Kibernetičke prijetnje u društvenim mrežama

Alerić, Slaven

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni preddiplomski studij Računarstvo

KIBERNETIČKE PRIJETNJE U DRUŠTVENIM MREŽAMA

Završni rad

Slaven Alerić

Osijek, 2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P: Obrazac za ocjenu završnog rada na sveučilišnom prijediplomskom studiju

Ocjena završnog rada na sveučilišnom prijediplomskom studiju

Ime i prezime pristupnika:	Slaven Alerić
Studij, smjer:	Sveučilišni prijediplomski studij Računarstvo
Mat. br. pristupnika, god.	R4169, 11.10.2021.
JMBAG:	0165076714
Mentor:	prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Naslov završnog rada:	Kibernetičke prijetnje u društvenim mrežama
Znanstvena grana završnog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada:	Različite vrste društvenih mreža postale su medijske društvene platforme koje obuhvaćaju vrlo brojnu i heterogenu skupinu korisnika. Predstavljaju okruženje u kojem je prisutan veliki broj različitih kibernetičkih prijetnji. Potrebno je sustavno analizirati sigurnosne aspekte društvenih mreža (postojeće prijetnje i protumjere), uz detaljniji osvrt na različite vrste napada (npr. društveni inženjering, phishing, malware...). Analizirati neke primjere zabilježenih incidenata, te definirati preventivni sigurnosni okvir i politiku prevencije zlouporabe ovih medija.

Datum prijedloga ocjene završnog rada od strane mentora:	18.09.2024.
Prijedlog ocjene završnog rada od strane mentora:	Izvrstan (5)
Datum potvrde ocjene završnog rada od strane Odbora:	27.09.2024.
Ocjena završnog rada nakon obrane:	Izvrstan (5)
Datum potvrde mentora o predaji konačne verzije završnog rada čime je pristupnik završio sveučilišni prijediplomski studij:	29.09.2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O IZVORNOSTI RADA

Osijek, 29.09.2024.

Ime i prezime Pristupnika:	Slaven Alerić
Studij:	Sveučilišni prijediplomski studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R4169, 11.10.2021.
Turnitin podudaranje [%]:	2

Ovom izjavom izjavljujem da je rad pod nazivom**: Kibernetičke prijetnje u društvenim mrežama**

izrađen pod vodstvom mentora prof. dr. sc. Krešimir Grgić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis pristupnika:

SADRŽAJ

1. UVOD

Društvene mreže su postale nezaobilazni dio suvremenog života, omogućujući milijunima korisnika diljem svijeta da komuniciraju, dijele informacije i povezuju se na načine koji su nekada bili nezamislivi. Platforme poput Facebooka, Twittera, Instagrama i LinkedIna ne samo da olakšavaju osobnu interakciju, već igraju ključnu ulogu u poslovanju, marketingu i političkim kampanjama. Ipak, uz sve prednosti koje donose, društvene mreže također predstavljaju značajan rizik kada je riječ o kibernetičkoj sigurnosti. Kibernetičke prijetnje na društvenim mrežama su složene i raznolike, uključujući krađu identiteta i širenje zlonamjernog softvera. Napadači koriste velike količine osobnih podataka dostupnih na ovim platformama za izvođenje sofisticiranih napada usmjerenih na pojedince, organizacije, pa čak i cijele države. Ove prijetnje mogu imati ozbiljne posljedice, uključujući financijske gubitke, narušavanje privatnosti, štetu po ugled i psihološki stres za žrtve.

Rad je podijeljen na 8 osnovnih poglavlja: uvod, vrste kibernetičkih prijetnji, posljedice kibernetičkih prijetnji, strategije za zaštitu od kibernetičkih prijetnji, analiza stvarnih primjera kibernetičkih napada, uloga umjetne inteligencije (AI), zakoni i regulative, zaključak.

1.1 Zadatak završnog rada

Različite vrste društvenih mreža postale su medijske društvene platforme koje obuhvaćaju vrlo brojnu i heterogenu skupinu korisnika. Predstavljaju okruženje u kojem je prisutan veliki broj različitih kibernetičkih prijetnji. Potrebno je sustavno analizirati sigurnosne aspekte društvenih mreža (postojeće prijetnje i protumjere), uz detaljniji osvrt na različite vrste napada (npr. društveni inženjering, phishing, malware...). Analizirati neke primjere zabilježenih incidenata, te definirati preventivni sigurnosni okvir i politiku prevencije zlouporabe ovih medija.

2. VRSTE KIBERNETIČKIH PRIJETNJI

Društvene mreže su zbog svog širokog dosega i česte uporabe postale ključna meta za različite vrste kibernetičkih napada. Te prijetnje mogu biti raznolike, krećući od jednostavnih napada na pojedince do složenih prijetnji koje mogu ugroziti velike skupine korisnika pa čak i cijele organizacije. Svaka prijetnja ima svoje specifične metode, ciljeve i posljedice, ali nekoliko faktora im je jednako, a to je da pokušavaju iskoristiti ljudske slabosti i tehničke ranjivosti kako bi došle do svojeg cilja. U ovom poglavlju su analizirane najčešće vrste kibernetičkih prijetnji koje se pojavljuju u društvenim mrežama, uključujući *phishing* napade, *malware* te DDoS napade.

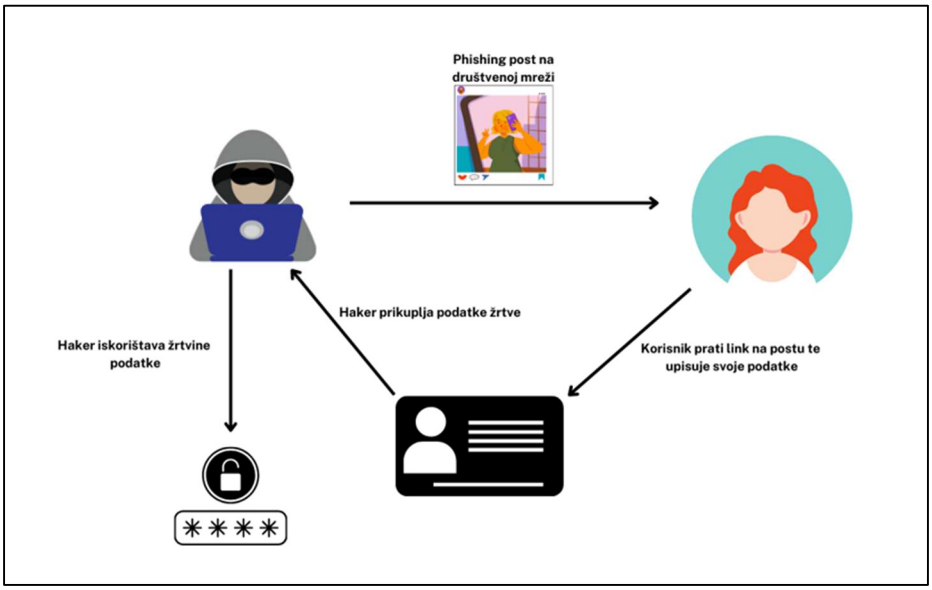
2.1 Phishing napadi

Phishing je mrežni napad u kojem napadač stvara lažnu postojeću web-stranicu kako bi prevario online korisnika da izvuče osobne podatke. *Phishing* je kombinacija društvenog inženjeringa i tehničkih metoda za uvjeravanje korisnika da otkrije svoje osobne podatke. Kibernetički kriminalci obično iskorištavaju korisnike koji su slabo informirani o ranjivostima na internetu. Napadači često koriste lažne profile ili kompromitirane račune kako bi poslali zlonamjerne linkove ili poruke. Glavni svrha *phishing* napada na društvenim mrežama je iskoristiti povjerenje koje korisnici imaju prema svojim prijateljima ili poznatim brendovima koje prate. Napadači primjenjuju složene tehnike kao što su kopiranje korisničkih računa ili imitacija poznatih platformi kako bi povećali šanse za uspjeh svojih napada.

Nekoliko načina kojima se izvode *phishing* napadi na društvenim mrežama su:

1. **Kloniranje profila**: Napadači kloniraju postojeće profile korisnika kako bi poslali poruke s lažnim zahtjevima za informacijama.
2. **Lažni nagradni programi**: Objavljuju se oglasi ili postovi koji obećavaju nagrade u zamjenu za osobne podatke ili dijeljenje sadržaja.
3. **Lažne aplikacije**: Napadači stvaraju lažne aplikacije koje izgledaju kao popularne društvene mreže ili alati, tražeći pritom pristup korisničkim podacima.

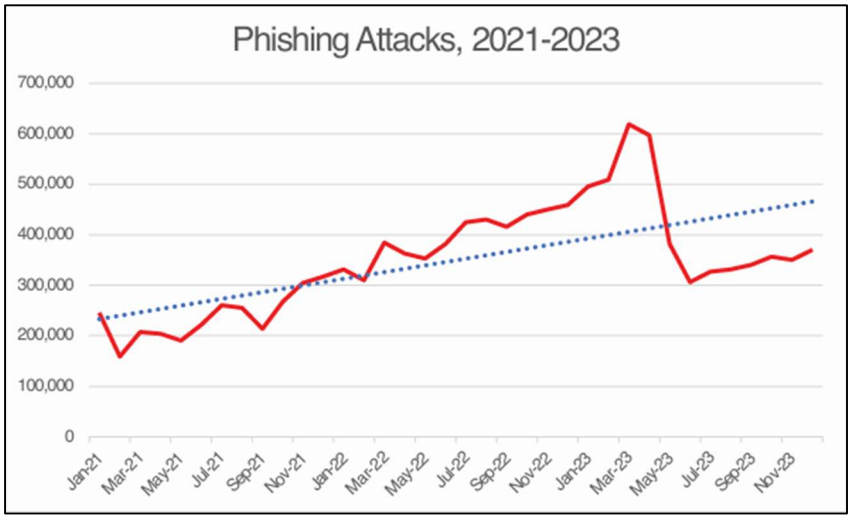
4. **Zlonamjerni linkovi**: Objavljuju se linkovi koji vode na lažne prijavne stranice ili stranice za unos osjetljivih informacija.



Slika 2.1 *Ilustracija ciklusa phishing napada*

Na slici 2.1 je ilustracija jednog primjera izvršavanja *phishing* napada. Napadač postavlja *phishing* post na društvenoj mreži koji sadrži link koji vodi na *phishing* web stranicu koja od žrtve zahtjeva da upiše svoje podatke za prijavu. Napadač zloupotrebljava dobivene podatke na način da s njima može pristupiti profilima žrtve ili da navedene podatke prodaje.

Prema izvješću APWG-a (engl. Anti-*Phishing* Working Group), međunarodne organizacije koja se bavi borbom protiv *phishing*a, o trendovima *phishing* napada između 2021. godine i 2023. godine može se uočiti veliki pad u *phishing* napadima u drugom kvartalu 2023. godine no zabilježen je kontinuirani porast nakon toga velikog pada [9]. Iako sve veća populacija internet korisnika svakom godinom postaje informatički pismenija *phishing* napadi se također razvijaju te prilagođavaju implementirajući bolje i vjerodostojnije metode varanja korisnika.



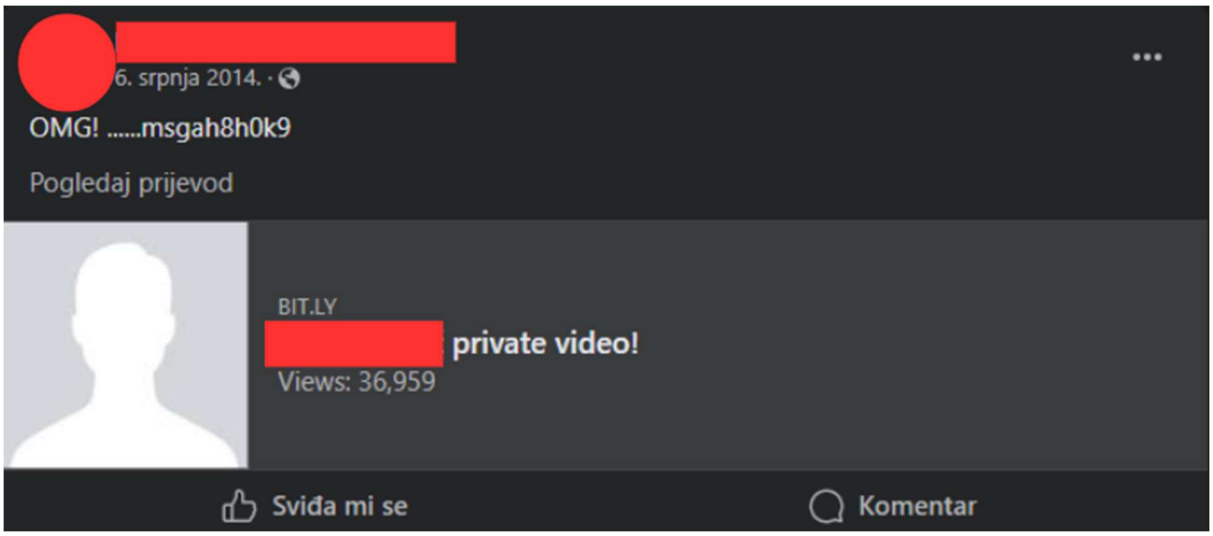
Slika 2.2 *Phishing napadi u razdoblju od 2021. do 2023. godine (Izvor: „APWG Phishing report“)*

2.2 Malware

Malware je zlonamjerni softver te je jedan od najučestalijih i najozbiljijih kibernetičkih prijetnji na društvenim mrežama. To je softver kojemu je glavni cilj prodrti u računalni sustav ili mrežu kako bi prouzročio štetu, ukrao podatke ili omogućio neovlašteni pristup. *Malware* se na društvenim mrežama širi na brojne načine poput lažnih linkova i privitaka te lažnih aplikacija, igara, *phishing* kampanja, clickjackingom i *malvertising*om.

2.2.1 Lažni linkovi i privitci

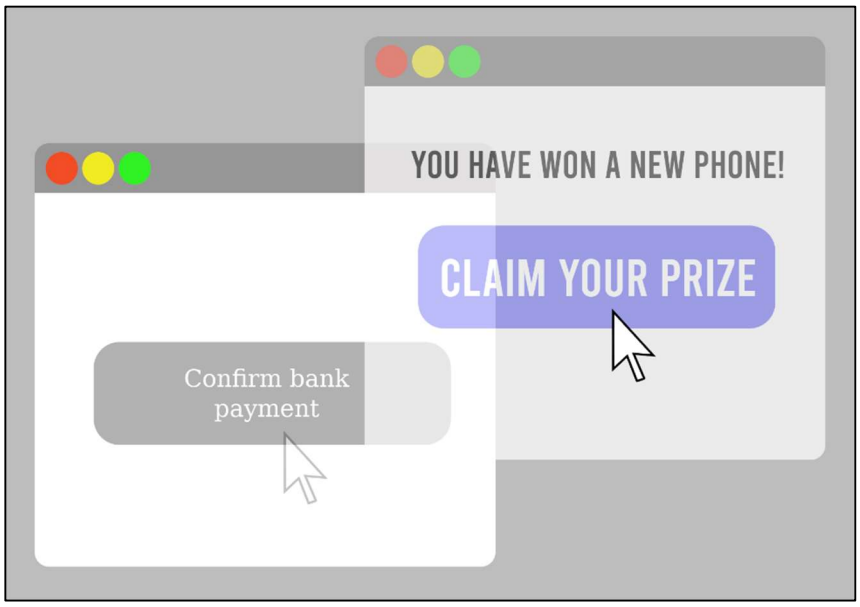
Malware se društvenim mrežama često širi putem lažnih linkova koji se dijele preko poruka, komentara ili objava. Ti linkovi su često predstavljeni kao nešto privlačno i legitimno te sadrže naslove poput „Provjeri tko je sve posjetio tvoj profil!“ ili „Pogledaj šokantan video svojeg prijatelja!“. Na slici 2.3 je primjer Facebook *phishing* posta koji sadrži bit.ly link koji vodi do download-a zaražene datoteke. Facebook račun s kojeg je objavljen *phishing* post je već zaražen te je pod potpunom kontrolom napadača. Koristeći šok faktor napadač koristi *phishing* post kako bi naveo korisnika da preuzme datoteku navodnog „videa“.



Slika 2.3 *Primjer phishing posta koji sadrži malware u sebi*

2.2.2 Clickjacking

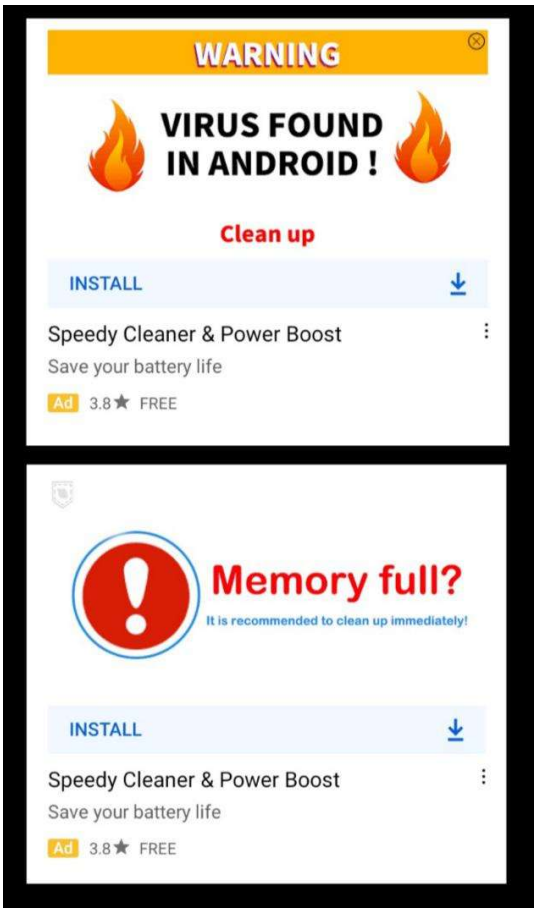
Clickjacking je metoda kojom napadač koristi „klikabilne“ objekte koji na prvi pogled izgledaju atraktivno i sigurno no iza sebe kriju zlonamjerne elemente, odnosno *malware*. Na slici 2.4 je prikaz načina na koji funkcionira *clickjacking.* Desni prozor prikazuje *iframe* kojeg je napadač napravio kako bi zamaskirao kako korisnik umjesto opcije „CLAIM YOUR PRIZE“ zapravo klikće na opciju s kojom odmah ide na plaćanje. Na jednaki način napadač može sakriti „Download“ gumb te bez pristanka korisnika skinuti *malware* na računalo. S primjerima *clickjackinga* se susrećemo svugdje diljem interneta, od različitih web stranica za online kupnju do samih društvenih mreža. Jedan od najpoznatijih primjera *clickjacking-a* je napad na Adobe-ovu Flash plugin stranicu. Napadač je učitao svoju stranicu u nevidljivi iframe preko Adobe-ove stranice za kontrolu različitih pristupa te na taj način prevario korisnika kako bi korisnik bez znanja dao dopuštenje bilo kojoj Flash animaciji da koristi korisnikovu kameru i mikrofon.



Slika 2.4 *Način na koji funkcionira clickjacking*

2.2.3 Malvertising

U *malvertising*-u napadač igra ulogu oglašivača te isporučuje oglase kojima je cilj prenijeti *malware* na uređaje korisnika. U praksi možemo uočiti dvije glavne vrste *malvertising* napada. Prvu vrstu napada obilježava to što ne zahtjeva proaktivnu akciju korisnika. Napadač ubacuje kod u oglas koji traži ranjivosti u korisnikovom uređaju za zarazu. U drugoj vrsti napada zlonamjerni oglašivači isporučuju atraktivne oglase kako bi uvjerili korisnika da klikne i proslijede ga na odredišnu web stranicu. Ova vrsta zapravo oponaša isti pristup koji se koristi u *phishing* napadima [14]. Napadači mogu iskoristiti informaciju o operacijskom sustavu korisnika kako bi kod automatski prilagodio reklamu, što je prikazano na primjeru na slici 2.5.



Slika 2.5 *Primjer malvertising reklama*

2.3 Socijalni inženjering

Socijalni inženjering predstavlja oblik manipulacije ljudskim ponašanjem radi dobivanja povjerljivih informacija ili izvršavanja nekih radnji koje bi koristile napadaču. Kada se primijeni u kontekstu društvenih mreža, postaje kibernetička prijetnja zbog svoje sposobnosti da iskoristi društvene veze i povjerenje korisnika za ostvarivanje svojih ciljeva.. Ova vrsta prijetnje često se oslanja na psihološke trikove i ljudske slabosti.

U kontekstu društvenih mreža, socijalni inženjering je posebno opasan zbog količine informacija koje korisnici svakodnevno dijele putem društvenih mreža. Napadači mogu koristiti te

informacije kako bi izgradili lažni identitet, stvorili uvjerljive scenarije te kako bi se što bolje prilagodili žrtvi.

Postoje različite tehnike socijalnog inženjeringa u društvenim mrežama. Stvaranjem lažnih profila na društvenim mrežama napadači se mogu pretvarati da su prijatelji ili kolege žrtve ili da su poznata osoba, te na taj način stvaraju posebnu vezu sa žrtvom što im donosi lakši put do krađe osjetljivih podataka korisnika. *Pretextingom* napadač stvara lažni scenarij poput kontaktiranja žrtve pretvarajući se da je iz tehničke podrške te traženjem lozinke ili drugih osjetljivih podataka. *Catfishingom* napadač stvara lažni identitet na društvenim mrežama kako bi prevario korisnike s ciljem uspostavljanja romantičnih veza.

2.4 Cyber-Stalking

Cyber-stalking označava digitalno praćenje te uznemiravanje uporabom interneta, najčešće putem društvenih mreža. Konstantno nadziranje žrtve može imati ozbiljne emocionalne i psihološke posljedice za žrtvu, uključujući strah, tjeskobu i gubitak osjećaja sigurnosti. Ključne karakteristike koje se vežu uz pojam cyber-stalkinga su nadzor žrtve što uključuje konstantno praćenje društvenih mreža žrtve kako bi napadač prikupio što više informacija, uznemiravanje koje uključuje kontinuirano slanje neželjenih poruka i komentara, te prijetnje koje je uvelike olakšano pojavom društvenih mreža zbog anonimnosti napadača.

2.4.1 Statistike o cyber-stalkingu

Brojne statistike su provedene u vezi cyber-stalkinga te pokazuju zabrinjavajući trend u porastu ovakvih aktivnosti:

- Prema istraživanjima američkog *Bureau of Justice Statistics*, čak **1 od 4 žrtve stalkinga** prijavila je da je bila žrtva stalkinga putem interneta.
- Žene su češće žrtve cyber-stalkinga. Prema izvještaju *Pew Research Center-a* iz 2021. godine oko **26% žena i 12% muškaraca** starijih od 18 godina u SAD-u doživjelo je cyber-stalking barem jednom u životu.
- Prema istraživanju *Pew Research Center* iz 2020. godine pokazano je da je oko **45% slučajeva cyber-stalkinga** povezano s **društvenim mrežama** (najviše Facebook, Instagram i Twitter).
- Samo oko 40% žrtava cyber-stalkinga prijavljuje ove incidente policiji [7]

3. POSLJEDICE KIBERNETIČKIH PRIJETNJI

3.1 Psihološke posljedice

Posljedice koje kibernetičke prijetnje predstavljaju često su puno teže nego što se na prvi pogled čini jer se odvijaju u digitalnom prostoru što može djelovati bezopasno. Postoji nekoliko vrsta psiholoških posljedica koje se ponavljaju najčešće, a to su: **stres** i **anksioznost**, **depresija**, **smanjeno samopoštovanje te socijalna anksioznost** i **izolacija**.

Prema teoriji socijalnog učenja, pojedinci usvajaju ponašanja i stavove kroz promatranje i imitaciju drugih. Ova teorija se može primijeniti i na kibernetičke prijetnje te njihov utjecaj na socijalni razvoj pojedinca. Stalna izloženost kibernetičkim prijetnjama putem društvenih mreža i online interakcija može uvelike oblikovati stavove i ponašanja pojedinca prema sebi i drugima. Na primjer, kontinuirana izloženost ***cyberbullyingu*** može rezultirati da pojedinac počne negativno razmišljati o sebi i drugima što može dovesti do pada samopoštovanja i povećanja socijalne anksioznosti. **Krađa identiteta** je jedna kibernetička prijetnja koja također može uvelike utjecati na socijalni razvoj pojedinca. Uzrokuje društvenu izolaciju te može trajno negativno utjecati na povjerenje pojedinca u odnosima s drugim osobama. Kibernetičke prijetnje se moraju shvatiti ozbiljno jer mogu ostaviti negativne posljedice na dugoročno mentalno zdravlje.

3.1.1 Statistike psiholoških posljedica kibernetičkih prijetnji

Cyberbullying među mladima: Cyberbullying je oblik nasilja koji se odvija putem digitalnih sredstava, uključujući društvene mreže, tekstualne poruke i druge online platforme. Prema istraživanju koje je provelo Nacionalno udruženje za obrazovanje (NEA), 43% adolescenata je iskusilo neki oblik cyberbullyinga.

Utjecaj na mentalno zdravlje: Cyberbullying može ozbiljno narušiti mentalno zdravlje žrtava, često uzrokujući depresiju i anksioznost. Studija objavljena u časopisu "Journal of Adolescent Health" otkriva da žrtve cyberbullyinga imaju 2,3 puta veću vjerojatnost da će iskusiti depresivne simptome u usporedbi s onima koji nisu žrtve.

Suicidalne misli i ponašanja: Izloženost kibernetičkom zlostavljanju može povećati rizik od suicidalnih misli i ponašanja kod žrtava. Istraživanje objavljeno u "JAMA Pediatrics" pokazuje da su žrtve cyberbullyinga 1,9 puta sklonije razviti suicidalne misli i 1,5 puta sklonije pokušaju samoubojstva u usporedbi s onima koji nisu izloženi kibernetičkom zlostavljanju.

3.2 Financijske posljedice

Rastom kibernetičkog kriminala rastu i financijske posljedice koje su ostavljene pojedincu ili organizaciji. Kibernetičke prijetnje mogu rezultirati značajnim gubicima.

Izravni financijski gubici predstavljaju direktan gubitak sredstava uslijed prijevara. Kibernetičke prijevare, kao što su recimo *phishing* napadi, mogu dovesti do krađe financijskih sredstava. Pojedinac ili organizacija može izgubiti novac putem neovlaštenih transakcija, krađe identiteta ili ransomwareom.

Troškovi oporavka predstavljaju popravak štete i obnovu sustava. Nakon kibernetičkog napada organizacije moraju uložiti značajna sredstva u popravak sustava te unaprjeđenje sigurnosnih mjera. Jedan od primjera je tvrtka Target koja je 2013. godine, kada su ukradeni podaci o kreditnim karticama milijuna korisnika, morala izdvojiti više od 200 milijuna dolara na troškove oporavka od kibernetičkog napada

Neizravni financijski gubici predstavljaju gubitak povjerenja i reputacije korisnika. Kada organizacija postane žrtva kibernetičkog napada može doći do gubitka povjerenja klijenata što dugoročno može imati velike financijske posljedice. Brojne organizacije koje posluju online susreću se sa raznim kibernetičkim prijetnjama te ukoliko organizacija nije dovoljno zaštićena dovodi u opasnost svoje korisnike. Primjer je Facebook koji je 2019. godine kažnjen s 5 milijardi dolara zbog kršenja zakona o privatnosti korisnika te je ujedno izgubio i velik broj korisnika.

3.3 Reputacijska šteta

Za organizacije i javne osobe, kibernetičke prijetnje mogu rezultirati značajnom reputacijskom štetom. Lažne informacije i dezinformacije mogu narušiti povjerenje javnosti i negativno utjecati na ugled.

Gubitak povjerenja nastupa kada se dogode kibernetički napadi, posebno ako uključuju krađu osobnih podataka. Dolazi do gubitka povjerenja među korisnicima društvene mreže zbog čega korisnici mogu izgubiti povjerenje u samu platformu. Jedan od primjera je ranije naveden napad na Facebook 2019. godine kada su otkriveni podaci milijuna korisnika. Uspješni kibernetički napadi donose uz sebe i **negativan medijski publicitet** što može dodatno pogoršati reputaciju organizacije. Brojne organizacije koje koriste društvene mreže kako bi promovirali svoj proizvod i uslugu mogu biti pogođene reputacijskom štetom ukoliko su žrtve napada. Navedene organizacije mogu biti žrtve krađe identiteta te mogu distribuirati dezinformacije što također nanosi štetu organizaciji kao korisniku društvene mreže. **Šteta na osobnoj razini** je također veliki problem koji nastaje prilikom kibernetičkih napada. Korisnici društvenih mreža mogu pretrpjeti ozbiljnu reputacijsku štetu ako se njihovi profili koriste za širenje lažnih informacija ili za širenje *malware*a. Stvaranje lažnih profila te širenje dezinformacija može dovesti do emocionalne i profesionalne štete.

Velika meta kibernetičkih napada su slavne osobe kojima napadači nastoje dobiti pristup privatnim datotekama kako bi preuzeli i objavili privatne fotografije, videe ili osjetljive informacije. Za primjer, objavljivanje privatnih, eksplicitnih fotografija rezultira ogromnom reputacijskom štetom za korisnika te uvelike utječe na njegovo psihičko zdravlje.

4. STRATEGIJE ZA ZAŠTITU OD KIBERNETIČKIH PRIJETNJI

4.1 Edukacija i svijest korisnika

Jedan od najvažnijih koraka u borbi protiv kibernetičkih prijetnji je edukacija korisnika o potencijalnim rizicima i načinima zaštite. To uključuje prepoznavanje *phishing* napada, pravilno korištenje lozinki i svijest o socijalnom inženjeringu. Ključni aspekti ove edukacije uključuju razumijevanje sigurnosnih postavki, prepoznavanje znakova kibernetičkog zlostavljanja, zaštitu osobnih podataka, te svijest o pravima i resursima dostupnim žrtvama.

Neki od najvažnijih aspekata edukacije i svijesti korisnika su:

1. **Razumijevanje sigurnosnih postavki**: Korisnici društvenih mreža trebaju biti svjesni o sigurnosnim postavkama koje im platforme nude. Na primjer, Facebook, Twitter i Instagram imaju opcije koje omogućuju korisnicima da kontroliraju tko može vidjeti njihove postove, kontaktirati ih ili označavati na fotografijama. Studija Pew Research Center-a iz 2019. godine otkriva da samo 42% korisnika društvenih mreža redovito provjerava i ažurira svoje postavke privatnosti [5].

2. **Svjesnost o phishingu i društvenom inženjeringu**: Ključno je da korisnici znaju prepoznati različite oblike kibernetičkog zlostavljanja, kao što su uznemiravajuće poruke, prijetnje, lažni profili i neprimjereni komentari. Edukacija može uključivati radionice, online tečajeve i informativne kampanje koje nude konkretne primjere i strategije za prepoznavanje i reagiranje na ove prijetnje.

3. **Zaštita osobnih podataka**: Korisnici moraju biti svjesni važnosti zaštite svojih osobnih podataka. To uključuje korištenje jakih lozinki, aktivaciju dvofaktorske autentifikacije i izbjegavanje dijeljenja osjetljivih informacija javno na društvenim mrežama. Također je važno znati kako se nositi s *phishing* napadima i drugim pokušajima krađe identiteta. Studija Norton Cyber Security Insights Report iz 2020. godine pokazuje da je 68% korisnika društvenih mreža zabrinuto zbog mogućnosti da njihovi osobni podaci budu ukradeni ili zloupotrijebljeni [6].

4. **Svijest o pravima i resursima**: Korisnici bi trebali biti informirani o svojim pravima i resursima koji im stoje na raspolaganju u slučaju da postanu žrtve kibernetičkog zlostavljanja. Ovo može uključivati informacije o tome kako prijaviti zlostavljanje na platformi, kako kontaktirati nadležne institucije i gdje potražiti emocionalnu i psihološku podršku. Prema istraživanju EU Kids Online, samo 29% djece i mladih u Europi zna kako prijaviti uznemiravanje na internetu, a još manji postotak zna gdje potražiti pomoć i podršku [7].

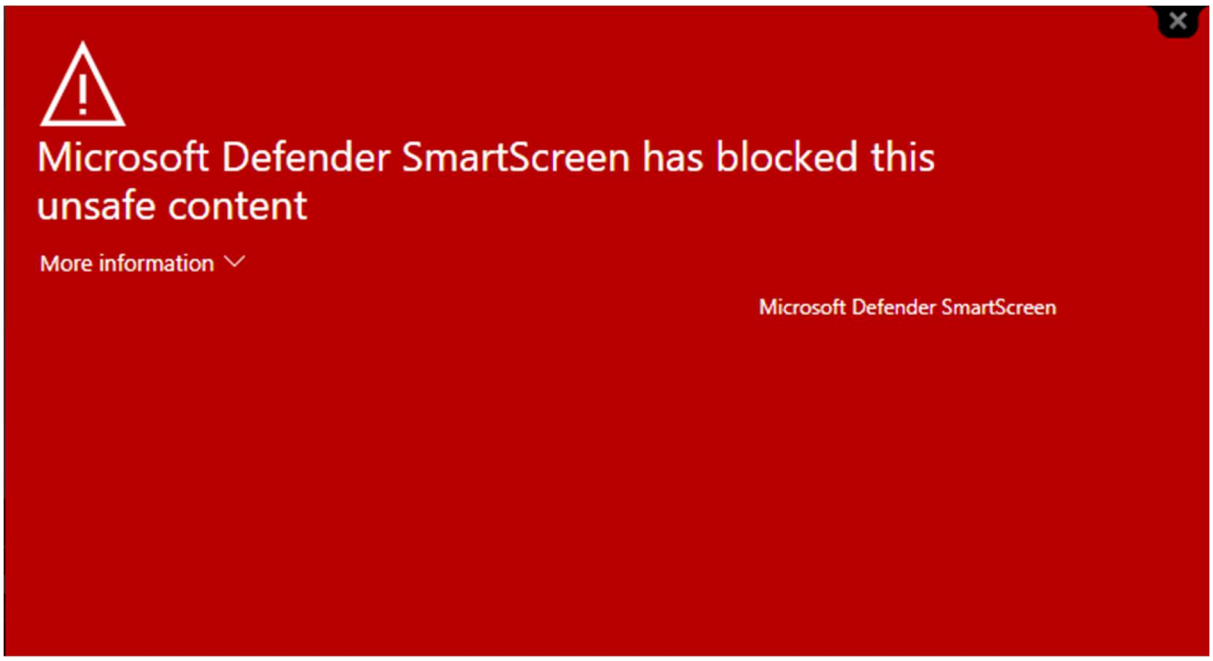
4.2 Korištenje sigurnosnih alata

Korištenje sigurnosnih alata predstavlja ključni faktor u strategiji zaštite od kibernetičkih prijetnji. Ovi alati služe za detekciju, sprječavanje i ublažavanje prijetnje koje se pojavljuju na društvenim mrežama i ostatku interneta.

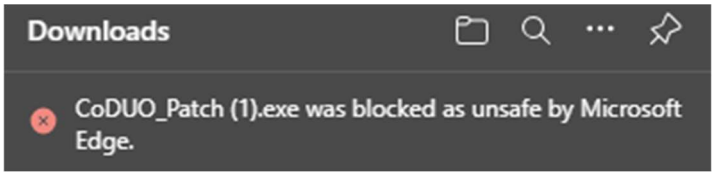
4.2.1 Antivirusni i anti-malware alati

Antivirusni i anti-*malware* su softveri koji pružaju detekciju te uklanjanje zlonamjernog softvera. Ovi alati pružaju zaštitu u stvarnom vremenu, skeniraju preuzete datoteke, URL-ove i druge podatke koje mogu sadržavati *malware*. Primjer antivirusnog softvera je Norton koji pruža zaštitu u stvarnom vremenu te se može koristiti za zaštitu osobnog računala te za zaštitu čitavih organizacija.

Antivirusni alati su izrazito korisni u zaštiti korisnika i organizacija od prijetnji na društvenim mrežama jer nude **zaštitu od zlonamjernih linkova** te **prepoznavanje zlonamjernih privitaka** na način da spriječi preuzimanje zaraženih datoteka podijeljenih putem društvenih mreža. Na slikama 4.1 i 4.2 možemo uočiti na koji način funkcionira Microsoftov antivirusni softver Microsoft Defender koji je također integriran i u sami Microsoft Edge preglednik. On odmah upozorava korisnika da je datoteka koju želi preuzeti sumnjiva te također nudi i opciju zadržavanja datoteke ukoliko je korisnik siguran da ona ne sadrži nikakav zlonamjerni softver.



Slika 4.1 *Microsoft Defender zaštita u stvarnom vremenu*



Slika 4.2 *Microsoft Edge zaštita u stvarnom vremenu*

4.2.2 Vatrozidi

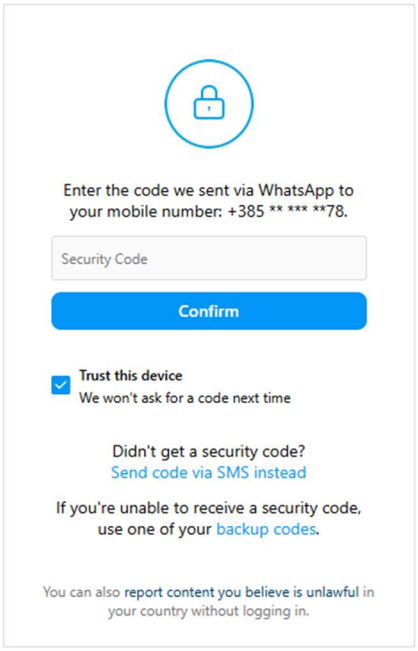
Vatrozidi su jedni od ključnih komponenti u zaštiti uređaja i mreža od kibernetičkih prijetnji. Oni funkcioniraju kao barijera između interne (osobne) mreže i internete tako što kontroliraju sav ulazni i izlazni promet. Vatrozidi mogu filtrirati sve podatke i blokirati neovlaštene pristupe te time štite korisnike i organizacije od potencijalnih napada, uključujući one koje dolaze putem društvenih mreža.

4.3 Višefaktorska autentifikacija (MFA)

Višefaktorska autentifikacija dodaje dodatni sloj zaštite prilikom prijave na određenu web stranicu što uključuje i društevene mreže. To može uključivati jedinstveni kod poslan na mobilni uređaj ili biometrijsku autentifikaciju koja je dio svih novijih mobitela. Ovo je odličan način zaštite koji poprilično otežava napadačima pristup računima i ako imaju lozinku računa.

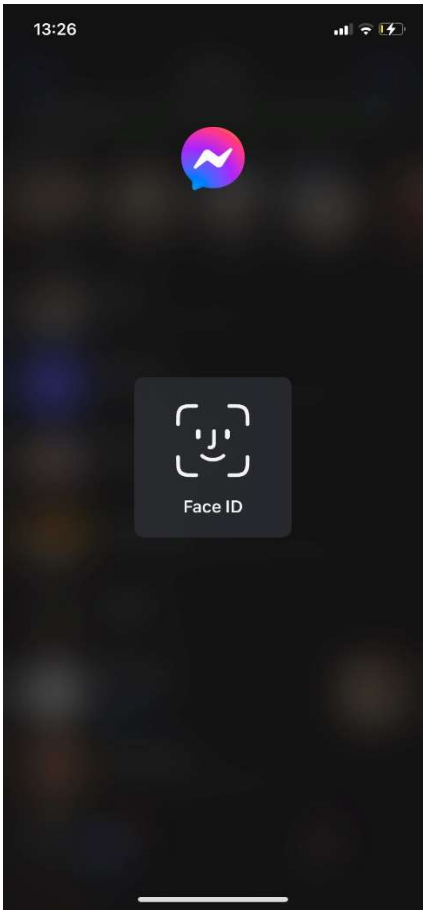
4.3.1 Primjeri višefaktorske autentifikacije u društvenim mrežama

Prvi primjer je društvena mreža **Instagram**. Nakon upisivanja točnih podataka za prijavu (*username* i lozinka) korisnik dolazi do zaslona na slici 4.3 koji od korisnika zahtjeva sigurnosni kod kojeg dobiva na broj mobitela koji je postavio prilikom registracije. Pristup računu ostvaruje tek kada upiše kod dobiven porukom. Ovaj način poprilično otežava napadaču da dobije kontrolu nad računom i ako posjeduje lozinku računa jer mora imati i pristup mobilnom uređaju korisnika.



Slika 4.3 *Primjer višefaktorske autentifikacije - Instagram*

Drugi primjer je primjer biometrijske autentifikacije za aplikaciju **Messenger** koja se može uključiti za gotovo sve aplikacije. Biometrijska autentifikacija je u ovom primjeru izvedena tako što aplikacija Messenger koristi biometrijske podatke mobilnog uređaja, u ovom slučaju Face ID koji je dio iOS operativnog sustava.



Slika 4.4 *Primjer biometrijske autentifikacije - Messenger*

4.4 Alati za praćenje društvenih mreža

Ovo su alati koji pružaju organizacijama praćenje te analizu aktivnosti na društvenim mrežama u realnom vremenu. Omogućuju praćenje različitih vrsta sadržaja kao što su objave, komentari, spominjanje njihovog brenda te određenih ključnih riječi, te nude uvid u potencijalne kibernetičke prijenje.

Jedan od primjera alata za praćenje društvenih mreža je **Hootsuite**, platforma za upravljanje društvenim mrežama koja se bavi gotovo svime što upravitelji društvenih medija rade svakodnevno. Nudi različite usluge poput planiranja postova, uređivanja sadržaja, upravljanja timova pa sve do analize komentara te pravovremene obavijesti o sumnjivim radnjama koje uključuju njihov sadržaj. Hootsuite se može integrirati s gotovo svim društvenim mrežama te omogućuje kontroliranje računa s jednog mjesta.

5. ANALIZA STVARNIH PRIMJERA KIBERNETIČKIH NAPADA

5.1 Napadi na društvenim mrežama

Cambridge Analytica je jedan od najznačajnijih napada na privatnost korisnika na društvenim mrežama. Britanska politička konzultantska firma ilegalno je prikupljala podatke više od 87 milijuna korisnika Facebooka bez njihovog pristanka. Ti podaci su korišteni za profiliranje korisnika te su korištenje za prilagođavanje oglasa u političke svrhe, točnije podaci su korišteni pretežito tijekom kampanja poput referenduma o Brexitu i predsjedničkih izbora u SAD-u 2016. godine. Podaci su prikupljani kroz aplikaciju „This Is Your Digital Life“ koja je bila postavljena kao kviz te je omogućavala prikupljanje osobnih podataka korisnika te njihovih Facebook prijatelja. Skandal je doveo do istraga u SAD-u i Ujedinjenom Kraljevstvu gdje je na kraju pred američkim Kongresom svjedočio čak i izvršni direktor Facebooka, Mark Zuckerberg. Facebook je dobio kaznu od 5 milijardi dolara te je sam skandal uvelike utjecao na razne regulacije u vezi privatnosti podataka na internetu implementiranjem GDPR-a u Europskoj Uniji te povećanjem svijesti korisnika o privatnosti osobnih podataka.

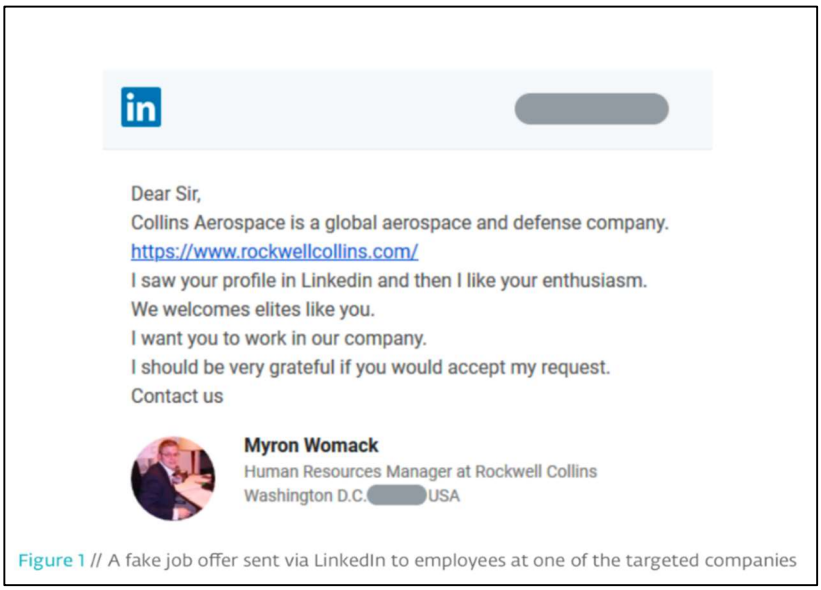
Hakerski napad na Twitter 2020. godine je jedan od najvećih sigurnosnih incidenata u povijesti društvenih mreža. Dogodio se 15. srpnja 2020. godina kada su hakeri uspješno preuzeli račune mnogih poznatih osoba i kompanija koristeći ih za širenje bitcoin prevare. Način na koji su hakeri uspjeli infiltrirati interni sustav Twittera je tako što su koristili tehniku socijalnog inženjeringa. Predstavljanjem kao zaposlenicima kompanija prevarili su stvarne zaposlenike Twittera kako bi došli do pristupa alatima za upravljanje korisničkim računima. Tako su došli do pristupa profilima mnogih poznatih osoba poput Elona Muska, Billa Gatesa, Jeffa Bezosa i kompanija poput Applea i Ubera. Tweetovi su većinom od korisnika tražili da pošalju bitcoin na određenu adresu kako bi nazad dobili dvostruko. Na slici 5.1 su primjeri tweetova koji su bili objavljeni s profila Joe Bidena i Baracka Obame.

Slika 5.1 *Primjeri hakerskih Twitter objava*

Twitter, kao mjeru opreza, je morao privremeno blokirati sve verificirane račune kako bi spriječio širenje prevare. Twitter je odmah pokrenuo internu istragu te su ubrzo pronašli nekoliko osoba, uključujući 17-godišnjeg hakera iz Floride koji je bio glavni organizator napada, koji su na kraju uhićeni i optuženi za brojna kaznena djela.

LinkedIn Spear Phishing se odnosi na seriju napada hakera koji su kreirali lažne poslovne ponude kako bi prevarili korisnike, pretežito one u visoko plaćenim sektorima poput IT industrije. Poruke koje su hakeri slali korisnicima su često sadržavale linkove i priloge s kojim bi korisnik preuzeo *malware* koji bi omogućio napadačima pristup računalima. Ovi napadi su često ciljali na poslovne korisnike što je rezultiralo krađom velike količine važnih poslovnih podataka i financijskih informacija. Sigurnosne tvrtke *Checkpoint i Proofpoint* uspjele su otkriti ovu seriju napada te su istaknuli kako su ovi napadi bili odlično osmišljeni jer su koristili stvarne informacije korisnika kako bi prilagodili poruke samim korisnicima i na taj način lakše došli do povjerenja samog korisnika. LinkedIn poduzeo je mjere za dodatno osiguranje svoje platforme poput provjere profila i informiranja korisnika o različitim kibernetičkim prijetnjama. Uvedena je i višefaktorska autentifikacija te je korisnicima preporučeno da je koriste ukoliko žele bolje zaštiti svoje račune. Na slici 5.2 je primjer jedne *phishing* poruke koja je korištena na mreži LinkedIn koja sadrži link koji vodi na web stranicu Collins Aerospace kompanija no u privitku

poruke je PDF datoteka koja sadrži informacije o poslu no zapravo datoteka je zaražena *malware*-om.



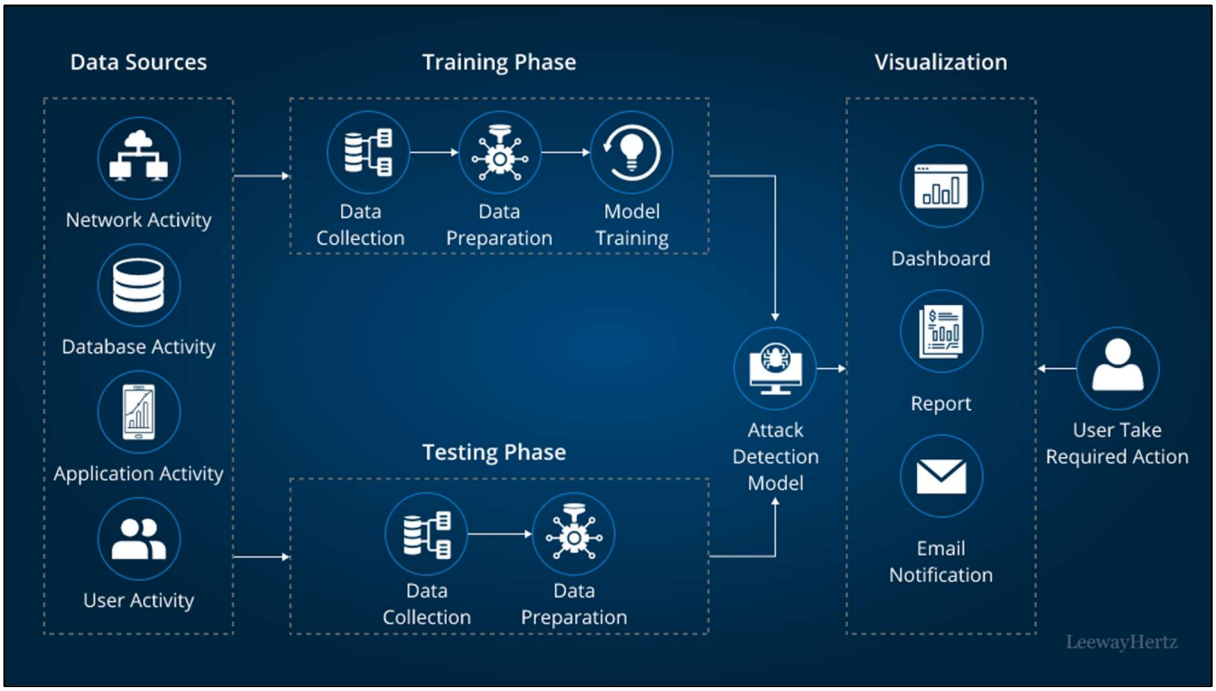
Slika 5.2 *Primjer LinkedIn phishing poruke*

6. ULOGA UMJETNE INTELIGENCIJE (AI)

Potreba za dinamičnim i učinkovitim rješenjima za kibernetičku sigurnost nikad nije bila veća. Ubrzanim razvojem umjetne inteligencije dovelo je do uvođenja i uključivanja umjetne inteligencije u kibernetičku sigurnost jer omogućuje dinamičku i pravovremenu detekciju te rješavanje problema. Umjetnu inteligenciju karakterizira sposobnost oponašanja i potencijalno nadmašivanje ljudskih kognitivnih funkcija što su ključni faktori za razvoj odličnog alata za jačanje kibernetičke sigurnosti. Koristeći složene algoritme, umjetna inteligencija može izvući uzorke iz ogromnih skupova podataka, prilagoditi se novim informacijama i predvidjeti s velikom točnošću. Njezina brzina, točnost i sposobnost prepoznavanja novih kibernetičkih prijetnji uvelike nadmašuju konvencionalne sigurnosne sustave, čineći umjetnu inteligenciju sve važnijom komponentom kibernetičkih sigurnosnih protokola.

6.1 Detekcija prijetnji

Prava moć umjetne inteligencije leži u njenoj sposobnosti da učinkovito analizira ogromne količine podataka, identificira značajne obrasce i filtrira nebitne informacije. Ova je sposobnost osobito korisna u današnjem hiper-povezanom okruženju, gdje generirani podaci često nadmašuju mogućnosti obrade tradicionalnim metodama lova na prijetnje [18]. Integracija analize ponašanja unutar umjetne inteligencije olakšava prilagodljiviji pristup otkrivanju prijetnji. Kroz ovu tehniku AI sustavi mogu analizirati opsežne podatke o krajnjim točkama u mreži organizacije, koji se kasnije koriste za stvaranje detaljnih profila aplikacija koji nude temeljito razumijevanje tipičnih operativnih ponašanja. Ovi profili služe kao mjerilo za otkrivanje anomalija u stvarnom vremenu, gdje svako odstupanje od norme može ukazivati na potencijalni sigurnosni rizik. Na slici 6.1 prikazan je način i tijek strojnog učenja u kontekstu stvaranja dobre obrane od kibernetičkih prijetnji. Faze za treniranje i testiranje koriste velike količine podataka kako bi se AI što bolje prilagodio svakoj mogućoj situaciji te kako bi pružio što bolju i bržu zaštitu.



Slika 6.1 *Prikaz primjene strojnog učenja u kibernetičkoj sigurnosti*

6.2 Upravljanje ranjivostima

Nakon identificiranja ranjivosti korištenjem umjetne inteligencije za detekciju kibernetičkih prijetnji idući korak je prioritizacija ranjivosti. Algoritmi za strojno učenje procjenjuju rizik koji određena ranjivost predstavlja za organizaciju, uzimajući u obzir čimbenike poput potencijalnih posljedica eksploatacije i dostupnosti *eskploita*. Ova prioritizacija omogućava organizacijama lako i pravovremeno reagiranje te planiranje kako će reagirati na određenu prijetnju [20]. Idući korak je proaktivno obavještavanje. AI sustavi mogu proaktivno pratiti sustave kako bi prepoznali nove ranjivosti ili prijetnje te imaju mogućnost automatskog generiranja upozorenja i preporuka [21].

6.3 Izazovi i ograničenja AI u kibernetičkoj sigurnosti

Iako umjetna inteligencija (AI) prednjači u razvoju inovativnih rješenja za kibernetičku sigurnost, suočava se s nekoliko izazova i ograničenja. Transformativne mogućnosti ove tehnologije su nezaobilazne međutim, prepoznavanje njegovih ograničenja ključno je za uravnotežen i pragmatičan pristup njegovoj primjeni.

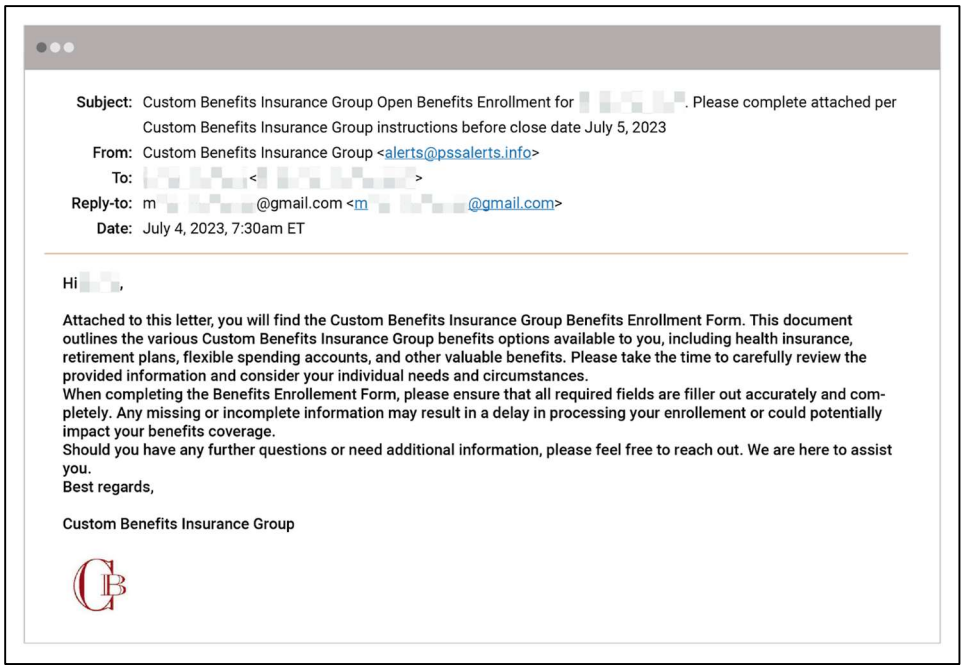
6.3.1 Ljudski faktor i AI

Međutim, iako je umjetna inteligencija revolucionirala područje kibernetičke sigurnosti, bitno je priznati da ona ne čini ljudski faktor nebitnim. Zapravo, sofisticirani kibernetički kriminalci sa specijaliziranim strategijama često mogu izbjeći AI sustave, dokazujući da ljudski element u kibernetičkoj sigurnosti još uvijek predstavlja značajan faktor. Prvo, ljudski protivnici nisu statične prijetnje koje imaju samo jednak način razmišljanja. Oni su kreativni, inteligentni, nepredviljivi i sposobni prilagoditi svoje strategije, što ih čini stalnim rizikom unatoč naprednoj obrani umjetne inteligencije. Oni mogu koristiti tehnike poput *data poisoninga* ili *adversial attackova* kako bi manipulirali procesom učenja sustava umjetne inteligencije. Ubacivanjem netočnih podataka, napadači mogu iksriviti razumijevanje umjetne inteligencije te direktno utjecati na samo donošenje odluka AI modela [22]. Također, zbog ovisnosti AI modela o podacima iz prošlosti postoji mogućnost da se AI model krivo prilagodi te donese krive odluke u vezi novih situacija koje odstupaju od uobičajenih podataka. Efektivni sustavi zahtijevaju

učinkovitu povezanost umjetne inteligencije i ljudskog faktora u protivnom sustav se može ponašati nekontrolirano i gubi na svojoj pouzdanosti.

6.3.2 AI kibernetički napadi

Phishing napadi provedeni korištenjem umjetne inteligencije koriste napredne tehnologije koje poboljšavaju točnost, učinkovitost i skrivenost kibernetičkih napada. Kibernetički kriminalci koriste algoritme strojnog učenja velikih skupova podataka za analizu ponašanja i preferencija meta, što im omogućuje izradu visoko personaliziranog sadržaja za krađu identiteta. To uključuje prilagođene e-mailove, poruke na društvenim mrežama ili obmanjujuće veze na web stranicama osmišljene za učinkovitije privlačenje pozornosti ciljanih korisnika. Upotrebom tehnika dubokog učenja, AI može čak replicirati i komunikacijske stilove i pristupe legitimnih subjekata poput tvrtki, organizacija ili pojedinaca. Na slici 6.2 je primjer AI generiranog e-maila kojeg je analizirala kompanija Abnormal security koja se bavi analiziranjem umjetne inteligencije u svrsi poboljšanja kibernetičke sigurnosti. Također na slici 6.3 je analiza teksta e-maila putem Giant Language Model Test Room-a koji pokazuje vjerojatnost AI generiranog teksta. Zelena boja predstavlja tekst koji sadrži riječi koje imaju najveću predviđenost, dok žute i crvene imaju malo manju predviđenost.



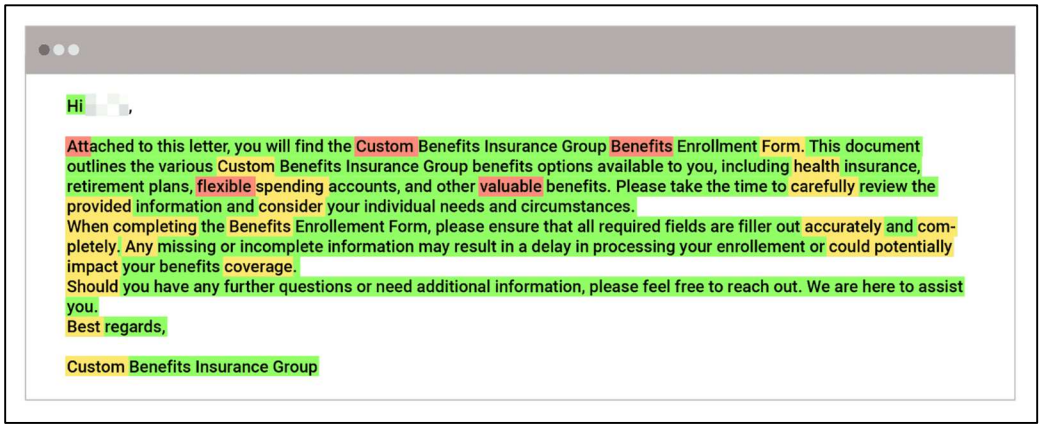
Subject: Custom Benefits Insurance Group Open Benefits Enrollment for [redacted]. Please complete attached per Custom Benefits Insurance Group instructions before close date July 5, 2023
From: Custom Benefits Insurance Group <alerts@pssalerts.info>
To: [redacted]
Reply-to: m[redacted]@gmail.com <m[redacted]@gmail.com>
Date: July 4, 2023, 7:30am ET

Hi [redacted],

Attached to this letter, you will find the Custom Benefits Insurance Group Benefits Enrollment Form. This document outlines the various Custom Benefits Insurance Group benefits options available to you, including health insurance, retirement plans, flexible spending accounts, and other valuable benefits. Please take the time to carefully review the provided information and consider your individual needs and circumstances.
When completing the Benefits Enrollement Form, please ensure that all required fields are filler out accurately and completely. Any missing or incomplete information may result in a delay in processing your enrollement or could potentially impact your benefits coverage.
Should you have any further questions or need additional information, please feel free to reach out. We are here to assist you.
Best regards,

Custom Benefits Insurance Group

Slika 6.2 *Primjer AI generiranog phishing e-maila*



Slika 6.3 *Analiza AI generiranog e-maila*

7. ZAKONI I REGULATIVE

7.1 Zakoni i regulative u Europi i svijetu

Regulative i zakoni koji se provide u Europi su opća uredba o zaštiti podataka (GDPR), Akt o digitalnim uslugama (DSA) i Akt o digitalnim tržištima (DMA). GDPR je uveden 25. svibnja 2018. [23]. Cilj GDPR je zaštita pojedinaca u pogledu obrade osobnih podataka i slobodnog kretanja istih podataka kako bi se uskladila zaštita temeljnih prava pojedinaca u vezi s aktivnostima obrade podataka i da osigura slobodan protok osobnih podataka između država članica EU [23]. Prati svako korištenje podataka kao npr. sakupljanje, snimanje, organiziranje, strukturiranje, spremanje i brisanje podataka [23]. To obuhvaća obradu osobnih podataka kroz korištenje računala, pametnih mobilnih telefona, kamera, dronova ili putem prijenosnih uređaja poput satova, automobila [23]. DSA se počeo primjenjivati 16. studenoga 2022.. Pruža opći okvir za pružanje posredničkih usluga te regulira određene oblike online pružanja usluga, uključujući određene aspekte internet trgovine [24]. Cilj je da digitalne tehnologije i internetske platforme poštuju prava korisnika kako bi oni mogli imati povjerenja u digitalne usluge. DSA zahtjeva da internetske platforme poput Youtube, Instagram, TikTok, Google i Snapchat vode računa o tome kako njihove usluge utječu na teme kao što su pošteni izbori, javna sigurnost, te mentalna i fizička dobrobit korisnika [25]. DMA odnosno Akt o digitalnim tržištima ima za cilj regulirati velike internetske platforme kako bi se osiguralo pravednije poslovno okruženje. Traži od internetskih platformi da moraju ispuniti stroge kriterije, poput jakog ekonomskog položaja, uloge posrednika između korisnika i poduzeća te stabilnosti na

tržištu kroz vrijeme. Prednosti DMA imaju poslovni korisnici koji će imati pravednije uvjete za poslovanje na digitalnom tržištu, inovatori i start-up poduzeća će dobiti bolje prilike za natjecanje i inovacije bez nepoštenih prepreka te će potrošači imati više opcija, bolju kvalitetu usluga i pravednije cijene. Internetske platforme neće smjeti zloupotrebljavati svoj položaj prema korisnicima i poslovnim partnetima, čime će se osigurati poštena konkurencija [26]. Nepoštivanje regulativa može snositi novčane kazne, periodične novčane kazne ili neke korektivne mjere npr. prodaja dijelova poduzeća.

Regulative koje se provide u SAD su Section 230 Communications Decency Act te Federalna trgovinska komisija (FTC). Cilj Zakona o pristojnosti u komunikacijama koji je doveden 1996-te godine je da se regulira nezakoniti ili štetni sadržaj na internetskim platformama. Problematika ovog zakona je što krši Prvi amandman koji služi za zaštitu slobode govora čime je proglašen neustavnim jer se regulacijom sadržaja na internetu može cenzurirati sadržaj kojeg netko želi objaviti [27]. Jedan od dijelova zakona koji je ostao na snazi je Section 230 koji pruža imunitet internet pružateljima usluga i društvenim mrežama od odgovornosti za sadržaj kojeg objavljuju njeni korisnici. To znači da platforme poput YouTube-a ili Instagram-a ne mogu pravno odgovarati za sadržaj kojeg njihovi korisnici postavljaju. Ali postoje odjeli u tvrtkama društvenih mreža koje se bave nadgledavanjem takvog sadržaja, brisanjem sadržaja ili cjelovitog računa korisnika. Također je uvedena cenzura sadržaja koji koristi neke prethodno označene riječi čime se takav sadržaj automatski uklanja. Prilikom stvaranja korisničkog računa, korisnik dobiva tekst „Terms of Service" kojeg mora pročitati te potvrditi suglasnost s korištenjem određene internet platforme. FTC je uveden 26. rujna 1914-te godine. Osnovana je u SAD-u s ciljem rješavanja problema monopola te je odgovorna i za druge zadatke poput prikupljanja ekonomskih statistika i izrade ekonomskih izvješća [28].

Primjeri iz drugih zemalja su poput Kine koja ima strogu kontrolu nad sadržajem na društvenim mrežama gdje se bave cenzurom i kontrolom podataka te Australija koja ima zakon o obaveznom uklanjanju terorističkog sadržaja s društvenih mreža.

7.2 Pravna odgovornost društvenih mreža

Postoji određena odgovornost korisničkog sadržaja koji se može dijeliti na nekoj društvenoj mreži. Svaki račun ima svoj algoritam koji je stvoren na temelju više čimbenika kao što su dijeljenje sličnog sadržaja, označavanje da im se sviđa sadržaj itd. Zbog toga, svaki korisnički račun ima svoje iskustvo na nekoj društvenoj mreži. Bez obzira na stvoreni algoritam, nedopušteni sadržaj se može iznenadno prikazati. Zbog toga je potrebna pravna odgovornost društvenih mreža koje će regulirati prikaz takvog sadržaja, odnosno moderirati i nadgledati te uklanjati. Mora postojati odgovornost za korisnički sadržaj kako bi spriječile širenje nezakonitog, štetnog ili nasilnog materijala (npr. govor mržnje, dezinformacije, zlostavljanje). Društvene mreže su postale ključni dio socio-političkog okruženja diljem svijeta, a s time su se i rasističke prakse sve više počele manifestirati na tim platformama. Rasistički govor se širi na društvenim mrežama, često kroz sakrivene taktike. Primjeri takvih taktika su korištenje meme-ova kao sredstvo za širenje rasističkih poruka na suptilan način što omogućava da rasistički sadržaj bude maskiran kao humor ili satira te korištenje lažnih profila i identiteta kako bi poticali mržnju i širili rasistički govor bez da otkriju svoj stvarni identitet. Političar Dean Browning je na taj način pokušao poticati mržnju, ali je zabunom zaboravio promijeniti korisnički račun čime je poruku mržnje objavio na svoj javni osobni račun.

Slika 7.1 *Tweet političara Deana Browninga*
https://twitter.com/Jezebel/status/1326296000219271168

Kao što je prije navedeno, postoji odgovornost društvenim mreža za zaštitu privatnosti te se provodi putem GDPR i zaštite maloljetnika. Društvene mreže imaju dodatnu odgovornost kada je riječ o zaštiti maloljetnika. Drugi korisnici imaju obvezu prijaviti korisničke račune ako smatraju da je osoba ispod 13 godina te društvena platforma mora ukloniti takav korisnički račun ako se utvrdi da

osoba ne poštuje pravila društvene mreže. YouTube se pojavio kao alternativa tradicionalnom dječjem sadržaju televizije, a na njemu se može pronaći mnoštvo popularnih dječjih sadržaja [29]. Nedavno je uveden Youtube Kids iz razloga što je sadržaj objavljen na normalnom Youtube-u bio nereguliran te se pod dječji sadržaj moglo ostavljati komentare gdje su djeca ostavljala poruke, a drugi korisnici sa zlim namjerama su mogli komunicirati s njima. Iz tog razloga je uvedena druga vrsta Youtube-a namijenjena za djecu gdje su komentari isključeni kako bi se spriječila ikakva komunikacija.

8. ZAKLJUČAK

Kibernetičke prijetnje na društvenim mrežama predstavljaju rastući problem u digitalnom dobu, koji nosi ozbiljne posljedice za pojedince, organizacije i društvo u cjelini. Ovaj rad analizirao je različite vrste kibernetičkih prijetnji, od *phishing* napada i malvera do socijalnog inženjeringa i cyber-stalkinga, ističući njihov utjecaj na psihološko, financijsko i reputacijsko zdravlje žrtava. Dok tehnologija nastavlja napredovati, prijetnje postaju sofisticiranije, čineći nužnim stalno prilagođavanje i unaprjeđivanje strategija zaštite.

Razmatranje stvarnih slučajeva, poput Cambridge Analytica skandala i hakerskog napada na Twitter 2020. godine, pokazalo je kako su društvene mreže postale kritična meta za kibernetičke napade, dok je analiza pravnog okvira i regulacija ukazala na izazove u osiguravanju odgovarajuće zaštite korisnika na globalnoj razini.

Ključnu ulogu u otkrivanju i prevenciji ovih prijetnji igra umjetna inteligencija (AI), koja kroz tehnike poput strojnog učenja i analize velikih podataka omogućava učinkovitije otkrivanje napada, prepoznavanje obrazaca zlonamjernog ponašanja i bržu reakciju na prijetnje. AI je također pokazao velik potencijal u upravljanju ranjivostima, automatizaciji zaštitnih mjera i unapređenju sigurnosnih alata.

U konačnici, zaštita korisnika društvenih mreža zahtijeva kombinaciju tehničkih alata, regulatornih mjera i obrazovanja korisnika. Samo kroz multidisciplinaran pristup može se odgovoriti na izazove koje donose kibernetičke prijetnje, te omogućiti sigurnije korištenje društvenih mreža u budućnosti.

LITERATURA

[1] Alseadoon, I., Chan, T., Foo, E., & Gonzales Nieto, J. (2012): "Who is more susceptible to *phishing* emails? A Pakistani perspective. In Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS)" [25.08.2024.]

[2] Jakoby, A., & Pfleeger, S. L. (2003): „Security Usability and Metrics. In Security Metrics Symposium" [25.08.2024.]

[3] Kumar, S., & Shah, N. (2018): „False information on web and social media: A survey. In Social Network Analysis and Mining" [25.08.2024.]

[4] Sood, A. K., & Enbody, R. J. (2013): „Crimeware-as-a-service: A survey of commoditized crimeware in the underground market. In International Journal of Critical Infrastructure Protection" [25.08.2024.]

[5] Pew Research Center, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information" [25.08.2024.]

[6] Norton Cyber Security Insights Report, "Internet Security Threats: Cyber Security Insights Report". [25.08.2024.]

[7] EU Kids Online, "EU Kids Online: Final Report". [25.08.2024.]

[8] Alkhalil, Z., Hewage C., Nawaf L., Khan I. (2021.): „*Phishing* Attacks: A Recent Comprehensive Study and a New Anatomy" [2.9.2024.]

[9] APWG: „*Phishing* activity trends report – 4th Quarter 2023" [2.9.2024.]

[10] Bureau of Justice Statistics – „Stalking Victimization statistics" [2.9.2024.]

[11] Pew Research Center – „Online Harassment" [2.9.2024.]

[12] Pew Research Center – „Social Media Use and Cyber Harassment" [2.9.2024.]

[13] Bureau of Justice Statistics – „Reporting to Police" [2.9.2024.]

[14] Arrate, A., Gonzalez-Cabanas J., Cuevas A., Cuevas R. (2020.): „*Malvertising* in Facebook: Analysis, Quantification and Solution" [2.9.2024.]

[15] Krombholz K., Hobel H., Huber M., Weippl E. (2015.): „*Malvertising* in Facebook: Analysis, Quantification and Solution" [2.9.2024.]

[16] Shehzad Qaiser, R. (2022.): „INFLUENCE OF CYBER THREATS ON SOCIAL DEVELOPMENT" [5.9.2024.]

[17] McAfee (Malekos Smith Z., Lewis A.) – „The Hidden Costs of Cybercrime" [5.9.2024.]

[18] A. Syrowatka, M. Kuznetsova, A. Alsubai, A. L. Beckman, P. A. Bain, K. J. T. Craig, J. Hu, G. P. Jackson, K. Rhee, D. W. Bates, “Leveraging artificial intelligence for pandemic preparedness and response: a scoping review to identify keyuse cases,” [10.9.2024.]

[19] M. Ebrahimi, J. F. Nunamaker, and H. Chen, “Semi-Supervised Cyber Threat Identification in Dark Net Markets: ATransductive and Deep Learning Approach” [10.9.2024.]

[20] Forrester Research - "AI-Driven Vulnerability Management: Automating Prioritization and Remediation" [10.9.2024.]

[21] SecurityWeek - "Proactive Vulnerability Management with AI and Machine Learning" [10.9.2024.]

[22] S. Zhou, C. Liu, D. Ye, T. Zhu, W. Zhou, and P. S. Yu, “Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity” [10.9.2024.]

[23] Voigt, P., Bussche. A (2017): „The EU General Dana Protection Regulation“ [14.9.2024.]

[24] Wilman, F. (2022.): „The Digital Services Act (DSA) – An Overview“ [14.9.2024.]

[25] Directorate-General for Communications Networks, Content and Technology (2023.): „The Digital Services Act explained“ [14.9.2024.]

[26] Europska komisija – „Akt o digitalnim tržištima: za pravedna i otvorena digitalna tržišta“ [14.9.2024.]

[27] Ehrlich, P. (2001): „Communications Decency Act“ [14.9.2024.]

[28] A. Posner, R. (1969): „The Federal Trade Commission“ [14.9.2024.]

[29] Papadamou, Papasavva, Zannettou, Blackburn, Kourtellis, Leontiadis, Stringhini, Strivianos (2019): „Disturbed YouTube for Kids: Characterizing and detecting Disturbing Content on YouTube“ [14.9.2024.]

SAŽETAK

Naslov: Kibernetičke prijetnje u društvenim mrežama

Završni rad podijeljen je u šest cjelina. U prvoj cjelini obrađene su najčešće vrste kibernetičkih prijetnji. Druga cjelina govori o posljedicama kibernetičkih prijetnji i njihovim utjecajima na korisnika i kompanije. Treća cjelina sadrži strategije za zaštitu od kibernetičkih prijetnji. U četvrtoj cjelini analizirani su stvari primjeri kibernetičkih napada. Peta cjelina se bavi detekcijom prijetnji, upravljanjem ranjivostima te izazovima i ograničenjima umjetne inteligencije u kontekstu kibernetičke sigurnosti. U šestoj cjelini obrađeni su zakoni i regulative koji se bave kibernetičkom sigurnosti u Europi i svijetu.

Ključne riječi: Društvene mreže, Kibernetička sigurnost, Kibernetički napad, Kibernetičke prijetnje, Umjetna inteligencija

ABSTRACT

Title: Cybersecurity threats in social networks

The bachelor thesis is divided into six parts. The first part deals with the most common types of cyber threats. The second part talks about the consequences of cyber threats and their impact on users and companies. The third unit contains strategies for protection against cyber threats. In the fourth unit, examples of cyber attacks are analyzed. The fifth unit deals with threat detection, vulnerability management, and challenges and limitations of artificial intelligence in the context of cyber security. In the sixth unit, the laws and regulations dealing with cyber security in Europe and the world are dealt with.

Key words: Artificial intelligence, Cyber attack, Cyber security, Cyber threats, Social networks