Zaštita privatnosti na društvenim mrežama

Bolšec, Lucija

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2020./2021.

Lucija Bolšec

Zaštita privatnosti na društvenim mrežama

Završni rad

Mentorica: dr. sc. Vjera Lopina

Zagreb, srpanj 2021.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj

1. Uvod

Kada se govori o pojmu privatnosti i pravu na privatnost, prve asocijacije su većinom povezane s privatnošću na internetu ili konkretnije na društvenim mrežama. Društvene mreže u današnjem modernom i tehnološki naprednom svijetu imaju veoma važnu ulogu za sve generacije. Postale su neizostavan dio ljudskih života te su omogućile laku i brzu komunikaciju između korisnika. Najčešće se koriste za upoznavanje novih ljudi, dijeljenje iskustava i znanja, ali i stjecanje novih. Osim toga, često služe i za zabavljanje i informiranje o zanimljivim temama i događanjima iz cijeloga svijeta.

Problem koji se tu javlja jest privatnost, odnosno zaštita privatnosti i osobnih podataka. U ovom završnom radu se raspravlja upravo o toj zaštiti privatnosti na društvenim mrežama. Na početku se definiraju dva pojma koja su usko povezana, a to su privatnost i osobni podaci. Zatim se skreće pažnja na Opću uredbu o zaštiti podataka (GDPR) i na Zakon o zaštiti osobnih podataka koji predstavljaju zakonske osnove kojima je regulirana zaštita privatnosti u Republici Hrvatskoj. Spominje se i pojam digitalnog otiska i IP-ja koji su važni za razumijevanje ove teme. Nakon toga se kratko izdvajaju najpopularnije društvene mreže, kao što su Facebook, WhatsApp, Instagram, YouTube, Snapchat . . . i Kemptovo istraživanje iz travnja 2021. godine koje pokazuje neku statistiku i teze vezane uz društvene mreže. Zatim se ističu najčešće prijetnje i napadi na privatnost korisnika na mrežama. Tu se izdvajaju Phishing, Spam, Hoax, Malware, a spominje se i krađa identiteta, gubitak podataka te dijeljenje neprikladnog sadržaja. Osmo poglavlje se bavi konkretno zaštitom osobnih podataka na društvenim mrežama – od korištenja jakih lozinki i redovitog održavanja računala, do otvaranja, odnosno neotvaranja različitih poveznica koje se nađu u inboxu i sandučiću elektroničke pošte korisnika te pravilima ponašanja i komunikacije na internetu i društvenim mrežama. Kao najpopularnija društvena mreža izdvaja se Facebook pa se kratko analiziraju mjere zaštite i postavke na toj društvenoj mreži, a vezano uz dijeljenje osobnih informacija. Na kraju se spominje Nacionalni CERT (CERT.hr) kao nacionalno tijelo u Hrvatskoj čija je zadaća prevencija i zaštita od ugrožavanja sigurnosti javnih informacijskih sustava. Zatim slijedi anketa na temu zaštite privatnosti na društvenim mrežama i analiza pitanja te dobivenih odgovora. Nakon toga slijedi zaključak ove teme, popis korištene literature te popis slika i kratki sažetak na hrvatskom i engleskom jeziku uz ključne riječi na kraju rada.

2. Pravo na privatnost i osobni podaci

Prema Hrvatskom jezičnom portalu, privatnost je definirana kao „osobna, intimna i obiteljska sfera života“, a kao osnovno ljudsko pravo, utvrđena je u raznim međunarodnim dokumentima, kao i kroz nacionalno zakonodavstvo. Kada se govori o privatnosti i njezinoj zaštiti, onda se govori i o osobnim podacima, odnosno informacijama jer su ti pojmovi povezani i isprepleteni. Najveći izazov zaštite privatnosti i osobnih podataka je upravo u današnjem digitalnom svijetu. Pod osobnim podacima podrazumijevaju se:

> svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, odnosno kojim se osoba može identificirati (izravno ili neizravno) uz pomoć identifikatora kao što su ime i prezime, identifikacijski broj (OIB), adresa stanovanja, adresa elektroničke pošte, podatak o stručnoj kvalifikaciji, podatak o radnom mjestu, bankovnom računu, kreditnoj zaduženosti, podatak o lokaciji, mrežni identifikator i sl. (e-Građani).

Postoji i posebna kategorija osjetljivih podataka u koju spadaju podaci o rasnom ili etičkom podrijetlu, političkim mišljenjima, vjerskim ili filozofskim uvjerenjima ili članstvima u sindikatu te genetski, biometrijski i zdravstveni podaci kao i podaci o spolnom životu i seksualnoj orijentaciji (AZOP, 2011). Razvoj interneta i raznih tehnologija koje su pridonijele brzoj komunikaciji i razmjeni velike količine informacija, doveo je do ugrožavanja privatnosti. Korisnici ostavljaju na raznim uslugama i sustavima te društvenim mrežama svoje podatke, često nesvjesni tragova koje ostavljaju iza sebe i opasnosti koje to nosi sa sobom – od zloupotrebe podataka kao na primjer neovlašteno prikupljanje, pohranjivanje i dijeljenje te krađa osobnih podataka pa do neovlaštene obrade podataka ili nadziranja komunikacije (Kuća ljudskih prava Zagreb, 2019). Upravo zbog takvih situacija, potrebno je informirati, osvijestiti i educirati korisnike o njihovoj zaštiti osobnih podataka, a s time i privatnosti. Tri najčešća slučaja dijeljenja osobnih podataka su:

1. Registracija putem online obrazaca (npr. registracija na društvenim mrežama, kod pristupa forumima, chatroom-u, online multiplayer igrama. . .),
2. Elektronička pošta,
3. Online plaćanja kreditnim karticama (AZOP, 2011).

3. Zakonske regulative u Republici Hrvatskoj

Kako bi se bolje razumjela zaštita privatnosti, odnosno zaštita osobnih podataka važno je spomenuti Opću uredbu o zaštiti podataka (engl. *General Data Protection Regulation*) te Zakon o zaštiti osobnih podataka.

3. 1. Opća uredba o zaštiti podataka (GDPR)

Opća uredba o zaštiti podataka ili engl. *General Data Protection Regulation* je zakon o zaštiti osobnih podataka i privatnosti koji se primjenjuje u zemljama Europske unije. Ova uredba se odnosi na osobne podatke, odnosno one podatke iz kojih se može otkriti identitet neke osobe, a tu spadaju: ime i prezime, broj osobne iskaznice, lokacija, informacije s kreditnih kartica i zdravstvenih kartona, zatim biometrijski i genetski podaci, vjerski i filozofski stavovi, etička pripadnost, financijsko stanje, članstvo u sindikatu, seksualna orijentacija, IP adrese, poruke elektroničke pošte, kolačići u pregledniku i pseudonimizirani podaci (GDPR informer, 2018). Pseudonimizacija se odnosi na obradu osobnih informacija tako da se one više ne mogu povezati sa nekom osobom bez pomoći dodatnih podataka (PrivazyPlan, 2018). Kada neka tvrtka (voditelj obrade) pribavlja osobne podatke od korisnika, odnosno ispitanika, mora u tom procesu biti transparentna, mora paziti na načela obrade kao što su: obrađivanje podataka samo na valjanoj zakonskoj osnovi, prikupljanje samo relevantnih podataka i podataka potrebnih za ispunjenje svrhe u koju se prikupljaju i obrađuju, zatim zaštita podataka od nezakonite i nedozvoljene obrade, gubitka ili uništenja i sl. Još jedna bitna stvar, na koju tvrtke moraju obratiti pažnju, je privola ispitanika za korištenje i obrađivanje njihovih podataka kao i rješavanje zahtjeva ispitanika. (GDPR informer, 2018).

3. 2. Zakon o zaštiti osobnih podataka

U Republici Hrvatskoj postoji Zakon o zaštiti osobnih podataka (2012) kojim je uređena zaštita osobnih podataka o fizičkim osobama te također nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka, a svrha i cilj tog zakona je zaštita privatnosti osoba, drugih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. U Zakonu je osobni podatak definiran kao „svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati“. To se odnosi na osobe čiji se identitet može utvrditi uz pomoć raznih obilježja specifičnih za tu osobu, od fizičkog izgleda do kulturnih ili socijalnih obilježja. Pod obradom osobnih podataka se podrazumijevaju radnje izvršene na osobnim podacima. Tu spada:

prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima (Zakon o zaštiti osobnih podataka, 2012).

Također, u članku 6. stoji da se osobni podaci mogu „prikupljati u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu sa zakonom i mogu se dalje obrađivati samo u svrhu u koju su prikupljeni . . .". Važno je istaknuti da se osobni podaci, između ostaloga, smiju prikupljati i dalje obrađivati ako je osoba sama objavila te podatke, a u svim ostalim slučajevima, osobu se prije prikupljanja njezinih osobnih podataka treba informirati o tome tko prikuplja podatke, u koju svrhu, o pravu na pristup podacima i njihov ispravak, o primateljima tih osobnih podataka, te jesu li podaci dati dobrovoljno ili obvezno i koje su posljedice ako osoba uskrati davanje podataka. Osim toga, osobni podaci osoba moraju se brisati čim prođe vrijeme koje je nužno za ostvarivanje svrhe u koju su podaci prikupljeni, a moraju se i poduzeti sve mjere zaštite osobnih podataka kako bi se oni zaštitili od svake zlouporabe, slučajnog ili namjernog gubitka ili uništenja, neovlaštenih promjena i objavljivanja i drugo. Prema članku 21. Zakona o zaštiti osobnih podataka svaka osoba „ima pravo usprotiviti se obradi osobnih podataka u svrhe marketinga" i zatim se ti podaci ne smiju dalje obrađivati u marketinške svrhe. Svaka povreda bilo kojeg prava koje je zaštićeno Zakonom o zaštiti osobnih podataka može se prijaviti Agenciji za zaštitu osobnih podataka putem zahtjeva za utvrđivanje povrede prava. Agencija prema članku 32., između ostaloga, nadzire provođenje zaštite osobnih podataka, ukazuje na zloupotrebu prikupljanja osobnih podataka te rješava povrede prava koja su zajamčena Zakonom, a na njihovoj mrežnoj stranici može se pronaći i obrazac zahtjeva za utvrđivanje povrede prava. Agencija u slučaju povrede neke odredbe Zakona o zaštiti osobnih podataka, odnosno ako se osobni podaci prikupljaju, obrađuju i koriste suprotno odredbama zakona ili ako su prikupljeni bez pravne osnove, može:

- tražiti otklanjanje nepravilnosti u određenom roku,
- zabraniti prikupljanje, obrađivanje ili korištenje tih podataka,
- tražiti brisanje osobnih podataka,
- zabraniti dijeljenje osobnih podataka drugima izvan Hrvatske.

Također, postoje i novčane kazne koje se kreću između 20 i 40 tisuća kuna za kršenje odredbi ovoga zakona, a na web stranici Agencije za zaštitu osobnih podataka postoji mnoštvo letaka, brošura i priručnika vezanih uz zaštitu osobnih podataka namijenjenih svim uzrastima.

4. Digitalni otisak (engl. *digital footprint*)

Glavna značajka interneta jest ta da se temelji na razmjeni informacija koja može biti vidljiva – ona se odvija kada korisnici interneta javno ili između sebe dijele informacije, a postoji i skrivena razmjena informacija gdje osobni podaci neke osobe, bez da je ona toga svjesna, završe na raspolaganju drugim osobama (Torić, 2018). Često ne razmišljamo o tome da iza sebe ostavljamo podatke koje bi netko drugi mogao iskoristiti protiv nas ili protiv nama bliskih osoba. Pojam digitalni otisak (engl. *digital footprint*) odnosi se na niz podataka koji se ostavljaju iza sebe svaki puta kada se koristi Internet, od stranica koje se posjećuju, elektroničke pošte koja se šalje, videozapisa i slika koje se stavljaju na mrežu, online igara koje se igraju pa sve do općenitih informacija koje se pretražuju (Deljac et al., 2020).

Digitalni otisci ili digitalni tragovi mogu se podijeliti na pasivne i aktivne. U pasivne digitalne otiske spadaju oni koji se plasiraju na Internet bez namjere. Tu se ubraja i kada netko drugi objavi određene podatke o nama, kao na primjer neka rang lista s natjecanja na kojoj se nalazi i naše ime. Objave na društvenim mrežama – tekstualne, slikovne ili video uradci, poslane poruke putem e-maila, objave na forumima, prijave na raznim lokacijama i drugo, spadaju u aktivne digitalne tragove jer se namjerno ostavljaju na internetu (Deljac et al., 2020).

5. IP (engl. *Internet Protocol*)

Osnovni protokol u radu Interneta naziva se IP, odnosno engl. *Internet Protocol*. IP se temelji na dodjeli jedinstvene adrese svakom uređaju koji je priključen na mrežu. To znači da svaki uređaj ima svoju jedinstvenu 32-bitnu adresu koja se sastoji od mrežnog prefiksa – odnosi se na mrežu na kojoj se nalazi uređaj i od identifikatora uređaja – identificira točan uređaj unutar mreže. Prvo su IP adrese bile podijeljene u tri razreda: A, B i C. Oni su se međusobno razlikovali po „točci u kojoj se dijeli dio adrese namijenjen identifikaciji mreže i dio namijenjen identifikaciji računala“ (CARNet, 2007). Također, postoji i dekadski zapis s točkama koji je olakšao rukovanje IP adresama. U to vrijeme nije se moglo predvidjeti da će se Internet tako brzo razvijati te su se adrese razdijelile, a adresni prostor se pokazao kao ograničen. 1993. razredno adresiranje zamijenio je CIDR sustav (engl. *Classless Inter-Domain Routing*). Takav sustav omogućava podjelu adresnog prostora u blokove, a adrese i dalje imaju dva dijela: dio koji predstavlja blok i dio koji predstavlja određeni uređaj unutar bloka. Za dodjelu i korištenje CIDR blokova zadužena je organizacija IANA (engl. *Internet Assigned Numbers Authority*) koja se sastoji od 5 RIR (engl. *Regional Internet Registries*) tijela u cijelom svijetu koja upravljaju dodjelom adresa. CIDR adresiranje omogućilo je fleksibilnost mreže te rješava pojavu neiskorištenih adresa. Važno je spomenuti i tri protokola automatskog dodjeljivanja IP adresa: RARP, BOOTP i DHCP.

RAPR (engl. *Reverse Address Resolution Protocol*) se koristi za prevođenje fizičke adrese u IP adresu, a naslijedili su ga BOOTP (engl. *Bootstrap Protocol*) i DHCP (engl. *Dynamic Host Configuration Protocol*). BOOTP je mrežni protokol koji se koristi za automatsko određivanje svojih IP adresa. U današnje vrijeme ga je DHCP istisnuo iz upotrebe. DHCP protokol koriste komunikacijski uređaji (npr. računala, usmjernici . . .) za dohvaćanje IP adrese, adrese preporučenoga pristupnog poslužitelja, adrese DNS poslužitelja i sličnih podataka. Postoje tri tehnike upravljanja IP adresama – dinamička, automatska i ručna dodjela. Kod dinamičke dodjele, klijentu se određena IP adresa „iznajmljuje“ na određeni period vremena. To može varirati od nekoliko sati do nekoliko dana. Automatska dodjela funkcionira tako da je jedna adresa trajno povezana s jednim klijentom, a kod ručne, klijent sam bira svoju IP adresu i obavještava poslužitelj o tome. Problem nastaje upravo između klijenta i poslužitelja jer se između njih ne odvija nikakva autorizacija niti autentikacija. DHCP poslužitelj ne može znati zahtjeva li legitimni korisnik mreže, odnosno računalo IP adresu. S druge strane, klijent ne može provjeriti legitimnost poslužitelja. Zlonamjerni korisnici to u većini slučajeva koriste za DoS (engl. *Denial of Service*) napade (CARNet, 2007).

6. Društvene mreže

U današnjem modernom i tehnološki naprednom svijetu, društvene mreže postale su neodvojivi dio ljudskih života. Ubrzale su i pojednostavile dopisivanje i razmjenu informacija između korisnika te praćenje novih proizvoda i trendova. Bitno je napomenuti da većina ljudi ne koristi samo jednu društvenu mrežu, već imaju otvoren profil na više njih. Sve to omogućuje zlonamjernim korisnicima lakši pristup osobama koje onda postanu žrtve različitih prijevara, ucjena ili krađe identiteta.

6. 1. Društvene mreže - statistika

Prema najnovijim Kemptovim statistikama iz travnja 2021. godine, ukupna populacija ljudi je 7.85 milijarda, a od toga su 4.33 milijarde aktivni korisnici društvenih mreža, a to je više od 50% ukupne populacije ljudi. Broj korisnika društvenih mreža, u odnosu na prošlu godinu, porastao je za gotovo 14%, a prosječno vrijeme po danu koje korisnici provode koristeći društvene mreže je 2 sata i 22 minute. Kao odgovor na pitanje o omiljenoj društvenoj platformi, 21,4% korisnika između 16 i 64 godina (ne uključujući Kinu) izjasnilo se da im je WhatsApp najdraža društvena platforma. Nakon toga slijedi Facebook za koji se izjasnilo 21,8% ispitanika, a Instagram 18,4 % ljudi navodi kao omiljenu društvenu mrežu. Na četvrtom mjestu se nalazi Twitter, nakon toga Fb Messenger i zatim TikTok. Kao glavni razlog korištenja društvenih mreža, najviše korisnika interneta, gotovo 50%, navodi mogućnost ostajanja u kontaktu s prijateljima i obitelji, nakon toga slijedi traćenje slobodnog vremena i čitanje novosti te traženje smiješnih i zabavnih sadržaja. Također, ljude zanima o čemu se priča na društvenim mrežama i traže inspiraciju za stvari koje bi radili ili nabavili, odnosno kupili. Popularno je i dijeljenje vlastitih razmišljanja te diskusija o različitim mišljenjima i stvaranje novih kontakata. Ljudi općenito koriste društvene mreže radi dijeljenja informacija i događaja iz svog života, radi praćenja i gledanja sportskih događanja, slavnih osoba te influencera.

Prema *Digital 2021 April Global Statshot Report*-u, 82,2% korisnika interneta između 16 i 64 godine posjećuje društvene mreže kako bi pronašli smiješan ili zabavan sadržaj, 73,5% prati, odnosno istražuje robne marke i proizvode na društvenim mrežama, a 22,6% korisnika interneta posjećuje društvene mreže radi potreba posla. Također, ljudi aktivno koriste ili posjećuju u prosjeku više od 6 platforma društvenih mreža svaki mjesec.

Iako je WhatsApp prema istraživanju najomiljenija platforma društvenih mreža, Facebook je sa skoro 2,8 milijarde aktivnih korisnika mjesečno, najkorištenija društvena mreža. Iza Facebooka slijedi YouTube sa gotovo 2,3 milijarde korisnika mjesečno, iako to ne uključuje

korisnike YouTube mobilne aplikacije i neregistrirane korisnike. Na trećem mjestu se nalazi WhatsApp, iza njega Fb Messenger i zatim Instagram.

Doduše, veoma mali postotak, odnosno manje od 1% ljudi između 16 i 64 godine je vjeran samo jednoj platformi društvene mreže i ne posjećuje niti jednu drugu, dok velika većina korisnika interneta zapravo aktivno koristi barem još jednu društvenu mrežu.

46,5% korisnika na društvenim mrežama prati prijatelje, obitelj ili druge ljude koje poznaju, 29,5% ljudi prati glumce, komičare i druge izvođače. Nakon toga, osobe najviše prate TV serije i kanale, a zatim profile za zabavu, bendove, pjevače i druge glazbenike. 24,6% korisnika izjavilo je da na društvenim mrežama prati restorane, kuhare, odnosno chefove i ostale sadržaje povezane sa hranom. Influencere prati nešto više od 20% korisnika društvenih mreža između 16 i 64 godine, a najmanje se prate stručnjaci za ljepotu i putopisci te putničke agencije.

6. 2. Popularne društvene mreže

Prema CERTu (2016), neke od popularnih društvenih mreža su:

- *Facebook* – društvena mreža koja korisnicima omogućava da održavaju kontakt s bliskim osobama, prijateljima, poznanicima, kolegama te im dopušta međusobno dijeljenje i komentiranje fotografija, videozapisa i ostalog sadržaja. Korisnici mogu pratiti razna događanja i stranice vezane uz vlastite interese te se mogu učlanjivati u razne grupe. Facebook Messenger je aplikacija Facebooka za razmjenu poruka.
- *WhatsApp* – aplikacija za čiju je registraciju potrebna minimalna dob od 16 godina, a služi besplatnoj razmjeni tekstualnih poruka, fotografija, zvučnih i video zapisa između jedne ili više osoba. Korisnik ne može pristupati, odnosno ograničen mu je pristup drugim osobama ako ih nema u imeniku, ali ako se korisnici nalaze u istoj grupi, onda mogu komunicirati međusobno, čak i ako nemaju razmijenjene i spremljene kontakte.
- *Instagram* – služi za snimanje, uređivanje i dijeljenje fotografija i kratkog video sadržaja, a minimalna dob za registraciju je 13 godina. Sadržaj koji se dijeli, može se u postavkama privatnosti učiniti javno dostupnim ili privatnim, a dopušteno je i dijeljenje i komentiranje različitih objava. Ako korisnik ima privatan račun, nitko ne može vidjeti, dijeliti ili komentirati njegove objave. Glavni problem je javno dijeljenje lokacije koju zlonamjerne osobe mogu iskoristiti protiv korisnika te dijeljenje neprimjerenog sadržaja.
- *YouTube* – usluga koja omogućuje razmjenu, postavljanje, pregledavanje i ocjenjivanje videozapisa. Registracija je potrebna za komentiranje i postavljanje vlastitog video sadržaja, dok za samo pregledavanje to nije potrebno. Zabranjeno je postavljanje

sadržaja u kojem se prikazuju i podržavaju kriminalne radnje te pornografski sadržaj kao i nasilje, sramoćenje, klevetanje.

- *Snapchat* – aplikacija za dijeljenje fotografija kod koje je minimalna dob za registraciju 13 godina. Korisnicima je dopušteno dijeljenje videozapisa i fotografija unutar određenog vremenskog perioda, a nakon toga perioda, sadržaj se briše automatski. To može kod korisnika stvoriti osjećaj lažne sigurnosti, ali zlonamjerni korisnici su pronašli razne načine kako da, unatoč automatskom brisanju, ipak pohrane i sačuvaju sadržaj. Također, korisnicima pristup do zlonamjernog sadržaja i neprimjerenih fotografija ili videozapisa, omogućuje opcija „Otkrij“ (engl. *Discover*).
- *Twitter* – društvena mreža na kojoj korisnici mogu pratiti svoje prijatelje, bliske osobe, kolege i razne poznate osobe. Korisnici dijele kratke objave koje mogu biti ili privatne ili javno dostupne te se one mogu obrisati, ali zlonamjerne osobe mogu sadržaj kopirati i pohraniti.

7. Prijetnje na društvenim mrežama

Pri korištenju interneta, a posebice društvenih mreža, svaki korisnik treba biti svjestan opasnosti i rizika koji se nalaze na društvenim mrežama. Neki od najčešćih oblika prijetnji su:

7. 1. Napadi uz pomoć socijalnog inženjeringa

Socijalni inženjering je niz tehnika i metoda pomoću kojih zlonamjerna osoba utječe na pojedinca kako bi ga potaknuo da učini nešto protivno vlastitom interesu. Često se koristi u svrhu otkrivanja povjerljivih podataka ili dobivanja pristupa drugim resursima što za posljedicu ima gubitak osobnih ili službenih povjerljivih podataka, zatim gubitak ugleda, materijalni gubitak i u krajnjem slučaju emocionalni pritisak žrtve napada. Napadači prvo sakupljaju informacije o osobi na koju planiraju napad, zatim uspostavljaju vezu sa žrtvom i pristupaju joj i na kraju slijedi realizacija napada. 3 najčešća oblika socijalnog inženjeringa su: *phishing*, *vishing* i *impersonation* (CERT, O socijalnom inženjeringu).

7. 1. 1. Phishing

Mrežna krađa identiteta ili engl. *phishing* spada među najčešće internetske prijevare. Korisniku se šalje poruka i želi se postići neka akcija od njega, odnosno on postaje žrtvom napada. Radi se o porukama kojima je osnovni cilj saznati osobne i povjerljive podatke nekog korisnika (CERT, Phishing). Najčešće su to podaci kao na primjer korisničko ime i lozinka, broj računa ili broj kreditne kartice, PIN. . . Zlonamjerni se korisnici služe raznim vrstama manipulacije kako bi uvjerili osobu u istinitost poruke i potrebu za određenim povjerljivim informacijama. Poruka u većini slučajeva izgleda vjerodostojno originalnim porukama koje se inače dobivaju od banaka ili servisa za elektroničko plaćanje te je stoga lako povjerovati u njezinu istinitost. Neki od razloga koji se navode u *phishing* porukama, a zbog kojih bi bilo potrebno odati svoje osobne informacije, su na primjer: provjeravanje podataka, nadogradnja i unapređenje sustava, verifikacija računa, oporavak računa, povrat poreza i slično (CERT, Phishing). Vrlo je važno biti oprezan prilikom čitanja poruka na društvenim mrežama ili elektroničke pošte te ne otvarati poveznice koje se čine sumnjive, čak i ako dolaze od prijatelja ili poznanika. Dobro je i pažljivo provjeriti je li URL adresa na kojoj se unose povjerljive informacije legitimna i koristi li stranica preko koje se unose te informacije HTTPS protokol. *Phishing* je doduše najčešći preko e-maila, ali je moguć i preko društvenih mreža pa stoga treba biti oprezan kod otvaranja poveznica koje su stigle u porukama manje poznatih osoba, ali i u porukama prijatelja.

7. 1. 2. Vishing i impersonation

Vishing se u usporedbi s *phishingom* odnosi na sakupljanje informacija od žrtve putem telefona uz lažan broj pozivatelja, a *impersonation* se odnosi na dobivanje pristupa podacima i utjecaja

korištenjem lažnog identiteta (CERT, O socijalnom inženjeringu). Zlonamjerni korisnici svakim danom razvijaju metode napada te je bitno kritički pristupiti sumnjivom sadržaju, provjeravati identitet osoba s kojima komuniciramo te odgovorno i savjesno postupati s osobnim podacima i promišljeno se služiti internetom.

7. 2. Krađa identiteta

Većina ljudi u današnje vrijeme koristi isto korisničko ime i lozinku za različite servise i društvene mreže. Također, često se koristi i opcija prijave na neke vanjske servise i usluge putem društvene mreže. Tako se korisnicima olakšava prijava jer se uvijek koristi isto korisničko ime i lozinka, ali s druge strane to znači da kompromitacija jednog računa automatski označava i kompromitaciju svih ostalih povezanih servisa i usluga (CERT, 2016). Nakon krađe identiteta, zlonamjerna osoba može žrtvine podatke zamijeniti ili prodati, može otvarati nove račune u njezino ime i raditi velike troškove, može se prijavljivati za razne usluge, a u krajnjem slučaju čak i iznajmljivati i kupovati skupocjene stvari (Miller, 2003: 280-281).

7. 3. Zlonamjerni sadržaj

Osim korisnika koji društvene mreže koriste samo radi komunikacije i razmjene informacija te traćenja vremena i zabave, postoje i osobe koje ih koriste za slanje zlonamjernog sadržaja. Ponekad, određena poruka ne djeluje kao zlonamjerna, ali preuzimanjem na uređaj ili slanjem, odnosno prosljeđivanjem na adrese ostalih kontakata, može prouzročiti veliki kaos i štetu za sve osobe do kojih je stigao taj sadržaj (CERT, 2016). Važno je pažljivo provjeravati i preuzimati sadržaj od nepoznatih i sumnjivih osoba te ga ne prosljeđivati dalje drugim korisnicima.

Postoji par glavnih kategorija u koje se zlonamjerni i neželjeni sadržaj može podijeliti, a to su:

- Spam,
- Hoax,
- Malware.

7. 3. 1. Spam

Spam je nezatražena, odnosno neželjena elektronička pošta koja je poslana na velik broj adresa elektroničke pošte te većinom uzrokuje uznemirenost, kako kod krajnjih korisnika tako i kod velikih tvrtki ili davatelja Internet usluga. Taj problem, kojega sve više ljudi doživljava kao svakodnevicu i nešto neizbježno, može utjecati i na narušavanje ugleda određene tvrtke ili pojedinca, a također može uzrokovati iskorištavanje računalnih resursa, kao na primjer procesnog vremena, prostora na hard disku, mrežne propusnosti i tako dalje (CARNet, 2005).

Spam za sobom povlači i velike troškove te između ostaloga utječe na pad produktivnosti kod korisnika zbog vremena i energije koju korisnici moraju utrošiti na konstantno pregledavanje, a zatim i brisanje neželjenih poruka.

Postoji nekoliko kategorija u koje se spam poruke mogu podijeliti, ovisno o izgledu, načinu njihovog slanja i tipu:

- Email spam:
    - neželjena komercijalna elektronička pošta (engl. *Unsolicited commercial* e-mail ili UCE) odnosi se na poruke u kojima se reklamira određeni proizvod ili usluga, ali bez korisnikovog pristanka. Takve poruke se nazivaju i junk e-mail te su najzastupljenija kategorija među spam porukama,
    - neželjena bulk elektronička pošta (engl. *Unsolicited bulk* e-mail ili UBE) podrazumijeva poštu koja sadrži najčešće politička lobiranja i uznemiravanje korisnika te je poslana velikom broju ljudi iz određenog interesa,
    - *Make money fast* ili MMF poruke traže od korisnika da na određene adrese pošalju neku svotu novca te tako i sami brzo i lako zarade. Najčešće se traži i da korisnik dalje proslijedi poruku,
    - napadi na reputaciju (engl. *Reputation attacks*) su poruke koje su lažirane sa ciljem da ugroze reputaciju i kredibilitet osobe ili organizacije u čije ime su poslane (CARNet, 2005).

Kod spam poruka najvažnije je prikupiti što veći broj adresa elektroničke pošte kako bi se određeni sadržaj poslao velikom broju osoba, udruga ili organizacija. *Spammeri*, odnosno osobe koje su zadužene za slanje spam poruka mogu na različite načine doći do korisničkih e-mail adresa. Neki od primjera i načina prikupljanja korisničkih adresa elektroničke pošte radi slanja neželjenih poruka na iste su:

- kupnja gotovih lista na kojima se nalazi veliki broj adresa elektroničke pošte za određenu svotu novca,
- korištenje e-mail *extractors* programa pomoću kojih se na Internetu na raznim Web stranicama, forumima, tematskim grupama (engl. *Newsgroups*) i slično traže adrese elektroničke pošte,
- ručno pretraživanje Interneta,
- korištenje *newsgroup harvesters* programa čija je svrha automatsko prikupljanje adresa elektroničke pošte s različitih *newsgrupa*,

- postavljanje Internet servisa na kojima se od korisnika traži da ostave svoju e-mail adresu ili krađa već gotovih lista od davatelja Internetskih usluga,
- popularno je također i korištenje programa koji pogađaju valjane adrese elektroničke pošte na određenoj domeni (CARNet, 2005).

Zaštita od spama

Za postizanje najbolje zaštite od spam poruka, u većini slučajeva potrebno je kombinirati i koristiti više metoda za zaštitu. Najčešća je instalacija antispam alata koji onda prepoznaju i filtriraju neželjenu poštu.

7. 3. 2. Hoax

Za razliku od spama, *hoax* poruke su najčešće neistinitog sadržaja, a cilj im nije uzrokovati neku štetu, već zastrašiti i dezinformirati osobu koja je zaprimila poruku. Slično kao i kod spam poruka, namjera pošiljatelja *hoaxa* je da ih pošalju na velik broj adresa te da ih primatelji nakon toga dalje prosljeđuju jer su uvjereni u istinitost sadržaja takve poruke. Većinom su to poruke u kojima se nalazi lažno upozorenje na različite štetne programe kao što su virusi, crvi, trojanski konji i slično te primatelji nakon toga, s dobrom namjerom, šalju takve poruke prijateljima i poznanicima. *Hoax* poruka može biti napisana i u obliku lanca sreće ili lanca zarade gdje se primateljima, ako pošalju, odnosno proslijede poruku, obećavaju razne svote novca, skupi uređaji, luksuzna putovanja i tako dalje. Još jedna vrsta *hoax* poruka koja je dosta raširena su lažni zahtjevi za pomoć. Takve poruke se baziraju na izazivanju suosjećanja kod primatelja prema siromašnim, bolesnim, nemoćnim osobama i djeci te kao rezultat imaju daljnje prosljeđivanje elektroničke pošte ili poruke na društvenim mrežama. Neki *hoaxi* sadrže pozive za potpisivanje, odnosno peticiju vezanu uz neku bitnu i popularnu temu, a postoje i kompromitirajuće *hoax* poruke koje za cilj imaju narušavanje nečijeg ugleda jer se u njima navode lažne ili iskrivljenje informacije o nekoj tvrtki, organizaciji, udruzi ili određenoj osobi (CERT, Hoax).

7. 3. 3. Malware

U Priručniku za informacijsku sigurnost i zaštitu privatnosti (2018) koji su uredili Tena Velki i Krešimir Šolić, stoji da je zlođudni kod, odnosno engl. *malware* „općeniti naziv za računalne programe kojima je cilj naštetiti računalnom sustavu na kojemu su pokrenuti“. 1971. godine eksperimentalno je napisan prvi takav zlođudni kod nazvan *Creeper* kojemu je cilj bio zastrašiti

korisnika ispisivanjem poruke na ekranu. Danas su glavni ciljevi zloćudnih programa najčešće financijske prirode. S vremenom se zlonamjerni programi sve više i više razvijaju i napreduju te se „usmjeravaju na pretvaranje računala u sredstvo kojim napadač može izvoditi daljnje napade ili pak zahtijevati otkupninu od korisnika kako bi uklonio zloćudni program“ (Borovac et al., 2018: 72).

7. 3. 3. 1. Ransomware

Od zloćudnih programa (engl. *malware*) u zadnjih par godina postao je vrlo raširen *ransomware*. *Ransomware* se odnosi na skup zlonamjernih programa čija je zadaća onemogućiti korisniku korištenje računala. Nakon toga, od korisnika se najčešće traži neka svota novca, odnosno otkupnina za uklanjanje zlonamjernog softvera i daljnje normalno korištenje računala (CERT, Ransomware). Radi toga je bitno da se ne otvaraju nepoznate i sumnjive poveznice koje su stigle na e-mail te da se redovito ažuriraju instalirane aplikacije na računalu i sam operacijski sustav. Otvaranje reklamnih poruka je također riskantno i treba se izbjegavati, a za preventivnu zaštitu računala dobro je imati instalirani neki antivirusni alat i anti-*ransomware* alat, kao na primjer *CryptoPrevent* ili *CryptoMonitor* (CERT, Ransomware). Upravo zbog takvih situacija, sve više ljudi izrađuje sigurnosne kopije (engl. *Backup*) svojih podataka, odnosno datoteka ili čak čitavog sustava na neki vanjski server ili prijenosni medij. Izrada takvih kopija je zapravo i najefikasniji način zaštite od zlonamjernih softvera kod kojih se nakon zaraze mogu izgubiti sve datoteke i onemogućiti korištenje cijelog računala.

7. 3. 3. 2. Spyware

Spyware programi nastoje neprimjetno zaraziti uređaj korisnika i onda u pozadini nadzirati sve radnje koje korisnik obavlja, s kojim podacima rukuje, koje usluge koristi i slično. Jedan primjer *spywarea* su prateći kolačići za mrežna sjedišta (engl. *tracking cookies*) koji se postavljaju u preglednik korisnika te se onda prati koja se svemrežna sjedišta posjećuju. Postoje i programi koji se zovu *keylogeri* i koji prate pokret miša i unose na tipkovnici korisnika. Neki primjeri *spyware* programa koji su usmjereni na financijske institucije su *Dridex*, *Neverquest* i *Gozi* (Borovac et al., 2018: 86-87).

7. 4. Gubitak podataka

Osim sakupljanja, preuzimanja i kopiranja osobnih podataka i njihovog iskorištavanja, zlonamjerni korisnici mogu s poslužitelja ili klijentskog računala obrisati podatke, što također predstavlja prijetnju sigurnosti sustava, odnosno mreže. Od ovakve vrste napada, najefikasnije

i najpraktičnije rješenje je izrada kopije podataka na nekom vanjskom uređaju za pohranu podataka. Također, podaci se mogu u obliku dokumenta ili datoteka pohraniti na uslugama na internetu koje nude spremanje podataka. Važno je redovito sinkronizirati kopije podataka sa svakog uređaja te nije loše imati čak i više od jedne kopije najbitnijih podataka (Borovac et al., 2018: 98-99).

7. 5. Dijeljenje neprikladnih informacija

Glavna svrha društvenih mreža je dijeljenje vlastitih stavova, mišljenja i drugih osobnih informacija kao i fotografija, videozapisa, glazbe . . . Često se te informacije ne dijele samo s obitelji, prijateljima i poznanicima, nego i s drugim manje poznatim ili potpuno nepoznatim osobama koje su korisnici određene društvene mreže. S obzirom da se osobna mišljenja i stavovi kao i društvene te kulturne norme s vremenom mogu promijeniti, bitno je obratiti pažnju na sadržaj koji se objavljuje na društvenim mrežama. Osim što neka objava može naštetit drugim osobama zbog svog neprikladnog sadržaja, može se desiti da u budućnosti našteti i vlastitom ugledu jer digitalni tragovi ne nestaju, već predstavljaju neodvojivi dio identiteta nekog korisnika (CERT, 2016).

8. Zaštita osobnih podataka na društvenim mrežama

Društvene mreže su se u zadnjih nekoliko godina veoma brzo razvile i stekle veliku popularnost kako kod mlađih generacija, tako i kod onih nešto starijih. Sa sobom su donijele puno dobroga, kao na primjer bolja povezanost sa ljudima iz cijeloga svijeta, ali također i mnoge opasnosti koje se tiču privatnosti korisnika na društvenim mrežama. Najčešće upravo ponašanje korisnika, kao na primjer nesmotrenost, neopreznost ili samo neznanje, dovode do otuđenja i krađe digitalnih podataka, a s time i njihove zlouporabe. Zbog toga je veoma važno obratiti pozornost na nekoliko stvari koje mogu pomoći u zaštiti osobnih podataka:

1. Objavljivanje osobnih i povjerljivih podataka – svaka informacija koja se objavi na internetu, ostaje tamo zauvijek, čak i nakon što se izbriše. U najosobnije podatke spadaju vlastito ime i prezime, e-mail, broj telefona, OIB, adresa stanovanja, brojevi kartica i pinovi, lozinke, imena rodbine i slično. Zlonamjerni korisnici najčešće iskorištavaju takve podatke putem različitih obrazaca, formulara ili upitnika čije ispunjavanje djeluje bezazleno i zabavno. Veoma često u takvim situacijama strada inbox ili e-mail sandučić, koji je onda zatrpan različitim lažnim, bezvrijednim ili reklamnim porukama. Također, treba se pripaziti i kod objavljivanja fotografija i video zapisa, lokacije te označavanja bliskih osoba jer se na taj način može saznati lokacija korisnika ili ugroziti bliske osobe (Europska komisija, 2019).
2. Objavljivanje osobnih podataka, slika i video zapisa djece – neki roditelji na društvenim mrežama redovito objavljuju najčešće fotografije, ali i video zapise i ostale osobne podatke svoje maloljetne djece. Zakonski ne postoji nikakva regulativa u takvim slučajevima, ali je bitno obratiti pozornost na opasnosti koje to predstavlja za djecu:
    a. lako se može saznati lokacija i aktivnosti kojima se dijete bavi,
    b. može doći do izrugivanja ili čak nasilja od strane vršnjaka u školi,
    c. fotografije su često sramotne za dijete, a i ono nema mogućnost, odnosno pravo glasa izreći želi li da ta fotografija bude objavljena (Europska komisija, 2019).
3. Prijavljivanje preko društvenih mreža u različite račune – važno je kod takvog prijavljivanja dobro razmisliti želi li se koristiti račun na društvenim mrežama. Općenito treba biti oprezan s prijavljivanjem i paziti na korisničko ime i lozinku i zapravo bi bilo najbolje, u takvim slučajevima, kreirati novi račun (Europska komisija, 2019).
4. Prihvaćanje prijateljstava i drugih zahtjeva na društvenim mrežama – svaka osoba koja dobije uvid u nečiji osobni profil na nekoj društvenoj mreži, može iskoristiti informacije koje sazna za ugrožavanje tuđe privatnosti, stoga treba prihvaćati poruke i online

prijateljstva samo od osoba koje se poznaju u stvarnom životu (Europska komisija, 2019).

Budući da se nove opasnosti na internetu pojavljuju iz dana u dan, javlja se potreba za poboljšanjem i razvijanjem novih oblika zaštite. Često je sam korisnik „najslabiji dio sigurnosti informacijsko komunikacijskog računalnog sustava“. (Borovac et al., 2018: 11.)

Činjenica koju mnogi često zaboravljaju je da sve što se objavi na društvenim mrežama i općenito na internetu, tamo i ostaje. Bilo da se radi o nekom tekstualnom sadržaju, fotografiji, videu . . . sve to ostaje zabilježeno na nekom internetskom serveru. Može se taj sadržaj u budućnosti ili čak odmah ukloniti i obrisati sa društvenih mreža, ali na internetskom serveru to će ostati zauvijek.

8. 1. Lozinke

Kako bi se osobni podaci na internetu, a posebice na društvenim mrežama zaštitili, bilo bi dobro da se koriste što složenije lozinke. Trebalo bi izbjegavati lozinke sa vlastitim imenom i prezimenom ili datumom rođenja ili pak česte lozinke kao na primjer neki predvidljivi slijed brojeva ili slova, a također nije dobro imati istu lozinku za sve postojeće račune. Lozinka bi trebala uvijek biti duža od 6 znakova jer postoje programi koji kraće zaporke razbijaju bez problema. Preporuča se korištenje kombinacije brojeva i znakova te velikih i malih slova, a uređaje koji se automatski, bez upisivanja korisničkog računa i lozinke, prijavljuju na društvene mreže, ne treba ostavljati bez nadzora (Što je to “sigurnost na internetu“ i kako zaštititi osobne podatke na internetu?).

8. 2. Osobni podaci i održavanje računala

Kako bi se zaštitila vlastita privatnost, najbolje bi bilo ukloniti osobne podatke s profila ili korisničkog računa na društvenim mrežama i pristup računu osigurati sigurnosnim pitanjem. Važno je i redovito održavanje računala, kao na primjer brisanje nepotrebne dokumentacije i sadržaja kako bi se rasteretila memorija i omogućio bolji rad, zatim redovito održavanje sustava i instalacija programa zaštite računala i dodatnih programa koji omogućuju zaštitu ili blokiranje neprimjerenih sadržaja (Borovac et al., 2018: 67-68).

8. 3. Otvaranje poveznica i virusi

Danas je potreban samo klik miša na neku internetsku poveznicu da bi se računalni virus preuzeo na taj uređaj i zarazio ga. Bitno je obratiti pozornost i više puta razmisliti prije otvaranja poveznica, čak i ako one dolaze s poznatih e-mail adresa ili poruka. Virusi mogu biti programirani na različite načine pa tako na primjer neometano i bez znanja korisnika imati uvid

u sve podatke koji se nalaze na zaraženom mobitelu, tabletu, laptopu ili računalu. Također, pažljivo odavati ili u najboljem slučaju, uopće ne odavati nekome osjetljive osobne informacije kao što su bankovni pin ili lozinka te ostale informacije koje na bilo koji način mogu ugroziti osobnu privatnost ili privatnost bliskih osoba (Što je to "sigurnost na internetu" i kako zaštititi osobne podatke na internetu?).

8. 4. Javna računala

Što se tiče javnih računala, ona su dostupna svima za korištenje pa su tako i svaka informacija, pretraživanje i svako povezivanje sa postojećim računima, bilo elektroničke pošte, društvene mreže ili usluge u banci, dostupni svima (Što je to "sigurnost na internetu" i kako zaštititi osobne podatke na internetu?).

8. 5. Pravila komunikacije

Uvijek treba poštovati pravila komunikacije kod dopisivanja ili objavljivanja sadržaja na društvenim mrežama, u online grupama, na portalima, forumima, a kod neprimjerene komunikacije, najbolje je blokirati osobu ili ju prijaviti administratoru (Borovac et al., 2018: 68). Naziv za smjernice, odnosno pravila ponašanja u internetskom okruženju je *Netiquette*. Svrha *Nettiquette*-a je pomoći u izgradnji i održavanju ugodnog i učinkovitog okruženja kao i izbjegavanja sukoba među korisnicima prilikom komunikacije na internetu (Shing-Ling, 2020).

9. Facebook

Facebook je društvena mreža koju je 2004. godine pokrenula skupina studenata s Harvarda koju su činili Mark Zuckerberg, Dustin Moskovitz, Chris Hughes i Eduardo Saverin. Prvotna namjera je bila omogućiti međusobno komuniciranje studenata na sveučilištu, a danas Facebook omogućuje razmjenu informacija ljudi diljem svijeta. Korisnici se mogu besplatno uključiti kreiranjem svojeg profila s osobnim podacima i zatim razmjenjivati poruke, fotografije, videozapise i drugo (Hrvatska enciklopedija, 2021).

Gotovo svi korisnici društvene mreže Facebook, odnosno 98,4% pristupaju Facebooku preko neke vrste mobilnog uređaja, a samo 1,6% korisnika pristupa samo putem laptopa ili stolnog računala. Upravo je i mobilna aplikacija Facebook prva na rang listi mobilnih aplikacija i igara prema broju aktivnih korisnika mjesečno prema istraživanju za prvu četvrtinu 2021. godine. Nakon Facebooka slijede WhatsApp na drugom mjestu, Facebook Messenger na trećem mjestu i Instagram na četvrtom mjestu, a svi su u vlasništvu Facebooka (Kempt, 2021).

Uvijek postoje osobe koje žele zloupotrijebiti informacije do kojih mogu doći na korisnikovim društvenim mrežama. Najčešće se želi uzrokovati šteta na račun ugleda osobe, te ucijeniti ili zastrašiti osobu (engl. *Cyberbullying*). Moguće su i zlouporabe kao prepoznavanje pomoću lica radi nanošenja fizičke boli, krađa potpomognuta podacima koji su prikupljeni s mreže, zatim krađa identiteta i lažno predstavljanje te uhođenje osobe (CARNet, 2015).
Svaka povjerljiva informacija o nekoj osobi može direktno ili indirektno poslužiti za krađu identiteta. Najčešće su to podaci o datumu i mjestu rođenja, prezimenu, adresi. Veoma je rizično na društvene mreže postavljati lokaciju na kojoj se korisnik nalazi kao i kućnu adresu ili informacije o dužim putovanjima i odsutnosti od kuće jer takvi podaci zlonamjernim korisnicima mogu poslužiti za provalu u kuću ili uhođenje osobe. *Cyberbullying* je čest kod mlađih osoba i djece koja se služe društvenim mrežama zato jer su upravo društvene mreže bitan dio njihovog života. Djeca i mladi mogu vrlo lako postati mete zadirkivanja i podrugivanja što ponekad ima ozbiljne posljedice na psihičko i fizičko zdravlje mladih. Također, neprimjereno ponašanje na društvenim mrežama, kao na primjer vulgarni statusi ili komentari te neprimjerene fotografije i videozapisi, mogu imati negativne posljedice na ugled osobe u budućnosti. Veliki problem predstavljaju i lažni profili koje zlonamjerne osobe koriste kako bi imale uvid u osobne i povjerljive informacije nekog korisnika. Lažni profili često djeluju vjerodostojno pa korisnici ponekad niti ne posumnjaju na opasnost koja im prijeti (CARNet, 2015).

Politika Facebooka se temelji na 4 glavne značajke:

1. pomoći ljudima da ostanu sigurni, kako offline tako i online – uklanjaju sadržaj, onemogućuju račune i surađuju s lokalnim odvjetnicima kada postoji sumnja za narušavanjem i ugrožavanjem javne sigurnosti,
2. poticanje uljudnog ponašanja – putem Facebooka ljudi izražavaju različita mišljenja i stavove i susreću se s drugačijim mišljenjima od vlastitih. Kako bi se izbalansirale potrebe, sigurnost i interesi zajednice, ponekad se određena vrsta osjetljivog sadržaja uklanja ili se ograničava publika koja ih vidi,
3. držanje korisničkih i osobnih podataka sigurnima – svaka sumnja u proboj sigurnosti se istražuje te se za svaki pokušaj ugrožavanja sigurnosti profila, uključujući prevaru, može tražiti podrška zakona,
4. zaštita intelektualnog vlasništva – traži se da ljudi poštuju autorska prava, zaštitne znakove i druga zakonska prava (AZOP, 2020).

Posebno se pokušava zaštititi mlade pa zbog toga Facebook zahtijeva minimalnu dob od 13 godina prije kreiranja korisničkog profila. Također, određene postavke su namještene na taj način da zaštićuju neke osobne informacije (kontaktne informacije, mjesto školovanja, datum rođenja), zatim upozoravaju mlade koje su posljedice mijenjanja nekih postavki te ih se upozorava da ne prihvaćaju zahtjeve za prijateljstva od nepoznatih osoba. Osim toga, Facebook ima i stroga pravila oglašavanja, osobito alkoholnih proizvoda, duhana, kockanja, upoznavanja novih ljudi i slično. Svaki oglas se pregledava prije nego se pokaže korisniku. Određeni alati omogućuju tinejdžerima da se zaštite od neželjenog sadržaja, neželjenih kontakata, maltretiranja i uznemiravanja na mreži (AZOP, 2020).

Facebook je dizajniran na način da ljudi imaju kontrolu nad sadržajem koji dijele, vide i iskuse, zatim tko ih može kontaktirati, s kime dijele doživljaje i tako dalje.

Platforma uključuje vezu „Prijavi“ za uznemiravanje, maltretiranje i ostale probleme, a omogućeno je i blokiranje drugih osoba pa blokirani više neće moći vidjeti nikakav sadržaj povezan sa osobom koja ih je blokirala. Svaki korisnik Facebooka može odlučiti koje osobe mogu, a koje ne mogu vidjeti osobne statuse, fotografije, videozapise i ostali sadržaj na profilu. Preporuča se osnovne kontaktne informacije, zatim prebivalište, mjesto i datum rođenja te informacije o školovanju i zaposlenju, ograničiti tako da ih vide samo prijatelji (AZOP, 2020).

Također, postoji i opcija „Obavijest o prijavi“ koja šalje upozorenje svaki put kada se netko prijavi na svoj korisnički račun s novog mjesta ili preglednika. Ako se ne prepozna aktivnost

prijave, može se obavijestiti Facebook i zatim se omogućuje poništavanje i resetiranje lozinke te se tako osigura račun (AZOP, 2020).

Opcija „Dnevnik aktivnosti“ dozvoljava korisnicima da pregledaju i urede svoje Facebook aktivnosti, prilagode privatnost bilo koje objave te odrede pokazuje li se ona ili ne pokazuje na njihovoj vremenskoj traci (AZOP, 2020).

Još jedna korisna postavka na Facebooku koja služi zaštiti privatnosti je tzv. „*secure browsing*“. Kada je korisniku uključeno sigurno pregledavanje, njegova aktivnost na Facebooku se šifrira, gdje je to moguće, te se tako otežava pristup svima drugima njegovim podacima bez njegovog dopuštenja (AZOP, 2020).

Postoji i opcija „Prijavi/Ukloni oznaku“ koja se odnosi na uklanjanje oznake s fotografije na kojoj je neki korisnik označen. To je veoma korisno ako je osoba označena na fotografiji neprikladnog i nepoželjnog sadržaja, na krivotvorenim slikama ili u slučaju kada se korisniku jednostavno ne sviđa fotografija i ne želi biti označen na njoj (CARNet, 2015).

Savjeti na „*news feedu*“ podsjećaju ljude na različite načine kojima mogu kontrolirati i upravljati svojom privatnošću. Korisnike se podsjeća na to tko može vidjeti njihove objave, njihovu vremensku liniju ili status veze te kako funkcionira označavanje (AZOP, 2020).

Opcija „*Think Before You Share*“, odnosno „razmisli prije nego dijeliš“, je vodič Facebooka i MediaSmarts-a koji pomaže tinejdžerima da budu pažljiviji oko toga što dijele na mreži (AZOP, 2020).

„Provjera privatnosti“ ili engl. *Privacy checkup* je opcija koja služi za brzu i jednostavnu provjeru privatnosti na Facebooku. Korisnici mogu provjeriti tko može vidjeti njihove objave – nitko (ja), prijatelji, prijatelji prijatelja. Zatim se može vidjeti preko kojih aplikacija je osoba prijavljena na Facebook, njihovo korištenje te njihovo brisanje ako se više ne žele koristiti. Uz to, na brzim postavkama privatnosti se može provjeriti kome su dostupne pojedine informacije s osobnog profila korisnika, kao na primjer podaci o zaposlenju, o završenoj školi te o lokaciji na kojoj osoba živi (CARNet, 2020).

10. CERT

Nacionalni CERT (CERT.hr) je odjel Hrvatske akademske i istraživačke mreže – CARNET koji je osnovan 30. listopada 2007. godine. To je nacionalno tijelo čija je zadaća prevencija i zaštita od ugrožavanja sigurnosti javnih informacijskih sustava. Osim poduzimanja proaktivnih mjera kao što su sigurnosne preporuke, diseminacija informacija iz područja računalne sigurnosti ili unapređenje svijesti te edukacija i obuka o značaju računalne sigurnosti, Nacionalni CERT također provodi i reaktivne mjere kojima se odgovara na incidente koji ugrožavaju kibernetičku sigurnost javnih informacijskih sustava. Također, objavljuju i godišnja izvješća, brošure za sigurnije korištenje interneta kao i razne prezentacije i dokumente koji govore o problemima i mjerama zaštite. Tijekom 2020. godine zaprimljeno je i obrađeno 1710 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti. Najviše je slučajeva phishing URL, phishing i pogađanje zaporki (CERT, 2020).

TIP INCIDENTA	BROJ	TREND
PHISHING URL	446	▲
PHISHING	277	▲
POGAĐANJE ZAPORKI	205	▲
WEB DEFACEMENT	188	▲
MALWARE URL	132	▲
HOAX	116	▲
SUSTAV ZARAŽEN ZLONAMJERNIM KODOM	83	▲
POKUŠAJ ISKORIŠTAVANJA RANJIVOSTI	59	▲
SCAM	45	▲
SPAM	35	▼
KORISNIČKI RAČUN	29	▲
DOS - VOLUMETRIČKI NAPAD	27	▲
SPAM URL	21	▲
PRIJEVARE	13	▼
C&C	12	▲
SKENIRANJE	12	▲
ISPAD USLUGE (ENG. OUTAGE)	5	-
OSTALO	2	▼
DOSTUPNOST	1	-
DOS - NAPAD NA APLIKACIJSKOM SLOJU	1	-
ZLONAMJERNO RUDARENJE KRIPTOVALUTE (ENG. CRYPTOJACKING)	1	-
UKUPNO	**1710**	▲

Slika 1. Prikaz incidenata po tipu u 2020. godini

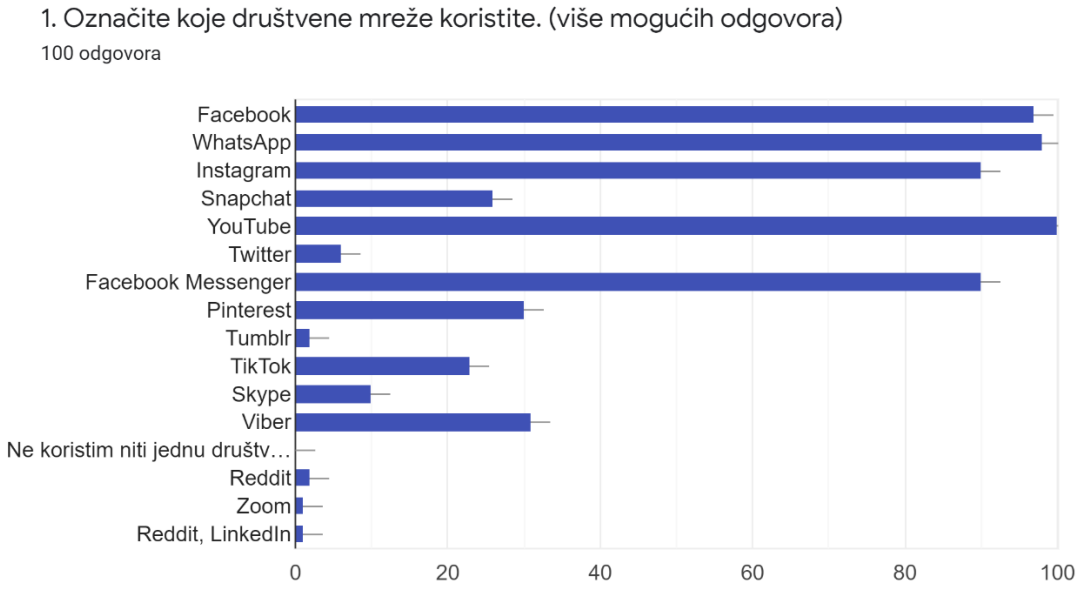
U prošloj godini CARNET-ov Nacionalni CERT predstavio je i dvije nove usluge – CERT ETA i CERT EPSILON. CERT ETA je namijenjena smanjenju količine neželjene pošte koju šalju pošiljatelji iz Hrvatske. CERT EPSILON omogućava korisnicima pretplatu i praćenje informacija o slabostima unutar programskih paketa nekih operativnih sustava (CERT, 2020).

11. Anketa „Zaštita privatnosti na društvenim mrežama“

U svrhu izrade završnog rada, provedena je kratka anketa na temu zaštite privatnosti na društvenim mrežama u kojoj je cilj bio ispitati sudionike kako oni koriste društvene mreže, u koju svrhu te kako štite svoje podatke i jesu li upoznati s prijetnjama na društvenim mrežama.

Istraživanje je provedeno preko Google obrazaca, bilo je u potpunosti anonimno i dobrovoljno. U anketi je sudjelovalo 100 ispitanika od kojih se 68% izjasnilo kao žensko, a 32% kao muško. Ispitanici su bili mlade osobe između 17 i 27 godina, od kojih je najviše osoba u dobi od 21 do 24 godine. Što se tiče obrazovanja, 25% ispitanika je završilo srednjoškolsko obrazovanje, 41% je na preddiplomskom studiju, a 23% na diplomskom studiju.

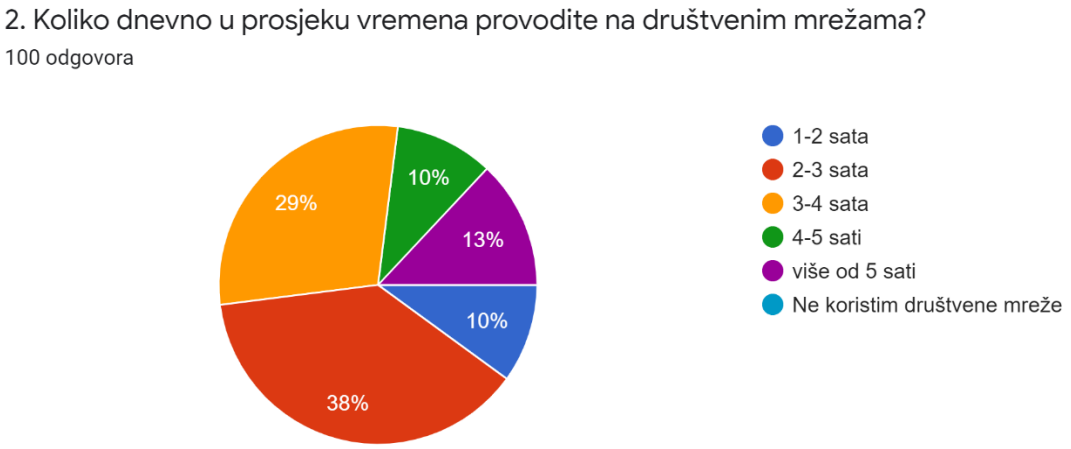
Prvo pitanje u anketi je višestruki izbor ponuđenih društvenih mreža koje ispitanici koriste uz mogućnost vlastitog nadopunjavanja. Svih 100 ispitanika je odgovorilo da koristi YouTube, 98 osoba koristi WhatsApp, 97 osoba se izjasnilo da koristi Facebook, a Instagram i Facebook Messenger koristi 90 ispitanika. Nakon toga slijedi Viber kojeg koristi 31 ispitanik, zatim Pinterest kojeg koristi 30 osoba, a Snapchat koristi 26 osoba, dok TikTok koriste 23 osobe. Na dnu ljestvice nalaze se Skype, Twitter, Tumblr, Reddit i Linkedln kao najmanje korištene društvene mreže.



Slika 2. Prvo pitanje iz ankete

Drugo pitanje se odnosi na dnevni prosjek vremena koje ispitanici provode na društvenim mrežama. Ispitanicima su ponuđeni odgovori: 1-2 sata, 2-3 sata, 3-4 sata, 4-5 sati, više od 5 sati i ne koristim društvene mreže. Najviše osoba, odnosno 38% koristi društvene mreže u prosjeku 2 do 3 sata dnevno. 29% osoba provodi 3 do 4 sata na društvenim mrežama, a 13% ispitanika

koristi društvene mreže više od 5 sati dnevno. 10 osoba provodi 1 do 2 sata, te također 10 osoba provodi 4 do 5 sati dnevno na društvenim mrežama. Nitko od ispitanika nije odgovorio da ne koristi društvene mreže.



Slika 3. Drugo pitanje iz ankete

Pitanje broj 3 vezano je uz uređaj preko kojeg se najčešće pristupa društvenim mrežama. Gotovo svi ispitanici, odnosno 96% se izjasnilo da društvenim mrežama pristupaju najčešće preko mobitela, što nije iznenađujuće jer je mobitel u današnje vrijeme uređaj bez kojeg se ne može, a i najlakše je na taj način pristupati svojim profilima na društvenim mrežama. 2% ispitanika najčešće koristi laptop, a također 2% najčešće koristi računalo za pristup društvenim mrežama.

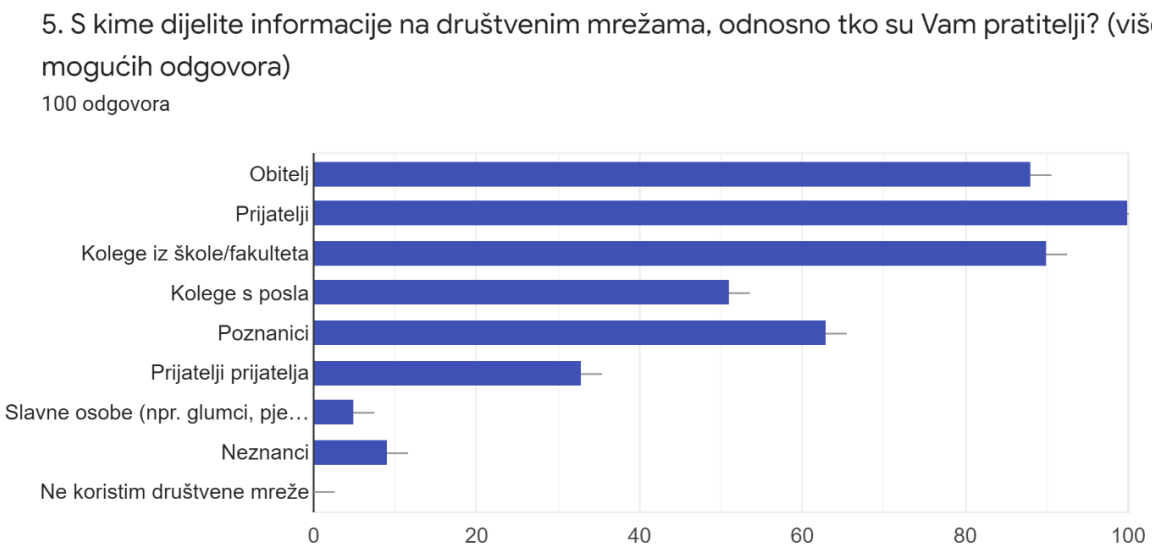
Slika 4. Treće pitanje iz ankete

Sljedeće pitanje odnosi se na konkretne informacije koje ispitanici dijele na svojim profilima na društvenim mrežama. Tu se ističu slike, 93% ispitanika odgovorilo je da na društvenim mrežama dijeli svoje fotografije. Zatim slijede informacije o školovanju koje dijeli 72%

ispitanika, datum rođenja dijeli 69% osoba, a događaje iz života kao na primjer odlazak na kavu, izlete, odmore. . . dijeli 68% osoba na svojim društvenim mrežama. Ispitanici također često dijele svoje videozapise, lokaciju te broj mobitela ili telefona. Najmanje se dijele informacije o poslu i zaposlenju te vlastiti stavovi i mišljenja o određenim popularnim temama, te informacije na društvenim mrežama dijeli samo 16% ispitanika. Većina tih informacija i podataka, kao na primjer datum rođenja, podaci o školovanju i zaposlenju te slike, vrlo su osobne prirode i prema navedenim postocima, velika većina osoba te podatke javno dijeli na svojim društvenim mrežama i oni su dostupni zlonamjernim korisnicima. Nitko od ispitanika ne dijeli na svojim društvenim mrežama informacije o osobnim financijama te informacije o svojim lozinkama i PIN-ovima.

Slika 5. Četvrto pitanje iz ankete

U pitanju broj 5 traži se od ispitanika da označe s kime sve dijele svoje informacije i podatke na društvenim mrežama, odnosno tko su im sve pratitelji. Svi ispitanici odgovorili su da svoje podatke dijele sa prijateljima. 90% osoba dijeli informacije sa kolegama iz škole, odnosno fakulteta, a 88% osoba dijeli na društvenim mrežama informacije s članovima obitelji. Sa poznanicima informacije dijeli 63% osoba, a s kolegama na poslu 51% ispitanika. 33% osoba dijeli svoje podatke sa prijateljima prijatelja, a čak 9% ispitanika dijeli informacije na društvenim mrežama s neznancima. Tu je vidljivo da većina korisnika obraća pažnju na to s kime točno dijele svoje informacije i da su to većinom prijatelji, obitelj, kolege i poznanici, a rjeđe su to prijatelji prijatelja ili neznanci.



Slika 6. Peto pitanje iz ankete

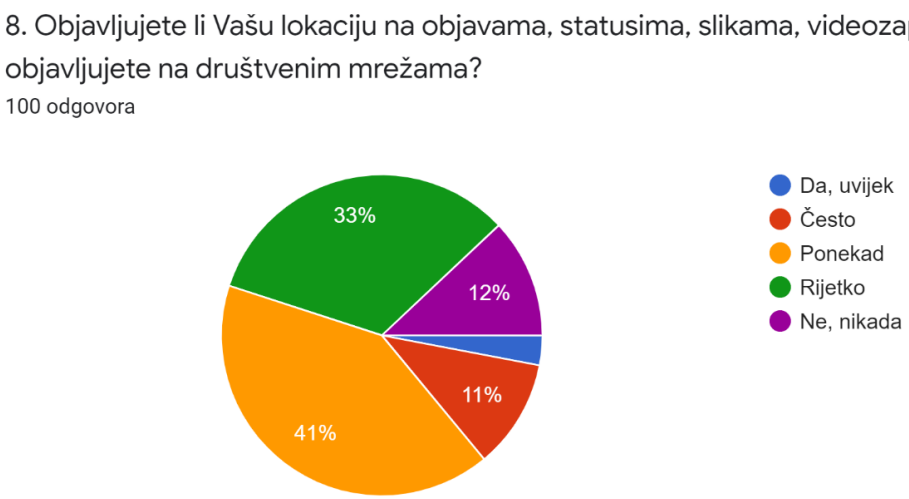
Pitanje broj 6 odnosi se na pratitelje ispitanika na društvenim mrežama, odnosno koje sve skupine ljudi ispitanici prate na svojim profilima. Najzastupljenija skupina koju ispitanici prate su prijatelji, tu skupinu prati 98% osoba, zatim slijede školski kolege i kolege s fakulteta koje prati 94% ispitanika i obitelj koje prati 89% ispitanika. Na četvrtom mjestu bi bila skupina poznanika koju prati 71% osoba na društvenim mrežama i zatim slavne osobe (npr. glumci, pjevači, plesači, sportaši, kuhari, influenceri . . .) koje prati 68% ispitanika. Kolege s posla preko društvenih mreža prati manje od 50% ispitanika, a prijatelje prijatelja prati malo više od 30% osoba. 9% ispitanika prati neznance preko svojih profila na društvenim mrežama, a 1% ispitanika izjasnilo se da ne prati nikoga na svojim društvenim mrežama.

Slika 7. Šesto pitanje iz ankete

Sedmo pitanje se odnosi na prihvaćanje zahtjeva za prijateljstvo/zahtjeva za praćenje od nepoznatih osoba. 57% ispitanika se izjasnilo da nikada ne prihvaća zahtjeve od stranaca, 33% odgovorilo je da rijetko prihvaća takve zahtjeve, a 10% ispitanika ponekad prihvaća zahtjeve od nepoznatih osoba. Može se zaključiti kako su korisnici društvenih mreža oprezni kod zahtjeva za praćenje ili zahtjeva za prijateljstvo koje dobivaju te da većinom nikada ili samo rijetko prihvaćaju takve zahtjeve od stranaca. Niti jedan sudionik nije izjavio da često ili uvijek prihvaća navedene zahtjeve.

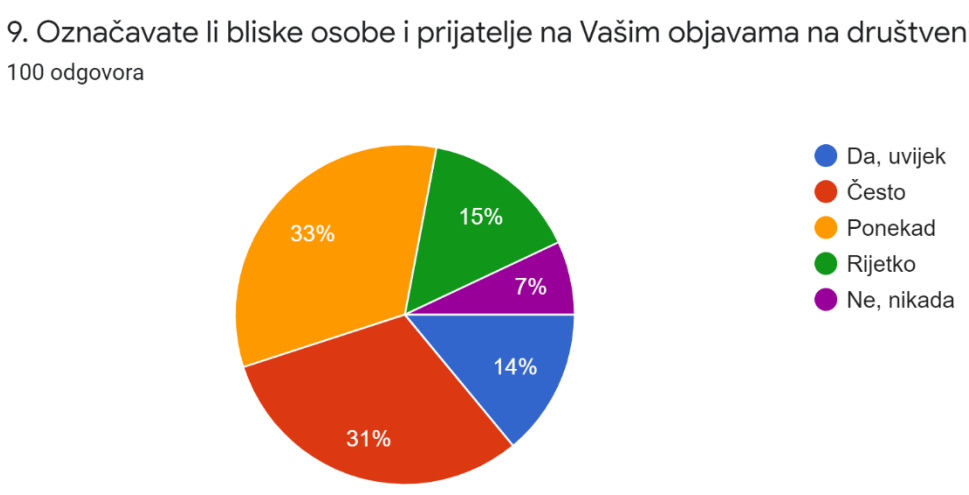
Slika 8. Sedmo pitanje iz ankete

U osmom pitanju se želi vidjeti objavljuju li ispitanici svoju lokaciju na objavama, statusima, slikama, videozapisima i slično na društvenim mrežama. 3 osobe odgovorile su da uvijek objavljuju svoju lokaciju, 11 osoba često objavljuje na društvenim mrežama lokaciju dok 12 osoba nikada ne objavljuje taj podatak. Najviše osoba, odnosno 41 osoba svoju lokaciju na društvenim mrežama objavljuje ponekad, a 33 ispitanika rijetko objavljuje svoju lokaciju na objavama i statusima, slikama ili videozapisima.



Slika 9. Osmo pitanje iz ankete

Deveto pitanje odnosi se na označavanje bliskih osoba i prijatelja na objavama na društvenim mrežama. Najzastupljeniji odgovori su ponekad i često. 33% ispitanika odlučilo se za ponekad, a 31% ispitanika za često. 15% osoba rijetko označuje bliske osobe i prijatelje na objavama na društvenim mrežama, a 14% uvijek. Samo 7% ispitanika odgovorilo je da nikada ne označavaju svoje prijatelje i bliske osobe na objavama koje stavljaju na društvene mreže. Označavanje bliskih prijatelja, obitelji ili poznanika može ugroziti njihovu privatnost u slučaju da zlonamjerni korisnik želi naštetiti što većem broju osoba.



Slika 10. Deveto pitanje iz ankete

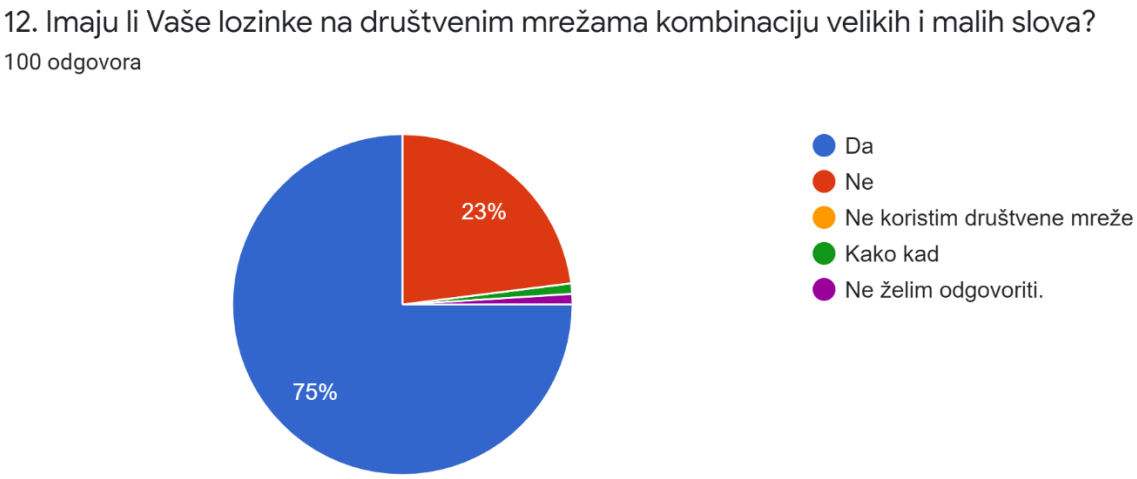
Sljedeća 4 pitanja odnose se na lozinke korisnika društvenih mreža. Prvo takvo pitanje je koriste li ispitanici istu lozinku za više društvenih mreža. 51% ispitanika izjasnilo se za „NE“, a 48% se izjasnilo za „DA“ dok 1 osoba nije htjela odgovoriti.

Slika 11. Deseto pitanje iz ankete

Zatim se od ispitanika htjelo saznati imaju li njihove lozinke više od 6 znakova. Tu je 98% osoba odgovorilo potvrdno, 1 osoba se nije htjela izjasniti, a 1 osoba je odgovorila kako na društvenim mrežama nema lozinke sa više od 6 znakova.

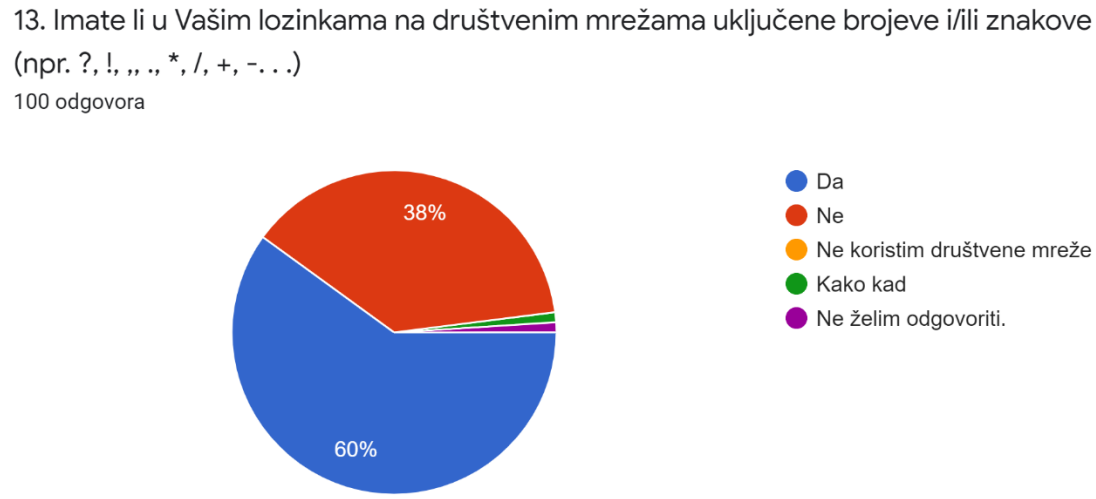
Slika 12. Jedanesto pitanje iz ankete

Nakon toga je postavljeno pitanje imaju li zaporke korisnika na društvenim mrežama kombinaciju velikih i malih slova. Na to pitanje 75% ispitanika odgovara da imaju, a 23% ispitanika nema u svojim lozinkama kombinacije velikih i malih slova. 1 osoba odgovara sa kako kad, a 1 osoba se ne želi izjasniti.



Slika 13. Dvanaesto pitanje iz ankete

Zadnje pitanje vezano uz lozinke je imaju li korisnici društvenih mreža u svojim lozinkama uključene brojeve i/ili znakove i simbole kao na primjer ?, !, ,, ., *, +, -, /, i slično. 60% ispitanika odgovara sa „DA“, dok 38% odgovara sa „NE“. Također, 1 osoba ne želi odgovoriti, a 1 osoba odgovara sa kako kad.

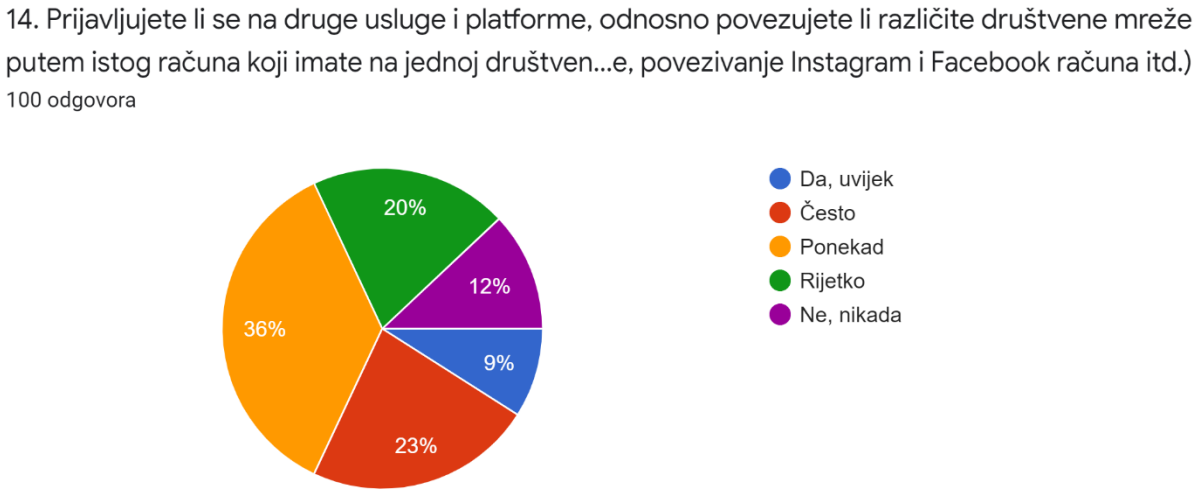


Slika 14. Trinaesto pitanje iz ankete

Ova pitanja vezana uz lozinke postavljena su na način da se iz njih sazna koliko jake i složene lozinke ispitanici koriste na društvenim mrežama. Što se tiče korištenja iste lozinke za više društvenih mreža, ispitanici su podijeljeni na pola i zapravo veliki postotak, odnosno 48% ispitanika ima istu zaporku koju koristi na više društvenih mreža, a za zaštitu korisničkih računa, najbolje bi bilo koristiti različite lozinke. Zatim je ispitana dužina lozinke na društvenim mrežama. Tu su rezultati veoma dobri i gotovo svi ispitanici (98%) koriste lozinke koje imaju više od 6 znakova na svojim društvenim mrežama. Sljedeće pitanje vezano je uz kombinaciju

velikih i malih slova u zaporkama. Tu je vidljivo kako jačina lozinke pomalo slabi jer čak 23% ispitanika ne koristi velika i mala slova u svojim lozinkama. Zatim je ispitana još veća složenost zaporke, a to je korištenje brojeva i/ili znakova i simbola kod zaporaka na društvenim mrežama. Tu se opet broj osoba koje nemaju uključene brojeve, znakove i simbole u svojim lozinkama povećao, odnosno 38% ispitanika odgovorilo je sa „NE“. Doduše, postotak ispitanika koji ima lozinke duže od 6 znakova, koji koristi kombinaciju velikih i malih slova te koji ima uključene brojeve i/ili znakove, još uvijek nije toliko nizak da bi to bilo zabrinjavajuće.

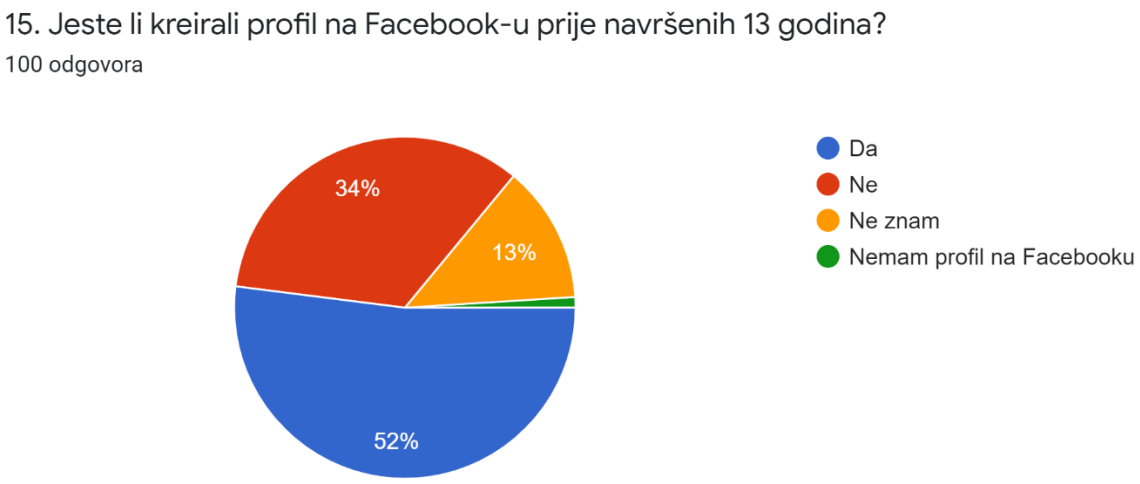
Pitanje broj 14 odnosi se na prijavljivanje na druge usluge i platforme putem računa na društvenim mrežama, kao i na prijavljivanje na različite društvene mreže putem istog računa koji se ima na jednoj društvenoj mreži. To bi na primjer bila prijava na online trgovine preko Facebook računa ili povezivanje Instagram i Facebook računa. 9% ispitanika odgovara kako se uvijek prijavljuju na druge usluge i platforme putem računa na nekoj društvenoj mreži, a 12% ispitanika odgovara da nikada to ne radi. Najviše osoba se odlučilo za odgovor „ponekad“, točnije 36% ispitanika, 23% ispitanika odlučilo se za „često“, a 20% ispitanika za „rijetko“. Korisnicima se takvom prijavom olakšava jer se uvijek koristi isto korisničko ime i lozinka, ali s druge strane to može imati i negativnu posljedicu jer kompromitacija jednog profila i računa na društvenoj mreži znači i kompromitaciju svih ostalih povezanih servisa i usluga preko tog računa.



Slika 15. Četrnaesto pitanje iz ankete

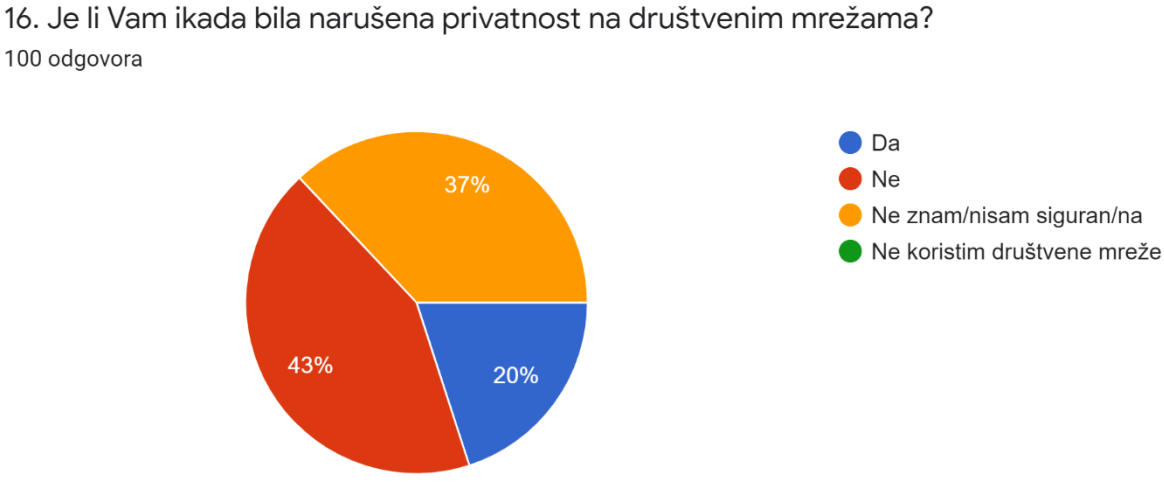
Petnaesto pitanje glasi: „Jeste li kreirali profil na Facebook-u prije navršenih 13 godina?“. 52% ispitanika odgovara potvrdno na ovo pitanje, a čak 13% ne zna kada su kreirali račun na Facebook-u. 34% ispitanika je bilo starije od 13 godina kada su pristupili navedenoj društvenoj mreži, a 1% ispitanika nema profil na Facebook-u. Ovdje je vidljivo da se Facebook račun može

bez problema otvoriti i prije navršenih 13 godina života i da je nešto malo više od 50% ispitanika uspjelo to iako Facebook zahtijeva minimalnu dob od 13 godina prije kreiranja korisničkog profila.



Slika 16. Petnaesto pitanje iz ankete

Šesnaesto pitanje odnosi se na narušavanje privatnosti korisnika društvenih mreža. 20% ispitanika odgovara da im je privatnost na društvenim mrežama na neki način bila narušena, a 43% osoba odgovara da nije. Iznenađujuće je da čak 37% osoba ne zna ili nije sigurno je li im ikada bila narušena privatnost.



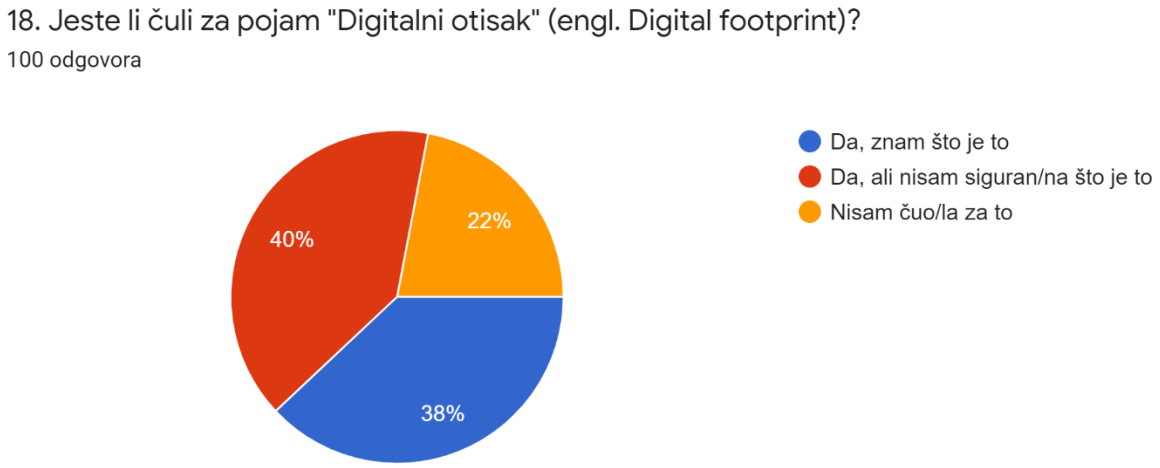
Slika 17. Šesnaesto pitanje iz ankete

Sljedeće pitanje je hipotetski postavljeno, odnosno pitanje glasi: „Mislite li da bi Vam privatnost na društvenim mrežama mogla biti narušena?“. 9% osoba smatra da ne bi, 12% posto

ne zna ili nije sigurno. Velik postotak ispitanika, odnosno 48% smatra da bi im privatnost možda mogla biti narušena, a 31% osoba odgovara sa „DA“.

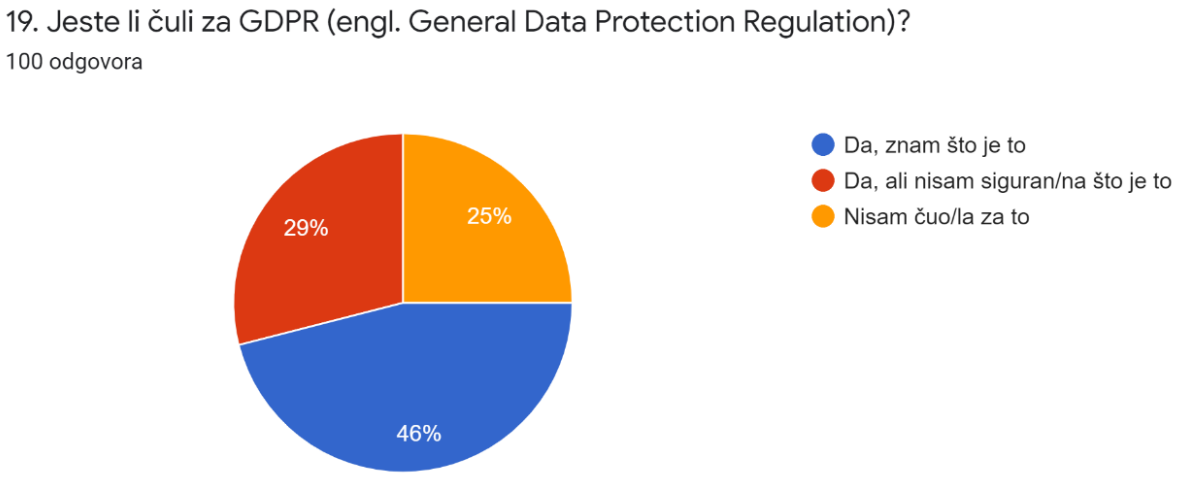
Slika 18. Sedamnaesto pitanje iz ankete

Osamnaesto pitanje se odnosi na pojam „Digitalni otisak“ (engl. *Digital footprint*). Ispitanicima su bila ponuđena tri odgovora: 1. da, znam što je to, 2. da, ali nisam siguran/na što je to i 3. nisam čuo/la za to. 38% osoba odgovara da znaju što je „Digitalni otisak“, dok 22% ispitanika nije čulo za taj pojam, a čak 40% osoba nije uopće sigurno što je „Digitalni otisak“ i na što se taj pojam odnosi.



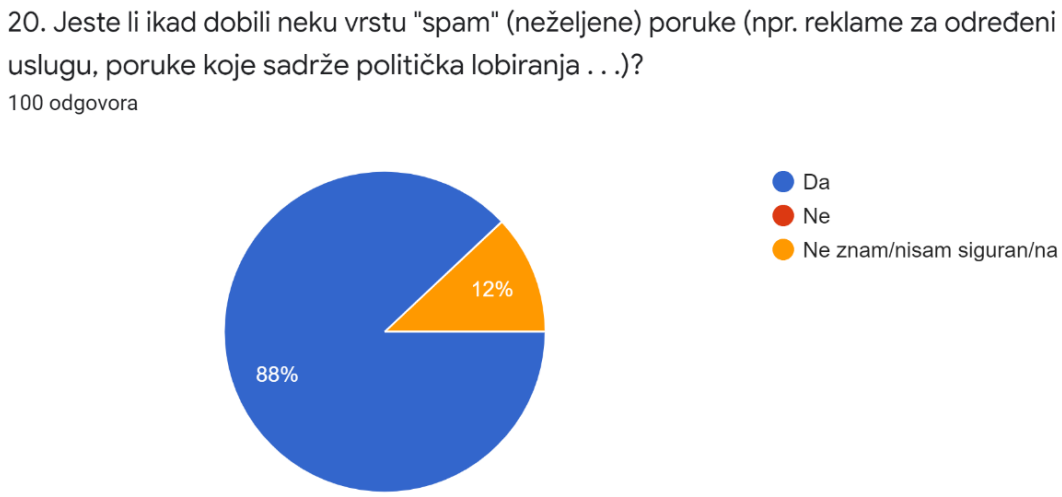
Slika 19. Osamnaesto pitanje iz ankete

Pitanje broj 19. odnosi se na *General Data Protection Regulation*, odnosno skraćeno GDPR. 25% ispitanika nije uopće čulo za taj pojam, dok je 29% ispitanika čulo za GDPR, ali nisu sigurni što je to. Ostalih 46% odgovara da su čuli i da znaju što je *General Data Protection Regulation*.



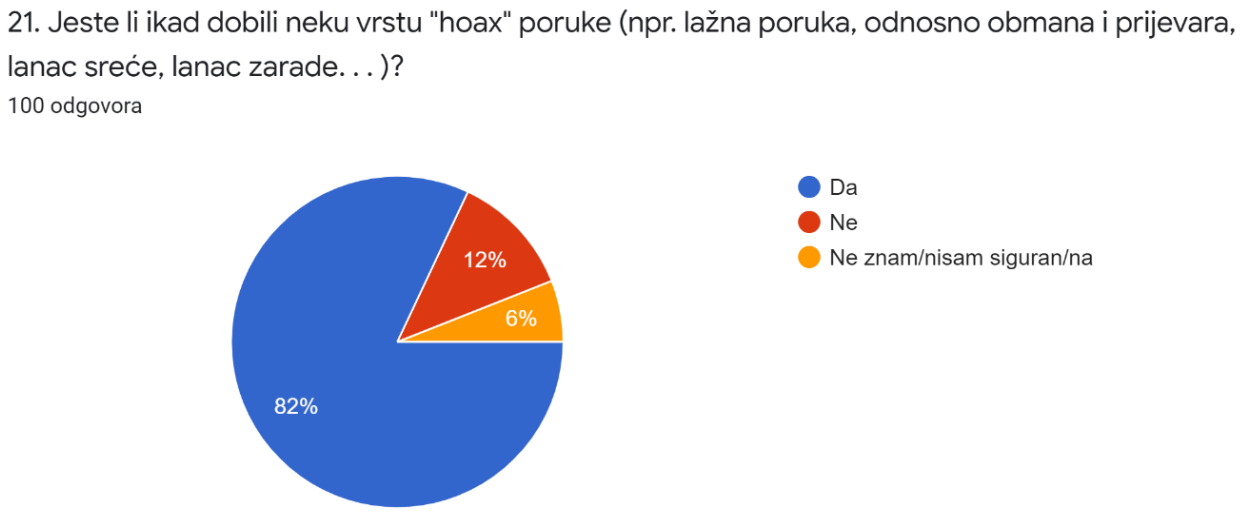
Slika 20. Devetnaesto pitanje iz ankete

U sljedećem pitanju se od ispitanika traži da odgovore jesu li ikad dobili neku vrstu „spam“ (neželjene) pošte, kao na primjer reklame za određeni proizvod ili uslugu, poruke koje sadrže politička lobiranja i slično. 88% korisnika društvenih mreža se izjasnilo da su primili poruke neželjene pošte, dok 12% ispitanika ne zna, odnosno nije sigurno jesu li dobili neku vrstu „spam“ poruke. Jasno je da je u današnjem svijetu gotovo nemoguće izbjeći „spam“ poruke.



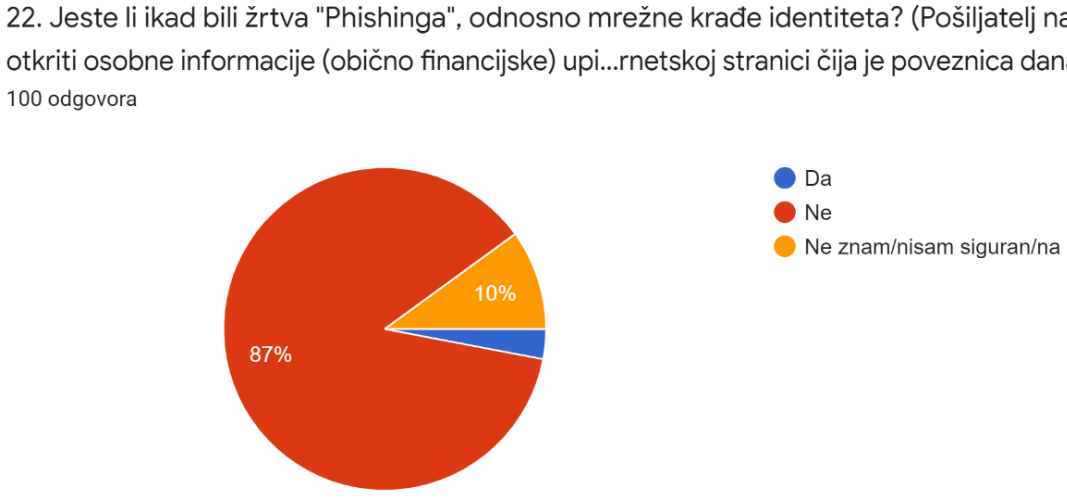
Slika 21. Dvadeseto pitanje iz ankete

Zatim se od ispitanika traži da odgovore na pitanje jesu li ikad dobili neku vrstu „hoax“ poruke. Također su im ponuđeni primjeri takvih poruka: lažna poruka, odnosno obmana i prijevara, lanac sreće, lanac zarade . . . 12 osoba odgovara da nisu dobili „hoax“ poruku u inbox ili e-mail sandučić. 82 ispitanika se izjašnjava da jesu primili takvu vrstu poruke, a 6 osoba nije sigurno ili ne zna. Uz neželjenu poštu, odnosno „spam“, vrlo je često da korisnici na društvenim mrežama dobivaju i „hoax“ poruke.



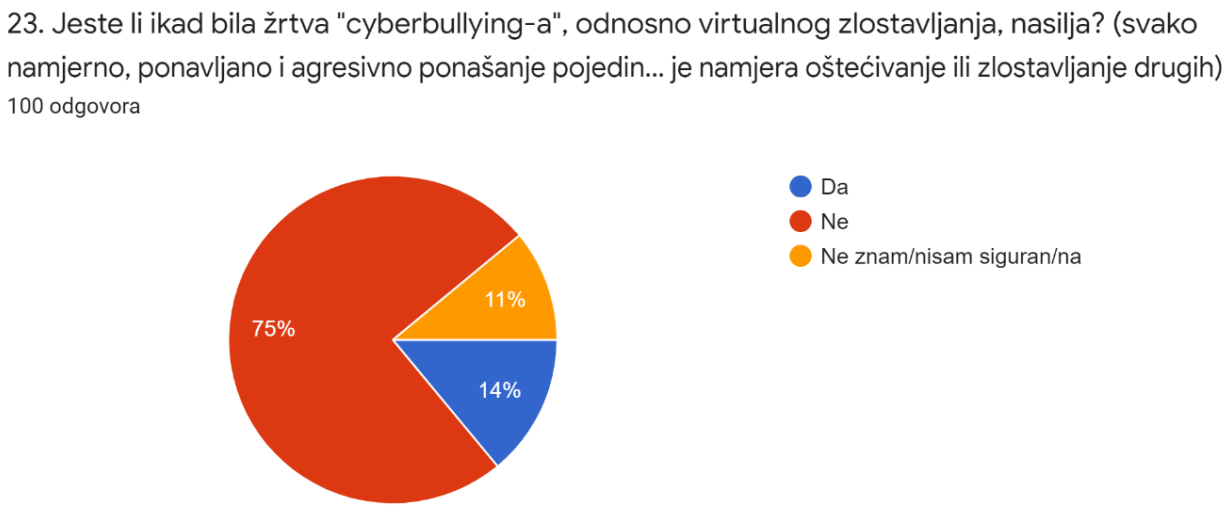
Slika 22. Dvadesetprvo pitanje iz ankete

U 22. pitanju se traži od ispitanika da odgovore jesu li ikad bili žrtva „*phishinga*“, odnosno mrežne krađe identiteta. Tu se radi o situacijama kada pošiljatelj takve poruke navodi osobu da mu otkrije osobne, često financijske informacije preko lažirane internetske stranice čija se poveznica također nalazi u poruci. 87% ispitanika izjašnjava se da nisu bili žrtve „*phishinga*“, dok je 3% ispitanika bilo. Ostalih 10% ne zna ili nije sigurno jesu li doživjeli mrežnu krađu identiteta.



Slika 23. Dvadesetdrugo pitanje iz ankete

Dvadesettreće pitanje odnosi se na virtualno zlostavljanje i nasilje, odnosno „*cyberbullying*“. 14% ispitanika izjasnilo se kako su bili žrtve zlostavljanja i nasilja na društvenim mrežama, 11% odgovara da nisu sigurni, a većina ispitanika, odnosno konkretnije 75% odgovara da se nisu našli u takvoj situaciji.



Slika 24. Dvadesettreće pitanje iz ankete

Pitanje broj 24 glasi: „Je li Vam ikad netko provalio na neki profil na društvenim mrežama?“. 63% osoba odgovara da nisu doživjeli provaljivanje na društvene mreže, dok 22% ispitanika nije bilo te sreće te im je netko provalio na profil. 15% osoba uopće nije sigurno ili ne znaju jesu li bili takav slučaj.

Slika 25. Dvadesetčetvrto pitanje iz ankete

U posljednjem pitanju u anketi želi se saznati smatraju li ispitanici da bi se o zaštiti privatnosti na društvenim mrežama trebalo više govoriti i osvijestiti ljude o tome. Jako velik postotak, konkretnije 94% smatra da je to svakako potrebno, 5% osoba odgovorilo je sa možda, a 1 osoba ne vidi potrebu za time. Iz ovog pitanja je jasno da ljudi nisu dovoljno informirani o opasnostima koje postoje na društvenim mrežama i konkretnoj zaštiti svoje privatnosti te da su

svjesni toga i smatraju da bi se puno više pažnje trebalo posvetiti osvještavanju korisnika društvenih mreža o mogućnostima zaštite svojih osobnih podataka.

Slika 26. Dvadesetpeto pitanje iz ankete

Ova anketa je provedena da bi se saznalo kako ispitanici koriste svoje društvene mreže, odnosno kako štite svoju privatnost, jesu li na neki način doživjeli ugrožavanje privatnosti te koliko su upoznati s nekim pojmovima vezanim uz prijetnje i zaštitu podataka na društvenim mrežama. Na temelju dobivenih rezultata, može se zaključiti da je anketa obuhvatila mlade i obrazovane ljude između 17 i 27 godina od kojih je većina završila srednju školu ili se nalazi trenutno na preddiplomskom ili diplomskom studiju. Kao najkorištenije i najpopularnije društvene mreže ističu se YouTube, WhatsApp, Facebook, Instagram, Facebook Messenger, Viber, Pinterest . . . S obzirom na to, jasno je da ispitanici nisu korisnici samo jedne društvene mreže i da nemaju profil na samo jednoj društvenoj mreži, nego na više njih. Prosječno vrijeme koje se provodi na društvenim mrežama bilo bi otprilike između 3 i 4 sata dnevno, a uređaj preko kojeg se najčešće pristupa profilima na društvenim mrežama je mobitel.

U osobne podatke ubrajaju se između ostaloga ime i prezime, datum rođenja, adresa stanovanja, e-mail adresa, podaci o školovanju i o zaposlenju, zatim lokacija, slike i videozapisi te podaci o političkim, vjerskim, filozofskim uvjerenjima i slično. Od ispitanika se tražilo da navedu koje konkretno informacije dijele na svojim društvenim mrežama te je iz Slike 5. vidljivo da velik broj ispitanika dijeli upravo takve informacije, kao na primjer datum rođenja, podatke o školovanju i poslu, svakodnevna događanja u životu, lokaciju te videozapise i slike. Doduše, takvi se podaci dijele i dostupni su najviše prijateljima, obitelji, kolegama iz škole, odnosno fakulteta i poznanicima. Vrlo rijetko osobe svoje podatke dijele sa prijateljima prijatelja, slavnim osobama ili neznancima iako ima i takvih slučajeva. Zlonamjerni korisnici prvo

prikupljaju sve dostupne informacije o potencijalnoj žrtvi, zatim uspostavljaju neki kontakt s njom i na kraju dolazi do realizacije napada i ugrožavanja privatnosti te je stoga potrebno obratiti pozornost kome su sve dostupni naši privatni podaci. Iz ankete je vidljivo da ispitanici zapravo postupaju s oprezom kada se radi o zahtjevima za prijateljstvo i zahtjevima za praćenje od nepoznatih osoba jer se takvi zahtjevi nikada ili samo rijetko prihvaćaju. Što se tiče objave lokacije, tu nedostaje opreza jer se takva informacija olako javno objavljuje na društvenim mrežama kao i objave u kojima se označavaju bliske osobe i prijatelji. Time se ugrožava vlastita sigurnost jer zlonamjerne osobe mogu lokaciju iskoristiti za uhođenje, a označavanjem bliskih osoba ugrožava se i njihova privatnost. Prva stavka kod zaštite vlastitih profila na društvenim mrežama je korištenje složenih i jakih lozinki. Na temelju rezultata ankete može se zaključiti da se gotovo uvijek koriste lozinke sa više od 6 znakova, te većina ispitanika ima neku kombinaciju velikih i malih slova i uključene brojeve i/ili znakove i simbole u lozinkama. Poželjno je imati što složenije lozinke i različite za različite društvene mreže jer je tako teže provaliti na profil neke osobe i zloupotrijebiti njezine podatke. Popularno je i povezivanje, odnosno prijava na druge platforme i usluge putem računa na nekoj društvenoj mreži.

Iznenađujuće je da određeni postotak ispitanika, odnosno mladih ljudi koji se svakodnevno služe društvenim mrežama, ne zna ili nije sigurno je li im privatnost na društvenim mrežama ikad bila narušena, ali smatraju da bi se to svakako ili možda moglo dogoditi u budućnosti. Također, pojam „Digitalni otisak“ (engl. *Digital footprint*) koji se odnosi na podatke koji se ostavljaju iza sebe svaki put kada se koristi Internet, bilo da je riječ o posjećenim stranicama, poslanoj elektroničkoj pošti, objavljenim slikama i videozapisima, pretraživanim pojmovima, prijavama na lokacijama i slično, većina osoba ne zna definirati ili nisu sigurni što bi to bilo ili uopće nisu čuli za to. Slična situacija je i sa pojmom GDPR (engl. *General Data Protection Regulation*). Čulo se za taj pojam, ali ga se ne može konkretno definirati ili se uopće ne zna što je to.

Od najčešćeg zlonamjernog sadržaja izdvaja se „spam“, „hoax“ i „phishing“. „Spam“ poruke, odnosno poruke neželjenog sadržaja vrlo su česta i gotovo svakodnevna pojava koju se teško izbjegava. Većinom su samo uznemirujuće za osobu i troše njezino vrijeme te energiju za pregledavanje i brisanje takvog sadržaja. Osim „spama“, jako česte su i „hoax“ poruke kojima je većinom cilj zastrašivanje i dezinformiranje osobe ili pak narušavanje nečijeg ugleda. Što se tiče „phishinga“, ono nije previše zastupljeno ili osobe jednostavno nisu svjesne da su bile žrtve takvog napada jer poruke većinom izgledaju vjerodostojno originalnim porukama iz banke ili servisa za elektroničko plaćanje, a razlozi su često logični kao npr. unapređenje sustava,

provjeravanje podataka, oporavak računa, nadogradnja i slično. Iako se obično smatra da je „*cyberbullying*“ dosta raširen među djecom i mladima, ova anketa je pokazala da to nije slučaj. Velika većina ispitanika nisu bili žrtve virtualnog zlostavljanja i nasilja.

Iz svega navedenoga, a i prema mišljenjima ispitanika, potrebno je informirati, osvijestiti i educirati ljude o zaštiti privatnosti na društvenim mrežama. Digitalni tragovi ne nestaju, već su neodvojiv dio identiteta nekog korisnika. Čak i nakon što se neka objava, slika, videozapis ili slično izbriše, svaka ta informacija koja se objavi na internetu, tamo i ostaje. Prema Zakonu o zaštiti osobnih podataka, određeni podaci se smiju prikupljati i dalje obrađivati ako je osoba sama objavila te podatke. To je činjenica o kojoj mnogi ne razmišljaju i stoga se ne obraća dovoljno pažnje na informacije koje se stavljaju dostupnima za javnost te da bi se među pratiteljima i osobama koje imaju pristup nečijim određenim osobnim podacima, mogli nalaziti i zlonamjerni korisnici kojima je u interesu nanijeti štetu i narušiti nečiju tuđu privatnost.

12. Zaključak

Društvene mreže su uvelike olakšale komunikaciju i upoznavanje te stupanje u kontakt, bilo s poznatim osobama i bližnjima, ali i s potpunim strancima. Dijeljenje osobnih podataka, interesa, slika i videozapisa može omogućiti pronalazak drugih osoba sa sličnim interesima. Ali s druge strane, nesmotreno i neoprezno te neprikladno ponašanje na internetu, može dovesti do raznih neželjenih posljedica. Zlonamjerni korisnici koriste svaku priliku kako bi pronašli žrtvu za napad i naštetili joj. Napadi mogu biti raznovrsni, od krađe osobnih podataka pa s time i identiteta osoba, do ubacivanja zlonamjernih programa u računalo žrtve. Mnogi ne razmišljaju o posljedicama klika na neku sumnjivu poveznicu ili o posljedicama dijeljenja lokacije i privatnih informacija s drugim korisnicima. Većinom svaka prevara, lažno predstavljanje, krađa osobnih i drugih podataka na kraju krajeva imaju neki financijski motiv u pozadini ili činjenje štete ugledu korisnika. Kako bi se izbjegle takve situacije, prva mjera bi trebala biti edukacija svih osoba koje su korisnici bilo koje društvene mreže i interneta općenito. Ako se osoba na internetu ne ponaša neodgovorno i ako ne zanemaruje sumnjive sadržaje i sumnjive korisnike te svoje privatne podatke drži samo za sebe ili sebi bliske osobe, onda je šansa za zlonamjerni napad na privatnost i osobne podatke takvog korisnika minimalna. Doduše, kratko istraživanje provedeno na ovu temu, pokazalo je da mladi danas s obzirom na mnogobrojne društvene mreže koje koriste i s obzirom na dnevni prosjek vremena koji provode na njima, vrlo olako shvaćaju opasnosti koje prijete vezano uz narušavanje privatnosti. Velika većina svakodnevno dobiva različite „spam“ i „hoax“ poruke, a postoje i oni koji su bili žrtve „*phishinga*“ ili „*cyberbullyinga*“ ili im je jednostavno provaljeno na profil na nekoj društvenoj mreži. Prva linija zaštite vlastite privatnosti jest korištenje jake i složene lozinke koja je različita za svaku društvenu mrežu. Zatim je važno ograničiti osobe kojima su dostupni naši osobni podaci i obratiti pažnju na sumnjive sadržaje i linkove stanica koji često dolaze kao privitak u porukama. Ohrabrujuće je to da su ljudi svjesni potrebe informiranja i educiranja o ovoj temi jer do zlouporabe tuđih osobnih podataka, a s time i narušavanja privatnosti neke osobe, dolazi zbog nesmotrenosti, neopreznosti, a ponajviše neznanja korisnika društvenih mreža.

13. Literatura

1. Agencija za zaštitu osobnih podataka, Promotivni materijali: Letci/brošure/priručnici, dostupno na: https://azop.hr/promotivni-materijali/, [02. lipnja 2021.]
2. Agencija za zaštitu osobnih podataka (2020), Safety@Facebook, dostupno na: https://azop.hr/wp-content/uploads/2020/12/safetyaoc_brochure_v3__uk.pdf, [14. lipnja 2021.].
3. Agencija za zaštitu osobnih podataka (2011), sigurno surfanje! zaštita osobnih podataka na internetu, dostupno na: https://azop.hr/wp-content/uploads/2020/12/sigurno_surfanje-1.pdf, [01. srpnja 2021.].
4. Borovac, T., Horvat, I., Nenadić, K., Romstein, K., Šolić, K., Velki, T., Vuković, M. (2018) Priručnik za informacijsku sigurnost i zaštitu privatnosti. Osijek: Fakultet za odgojne i obrazovne znanosti.
5. CARNet (2007), Dodjeljivanje IP adresa, dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-09-203.pdf, [05. svibnja 2021.].
6. CARNet (2005), Spam, dostupno na: https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2005-02-108.pdf, [11. svibnja 2021.].
7. CARNet (2015), Zaštitite privatnost na Facebooku, dostupno na: https://www.cert.hr/wp-content/uploads/2018/02/BrosuraPrivatnost_2015_0.pdf, [14. lipnja 2021.].
8. CERT.hr surfaj sigurnije (2020), Godišnji izvještaj Nacionalnog CERT-a za 2020. godinu, dostupno na: https://www.cert.hr/wp-content/uploads/2021/02/Carnet_Cert_godisnji_izvjestaj_2020_0402-3.pdf, [05. svibnja 2021.].
9. CERT.hr surfaj sigurnije, Hoax, dostupno na: https://www.cert.hr/19795-2/hoax/, [11. svibnja 2021.].
10. CERT.hr surfaj sigurnije (2016), Ne budi i ti hrvatski naivac: #SurfajSigurnije na društvenim mrežama, dostupno na: https://www.cert.hr/wp-content/uploads/2019/04/bro%C5%A1ura-sigurnost-dru%C5%A1tvenih-mre%C5%BEa.pdf?fbclid=IwAR0jc0O0AvRPh1etvjVZqWimWzv6fN72VUikdnWksI9Yv7mQFn3NpqhBFSc, [28. lipnja 2021.].
11. CERT.hr surfaj sigurnije, O socijalnom inženjeringu, dostupno na: https://www.cert.hr/socijalni_inzenjering/, [01. srpnja 2021.].

12. CERT.hr surfaj sigurnije, Phishing, dostupno na: https://www.cert.hr/phishing/, [12. svibnja 2021.].
13. CERT.hr surfaj sigurnije, Ransomware, dostupno na: https://www.cert.hr/19795-2/ransomware/, [12. svibnja 2021.].
14. Deljac, S., Gregurić, V., Hajdinjak, N., Počuča, B., Rakić, D. i Svetličić, S. (2020) Informatika 6: udžbenik u šestom razredu osnovne škole. Zagreb: Profil Klett d. o. o. , str. 120-122.
15. e-Građani, Osobni podaci – zaštita osobnih podataka, dostupno na: https://gov.hr/hr/osobni-podaci-zastita-osobnih-podataka/1888, [01. srpnja 2021.].
16. Europska komisija, predstavništvo u Hrvatskoj, Što je to „sigurnost na internetu“ i kako zaštititi osobne podatke na internetu?, dostupno na: https://ec.europa.eu/croatia/education/what_is_safety_on_internet_and_how_to_protect_personal_data_online_hr, [05. svibnja 2021.].
17. Europska komisija, predstavništvo u Hrvatskoj (2019), Zaštitite svoju privatnost na društvenim mrežama, dostupno na: https://ec.europa.eu/croatia/secure_privacy_on_social_networks_hr, [03. svibnja 2021.].
18. GDPR informer (2018), Vodič kroz GDPR za početnike, dostupno na: https://gdprinformer.com/hr/vodic-kroz-gdpr, [31. svibnja 2021.].
19. Hrvatska enciklopedija, mrežno izdanje (2021) Facebook, Leksikografski zavod Miroslav Krleža, dostupno na: https://www.enciklopedija.hr/natuknica.aspx?id=68087, [03. srpnja 2021.].
20. Hrvatski jezični portal – Znanje, privátnōst, dostupno na: https://hjp.znanje.hr/index.php?show=search_by_id&id=dl9mWxc%253D, [01. srpanja 2021.].
21. Kempt, S. (2021), Digital 2021 April Global Statshot Report, dostupno na: https://datareportal.com/reports/digital-2021-april-global-statshot, [06. svibnja 2021.].
22. Kuća ljudskih prava Zagreb / Human Rights House Zagreb (2019), Privatnost kao ljudsko pravo, dostupno na: https://www.kucaljudskihprava.hr/2019/12/18/privatnost-kao-ljudsko-pravo/, [01. srpnja 2021.].
23. Miller, M. (2003) Apsolutna zaštita PC-ja i privatnosti. Čačak: Kompjuter biblioteka. str. 280.-281.
24. Narodne novine (2012), Zakon o zaštiti osobnih podataka (pročišćeni tekst), Zagreb: NN, broj 103/03, 118/06, 41/08, 130/11, 106/12 pročišćeni tekst, dostupno na:

https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html, [31. svibnja 2021.].

25. PrivazyPlan (2018), Članak 4: EU Opća uredba o zaštiti podataka „Definicije“, dostupno na: https://www.privacy-regulation.eu/hr/4.htm, [31. svibnja 2021.].
26. Shing-Ling, S. C. (2020) Netiquette: social behaviour. Britannica. Dostupno na: https://www.britannica.com/topic/netiquette, [06. srpnja 2021.].
27. Torić, A. (2018) Privatnost na mreži, moguće zlouporabe podataka i načini zaštite. Završni rad. Zagreb: Sveučilište u Zagrebu, dostupno na: https://core.ac.uk/download/pdf/299374986.pdf, [05. svibnja 2021.].

14. Popis slika

Zaštita privatnosti na društvenim mrežama

Sažetak

Tema ovog završnog rada je „Zaštita privatnosti na društvenim mrežama“. U radu su definirani pojmovi privatnosti i osobnih podataka i važnost njihove zaštite na društvenim mrežama. Društvene mreže uvelike su promijenile način života, a s njihovim razvojem, došlo je i do raznih opasnosti i prijetnji za privatnost te razvoja zlonamjernih programa. Važno je obratiti pažnju na to da svaka objavljena informacija na društvenim mrežama, zauvijek ostaje na nekom internetskom serveru, čak i nakon što se izbriše. Osim ljudi koji društvene mreže koriste za komunikaciju s drugima i praćenje zanimljivih, edukativnih ili zabavnih sadržaja te objavljivanja statusa, slika ili videozapisa, postoje i ljudi koji društvene mreže koriste radi nanošenja štete ostalima. Neke od najčešćih prijetnji su *phishing, spam, hoax, malware* – tu se izdvaja *ransomware* i *spyware*, zatim krađa identiteta, gubitak i brisanje osobnih podataka i dijeljenje neprikladnog sadržaja. Zbog toga treba biti oprezan kod objavljivanja osobnih informacija i kod prijave u druge račune putem društvenih mreža. Važno je koristiti jake lozinke i ne otvarati sumnjive e-mailove i poruke. Također, bitno je uvijek poštovati pravila komunikacije kod dopisivanja ili objavljivanja sadržaja na društvenim mrežama, u online grupama, na portalima, forumima i slično.

Ključne riječi: zaštita privatnosti, osobni podaci, društvene mreže, Facebook, zlonamjerni sadržaj

Protection of Privacy on Social Networks

Summary:

The topic of this final paper is "Protection of Privacy on Social Networks". The paper defines the concepts of privacy and personal data and the importance of their protection on social networks. Social networks have generally changed the way of life, and with their development, there have been various dangers and threats to privacy and development of malware. It is important to pay attention to the fact that any information published on social networks remains on an Internet server forever, even after it is deleted. In addition to people who use social networks to communicate with others and follow interesting, educational, or entertaining content, and to post textual content, pictures or videos, there are also people who use social networks to harm others. Some of the most common threats are phishing, spam, hoax, malware - ransomware and spyware stand out, as well as identity theft, loss and deletion of personal data and sharing inappropriate content. Therefore, one should be careful when publishing personal information, when logging into other accounts via social networks. It is important to use strong passwords and not to open suspicious emails and messages. Also, it is important to always follow the rules of communication when corresponding or posting content on social networks, online groups, portals, forums and so on.

Key words: privacy protection, personal data, social networks, Facebook, malicious content