Sigurnosni rizici društvenih mreža

Dalić, Elena

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET TURIZMA I RURALNOG RAZVOJA U POŽEGI

STUDENT: Elena Dalić, JMBAG: 0253049641

SIGURNOSNI RIZICI DRUŠTVENIH MREŽA

ZAVRŠNI RAD

Požega, 2024. godine.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET TURIZMA I RURALNOG RAZVOJA U POŽEGI

PRIJEDIPLOMSKI STUDIJ UPRAVNI STUDIJ

MODERNI OBLICI ELEKTRONIČKIH PLAĆANJA

ZAVRŠNI RAD

IZ KOLEGIJA INFORMATIKA II

MENTOR: doc.dr.sc. Kristian Đokić

STUDENT: Elena Dalić

JMBAG studenta: 0253049641

Požega, 2024.godine

SAŽETAK

U ovom radu radu definirani su pojmovi društveni medij te je objašnjeno kako funkcioniraju društvene mreže. Također, opisane su društvene mreže koje se najčešće koriste. U središnjem djelu rada prikazane su opasnosti koje prijete na Internetu te opasnosti koji prijete koje na društvenim mrežama. U posljednjem djelu rada, navedeni su primjeri zlouporabe društvenih mreža te je dano zaključno razmatranje o tome kako se koriste društvene mreže.

Ključne riječi: društvena mreža, rizici, opasnost, zlouporaba

In this paper, the terms of social media are defined and how social networks work is explained. The most frequently used social networks are also described. In the central part of the paper, the dangers that threaten the Internet and the dangers that threaten those on social networks are presented. In the last part, of the paper, examples of abuse of social networks are given and a key consideration is given on how social networks are used.

Keywords: social network, risks, danger, misuse

SADRŽAJ

1. UVOD

Društvene mreže su besplatne platforme koje omogućuju korisnicima komunkikaciju razmjenivanjem poruka. Na taj način korisinici mogu upoznavati ljude koji su na drugom kraju svijeta bez potrebe ostvarenja fizičkog kontakta. Korisnici samo odlučuju koga će pratiti, sa kime će uspostavljati komunikaciju te ćak koristiti društvene mreže radi ostvarenja poslovnog kontakta. Najpopularnije društvene mreže su Facebook, Instagram, Twitter te Tik Tok. Korisnički računi često nisu primjereno zaštičeni te zbog toga dolazi do zlouporabe podataka.

U ovome završnom radu u prvom djelu su opisani društveni mediji, objašnjeno je društveno umrežavanje te kako funkcioniraju društvene mreže. U središnjem djelu rada opisan je nastanak društvenih mreža, te su navaedene opasnosti koje prijete na društvenim mrežama. U posljednjem djelu ovog rada navedeni su primjeri zlouporabe društvenih mreža iz medija.

2. DRUŠTVENI MEDIJ

Pojam društveni medij označava skup internetskih alata pomoću koje se djele iskustva u nekoj zajednici, neoivisno o tome radi li se uživo ili on-line. Otvorena konverzacija je jedna od karakteristika društvenih medija. Pod otvorenom konverzacijom podrazumjevaju se televizija, radio i novine. Socijalni mediji ohrabruju svakog tko primi neku informaciju da na nju reagira šaljući povratnu informaciju (Panian, 2013: 258). Karakteristikama društvenog medija pripada i utemeljenost na zajednici. Zajednice se brzo formiraju i omogućuju efikasno komunikaciju. Sudjelovanje i povezivost također pripadaju karakteristikama društvenog medija. Sudjeovanje znači da članovi zajednice se ohrabruju na sudjelovanje (participaciju) u zajedničkim akcijama, na davanju vlastitog doprinosa u osmišljavanju i provedbi akcija i na dijeljenje učinaka ili koristi of zajedničkih akcija (Panian, 2013: 259). Povezivost znači da se uporabom društvenih medija sve informacije mogu lako pronaći. Društveni mediji omogućuju izgradnju osobnih odnosa među ljudima. Na taj način oni pomažu i tvrtkama jer tvrtke mogu saznati kakvo je mišljenje ljudi te učiti od njih.

2.1. DRUŠTVENO UMREŽAVANJE

Osobe koje aktivno sudjeluju u društvenom umrežavanju se nazivaju čvorovima, a odnosi među njima se mogu mjeriti na više načina. Društveno umrežavanje ima stratešku, istraživačku i tehnološku perspektivu. Strateška perspektiva se odnosi na sustave pomoću kojih članovi nekog Web mjesta uče o vještinama, talentima i znanjima ostalih članova. Istraživačka perspektiva je on-line lokacija na kojoj korisnik kreira svoj profil ili gradi osobnu mrežu koja nju ili njega povezuje s drugim korisnicima (Panian, 2013: 267). U tehnloškoj perspektivi postoji više oblika i načina na koji se može komunicirati, a to su: elektronička pošta, videi, pisanje blogova i dijeljenje datoteka.

2.2. NAČINI FUNKCIONIRANJA DRUŠTVENIH MREŽA

Uporaba društvenih mreža je besplatna. Korisnik se tipično prijavljuje na web mjestu koje djeluje kao sučelje cjelokupne društvene mreže kako bi mogao postaviti svoju web stranicu, uobičajeno nazivanu profilom (Panian, 2013: 269). Na toj stranici korisnik može dijeliti informacije koje želi. Većina društvenih mreža daje mogućnost dijeljenja fotografija, kreiranje blogova te pronalazak ljudi sa sličnim interesima. Korisnici imaju mogućnost kontrolirati tko im prati profil tako što će ga prethodno zaštititi. Ne žele svi ljudi ostvarivati virtualne veze.

Društvene mreže mogu biti idealna platforma za ostvarivanje poslovnih partnerstava i poduzetničkih pothvata. Svi koji su jako zaposleni mogu biti na društvenoj mreži onda kada završe sa svojim obvezama, jer im je mreža lako dostupna. Društveno umrežavanje ima i lošu stranu. Naime, postavljanje svojih osobnih informacija može sa sobom nositi određene rizike. Uz određene mjere predostrožnosti ti se rizici mogu smanjiti.

2.3. DRUŠTVENE MREŽE U POSLOVNOM OKRUŽENJU

Prednost društvenih mreža je što ljudi mogu razmjenjivati svoja iskustva te razgovori o poslovnim temama koje ih zanimaju. Postoji nekoliko web mjesta koja su pogodna za društveno umrežavanje zbog posla. *Biztoo* je francuska društvena mreža koju koriste poduzetnici. Ona im pomaže pronaći ulagače te je mjesto gdje se mogu pronaći oglasi o slobodnim radnim mjestima. *Linkedln* je također društvena mreža koju koriste poslovni ljudi. *Plaxo* je on-line adresar kojem je cilj postavljanje kontaktnih informacija te omogućava povezanost korisnika. *Ryze* je aplikacija koja ima dvije razine. Prva je opća, omogućava besplatno korištenje. Druga je poslovna, za njenu upotrebu potrebno je platiti članarinu. Panian, Ž. (2013.) Elektroničko poslovanje druge generacije, Ekonomski fakultet Zagreb

Društvene mreže olakšavaju izgradnju odnosa sa postojećim klijentima te zaposlenicima. Privatne društvene mreže mogu se također proširiti kako bi uključile i ljude izvan kruga zaposlenika, klijenata i partnera tvrtke, ovisno o situacijama, potrebama i ciljevima (Panian, 2013: 271).

Poslovni odnosi se većinom baziraju na komunikaciji jednog ili više ovlaštenih predstavnika tvrtke. Ukoliko bi se komunikacija proširila dalje na druge osobe ili organizacije, moglo bi doći do bolje učinkovitosti procesa. Osnovna svrha društvenih mreža je kreiranje osobnih kontakata kako bi oni ostvarili poslovne suradnje.

Postoji mogućnost da predstavnici tvrtke potroše previše vremena na komunikaciju sa ljudima koji im ne mogu pomoći. Iz tog je razloga najbolje da tvrtke ostanu u granicama svoje djelatnosti i da ograniči mogućnost pristupa mreži omim osobama ili organizacijama za koje se smatra da neće pridonijeti poslovnoj uspješnosti.

2.4. ANALIZA DRUŠTVENIH MREŽA

Zahvaljujući analizi društvenih mreža može se vidjeti struktura društvenih odnosa u skupini te se otkrivaju neformalne veze među ljudima. Upravo tako se vidi tko sa kime te koliko

često komunicira. Analiza društvenih mreža pretpostavlja da su svi ljudi međusobno ovisni. Skupine, interakcije i atributi su poslovne činjenice na koje treba misliti prilikom uporabe odgovarajuće metode analize društvene mreže.

Skupine su prva poslovna činjenica na koju treba obratiti pozornost prilikom analiziranja društvene mreže. Potrebno je utvrditi koju će se društvenu skupinu istraživati. Skupine se mogu sastojati od pojedinaca sa posebnim ulogama odnosno zadacima koje izvršavaju ili, pak, čitava zajednica u kojoj specifične uloge pojedinaca nisu prepoznatljive (Panian, 2013: 273).

Interakcije podrazumijeva da analiza društvenih mreža istražuje kakvi su odnosi među članovima skupine. Cilj analize može biti postoji li u mreži pojedinac ili skupina koji utječu na mišljenje ostalih u mreži. Atributi pomažu pri otkrivanju postoje li ne sistemski čimbenici koji utječu na interakciju članova skupine. Na taj način se može otkriti da neki pojedinci više komuniciraju, a neki manje. Svrha analize društvenih mreža može biti prepoznavanje različitosti među članovima.

Tvrtke mogu analizu društvenih mreža koristiti za analizu kupaca, razvoj informacijskog sustava te marketing. Analiza društvenih mreža je aktualna i u obavještajnim i protuobavješnim poslovima. Agencija za nacionalnu sigurnost ima svoje programe elektroničkog nadzora pomoću kojih generira podatke potrebnih za analizu terorističkih ćelija. Nakon što se završi početno mapiranje društvenih mreža, potrebno je provesti analizu zbog utvrđivanja strukture mreže.

Analiza društvenih mreža može se koristit za razumijevanje ponašanja pojedinaca, organizacija i odnosa između web stranica. Analiza hiperveza se upotrebljava kako bi se analizirale veze između web mjesta ili web stranica. Analiza društvenih mreža koristi se na društvene medije kako bi se razumjelo ponašanje između pojedinaca ili organizacija putem njihovih poceznica na Facebooku ili Twitteru.

3. PREDUVJETI I NASTANAK DRUŠTVENIH MREŽA

Osnovni preduvjet za nastanak društvenih mreža je infrastruktura na kojoj se bazira, a to je internet. Ministarstvo obrane SAD je odlučio da mora unaprijediti svoj sustav zbog vojnog komuniciranja te obrade podataka na daljinu. Odlučili su razviti računalnu mrežu kojom će se upravljati decentralizirano. Zadatak osmišljavanje te računale mreže bio je povjeren agenciji ARPA. U svome radu Varga et al. (2007.) otkrili su da je ponuđeno rješenje računalne mreže trebalo zadovoljiti dva temeljna uvjeta, prvo da mreža ne smije biti ovisna o centralnom upravljanju, a drugo da sustav mora biti uspostavljen tako da može raditi i unatoč eventualnim oštećenjima nekih njegovih dijelova.

Distribuirani informacijski sustavi koji su utemeljeni na punoj mrežnoj telekomunikacijskoj infrastrukturi donose najbolje rješenje za navedene zahtjeve. Važna je činjenica da je potkraj 1969. godine započeo intenzivan znanstveno-istraživački rad i zahvaljujući njemu živimo u svijetu u kojemu su nam informacije lako dostupne. Ray Tomlinson je 1971. godine poslao prvo elektroničko pismo (*e-mail*) na način da je koristio dva računala koja su bila jedan pored drugog. Tim Berners Lee je izumio HTML jezik na kojem se bazira usluga web, odnosno *word wide web*. Varga, M. (2007.) Informatika u poslovanju, Zagreb.

Prije pojave društvenih mreža korisnicima je bio dostupan servis pod nazivom blog. Najjednostavniji opis istog je digitalni dnevnik na internetu. Omogućavanjem ubacivanja komentara na tekstove taj servis sve više je imao funkcionalnost društvenih mreža. Godine 1997. se stvarala web prva stranica za društveno umrežavanje AOL Instant Messenger. Stvorena je kako bi omogućila svojim korisnicima stvarnu komunikaciju. Stranica je bila popularna sve do kraja 2000. godina kada su se pojavile druge web stanice koje su nudile neke dodatne mogućnosti. Varga, M. (2007.) Informatika u poslovanju, Zagreb.

My Space je prva društvena mreža koja je doživjela popularnost na našim prostorima. Veliki broj korisnika se u početku nije osjećao povezan sa mrežama. Kako bi društvena mreža bila uspješna nije dovoljno samo imati neznance i poznanike već i povezane ljude.

Friendster je osnovan 2002. godine, bio je jedno od najpopularnijih mjesta za društveno umrežavanje. Cilj te stanice je bilo upoznavanje te se unatoč tome smatra jednom od prvih originalnih društvenih mreža. Omogućavao je svojim korisnicima da komuniciraju, da međusobno dijele objave te pronalaze hobije. 2008. godine broj korisnika se počeo smanjivati. Varga, M. (2007.) Informatika u poslovanju, Zagreb.

Reid Hoffman je 2002. godine u prosincu pokrenuo stranicu za društveno umrežavanje imena *Linkedln*. Stranica se i danas smatra popularnom. *Linkedln* je želio svojim korisnicima osigurati profesionalnu društvenu mrežu. Omogućuje korisnicima otvaranje profila, dijeljenje radnog i-skustva, vještina i slika. Tvrtke koje traže zaposlenike mogu provjeriti njihov *Linkedln* profil prije zapošljavanja. Korisnici mogu spremiti one poslove za koje se u budućnosti žele prijaviti. Tijekom prijave, putem *Linkedlna* korisnici mogu slati svoje životopise. Na temelju toga, tvrtke se sa njima dalje povezuju kako bi komunicirali. Društvene mreže-definicija i concept, URL:https://hr.economy-pedia.com/11040338-social-media#google_vignette

Facebook je najpopularnija mreža na svijetu koju je osnovao Mark Zuckerberg. On je inzistirao da korisnici koriste prava imena, a ne nadimke. Druga, najpopularnija globalna mreža je *YouTube* koja je osnovana 2005. godine. Posljednjih godina najpopularnije mreže su osim navedenih, *Instragram* i *Tiktok*. Nakon što je *Instagram* preuzet od strane *Facebook-a*, on doživljava još veću popularnost. *TikTok* je kreiran 2016. godine, a svrha mu je razmjena kratkih videoisječaka.

2011-2014. godine pokrenut je *Snapchat* kao nova aplikacija za mlade. Aplikacija se koristi diljem svijeta. *Facebook* je kupio *Instagram* za milijardu dolara kao potencijalnog konurenta *Snapchatu*. Društvene mreže-definicija i concept, URL:https://hr.economy-pedia.com/11040338-social-media#google_vignette

U nastavku su opisane neke od trenutno najpopularnijih društvenih mreža.

3.1. YOUTUBE

YouTube je jedna od društvenih mreža koja ima za cilj povezivanje osoba vezanih uz sličan interes prema video isječcima. Osnovan je 14.2.2005 godine, a stranica se razvijala velikom brzinom. Svaka osoba može otvoriti svoj *YouTube* kanal. Može se oformiti i u poslovne svrhe kako bi svi video sadržaji bili na jednom mjestu. Moguće je unijeti kratki opisi posla te svoj kontakt. Korisnici *YouTube* kanala se mogu pretplatiti na druge kanale. Dozvoljeno je komentiranje, ocjenjivanje te dijeljenje drugima video sadržaje. YouTube, URL:https://gradanskiodgoj.rijeka.hr/drustvo-i-ja/uloga-medija/drustvene-mreze/

Slika 1. prikazuje logo *YouTube* (*YouTube*, 2024.)

3.2. FACEBOOK

Facebook je osnovao Mark Zuckberger 2004. godine tako što je isprva osnovao *Facemash*. *Facemash* je služio korisnicima da ocjenjuju izgled svojih prijatelja. Mark Zuckberger je snosio posljedice toga čina tako što ga je odbor fakulteta kaznio. Početna namjena korištenja *Facebook-a* je bila kako bi studenti mogli razmjenjivati podatke. *Facebook Feed* je nudio mogućnost praćenja svih prijatelja. 2011. godine su se na *Facebooku* moglo objavljivati naslovne fotografije te se vidi napredak kroz vremensku crtu. *Facebook* danas nudi mnogo mogućnosti koje uključuju gledanje videa, stvaranje grupa za zajedničkim interesima, gledanje prijenosa koji se emitira uživo, igranje igrica, pronalaženje prijatelja pa čak i partnera.

Uz prednosti, *Facebook* ima i određene nedostatke. Naime, korištenjem *Facebook-a* kod korisnika može doći do depresije. Korisnici se konstantno uspoređuju s drugima, a time njihovo samopouzdanje pada. Moguće je da osobe smatraju na temelju onoga što vide da je njihov život lošiji od drugih. Moguće je vidjeti koliko svaka osoba ima prijatelja na *Facebooku*. Hoće li korisnik *Facebooka* imati negativno ili pozitivno raspoloženje ovisi o tome koliko vremena na njemu provodi. Ukoliko, provode više vremena, mogu postati asocijalni za druženje van mreža. Isto tako i tijekom stvarnog druženja mogu postati ovisni o tome da sve neprestano dokumentiraju. Hoće li neka osoba postati žrtvom prevare, vjerojatnije je za one koji su ovisni o internetu nego za one koji *Facebook* koriste za komunikaciju sa prijateljima. Društvene mreže-definicija i concept, URL:https://hr.economy-pedia.com/11040338-social-media#google_vignette

Ukoliko dođe do prekida veze, *Facebook* daje mogućnost nadzora bivšeg partnera što odgađa emotivni oporavak.

Prilikom uporabe *Facebook*-a kod korisnika se mogu javiti sljedeći negativni osjećaji:

1. Živciranje - zbog ne postignuća određenog nivoa u igrici
2. Šok - kada prijatelj objavi neku sliku za koju se smatra da nije primjerena
3. Zaprepaštenje- kada određenu bitnu vijest vide na *Facebook*-u, a ne uživo

4. Iritaciju - kada prijatelj objavi vijest za koju smatraju da nije smislena.

Slika 2. prikazuje logo Facebooka (Facebook, 2024.)

3.3. INSTAGRAM

Instagram je društvena mreža namijenjena dijeljenju fotografija, osnovana 2010. godine. Mogućnosti koje nudi *Instagram* su:

1. Dijeljenje fotografija
2. Komunikacija s drugima na način komentiranja te razmjena privatnih poruka
3. Praćenje raznih profila

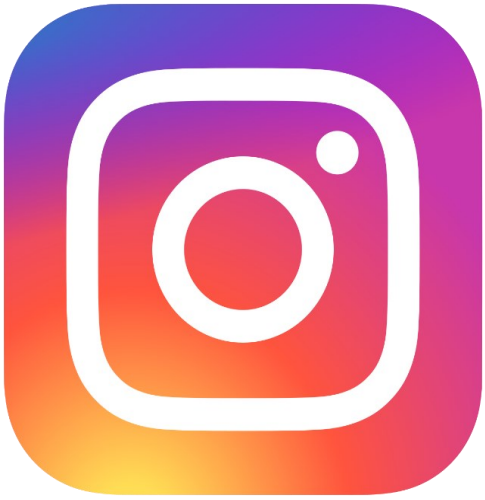
Postoji i algoritam koji korisnicima nudi druge profile koji bi im mogli biti zanimljivi, a time bi ih mogli i zapratiti. Kako bi se Instagram mogao koristiti potrebno je unijeti korisničko ime, lozinku te e-mail adresu.

Korisnici također, mogu otvoriti i poslovni račun. Kako bi određeni proizvod što bolji prezentirali, influenceri tu imaju važnu ulogu. Oni služe za osmišljavanje najbolje reklame kako bi se brendovi proširili na cijelom svijetu. Brendovi su prepoznali važnost influencera. Takav način rad na *Instagram*-u, nekim influencerima je pomogao da zarade bogatstvo od svojih popularnih objava. Influenceri mogu vidjeti analitiku svojih objava te tako zaključiti što je to što publika želi.

Kako bi korištenje *Instagram*-a bilo donekle sigurno korisnici se mogu zaštiti tako što odvoje privatni račun od javnog. Tako ne može doći do zlonamjerne aktivnosti zvane hakiranje. Odvajanjem privatnog računa od javnog znači da korisnik kontrolira tko može vidjeti njegove objave i priče. Naime, tako njegove objave i priče mogu vidjeti samo oni koji ga prate. To je važno za osobe koje ne žele da informacije koje djela na toj platformi svi vide. Ukoliko korisnik smatra da je neka objava uvredljiva, postoji mogućnost prijave te objave. Postavljanjem jače lozinke

profil se dodatno štiti. Što je Instagram, URL:https://dir.hr/sto-je-instagram-i-zasto-je-tako-popularan/

Slika 3. prikazuje logo Instagrama (Instagram, 2024.)



3.4. TWITTER

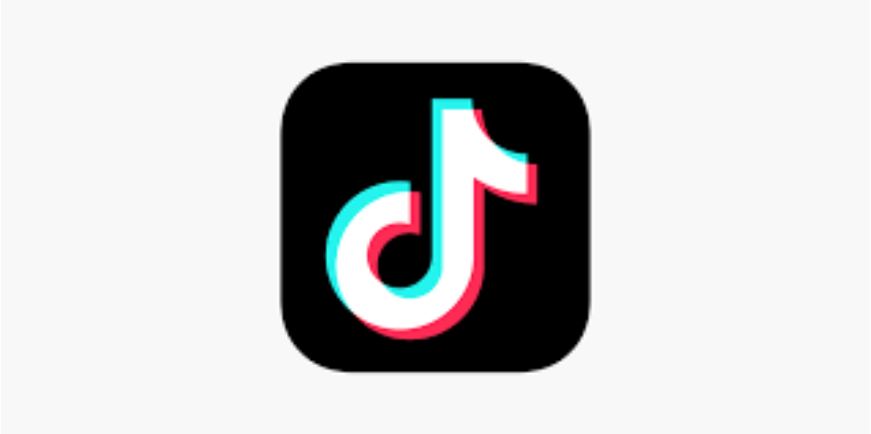
Twitter je osmislio Jack Dorsey, a namjena mu je bila javljanje svojim prijateljima putem SMS-a kako bi mogli znati što točno radite u određenom trenutku. Stvoreni su i privatni profili iz razloga što je ljudima bilo čudno da ih prati netko koga ne poznaju. Broj znakova koji se može poslati na Twitteru je ograničen na 140. Smatra se da je to dovoljno jer je namjena Twittera slanje kratke i jasne poruke. Twitter nudi mogućnost praćenja poznatih osoba kako bi znali što oni rade. Kako bi otvorili Twitter potrebno je otvoriti internet preglednik te upisati svoje korisničko ime, e-mail adresu, ime i prezime te lozinku. Kako je nastao Twitter, URL: https://www.netokracija.com/twitter-povijest-3094

Slika 4 prikazuje logo Twittera, (Twitter, 2024.)

3.5. TIK TOK

Tik Tok je popularna aplikacija koja dolazi iz Kine, a namjena joj objavljivanje kratkih video sadržaja. Sadržaj koji je može vidjeti na *Tik Toku* vezan ja za glazbu, ples, sport, kuhanje, kućne ljubimce i slično. Svatko tko koristi *Tik Tok* može objaviti takav sadržaj. Što je Tik Tok i kako se koristi, URL:https://www.ucionica.net/aplikacije/sto-je-tik-tok-i-kako-se-koristi-6515/

Slika 5. prikazuje logo *Tik Toka*.



4. OPASNOSTI KOJE PRIJETE NA INTERNETU

Danas bi u većini slučajeva život bez interneta bio nezamisliv. U jako kratkom vremenu tehnologija nam je postala važno sredstvo na koje se oslanjamo prilikom komuniciranja te radi zabave, informiranja i trgovanja. Isto tako, internetom se služe lopovi, vandali te stručnjaci kako bi otkrili tajne podatke. Conry-Murray i Weafer (2005.) kažu da su internet i web pod sve žešćim udarom kriminalaca koji moć globalne mreže koriste za uništavanje vaših podataka, narušavanje vaše privatnosti, otimanje ili uništavanje računala, pa čak i za krađu vašeg novca i terećenje vaših kreditnih kartica. Kako bi se ti rizici izbjegli postoje brojni alati i tehnike. Conry-Murray i Weafer (2005.) kažu da čak i naoko bezazlene lokacije poput popularnih odredišta za e-trgovinu ili *online* zabavu mogu preplaviti računalo softverom koji generira oglase (i usporava rad računala) ili prati korištenje Interneta. Kako bi se zaštitili od mogućih rizika potrebno je imati vatrozid i antivirusni softver. U nastavku je sistematiziran popis opasnosti kojima su izloženi korisnici interneta.

4.1. PREVARANTI I OTMIČARI

Računalna prijevara ima za cilj izmamljivanje novca tako što nude sumljive proizvode e-poštom ili oglasima na webu. Također, putem njih se žele otkriti osobne informacije i podatke o bankovnim računima. Conry-Murray i Weafer (2005.) kažu da otmičari pokušavaju preuzeti kontrolu na računalima kako bi proveli svoje zle namjere poput praćenja *online* aktivnosti.

4.2. KRAĐA IDENTITETA

Krađa identiteta je jedna od prijetnji na internetu koja ima za cilj praćenje informacija kao što su brojevi kreditnih računa, lozinki i osobnih matičnih brojeva. *Phishing* napadi su oblik krađe identiteta koji radi tako da se dobije poruka e-pošte na kojoj piše da je od neke velike banke ili kompanije za izdavanje kreditnih kartica. U poruci je naznačeno da osoba koja je dobila poruku mora poslati korisničko ime, broj računa i lozinku jer postoji problem sa računalom. Takva poruke je lažna i odgovaranjem na nju se otkrivaju svoji povjerljivi podatci prevarantima. Conry-Murray, A; Weafer, V. (2005.) Sigurni na Internetu, Zagreb, Tisak.

4.3. MAMLJENJE DJETETA ZA ZADOVOLJAVANJE SPOLNIH POTREBA

Seksualno zlostavljanje djece je osjetljiva tema koja je jako zastupljena u posljednje vrijeme. Žrtve su neosjetljivija skupina društva. Kako bi se suzbilo takvo ponašanje, zakonodavac kaznenog prava mora imati poseban pristup. Potrebno je imati posebno educirane osobe koje sa djetetom komuniciraju u svim stadijima kaznenog postupka. Takva situacija ostavlja kod djeteta posljedice za cijeli život. Počinitelj spolnog uznemiravanja stvara lažan profil kako bi sakrio svoj identitet. Počinitelji spolnog uznemiravanja se dijele na tri vrste:

- oni koji traže intimnost (nisu prethodno učinili seksualno kazneno djelo)
- one osobe koje su prilagodljive (ranije osuđene za seksualno kazneno djelo te imaju neprikladne fotografije djece)
- hiperseksualizirane osobe (posjeduju neprimjerene fotografije djece, ranije su osuđeni za seksualno kazneno djelo te stvaraju više različitih lažnih profila)

Velki i Šolić (2019.) navode da kazneno pravo nastoji razvijati prikladne odgovore na virtualne modalitete specifičnim opisima kaznenih djela i predviđanjem odgovarajućeg sustava kazneno-pravnih sankcija. Počinitelju spolnog uznemiravanja osim kazne zatvore bude dodijeljena zabrana korištenja interneta od 6 mjeseci do dvije godine.

4.4. SPAM PORUKE

Većina ljudi je upoznata sa *spam* porukama odnosno neželjenom poštom. *Spam* poruke se odnose na reklame koje nas najčešće ne zanimaju. Ukoliko napadač ima veliki broj e-adresa, njemu nije problem poslati reklamu velikom broju ljudi i poduzeća. Dovoljno je da se mali broj ljudi zainteresira za proizvod te otvori poruku. U tom slučaju slanje neželjene pošte je uspješna. Riječ je o poduzeću koje ima za cilj da se određeni proizvod reklamira te će platiti napadaču određen iznos da šalje neželjenu poštu. Tako da napadač od toga može imati veliku novčanu korist. Napadač je do tih adresa došao pomoću zloćudnog koda. Velki, T; Šolić, K. (2019.) Izazovi digitalnog svijeta, Osijek, Društvena psihologija.

4.5. NAPLATA OTKUPNINE OD ŽRTVE

Ovaj način ugroze se uglavnom koristi na osobna računala, iako se razvio i na pametne telefone. Ovaj zloćudni program ima svrhu da onemogućiti pristup korisniku njegovim podatcima. Na taj način korisnik ne može pristupiti svojim podatcima bez odgovarajućeg ključa koji je u vlasništvu napadača. Napadač će otkriti odgovarajući ključ žrtvi ukoliko mu ona plati od-

ređenu otkupninu. Žrtva nema garanciju da će ukoliko plati otkupninu zaista dobiti odgovarajući ključ. Napadači često za žrtve uzimaju računovodstvene odjele. Napadaju ih tako što im pošalju privitke koji izgledaju kao računi. Na taj način žrtva će otvoriti privitak i pokrenuti zloćudni kod. Velki, T; Šolić, K. (2019.) Izazovi digitalnog svijeta, Osijek, Društvena psihologija.

4.6. ŠPIJUNAŽA

Kako bi poslovanje neke tvrtke bilo uspješno, zaposlenici tvrtke sukladno njezinim ovlastima imaju pristup povjerljivim dokumentima i podatcima. Ukoliko napadač ostvari pristup na jednom računalu zaposlenika, on može kompromitirati cijelu mrežu poduzeća. Velki i Šolić (2019.) navode da je ovdje kao i kod ostalih zloćudnih programa prvi korak slanje poruke u svrhu krađe podataka koja sadrži zloćudni kod i tipično sadrži metode društvenog inženjeringa. Napadač dobiva sve ovlasti žrtve nakon što je instalirao zloćudni kod na računalu žrtve. Poduzeća, kako bi sačuvala svoj ugled često ne žele priznati primjere industrijske špijunaže.

4.7. ELEKTRONIČKO RATOVANJE

Najčešće se ne znaju autori niti tko je financirao zloćudne programe. Moguće je da su ih razvili specijalizirani timovi, ako se uzme u obzir činjenica da troškovi za izradu takvih programa iznose milijune dolara. Crv *Stuxnet* je bio najpoznatiji zloćudni program u povijesti. Velki i Šolić (2019.) kažu da kod takvih složenih programa, nakon inicijalne zaraze jednog računala u lokalnoj ili štićenoj mreži, zloćudni programi se dalje sami šire mrežom i na taj način dolaze do novih računala s traženim podacima ili upravljačkim sklopovljem. Smatra se da je *Struxnet* pokrenut tako što je žrtva našla USB štapić koji je netko ostavio blizu nuklearnog pogona. Žrtva je taj USB štapić priključila na računalo. Nakon što je žrtva to učinila, *Struxnet* je pokrenut. Sumnja se da se radilo o napadu tajnih službi Izraela na nuklearne pogone Irana.

4.8. NAPLATA SMS PORUKA

Pametni telefoni se danas sve više koriste, stoga se i zloćudni programi na njima brzo razvijaju. Napadačima su pametni telefoni privlačniji od računala jer postoji mogućnost direktne naplate od telekomunikacijskog operatera. Na taj način napadač lako dolazi do financijske koristi. Jedan od primjera zarade je kada napadač pošalje SMS poruku i time koristi uslugu koja se plaća i koja je u njegovom vlasništvu. Velki i Šolić (2019.) kažu da se na taj način napadač koristi pametnim telefonom žrtve kako bi u pozadini slao SMS poruke na vlastitu uslugu i time

zarađivao novac, a žrtva uopće nije svjesna slanja poruke. Isto tako ne treba zaboraviti da pametni telefoni prikupljaju o nama podatke kao npr. našu lokaciju, kontakti i slično pa na taj način napadači imaju osobne podatke o korisnicima. Za očekivati je da će prijetnje na pametnim telefonima i dalje rasti.

4.9. RAČUNALNI VIRUSI

Računalni virusi se samostalno izvršavaju sa ciljem nanošenja štete sustavu u kojem se pokreće. Virus se može ugraditi u datoteku, tako da nakon što korisnik otvori aplikaciju, virus zarazi računalo. Velki i Šolić (2019.) kažu da se virusi često nadograđuju na početku ili kraju legitimne datoteke kako bi se neprimjetno pokrenuli pa će se tako virus izvršiti, a ostatak legitimne datoteke korisniku će se uobičajeno pokazati kako on ne bi posumnjao u moguću zarazu.

Virus će se nakon pokretanja sam pokušati replicirati unutar računala. Kako bi se replikacija mogla provesti, virus mora znati na kojem je operacijskom sustavu pokrenut, tako da zna koje sve datoteke postoje i gdje se može ubaciti.

5. OPASNOSTI KOJE PRIJETE NA DRUŠTVENIM MREŽAMA

Društvene mreže se koriste kako bi se korisnici međusobno povezali te dijelili informacije. Međutim, one mogu biti izvrstan alat za uznemirivanje korisnika društvene mreže i njihove obitelji. Stoga je iznimno važno znati se zaštititi. Kako bi se zaštititi prvo je potrebno identificirati prijetnju, kroz informacije koje su na raspolaganju.

Kritičnom informacijom se smatra svaka informacija koja je osjetljiva ili bi mogla naštetiti. Jedan od problema s kritičnim informacijama je neovlašteni pristup podatcima. Može doći do problema kada ljudi objavljuju informacije o putovanjima te druge privatne podatke. Objavljivanje takvih informacija mogu dovesti do novčanog gubitka, krađe identiteta te gubitka imovine. Krađa identiteta i ugrađivanje zlonamjernog softvera igre, može dovesti do preuzimanje računa, zlouporabe materijala te do pristupa u privatni život korisnika.

Nakon identificiranja kritičnih informacija, analize ranjivosti te procjene rizika, potrebno je primijeniti protumjere. Te protumjere podrazumijevaju: zaključivanje informacija o lokaciji, postavke privatnosti i lozinki, upoznavanje sa društvenim inženjeringom, taktikama dezinformiranja te drugo. Također je potrebno osiguravati računalne uređaje te pregledavati svoje postavke privatnosti i ažurirati ih kako bi bili sigurni da se nisu resetirali. Korištenjem mobilnog uređaja se izlaže opasnost vidljivosti lokacije. Iako se na društvenim mrežama nešto objavi privatno, postoji opasnost da jednog dana ti podatci budu javni.

Iako to nije potrebno za njihovo funkcioniranje, mnoge aplikacije traže pristup lokaciji. Kako bi se to izbjeglo potrebno je onemogućiti postavke usluga lokacije na uređaju/aplikaciji te ne dijeliti lokaciju dobrovoljno. Osim toga, aplikacijama društvenih medija treba dati što manje dopuštenja.

Ciljani *spear-phishing* podrazumijeva da protivnici traže informacije kako bi otkrili osobne podatke. Stoga je potrebno provjeriti svaki zahtjev za prijateljstvo kako bi se otkrilo poznajemo li ti osobu. Važno je isključiti opciju spremanja lozinki za prijavu unutar postavki aplikacija. Isto tako, potrebno je obratiti pozornost na ankete koje se objavljuju na društvenim mrežama. Naime, te ankete mogu sadržavati privatna pitanja koje mogu koristiti protivnicima da kompromitriaju račune. Najčešća pitanja koja sadržavaju ankete na kojima se otkrivaju privatni podatci su:

- koje je ime Vašeg ljubimca?

- kako se zove osnovna/srednja škola koju ste završili?
- koje je ime Vaše učiteljice?
- koji Vam je najljepši grad na svijetu?
- koji je najneugodniji trenutak u Vašem životu?

Ova pitanja otkrivaju osobne informacije o korisniku, ali prva tri pitanja predstavljaju ozbiljnu opasnost. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Potrebno je izbjegavati povezivanje osobnih računa na mreže i računala u poslovnom okruženju. Također je važno korištenje virtualne privatne mreže kako bi se šifrirao web promet. Kako bi se što bolje zaštitili, potrebno je osigurati svoje lozinke. Za svaki on-line račune važno je koristiti jake lozinke. Važno je koristiti lozinke koje u sebi sadrže kombinaciju brojeva, slova i posebnih znakova. Isto tako je važno ne dijeliti lozinke te izbjegavati objavljivanje informacija na društvenim mrežama na temelju kojih bi ih netko mogao naslutiti. Protivnici mogu ukrasti podatke tako što navedu na klikanje na pozivnicu ili preuzimanje privitka koji može sadržavati zlonamjerni softver. Kako bi se zaštitili, važno je onemogućiti sigurnosne značajke protiv spama i krađe identiteta. Ukoliko se smatra da je račun ugrožen, potrebno je obratiti se osoblju za podršku. Oni pomažu ponovno se vratiti na svoj račun. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Jedan od opasnosti na društvenim mrežama je cyberbullying. Ljudi koriste društvene mreže kako bi komentirali nešto što ne bi rekli direktno u lice. Uhođenje se također smatra društvenom prijetnjom. Ono podrazumijeva prijeteće ponašanje u kojem izvršitelj zahtjeva fizički kontakt sa onom osobom koju uhodi. Pod rizicima uhođenja smatra se:

- zastrašivanje
- gubitak privatnosti
- nanošenje fizičke i psihičke boli.

Pod društvenom prijetnjom spada i industrijska špijunaža. Za tvrtku je veoma rizično otkrivanje povjerljivih podataka. Industrijska špijunaža podrazumijeva da napadači na prijevaru žele prikupiti neke informacije od zaposlenika koje će im koristiti. Pod rizicima industrijske špijunaže smatra se:

- gubitak intelektualnog vlasništva
- napad na računalnu infrastrukturu tvrtke

- ucjena zaposlenika tvrtke
- pristup materijalnoj imovini pojedinca/tvrtke. Carnet, (2009.) Sigurnosni rizici drrštvenih mreža.

5.1. SIGURNOSNI PROPUSTI

Jedan od starijih sigurnosnih propusta na društvenoj mreži *Facebook* dogodio se zbog nepravilnog rukovanja *ActiveX* kontrolama za učitavanje fotografija na korisnički profil. Kada je korisnik pokušao prebaciti fotografije na profil, dobio je upozorenje da je potrebno ugraditi dodatnu *ActiveX* kontrolu kako bi izvršio učitavanje željene fotografije. Ako korisnik pristane ugraditi zlonamjernu *AcitiveX* kontrolu na svoje računalo, postoji mogućnost da napadač preuzme kontrolu nad računalom korisnika. Također je postojala mogućnost da izvrši proizvoljni programski kod. Za kratak period, navedeni propust je otklonjen. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Na mreži *Facebook* postoji nekoliko slučajeva u kojima su napadači uspjeli ukrasti korisnička imena i lozinke određenih korisnika. Napadač je na taj način ugrozio privatnost podataka koji su bili pohranjeni na profilu. Pojava crva *Net Worm.Win32.Koobface.b.* je također ugrozila sigurnost korisnika. Crv se širio preko *spam* poruke te su se automatski slale poruke korisnicima na listi prijatelja kompromitiranog korisničkog računa. *Spam* poruke imaju poveznicu te u poruci sugeriraju korisniku na provjeri poveznicu. S obzirom na to da je poslana od osobe koje je na listi prijatelja, većina će tu poveznicu provjeriti. Nakon što korisnik posjeti poveznicu, pojaviti će mu se multimedijsko sučelje na kojemu može pogledati video. Nakon što korisnik pokuša očitati video, pojaviti će mu se upozorenje da mora ugraditi novi *Flash* dodatak kako bi mogao vidjeti multimedijski sadržaj. Međutim, na taj način će se računalo korisnika zaraziti crvom. Napadač će tako moći na računalu korisnika širiti zlonamjerne programe te izvršavati druge oblike napada. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Jedan od propusta na mreži *Twitter* je je vezan uz dozvoljavanje izvršavanja proizvoljnog programskog koda na nečijem profilu. Crv pod imenom „*StalkDaily*“ je iskoristio takav sigurnosni propust. On se brzo širio mrežom. Korisnik koji je pregledavao drugi profil koji je zaražen zlonamjernim programom, također se mogao zaraziti. U svaki zaraženi profil crv je ugradio *Javascript* datoteku. Nakon što je pregledavao zaraženi profil, korisnik je učitao zlo-

namjernu *Javascript* datoteku. Otuđeni su korisnički podatci za pristup mreži *Twitter* svim korisnicima čiji su profili bili zaraženi ovim crvom. Na taj način je korisnicima ugrožena sigurnost podataka. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Još jedan napad na mrežu Twitter uzrokovan je lošom autentikacijom pri pristupu mreži. Hacker Croll je haker koji je uspio saznati korisničko ime i lozinku jednog od administratora mreže *Twitter*. Na taj način je haker Hacker Croll mogao ugroziti sigurnost milijuna korisnika. Haker je to uspio tako što je provalio u sandučić e-pošte administratora te je tamo pronašao korisničko ime i lozinku za mrežu *Twitter*. Haker je, kako bi dokazao navedeno prikazao sliku administrativnog sučelja u koje je ušao. Nadalje, upozorio je vlasnike društvene mreže *Twitter* na nedovoljnu autentifikaciju administratorskih računa. Kako bi se zaštitili protiv ovakvih napada, potrebno je koristiti više faktorske autentifikacije pri prijavi na administratorski račun. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Napad koji također uzrokuje štetu je napad kojemu je svrha slanje *spam* poruka preko korisničkih profila. Još uvijek se ne zna kako su napadači uspjeli saznati korisničke podatke korisnika.

Sigurnosni pripust mreže *Linkedln* otkriven je u njegovom dodatku za preglednik *Internet Explorer*. Napadač je korisnika *spam* porukom prevario da posjeti zlonamjernu stranicu. Na taj način je napadač preuzeo programski kod. Također, dogodio se propust u *ActiveX* kontroli te je napadač prepisivanjem spremnika preuzeo kontrolu nad računalom. Takav sigurnosni propust u *Linkedln* je ispravljen. Svi koji često upotrebljavaju *Linkedln* dobivaju poruke e-pošte od administratora mreže ili drugih korisnika mreže. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Postoji slučaj u kojemu je napadač na adrese e-pošte, 10000 korisnika *Linkdeln* mreže poslao *spam* poruku e-pošte. Isprva se mislilo da su poruke poslane od administratora mreže. Napadač je ciljano slao poruke misleći da će zainteresirati korisnika. Napadač je znao osobne podatke korisnika kojemu je slao *spam* poruke. Napadač je naštetio korisniku tako što mu je ugrožena privatnost. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

Sigurnost korisnika *My Space* je također bila ugrožena. Naime, crv *Koobface* je djelovao jednako kao inačica za *Facebook* mrežu. Na taj način je zaraženo više od milijun korisnika za manje od 20 sati. Poznate osobe su također bile ugrožene na mreži *My Space*. Napadnuti su njihovi korisnički profili kako bi se izvršio napad. Napadnuti su tako što je napadač na otuđeni

korisnički profil ugradio zlonamjerni HTML kod u obliku poveznice. Pomoću poveznice korisnik dolazi do zlonamjerne stranice koja sadrži multimedijsku datoteku koja bi se korisniku mogla učiniti zanimljivom. Na taj način korisnik riskira sigurnost svojih podataka. Nakon što je korisnik, došao na zlonamjernu stranicu na računalu se u pozadini, bez znanja korisnika preuzima zlonamjerni program. Nakon korisnikovog pokušaja pokretanja multimedijske datoteke, pojavio se okvir dijaloga. Okvir dijaloga je tražio da se ugradi pokretački program. Napadač je imao za cilj da na taj način korisnik pokrene zlonamjerni program. Carnet, (2009.) Sigurnosni rizici društvenih mreža.

6. PRIMJERI ZLOUPOTREBE IZ MEDIJA

Mnogi pojedinci, udruge i brendovi su korištenjem društvenih mreža profitirali. Unatoč tome, društveno umrežavanje ima i svoju tamnu stranu. U nastavku je dan pregled informacija iz medija koje prikazuju tu stranu društvenih medija.

2014. godine je provedeno istraživanje pod nazivom "Računala u ljudskom ponašanju". Na temelju istraživanja otkriveno je većina ne koristi društvene mreže kako bi bili društveni. Otkriveno je da koriste mreže kako bi čitali podatke, nakon kojih se osjećaju nezadovoljno i tužno (*Securing social Network in Cyberspace*, URL: https://www.routledge.com/Securing-Social-Networks-in-Cyberspace/Pathan/p/book/9780367681753?srsltid=AfmBOopElGHoK5EMS8YU4wks7XmBb5eKvzKrYnJLC48BnNV1dZkNyyUf

Edward Snowden je jedan od najistaknutijih haktivista koji je odavao podatke iz Nacionalne sigurnosne Agencije. Također, poznat je slučaj širenja informacija o Ashely Madison. Programerima tada nije trebao novac, već su željeli srušiti stranicu (*Securing social Network in Cyberspace,* URL: https://www.routledge.com/Securing-Social-Networks-in-Cyberspace/Pathan/p/book/9780367681753?srsltid=AfmBOopElGHoK5EMS8YU4wks7XmBb5eKvzKrYnJLC48BnNV1dZkNyyUf

U ljeto 2015. godine pripadnici takozvane Islamske države oteli su Tomislava Salopeka koji je nakon mučenja ubijen. Na *Twitteru* je objavljena slika njegovog tijela. Hrvatski medji sliku njegovog tijela nisu objavili jer bi se time širila propaganda takozvane Islamske države. Unatoč tome, neki mediji iz regije su tu sliku ipak objavili (Emanović, T. 2019. Društvene mreže i sigurnosni rizici, Završni rad, Požega: Veleučilište u Požegi).

Društvene mreže često dovode do sukoba između ljudi. Isto tako, lako može doći do sukoba koji se kasnije rješavana na sudu. U nastavku su navedeni primjeri zloupotrebe društvenih mreža koji su javno objavljeni.

U svibnju 2019. godine profil Alexa Jonesa je zabranjen od strane *Facebooka*. Zabranjen je zbog kršenja pravila *Facebooka* "o opasnim pojedincima i organizacijama". *Facebook* želi stati na kraj promociji krajnjih desničara. Desničari su njih optužili za cenzuru. *Facebook* je na to odgovorio da svoja pravila provode bez predrasuda (Emanović, T. 2019. Društvene mreže i sigurnosni rizici, Završni rad, Požega: Veleučilište u Požegi).

Na općinskom sudu u Čakovcu gradski je vijećnik nepravomoćnom presudom proglašen krivim za kazneno djelo uvrede i klevete protiv gradonačelnika Kovač Stjepana i grada Čakovca. Presudom je određeno da će okrivljeni Kočila morati platiti kaznu od 25.000 kuna, 7.150 kuna troškova odvjetnika te 1.000 kuna sudskih troškova. Gradonačelnik Stjepan Kovač tužio ga je zbog vrijeđanja na *Facebooku*. Optuženi vijećnik Kočila smatra da se to što je objavljivao odnosilo na na gradonačelnika i saborskog zastupnika. Isto tako smatra da mora javnost informirati o radu gradonačelnika (Emanović, T. 2019. Društvene mreže i sigurnosni rizici, Završni rad, Požega: Veleučilište u Požegi).

Cambridge Analytics je neovlašteno prikupljala i koristila osobne podatke *Facebook-ovih* korisnika. Upravo iz tog razloga je ured australskog povjerenika za informacije podigao tužbu protiv *Facebooka* jer je povrijeđena privatnost više od 300 tisuća Australaca. U slučaju ponovnog kršenja privatnosti, kazna bi mogla biti i do 7 milijuna kuna (Facebook na sudu: Australija podiže tužbu zbog skandala sa Cambridge Analyticsom, URL: https://zimo.dnevnik.hr/clanak/facebook-na-sudu-australija-podize-tuzbu-zbog-skandala-s-cambridge-analyticom---596900.html

Sljedeći primjer je vezan za to da je žena zbog objave na *Facebooku* završila na sudu. Naime, radi se o tome da je žena preko *Facebooka* optužila supruga za obiteljske probleme. Suprug je iz toga razloga podnio tužbu protiv nje te je ona izbila spor i shodno tome morali platiti iznos troškova. Žena je kriva iz razloga što je javno sramotila supruga (Žena zbog objave na Facebooku završila na sudu: Presudili da je kriva pa zbog teškog sramoćenja dobila ogromnu kaznu, URL: https://www.dnevno.hr/vijesti/zbog-objave-na-facebooku-zavrsila-na-sudu-presudili-da-je-kriva-pa-zbog-teskog-sramocenja-dobila-ogromnu-kaznu-1399898/

Potrebno je skretati pozornost na pravna pitanja prilikom objava na društvenim mrežama. Naime, Europska komisija je 18.5.2017. izrekla kaznu *Facebooku* zbog davanja lažnih informacija prilikom *Facebook*-ovog preuzimanja aplikacije *WhatsApp*. Komisija je istraživala mogućnosti spajanja njegovih korisničkih računa s računima *WhatsApp*-ovih korisnika. *Facebook* je to negirao rekavši da mogućnost uspostavljanja sigurnog i automatskog načina međusobnog povezivanja ne postoje. Ispostavilo se da to nije točno jer *WhatsApp*-ova pravila o sigurnosti iz 2016.godine navode to kao mogućnost. Objašnjeno je kako se radi o poboljšanju usluga tako što primjerice dopustili da *Facebook* nudi bolje zahtjeve za prijateljstvo. Komisija je došla do zaključka da da je još od 2014.godine mogućnost spajanja postojala. Također smatraju da je *Facebook*-ovo osoblje toga bilo svjesno. Komisija smatra da je *Facebook* učinio

dvije proceduralne povrede. Prva je davanje netočnih informacija u objavi o preuzimanju, a druga je davanje netočnih informacija u odgovoru na Komisijin zahtjev za davanje informacija. *Facebook* je surađivao u postupku. Isto tako, priznao je kršenje prava te je to Komisiji olakšalo provedbu istrage. Iz toga razloga, *Facebook* je kažnjen je u iznosu od 110 milijuna eura. (Društvene mreže i pravna odgovornost, URL:https://informator.hr/strucni-clanci/drustvene-mreze-i-pravna-odgovornost-na-mrezi)

Presuda Europskog suda pravde u slučaju Screems protiv irskog Povjerenika za zaštitu podataka također je skrenula pozornost na važnost zaštite podataka. Screems je pokrenuto postupak protiv odluke irskog Povjerenika vezane za zaštitu podataka o odbijanju pritužbe. Pritužba je vezana uz to za *Facebook* Irska prenosi podatke svojih korisnika u SAD. Screems je iznio činjenice da zakonodavstvo i praksa Sjedinjenih Američkih država ne štite dovoljno podatke. Sud je došao do zaključka da se to primjenjivalo samo na američka poduzeća koja im pristupe. Isto tako, utvrđeno je da se američka tijela imaju prava miješati u prava pojedinaca. (Društvene mreže i pravna odgovornost, URL:https://informator.hr/strucni-clanci/drustvene-mreze-i-pravna-odgovornost-na-mrezi)

Zaštita privatnosti bila je predmet tužbe u Americi protiv *Facebooka*. Naime, *Facebook* je u oglasne svrhe koristio poruke koje se razmjenjuju. *Facebook* je na to odgovorio da takve poruke više ne posjeduje te se na taj način nagodio. (Društvene mreže i pravna odgovornost, URL:https://informator.hr/strucni-clanci/drustvene-mreze-i-pravna-odgovornost-na-mrezi)

Ono što se objavi na društvene mreže može imati velike posljedice na druge ljude. Primjerice, u Velikoj Britaniji dvojica braće su zbog prodavanja marihuana dobili uvjetnu osudu s rokom kušnje od dvije godine. Jedan od braće se pohvalio objavom na *Facebooku* kako je dobio blagu kaznu, dok je drugi brat tu objavu komentirao. Sudac im je iz toga razloga presudio kaznu zatvora. Sudac je shvatio da braća nisu promijenila svoje ponašanje te shvatili ozbiljnost svoga postupka (Društvene mreže i pravna odgovornost, URL:https://informator.hr/strucni-clanci/drustvene-mreze-i-pravna-odgovornost-na-mrezi)

Isto tako, postoje slučajevi davanja otkaza zbog objava na *Facebooku*. Na temelju istraživanja utvrđeno je da čak 45% američkih poslodavaca koristi društvene mreže kako bi provjerili svog budućeg zaposlenika te 35% odustane od zaposlenja svog zaposlenika zbog slike koju je dobio o njemu prilikom pregledanja njegovog korisničkog računa (Društvene mreže i pravna odgovornost, URL:https://informator.hr/strucni-clanci/drustvene-mreze-i-pravna-odgovornost-na-mrezi)

7. ZAKLJUČAK

Korištenje društvenih mreža postala je rutina većine. Društvene mreže su postale važna platforma koja informira o svemu što se događa u svijetu. Društvene mreže omogućuju svakom korisniku da proširi svoj krug prijatelja. Korisnik može proširiti svoj krug prijatelja tako što vidi koji su to zajednički interesi njega i osobe koja mu šalje zahtjev za prijateljstvo. Pojavom i nastankom interneta globalizacija je postigla svoj najveći nivo u povijesti.

Unatoč tome, društvene mreže imaju i svoju tamniju stranu. Zbog zlouporabe podataka te drugih mogućih opasnosti, potrebno je voditi računa što se objavljuje na društvenim mrežama. Isto tako, važno je educirati osobu kako bi na pravilan način upotrebljavala društvene mreže. Svaki korisnik se korištenjem društvenih mreža djelomično odriče svoje privatnosti. Nažalost, unatoč lošim primjerima koji se događaju na društvenim mrežama, pojedinci još uvijek nisu toga svjesni te se ne pridaje dovoljna važnost zaštiti svojih podataka.

8. LITERATURA

1. Panian, Ž. (2013.) Elektroničko poslovanje druge generacije, Ekonomski fakultet Zagreb

2. Conry-Murray, A; Weafer, V. (2005.) Sigurni na Internetu, Zagreb, Tisak

3. Velki, T; Šolić, K. (2019.) Izazovi digitalnog svijeta, Osijek, Društvena psihologija

4. Povijest društvenih mreža, URL: https://www.slideshare.net/slideshow/povijest-drutvenih-mrea/59016374#9

5. Medijska i informacijska pismenost, URL: https://medijskapismenost.ba/hr/o-nastanku-i-popularnosti-drustvenih-mreza-2/

6. Društvene mreže-definicija i concept, URL:https://hr.economy-pedia.com/11040338-social-media#google_vignette

7. Društvene mreže, URL:https://gradanskiodgoj.rijeka.hr/drustvo-i-ja/uloga-medija/drustvene-mreze/

8. YouTube, URL:https://gradanskiodgoj.rijeka.hr/drustvo-i-ja/uloga-medija/drustvene-mreze/

9. Povijest i razvoj YouTuba, URL:https://www.sutori.com/en/story/povijest-i-razvoj-youtube-a--1zZwiyepNahgzfTWertrmVrB

10. Povijest društvenih mreža, URL:https://marketingiraj.me/povijest-drustvenih-mreza/

11. Što je Instagram, URL:https://dir.hr/sto-je-instagram-i-zasto-je-tako-popularan/

12. Kako je nastao Twitter, URL:https://www.netokracija.com/twitter-povijest-3094

13. Što je Tik Tok i kako se koristi, URL:https://www.ucionica.net/aplikacije/sto-je-tik-tok-i-kako-se-koristi-6515/

14. Zbog objave na Facebooku završila na sudu, URL:https://www.dnevno.hr/vijesti/zbog-objave-na-facebooku-zavrsila-na-sudu-presudili-da-je-kriva-pa-zbog-teskog-sramocenja-dobila-ogromnu-kaznu-1399898/#google_vignette

15. Društvene mreže i pravna odgovornost, URL:https://informator.hr/strucni-clanci/drustvene-mreze-i-pravna-odgovornost-na-mrezi

16. Carnet, (2009.) Sigurnosni rizici društvenih mreža

17. Emanović, T. (2019.) Društvene mreže i sigurnosni rizici, Završni rad, Požega: Veleučilište u Požegi

18. Varga, M. (2007.) Informatika u poslovanju, Zagreb

19. Facebook na sudu: Australija podiže tužbu zbog skandala sa Cambridge Analyticom, URL: https://zimo.dnevnik.hr/clanak/facebook-na-sudu-australija-podize-tuzbu-zbog-skandala-s-cambridge-analyticom---596900.html

20. Žena zbog objave na Facebooku završila na sudu: Presudili da je kriva pa zbog teškog sramoćenja dobila ogromnu kaznu, URL: https://www.dnevno.hr/vijesti/zbog-objave-na-facebooku-zavrsila-na-sudu-presudili-da-je-kriva-pa-zbog-teskog-sramocenja-dobila-ogromnu-kaznu-1399898/

21. National Security Agency, URL: https://media.defense.gov/2021/Sep/16/2002855950/-1/-1/0/CSI_KEEPING_SAFE_ON_SOCIAL_MEDIA_20210806.PDF

22. Securing social Networks in Cyberspace, URL: https://www.routledge.com/Securing-Social-Networks-in-Cyberspace/Pathan/p/book/9780367681753?srsltid=AfmBOopElGHoK5EMS8YU4wks7XmBb5eKvzKrYnJLC48BnNV1dZkNyyUf

IZJAVA O AUTORSTVU RADA

Ja, **Elena Dalić**, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor završnog/diplomskog rada pod naslovom: **Sigurnosni rizici društvenih mreža** te da u navedenom radu nisu na nedozvoljen način korišteni dijelovi tuđih radova.

U Požegi, 11.09.2024.

Potpis studenta

EDalić