://lidermedia.hr/tehno/tiktok-u-2022-ostvario-najvise-preuzimanja-metine-platforme-zauzele-cak-tri-mjesta-medu-top-10-147958 (Pristupljeno: 6.8.2023.)

Nyoni, P., & Velempini, M. (2015). Data protection laws and privacy on Facebook, SA Journal of Information Management, 17(1). 1-10.

Petrauskas, K. (2019). What Are The Differences Between Social Media Platforms, KJP Creative, https://kjpcreative.com/what-are-the-differences-between-the-big-social-media-platforms/ (Pristupljeno: 15.6.2023.)

Phishing (2023). PHISHING | English Meaning – Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/phishing (Pristupljeno: 16.6.2023.).

Podobnik, V., Ackermann, D., Grubišić, T., & Lovrek, I. (2013). Web 2.0 as a Foundation for Social Media Marketing: Global Perspectives and the Local Case of Croatia.

Recenzija filma „The Social Dilemma" (2020). Kišobran. https://kisobran.uniri.hr/2020/12/08/recenzija-filma-the-social-dilemma/ Pristupljeno: (17.6.2023.)

Reuters. TikTok's lead EU regulator opens two data privacy probes. https://www.reuters.com/technology/ireland-regulator-opens-data-privacy-probes-into-tiktok-2021-09-14/ (Pristupljeno: 1.9.2023.)

Romansky, P. R., i Noninska, S.I. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), 5288–5303.

Schläpfer, P. (2022). PDF Malware Is Not Yet Dead, HP Wolf Security. https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/ (Pristupljeno: 10.6.2023.)

Senthil Kumar N, Saravanakumar K, & Deepa K. (2016). On Privacy and Security in Social Media – A Comprehensive Study, Procedia Computer Science, 78, 114-119.

Sfetcu, N. (2014). Small Business Management for Online Business – Web Development, Internet Marketing, Social Networks, 1-4.

Shepardson, D., (2023.). TikTok CEO: App has never shared US data with Chinese government, Reuters. https://www.reuters.com/technology/tiktok-ceo-app-has-never-shared-us-data-with-chinese-goverment-2023-03-22/ (Pristupljeno: 1.9.2023.)

The New York Times. "The Social Dilemma' Review: Unplug and Run., https://www.nytimes.com/2020/09/09/movies/the-social-dilemma-review.html (Pristupljeno: 15.6.2023.)

Topic: YouTube. (n.d.). Statista. https://www.statista.com/topics/2019/youtube/ (Pristupljeno: 16.6.2023.)

Tiktok, "About tiktok", https://www.tiktok.com/about?lang=en (Pristupljeno: 25.4.2023)

Twitter Revenue and Usage Statistics - *Business of Apps.* https://www.businessofapps.com/data/twitter-statistics/.com (Pristupljeno:10.9.2023.)

Van Schaik, P., Jansen, J., Onibokun, J., i dr. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour, Computers in Human Behavior, 78, 1-95.

Wallin, P. (2014). Punishment for Stealing Personal Information through Public WiFi. https://www.wklaw.com/stealing-personal-information-public-wifi/ (Pristupljeno: 17.6.2023)

Wang, Z., Liu, H., Zhou, L., i dr. (2022). Does Internet Use Affect Citizens' Perception of Social Safety? A Cross-Sectional Survey in China, Systems, 10(6), Str. 1-20.

What Is Ransomware and How Do You Prevent It? (2023). What Is Ransomware and How Do You Prevent It? https://www.antivirusguide.com/cybersecurity/ransomware/ (Pristupljeno: 13.6.2023.)

What Legally Constitutes Identity Theft? (2020), Newman & Allen https://www.newmanallen.com/blog/2020/october/what-legally-constitutes-identity-theft-/. (Pristupljeno: 17.6.2023.)

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. Future Generation Computer Systems, 86, str. 914-925.

Popis ilustracija

Popis Slika

Slika 1. Taksonomija internetskih odnosa 9

Popis Grafikona

Grafikon 1. Korisnika sam društvenih mreža 39
Grafikon 2. Spol ispitanika 40
Grafikon 3. Dobna skupina ispitanika 40
Grafikon 4. Stupanj obrazovanja 41
Grafikon 5. Stupanj obrazovanja 42
Grafikon 6. Koje društvene mreže koristite 42
Grafikon 7. Društvene mreže koristim kako bih mogao/-la 43
Grafikon 8. Koliko vremenski provedete sati u danu na društvenim mrežama? 44
Grafikon 9. Za korištenje društvenih mreža najčešće koristim 45
Grafikon 10. Doživio sam krađu identiteta ili zloupotrebu osobnih podataka na društvenim mrežama. 45
Grafikon 11. Upoznat/a s praksama zaštite osobnih podataka na društvenim mrežama. 46
Grafikon 12. Koje vrste prijetnji sigurnosti smatrate najvećim rizikom na društvenim mrežama? 47

Popis Tablica

Tablica 1. Društvene mreže 48
Tablica 2. Stavovi ispitanika o sigurnosti na društvenim mrežama 48
Tablica 3. Stavovi ispitanika o djeljenju podataka na društvenim mrežama 49
Tablica 4. Educiranje korisnika 50

Anketni upitnik

Korisnik sam društvenih mreža.

Da/Ne

Koje društvene mreže koristite

Facebook
Instagram
Twitter
Tik Tok
Youtube
Reddit
Pinterest
Other…

Društvene mreže koristim kako bih mogao/-la: (mogućnost zaokruživanja više odgovora)

Pronaći prijatelje
Slušati glazbu
Dijeliti videozapise i fotografije
Čitati komentare koji su ostavljeni kao odgovor na zajedničke objave
Pisati komentare na objave
Pridružiti se grupama prema interesu
Igrati igre
Dijeliti školske materijale
Slati/čitati poruke
Raspravljati o određenim temama
Other…

Koliko vremenski provedete sati u danu na društvenim mrežama?

do 1h
od 2 - 5h

više od 5 h

Za korištenje društvenih mreža najčešće koristim

Mobitel
Računalo
Laptop
Tablet

Osjećam se sigurno pri dijeljenju osobnih podataka na društvenim mrežama.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Svoje osobne podatke smatram osjetljivim sadržajem na društvenim mrežama.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Doživio sam kradu identiteta ili zloupotrebu osobnih podataka na društvenim mrežama.

Da
Ne

Upoznat/a s praksama zaštite osobnih podataka na društvenim mrežama.

Da
Ne

Koje vrste prijetnji sigurnosti smatrate najvećim rizikom na društvenim mrežama?

Ransomware
Phishing
Malware

Jasne su mi postavke privatnosti i sigurnosti na društvenim mrežama.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Važna mi je mogućnost kontroliranja pristupa svojim osobnim podacima na društvenim mrežama.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Osjećam se sigurnije na društvenim mrežama koje pružaju više opcija zaštite osobnih podataka.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Bitna mi je transparentnost društvenih mreža u vezi s njihovim postupanjem s mojim osobnim podacima.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Mislim da su moji podaci zaštićeno dok dijelim osobne podatke na društvenim mrežama?

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Smatram da sam dovoljno informiran/a o sigurnosnim prijetnjama na društvenim mrežama

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Vjerujem vlastitim sposobnostima procjene rizika od sigurnosnih prijetnji na društvenim mrežama.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Dostupna su mi sredstva ili resursi za poboljšanje sigurnosti pri dijeljenju osobnih podataka na društvenim mrežama.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Osjećam se samopouzdano u vezi s odlukama koje donosim o dijeljenju osobnih podataka na društvenim mrežama.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Smatram kako bi svaki korisnik društvene mreže trebao proći edukaciju o sigurnosti.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Smatram da je trenutna edukacija o sigurnosti na društvenim mrežama dovoljna.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Smatram da bi korisnici pažljivije koristili svoje podatke nakon edukacije o sigurnosti.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Smatram kako bi edukacija o sigurnosti trebala biti besplatna i obavezna svima.

Ne osjećam se nimalo sigurno 1 2 3 4 5 Osjećam se sasvim sigurno

Od kojeg razreda osnovne škole bi trebali uvesti edukaciju o sigurnosti?

Otvoreno pitanje_____

Socio-demografski podaci

Spol

M
Ž
Other…

Dob

Do 25
25 - 35
36 - 45
46 - 55
Iznad 55

Stupanj obrazovanja

Osnovna škola
Srednja strukovna škola
Gimnazija
Preddiplomski studij
Diplomski studij
Doktorski studij
Other…

Radni status

Zaposlen/a
Nezaposlen/a
Učenik/ica
Student/ica
Umirovljenik/ica