# Prijetnje sigurnosti i privatnosti mladih na internetu

**Biškupec, Stela**




**SVEUČILIŠTE U ZAGREBU**

**UČITELJSKI FAKULTET**

**ODSJEK ZA UČITELJSKE STUDIJE**

**Stela Biškupec**

# PRIJETNJE SIGURNOSTI I PRIVATNOSTI MLADIH NA INTERNETU

Diplomski rad

Zagreb, lipanj 2022.

**SVEUČILIŠTE U ZAGREBU**

**UČITELJSKI FAKULTET**

**ODSJEK ZA UČITELJSKE STUDIJE**

**Stela Biškupec**

# PRIJETNJE SIGURNOSTI I PRIVATNOSTI MLADIH NA INTERNETU

Diplomski rad

Mentor rada: Izv. prof. dr. sc. Predrag Oreški

Zagreb, lipanj 2022.

# SADRŽAJ

## Sažetak

Internet je moćan alat suvremenog doba koji služi za učenje i povezivanje. Omogućuje pristup gotovo neograničenom znanju i povezuje različite ljude diljem svijeta. Međutim, na internetu postoje brojni rizici, kojima su posebno izložena djeca i adolescenti. Postoje opasnosti u koje djeca i adolescenti mogu biti uključeni, među kojima je gubitak kontrole nad vlastitom privatnošću, prekomjerno korištenje ekrana i ono najopasnije različite vrste nasilja na internetu. Iako prijetnje sigurnosti interneta mogu utjecati na svakog korisnika interneta bez razlike, najugroženija skupina su definitivno djeca i mladi. Danas postoje mnogobrojne zaštite na internetu, a Zakon o zaštiti osobnih podataka ima veliku ulogu u sigurnosti mladih na internetu. U digitalnom dobu zaštita privatnosti mladih jedna je od tema koja zahtijeva posebnu pozornost. Prekomjerna izloženost osobnim podacima mladih na internetu i društvenim mrežama upozorava na niz rizika za njihovu privatnost, integritet, sliku o sebi i razvoj osobnosti. Iz ove perspektive, ovaj rad opisuje važnost zaštite osobnih podataka za mlade. Zaštitu osobnih podataka jedno je od onih prava koja u informacijskom društvu, među ostalim, predstavljaju jamstvo privatnosti, povjerljivosti i digitalne sigurnosti i koja štite njihove osobne podatke u sferi osobe.

**Ključne riječi:** internet, mladi, opasnosti, prijetnje, sigurnost,

## Summary

The Internet is a powerful tool of the modern age that serves to learn and connect. It provides access to almost unlimited knowledge and connects different people around the world. However, there are a number of risks on the Internet, to which children and adolescents are particularly exposed. There are dangers that children and adolescents may be involved in, including loss of control over their own privacy, excessive screen use, and the most dangerous types of online violence. Although Internet security threats can affect every Internet user without distinction, the most vulnerable groups are definitely children and young people. Today, there are many protections on the Internet, and the Personal Data Protection Act plays a major role in the safety of young people on the Internet. In the digital age, protecting the privacy of young people is one of the topics that requires special attention. Excessive exposure to personal data of young people on the Internet and social networks warns of a number of risks to their privacy, integrity, self-image and personality development. From this perspective, this paper describes the importance of personal data protection for young people. The protection of personal data is one of those rights which in the information society, inter alia, guarantee privacy, confidentiality and digital security and which protect their personal data in the sphere of the person.

**Key words:** internet, youth, dangers, threats, security

# 1. UVOD

Internet je danas svakodnevica, kako za odrasle ljude, tako i za djecu. Puno je radnji koje su danas potrebne, a da se trebaju izvršiti na internetu. Za mlade ljude danas je odlazak na internet radi povezivanja i interakcije s drugima prirodan i sastavni dio svakodnevnog života. Dok se prijavljuju na e-poštu, blog, chat ili sudjeluju na mrežnim društvenim mrežama, mladi ljudi više ne vide internet samo kao alat, već kao produžetak svog društvenog života i javnog identiteta. Iako je većina internet iskustva za mlade iznimno pozitivna, pa čak i korisna, mnogi mladi ljudi idu na idu izvan granica sigurnosti kada su na mreži, ne razmišljajući dvaput o objavljivanju intimnih detalja o sebi na raznim web stranicama. Nažalost, to je rezultiralo zloporabama i neočekivanim posljedicama u rasponu od internet maltretiranja, krađe identiteta i uhođenja, do isključenja iz škole i budućih izgleda za posao koji su uništeni indiskrecijama objavljenim na internetu. Sigurnost mladih na internetu je danas veoma aktualna tema o kojoj se sve više može pročitati. Iako su mnogi mladi ljudi svjesni mogućnosti prijetnji koje proizlaze iz internetskih aktivnosti, poput onih koje predstavljaju internet grabežljivci, malo njih u potpunosti razumije raspon dodatnih rizika povezanih s objavljivanjem previše osobnih podataka na internetu. Većina nije svjesna da informacije mogu ostati na internetu gotovo bez vremenskog trajanja, te da ih milijuni ljudi mogu pregledavati, kopirati ili preuzimati. Kao rezultat toga, osobni podaci koje danas dijele mogu se kasnije iskoristiti da ih posrame, povrijede ili stigmatiziraju. Njihove aktivnosti koje obavljaju preko interneta mogu se tajno koristiti u marketinške ili komercijalne svrhe. Cilj diplomskog rada je prikazati potencijalne prijetnje i opasnosti s kojima se mladi susreću na internetu, te prikazati eventualna rješenja za smanjenje prijetnji na internetu.

## 2. CYBER KULTURA

Puno tehnologija u ljudskoj povijesti se brzo razvijalo, međutim jako je malo onih koje se mogu uspoređivati s brzinom širenja interneta, te po brzini usvajanja od strane cijele ljudske populacije. Utjecaj interneta generira niz reakcija različitih ljudi, u rasponu od idealizma do cinizma, ali kako god ga primili, ne može se poreći da je doveo do dramatičnih pomaka u područjima kao što su međuljudska interakcija, radna kultura, odnos prema vremenu, očekivanja od brzina i praktičnost, umrežavanje između pojedinaca i grupa, pa čak i korištenje jezika.

Cyberkultura predstavlja novu kulturu informacijskog društva koja prevladava u modernom društvu (Kuleš, 2015, str. 7).

Sam pojam "Cyberkultura" se koristi i tumači na mnoge načine, često se odnosi na određene kulturne proizvode i prakse nastale iz računalnih i internetskih tehnologija, ali i na specifične subkulture koje se zalažu za računalne hobije, umjetnost i jezik.

U svijetu je poznat pojam virtualne stvarnosti, a kao najbolji promjer toga se može spomenuti internetski marketing (Kuleš, 2015, str. 7) koji je postao nezaobilazan u prodaji roba i usluga, te predstavlja jedno od najvažnijih promocija.

Cyberkultura ima značajan izražaj, ali ne ograničava se na globalno dijeljenje, distribuirano stvaranje, društveno umrežavanje, streaming, masovnu suradnju, suradničku procjenu ili društveno označavanje (Gómez, 2012). Ove rutine potiču predanost, sudjelovanje i empatiju, čineći ljude nepovratno uključene i odgovorne jedne za druge u cyber prostoru, to utječu na cijelu ljudsku populaciju mijenjajući način na koji ljudi razmišljaju, oblik zajednica i samog identiteta čovjeka.

## *2.1. Utjecaj internetskih mreža na način života*

Internet uvelike utječe na svakodnevnicu ljudi mijenjajući njihov način života. Gotovo sve što ljudi rade uključuje korištenje interneta, a život bez njega je postao gotovo nezamisliv. Naručiti hranu, kupiti televizor, kupiti robu ili hranu, ili podijeliti trenutak s prijateljem, poslati sliku ili podijeliti neki važan životni događaj – uključuje Internet. Prije postojanja interneta, ako je čovjek htio vidjeti novosti ili pročitati zanimljivosti, trebao je prvo kupiti novine. Samim razvojem interneta, ubrzalo se i širenje informacija (Gómez, 2012).

Sam internet je transformiran. U svojim ranim danima - koji su iz povijesne perspektive još uvijek relativno novi - bila je to statična mreža dizajnirana za prijenos male količine bajtova ili kratke poruke između dva terminala, bio je to spremište informacija u kojem su sadržaj objavljivali i održavali samo stručni koderi. Danas se, međutim, goleme količine informacija učitavaju i preuzimaju preko elektroničkog levijatana, a sadržaj je uvelike od svakog korisnika pojedinačno, za sada su svi komentatori, izdavači i kreatori.

Danas se pojedinci sve teže mogu zaštititi od ljudi koji pregledavaju tuđe podatke jer je sve javno dostupno i anonimnost je spala na najniži nivo. Ipak, nova komunikacijska okolina je omogućila korisnicima mnoštvo informacija koje su potrebne te samim time olakšala studiranje, pronalazak posla, kupnju određenih proizvoda, promociju i sl (Gómez, 2012). Iz svega navedenog daje se zaključiti da internet, odnosno cyber-okolina i internetske forme oglašavanja imaju svoje dobre i loše strane, a korisnici bi ih trebali iskoristiti na za njih najbolji način. Sve je dostupno u svega nekoliko klikova te je time omogućeno puno lakše i brže dobivanje informacija o stanjima na cestama, vremenskoj prognozi i brojne druge stvari bitne za funkcioniranje u svakodnevnom životu. Neki predviđaju da se u budućnosti niti neće moći zamisliti svakodnevno funkcioniranje bez internetskih mreža jer će se sve prebaciti na računala čime se smanjuje potreba za radnom snagom. Ipak, nedostatak svega toga je što autor informacija na internetu može biti bilo tko, odnosno ne možemo sa sigurnošću tvrditi da su informacije pouzdane i istinite. Velik broj informacija su upravo lažne te je to jedan od glavnih problema cyber društva. Kada je riječ o marketingu, internet može uvelike pomoći u marketinškim trikovima prilikom prodaje proizvoda (Gómez, 2012). Korisnici naručuju proizvode na osnovu slika i dostupnog

opisa te eventualnih komentara o proizvodu, a kada im proizvod dođe na kućnu adresu dobiju sasvim nešto drugo.

### *2.1.1. Pregled razvijenosti društvenih mreža*

Od svog osnutka 1996. godine, društveni mediji uspjeli su se infiltrirati u polovicu od 7,7 milijardi ljudi u svijetu. Platforme društvenih mreža gotovo su utrostručile svoju ukupnu bazu korisnika u posljednjem desetljeću, s 970 milijuna u 2010. na broj koji je premašio 4,48 milijardi korisnika u srpnju 2021. Međutim, spektakularno usvajanje novih korisnika na platformama iz godine u godinu usporava. Sada se oslanja na kontinuirani rast broja ljudi s pristupom internetu i pametnim telefonima, osobito u regijama u razvoju (https://backlinko.com/social-media-users).

U 2021. godini u svijetu ima 4,48 milijardi ljudi koji aktivno koriste društvene mreže, a to je povećanje od 13,13% u odnosu na prethodnu godinu u odnosu na 3,69 milijardi u 2020. godini. U 2015. bilo je samo 2,07 milijardi korisnika – to je sveukupni porast u korisnika od 115,59% u samo šest godina (https://backlinko.com/social-media-users).

Prikaz rasta društvenih mreža je prikazan Tablicom 1.

**Tablica 1.**

*Prikaz rasta društvenih mreža*

| Godina | Aktivni korisnici (milijardi) | % rasta broja korisnika |
|---|---|---|
| 2015. | 2.078 | - |
| 2016. | 2.307 | +11% |
| 2017. | 2.796 | +21% |
| 2018. | 3.196 | +9.0% |
| 2019. | 3.484 | +9.2% |
| 2020. | 3.960 | +13.7% |
| 2021. | 4.480 | +13.13% |

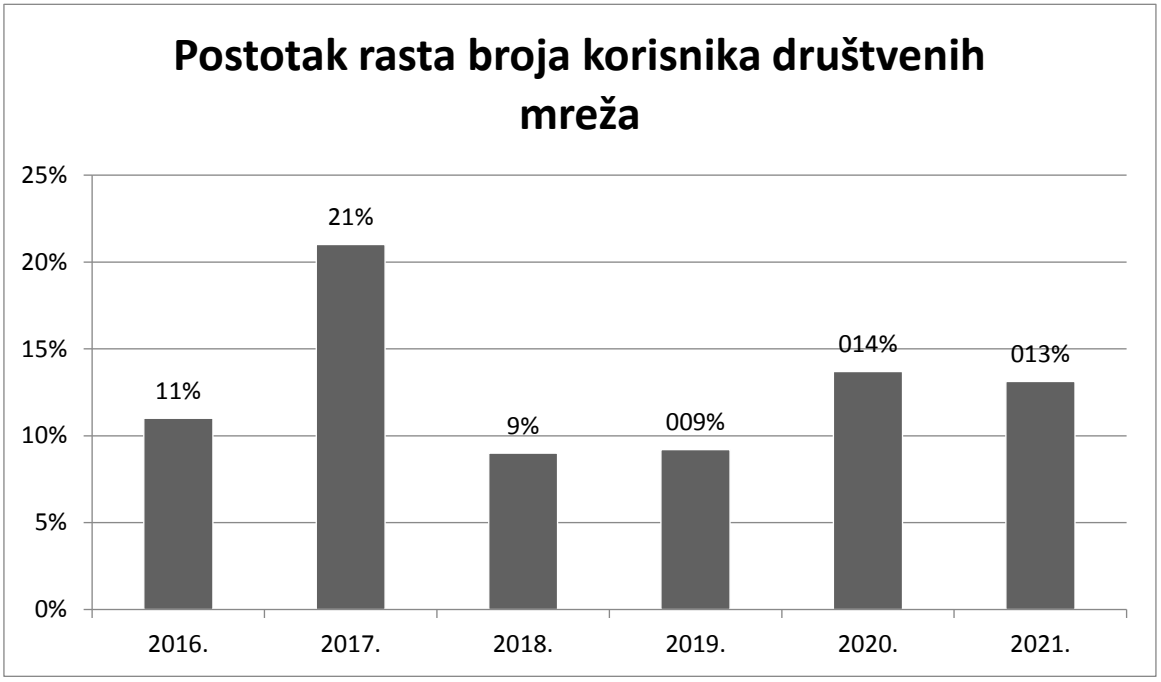
Izvor: Obrada autorice prema Social Media & User-Generated Content, 28. Travnja 2022.

U Tablici 1. vidi se da je broj aktivnih korisnika društvenih mreža se udvostručio od promatrane 2015. godine do 2021. godine.

U nastavku rada, grafički je prikazan postotak rasta broja korisnika društvenih mreža na Grafikonu 1.

**Grafikon 1.**

*Postotak rasta broja korisnika društvenih mreža*




Izvor: Obrada autorice prema Social Media & User-Generated Content, 28. Travnja 2022.

Na Grafikonu 1. vidi se da je najveći rast na društvenim mrežama zabilježen 2017. Godine.

### *2.1.2. Prijetnje društvenih mreža*

Metode koje koristi napadač ovise o ciljanoj platformi društvenih medija. Facebook omogućuje korisnicima da svoje slike i komentare zadrže privatnima, pa će napadač često biti prijatelj s prijateljima ciljanog korisnika ili izravno poslati zahtjev za prijateljstvo ciljanom korisniku kako bi pristupio njihovim objavama. Ako se napadač može povezati s nekoliko prijatelja ciljanog korisnika, vjerojatnije je da će ciljani korisnik prihvatiti zahtjev za prijateljstvo na temelju broja povezanih prijatelja (https://blog.microfocus.com/social-media-in-the-workplace-the-risks/).

LinkedIn je još jedna uobičajena meta društvenih medija. LinkedIn je poznat po poslovnom umrežavanju, a mreže korisnika obično su ispunjene kolegama i drugim zaposlenicima unutar iste organizacije. Ako napadač cilja na tvrtku, LinkedIn je izvrsna stranica društvenih medija za prikupljanje poslovnih e-poruka za phishing napad. Veliko poduzeće moglo bi imati nekoliko umreženih zaposlenika koji navode svog poslodavca i svoja zvanja. Napadač može upotrijebiti ove javne informacije da pronađe nekoliko zaposlenika koji imaju pristup financijskim informacijama, privatnim podacima o klijentima ili pristup mreži s visokim privilegijama (https://blog.microfocus.com/social-media-in-the-workplace-the-risks/).

Prikupljanje informacija za krađu podataka nije jedini razlog za korištenje društvenih mreža za izviđanje. Informacije objavljene na društvenim mrežama mogu se koristiti za dobivanje lozinki ili lažno predstavljanje poslovnih korisnika.

Mnogi mrežni računi omogućuju korisnicima poništavanje lozinki ako unesu sigurnosno pitanje. Uz dovoljno informacija iz objava na društvenim mrežama, napadač bi mogao pogoditi odgovor na ova sigurnosna pitanja na temelju privatnih podataka koje je objavio ciljani korisnik (https://www.shrm.org/resourcesandtools/tools-and-samples/hr-qa/pages/socialnetworkingsitespolicy.aspx).

Lažno predstavljanje robne marke još je jedna prijetnja društvenih medija. Uz dovoljno prikupljenih informacija, napadač može imitirati poslovnu marku kako bi prevario korisnike da pošalju novac, otkriju privatne podatke ili daju napadaču vjerodajnice računa. Napadači također koriste ovu prijetnju za izvođenje napada skriptiranja na više mjesta ili krivotvorenja zahtjeva na više mjesta. Ovi napadi mogu dovesti do masovnijih povreda podataka i ugrožavanja poslovne infrastrukture (https://www.shrm.org/resourcesandtools/tools-and-samples/hr-qa/pages/socialnetworkingsitespolicy.aspx).

Budući da mnoge platforme društvenih medija javno prikazuju objave korisnika, napadači mogu u tišini prikupljati podatke bez znanja korisnika. Neki će napadači poduzeti daljnje korake u dobivanju pristupa korisničkim podacima kontaktirajući ciljane korisnike ili njihove prijatelje (https://www.oxbridgeacademy.edu.za/blog/happens-underestimate-dangers-social-media-workplace/)

Način na koji napadač provodi prijetnju društvenih medija ovisi o njihovim ciljevima.

Ako napadač traži nagradu s visokim ulozima, najbolji način da brzo zaradite novčanu nagradu za svoje napore je ciljanje na tvrtke. Napadač bi mogao prvo pregledati LinkedIn za popis mogućih meta. Ciljevi mogu biti mješavina korporativnih zaposlenika na visokoj razini i korisnika s niskim privilegijama koji bi mogli biti prevareni da pošalju dodatne korporativne podatke ili nasjedati na phishing napad koji napadaču daje pristup vjerodajnicama računa. Uz popis meta, napadač bi tada mogao pregledati račune društvenih medija u potrazi za osobnim podacima. Osobni podaci mogu pomoći napadaču da stekne povjerenje mete u napadu društvenog inženjeringa. Također se može koristiti za pogađanje odgovora na sigurnosna pitanja za preuzimanje računa ili za približavanje korisniku s višim privilegijama. Imena kućnih ljubimaca, omiljeni sportski timovi i povijest obrazovanja potencijalni su tragovi lozinke ili odgovori na pitanja koja se koriste za provjeru identiteta korisnika za poništavanje lozinke.

## *2.2. Budućnost cyber-društva*

Vrlo teško je predvidjeti budućnost, no kada je u pitanju budućnost cyber-društva tu možemo govoriti o munjevitim promjenama na dnevnoj razini. Svakim danom sve je veći broj ponuda što na internetu, odnosno sve veći broj internetskih stranica i društvenih mreža, ali isto tako i sve je veći broj medijskih uređaja koji su svakim danom sve napredniji. Ako se vratimo unazad samo nekoliko godina mobiteli su jedva imali kamere u boji, a danas omogućuju gledanja na kilometarskim udaljenostima preko prednjih kamera. To je samo jedna od brojnim mogućnosti koje nude današnji pametni uređaji. Promjene se događaju na dnevnoj razini u znanstvenim i programerskim kućama koji svakim danom pokušavaju nešto novo i bolje nametnuti na tržište (Hajdarović, 2005, str. 72.). U tijeku je nastojanje da se poveća brzina širenja informacija, odnosno brzina pristupa informacijama putem internetskih mreža. Veliki je broj telefonskih operatera koji svakodnevno povećavaju svoj signal i brzinu mreže, pa je danas u upotrebi 5G mreža kojom se munjevitom brzinom može doći do željenih informacija i internetskih stranica. To je danas mladim ljudima vrlo važno jer vrijedi izreka "vrijeme je novac", odnosno omogućeno je da vrlo brzo dođu do željenih informacija, preuzmu ih i koriste u daljnjim preradama istih. U tijeku je također i pad cijena informatičke tehnologije i informatičkih usluga jer je sve brži njegov

razvoj pa se mnogi proizvodi ni ne uspiju plasirati na tržište. Određeni proizvodi, odnosno informacije u cyber-okruženju na internetskim stranicama su dostupni, no veliki broj informacija se također naplaćuje. Nastoji se trgovati kako proizvodima tako i informacijama u virtualnom svijetu koristeći računala, a bez neposrednog kontakta sa samim klijentima odnosno kupcima. U domenu internetskih tehnologija sve više ulazi i telefonija te multimedijski sadržaji poput glazbe i filmova, dok edukativni sadržaji još uvelike kaskaju i zaostaju zbog nedostatka sredstava. Jasno je da ono što nosi profit ima i prednost.

# 3. SIGURNOST NA INTERNETU

Internetska sigurnost je specifičan aspekt širih koncepata kao što su kibernetička sigurnost i računalna sigurnost, usredotočujući se na specifične prijetnje i ranjivosti internetskog pristupa i korištenja interneta.

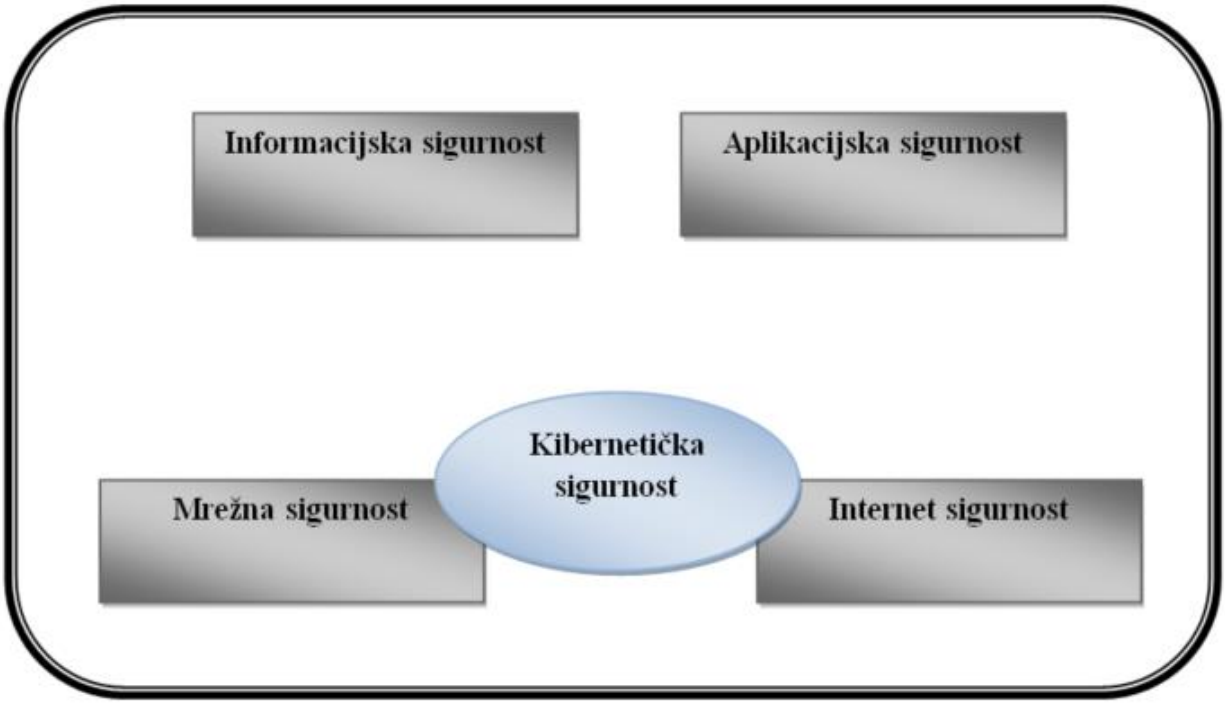
Internetska sigurnost sastoji se od niza sigurnosnih taktika za zaštitu aktivnosti i transakcija koje se provode online putem interneta (Vuković, 2012). Ove taktike namijenjene su zaštiti korisnika od prijetnji kao što su hakiranje računalnih sustava, adresa e-pošte ili web-mjesta; zlonamjerni softver koji može zaraziti i inherentno oštetiti sustave; i krađu identiteta od strane hakera koji kradu osobne podatke kao što su podaci o bankovnom računu i brojevi kreditnih kartica (Vuković, 2012). Internetska sigurnost je specifičan aspekt širih koncepata kao što su kibernetička sigurnost i računalna sigurnost, usredotočujući se na specifične prijetnje i ranjivosti internetskog pristupa i korištenja interneta.

Kibernetika je definirana kao skup znanstvenih disciplina i postupaka koji se implementiraju pri upravljanju i vođenju složenih sustav (https://enciklopedija.hr/natuknica.aspx?id=31381).

Odnos kibernetičke sigurnosti i ostalih vrsta sigurnosti je prikazana na Slici 1.

**Slika 1.**

*Odnos kibernetičke sigurnosti i ostalih vrsta sigurnosti*




Izvor: Izrada autorice prema Hamidović, H., 2015.

Informacijska sigurnost ima za cilj zaštititi privatnost korisnika te osigurati trajnost i dostupnost informacija. Iako se danas često vode kao sinonimi, informacijsku sigurnost treba razlikovati od kibernetičke po tome što je kibernetička sigurnost skup praksi koje se koriste za pružanje sigurnosti od internetskih napada, dok je informacijska sigurnost samo poddisciplina kibernetičke sigurnosti (Vuković, 2012).

S druge strane, aplikacijska sigurnost predstavlja proces koji se obavlja kako bi se primijenile odgovarajuće kontrole i mjerenja na organizacijske aplikacije.

Zadaća mrežne sigurnosti je da dizajnira, implementira i radi na mrežama, a internetske sigurnosti da zaštiti internetski povezane usluge (Vuković, 2012). Ona se sastoji od niza

sigurnosnih taktika za zaštitu aktivnosti i transakcija koje se vrše putem interneta te su namijenjene zaštiti korisnika od prijetnji, poput provala u računalne sustave, adrese e-pošte ili mrežne stranice.

Budući da ljudi društvene mreže smatraju osobnim komunikacijskim alatom, važnost zaštite svojih informacija pohranjenih na tim društvenim mrežama često se uzima zdravo za gotovo. S vremenom ljudi stavljaju sve više informacija u različite oblike na društvene mreže što može dovesti do neviđenog pristupa informacijama o ljudima i poslovnim subjektima. Količina informacija pohranjenih na društvenim mrežama vrlo je primamljiva za protivnike čiji je cilj nekome naštetiti.

## *3.1. Opasnosti interneta*

Opasnost interneta je velika, od kibernetičkog kriminala do objava na društvenim mrežama koje se mogu vratiti i imati posljedice u životu. Opasnosti interneta mogu imati ozbiljne, skupe, čak i tragične posljedice.

Jedna od prevladavajućih opasnosti interneta su kibernetički kriminalci i kibernetički zločini koji se neprestano razvijaju. Budući da je toliko kibernetičkih zločina pokrenuto s ciljem napada na bilo kojeg korisnika interneta, vjerojatno niti jedan član obitelji nije izuzet od takvih napada (Spitzer, 2018, 14). Postoje mnoge prijetnje s kojima se djeca susreću na internetu, kao i odrasli i tinejdžeri.

Prijetnje na internetu se stalno razvijaju, a najčešće prijetnje uključuju:

- krađa identiteta,
- Cyberbullying,
- prijetnja za privatnost,
- zlonamjerni softveri,
- neprikladni sadržaji,
- online prijevare,
- napadi na korisnike.

Krađa identiteta je krađa osobnih podataka u svrhu prijevare. To se može dogoditi putem računa e-pošte, ali također može biti rezultat kupnje preko interneta ili drugih situacija u kojima se daju osjetljivi podaci kao što su podaci o kreditnoj kartici (Težak, 2010.). Krađa identiteta događa se kada netko koristi osobne identifikacijske podatke neke osobe i pretvara se da je ta osoba kako bi počinio prijevaru ili stekao drugu financijsku korist.

Krađa identiteta je direktna prijetnja za privatnost.

Zlonamjerni softver je nametljiv softver koji je dizajniran da ošteti i uništi računala i računalne sustave. Primjeri uobičajenog zlonamjernog softvera uključuju viruse, crve, trojanske viruse, špijunski softver, adware i ransomware. Zlonamjerni softver see odnosi na svaki nametljivi softver koji su razvili kibernetički kriminalci (često se nazivaju "hakeri") za krađu podataka i oštećenje ili uništavanje računala i računalnih sustava (Težak, 2010.). Primjeri uobičajenog zlonamjernog softvera uključuju viruse, crve, trojanske viruse, špijunski softver, adware i ransomware. Nedavni napadi zlonamjernog softvera infiltrirali su podatke u velikim količinama.

Virusi su podskupina zlonamjernog softvera. Virus je zlonamjerni softver priložen dokumentu ili datoteci koji podržava makronaredbe za izvršavanje njegovog koda i širenje s hosta na host. Nakon preuzimanja, virus će ostati neaktivan dok se datoteka ne otvori i počne koristiti. Virusi su dizajnirani da ometaju rad sustava (Težak, 2010.). Kao rezultat toga, virusi mogu uzrokovati značajne probleme u radu i gubitak podataka.

Crvi su zlonamjerni softver koji se brzo replicira i širi na bilo koji uređaj unutar mreže. Za razliku od virusa, crvi ne trebaju host programe za širenje. Crv inficira uređaj putem preuzete datoteke ili mrežne veze prije nego što se umnoži i rasprši eksponencijalnom brzinom (Težak, 2010.). Poput virusa, crvi mogu ozbiljno poremetiti rad uređaja i uzrokovati gubitak podataka.

Trojanski virusi su prikriveni kao korisni program. No, nakon što ga korisnik preuzme, trojanski virus može dobiti pristup osjetljivim podacima, a zatim ih izmijeniti, blokirati ili izbrisati (Težak, 2010.). To može biti izuzetno štetno za performanse uređaja. Za razliku od normalnih virusa i crva, trojanski virusi nisu dizajnirani da se samorepliciraju.

Špijunski softver je zlonamjerni softver koji se potajno izvodi na računalu i javlja udaljenom korisniku. Umjesto da jednostavno ometa rad uređaja, špijunski softver cilja osjetljive informacije i može dati daljinski pristup grabežljivcima. Špijunski softver se često koristi za krađu financijskih ili osobnih podataka (Težak, 2010.). Specifična vrsta špijunskog softvera je keylogger, koji bilježi vaše pritiske tipki kako bi otkrio lozinke i osobne podatke.

Adware je zlonamjerni softver koji se koristi za prikupljanje podataka o korištenju vašeg računala i pružanje odgovarajućih reklama za korisnike. Iako adware nije uvijek opasan, u nekim slučajevima adware može uzrokovati probleme sustavu. Adware može preusmjeriti preglednik korisnika na nesigurne stranice, a može čak sadržavati trojanske konje i špijunski softver (Težak, 2010.). Osim toga, značajne razine adwarea mogu značajno usporiti sustav. Budući da nije svaki adware zlonamjeran, važno je imati zaštitu koja neprestano i inteligentno skenira te programe.

Ransomware je zlonamjerni softver koji dobiva pristup osjetljivim informacijama unutar sustava, šifrira te informacije tako da im korisnik ne može pristupiti, a zatim zahtijeva financijsku isplatu za objavljivanje podataka. Ransomware je obično dio phishing prijevare. Klikom na prikrivenu vezu korisnik preuzima ransomware. Napadač nastavlja s šifriranjem određenih informacija koje se mogu otvoriti samo pomoću matematičkog ključa koji im je poznat (Težak, 2010.).

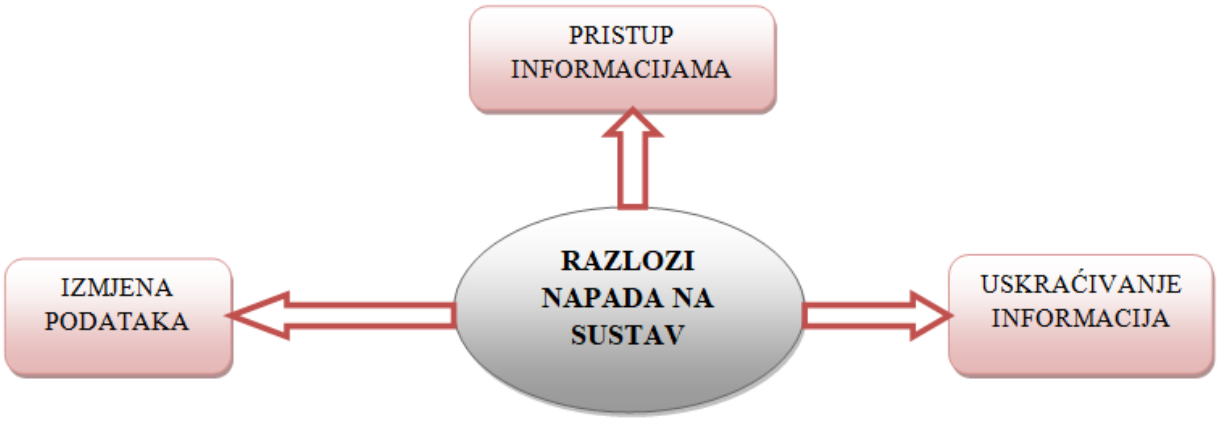
Zlonamjerni softver bez datoteka je vrsta zlonamjernog softvera rezidentnog u memoriji. Kao što izraz sugerira, zlonamjerni softver radi iz memorije računala žrtve, a ne iz datoteka na tvrdom disku. Budući da nema datoteka za skeniranje, teže ga je otkriti nego tradicionalni zlonamjerni softver (Težak, 2010.). Također otežava forenziku jer zlonamjerni softver nestaje kada se računalo žrtve ponovno pokrene.

Sigurnosti informacijskih sustava prijete svakodnevni napadi različitih hakera koji žele ugroziti podatke i sustav sigurnosti podataka. Napadi su djela ili postupci koji pokušavaju iskoristiti ranjivost informacijskih sustava kako bi u isti ušli te ukrali ili saznali podatke za koje nemaju ovlašteni pristup (Težak, 2010.). Napadi na informacijske sustave mogu biti različiti, ovisno o tome što napadač ili haker točno želi napraviti s informacijama do kojih dođe te koji su mu ciljevi zbog kojih napada informacijski sustav.

Slika 2. prikazuje najčešće razloge napada na sustave informacija zbog kojih napadači provaljuju u iste te žele izvršiti nezakonite radnje na štetu sigurnosti određenih podataka.

**Slika 2.**

*Razlozi napada na sustav informacija*




Izvor: Izrada autorice prema Revizijska izvješća, 2021.

Tako napadači mogu napadati sustave sigurnosti informacija kako bi došli do informacija do kojih normalnim, zakonitim putem ne mogu doći te kako bi saznali neke povjerljive ili tajne podatke koji ih zanimaju bez da bilo što rade s njima, već da ih saznaju.

Napadači kao cilj svog ulaska u informacijski sustav mogu imati mijenjanje podataka, pa oni u sustav sigurnosti provaljuju kako bi na silu izmijenili neke podatke što im inače nije dozvoljeno ili za to nisu ovlašteni.

Kao treći razlog napada na informacijski sustav postavlja se problem kada napadači ulaskom u informacijski sustav žele uskratiti uslugu ili informacije onima koji imaju pristup njima ili žele poremetiti rad cijelog sustava informacija ili mreže podataka te tako naštetiti sigurnosti samih podataka.

S obzirom na navedene ciljeve napadača pri napadu na podatke, ti napadi se mogu podijeliti i na one napade prilikom kojih informacije ostaju nepromijenjene, a napadač ih čita i saznaje ali ne mijenja. Takvi napadi su pasivni napadi. Za razliku od njih, aktivni napadi na podatke rezultiraju promjenom postojećih podataka.

Naravno, napadi na podatke ne moraju uvijek biti od strane onih koji za pristup podatcima nisu ovlašteni. Napadi se mogu dogoditi i od strane zaposlenika neke tvrtke ili onih koji su ovlašteni za pristup podatcima, ali svejedno žele namjerno i bez valjanog zakonitog razloga promijeniti podatke iako ne bi smjeli.

Napadi na sigurnost informacijskih sustava uvelike ovise o učinkovitosti sustava zaštite podataka. Ovisno o tome je li sustav uspio obraniti podatke ili je u sustav provaljeno te je došlo do krađe podataka ili njihove izmjene, napade se može podijeliti na uspješne i neuspješne.

Uspješni napadi rezultiraju negativnim posljedicama po vlasnike tih podataka te dolazi do neovlaštenog pristupa istima, krađe ili izmjene podataka koji su bili cilj napadača. Za razliku od njih, neuspješni napadi označavaju one pri kojima je informacijski sustav uspio podatke očuvati sigurnima te je onemogućen pristup napadačima na podatke koji su ostali sigurni.

## *3.2. Cyberbullying*

Nasilje na internetu (elektroničko nasilje, cyberbullying, online nasilje, digitalno nasilje) podrazumijeva svaku komunikacijsku aktivnost cyber-tehnologijom koja se može smatrati štetnom za pojedinca, ali i za opće dobro (Bedić, Filipović, 2014, 24).

Cyberbullying je nasilje koje se događa preko digitalnih uređaja poput mobitela, računala i tableta. Cyberbullying se može dogoditi putem SMS-a, MMS-a, aplikacija ili na društvenim medijima, forumima ili igrama gdje ljudi mogu gledati, sudjelovati ili dijeliti sadržaj. Cyberbullying uključuje slanje, objavljivanje ili dijeljenje negativnog, štetnog, lažnog ili nasilnog sadržaja o nekom drugom. To može uključivati dijeljenje osobnih ili privatnih podataka o nekom

drugom izazivajući neugodu ili poniženje. Neki cyberbullying prelazi granicu u protuzakonito ili kriminalno ponašanje.

Istraživanje Pew Researcha iz 2018. pokazalo je da je većina tinejdžera (59%) doživjela neki oblik cyberbullyinga. Opsežnija studija iz 2021. pokazuje da to nije jedinstveno samo za tinejdžere, jer je oko 40 posto Amerikanaca mlađih od 30 godina iskusilo uznemiravanje na internetu. Od njih, 50% je navelo politiku kao razlog incidenta (https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/)

Najčešći specifični tipovi cyberbullyinga uključuju:

- Uvredljivo prozivanje,
- namjerno posramljivanje,
- fizičke prijetnje,
- uhođenje,
- seksualno uznemiravanje,
- trajno uznemiravanje (Bedić, Filipović, 2014).

Nasilje na internetu koje uključuje djecu i mlade, uključujući cyberbullying, može se razlikovati po dva glavna oblika nasilja, iako se oni često preklapaju, a uključuju:

- psihološko nasilje,
- seksualno nasilje, prepoznavanje da seksualno nasilje na internetu ima snažnu psihološku dimenziju i psihološke implikacije (Madigan, Rash i sur., 2017, 329).

Psihološko nasilje između djece na internetu uključuje verbalne agresije i agresije koje se mogu opisati kao društvene ili relacijske. Primjeri verbalne agresije uključuju:

- slanje uvredljivih, uvredljivih ili zlonamjernih poruka drugom djetetu ili skupini djece,
- razmjenjivanje vulgarnog jezika,

- slanje poruka za prijetnju ili zastrašivanje drugog djeteta ili sudjelovanje u drugim aktivnostima na mreži zbog kojih se drugo dijete boji za svoju sigurnost (Madigan, Rash i sur., 2017, 331).

Primjeri društvenih ili relacijskih agresija uključuju:

- namjerno izdvajanje i isključivanje drugog djeteta iz mrežnih grupa kao što su chatovi i web-lokacije,
- slanje ili objavljivanje tračeva ili glasina o osobi kako bi se oštetio ugled ili prijateljstvo,
- dijeljenje osobnih i privatnih podataka, slika ili videozapisa o drugom djetetu javno bez pristanka djeteta (Madigan, Rash i sur., 2017, 331).

Odrasle osobe mogu počiniti iste oblike psihičkog nasilja nad djecom i mladima mlađima od 18 godina kao i gore opisani (Madigan, Rash i sur., 2017, 331). Osim toga, neke odrasle osobe su uključene u elektronički omogućenu trgovinu ljudima. Iako se tradicionalno ne smatra oblikom zlostavljanja na internetu, elektronička trgovina uključuje odrasle koji koriste društvene mreže kako bi dobili kompromitirajuće informacije o mladoj žrtvi (kao što su slike ili video zapisi) kao sredstvo prijevare, prijetnji i obmane kako bi stekli kontrolu.

Na isti način kao i psihološko nasilje na internetu, seksualno nasilje na internetu uključuje agresije koje mogu biti verbalne ili relacijske.

Jedan primjer verbalne agresije je davanje seksualnih komentara o drugom djetetu (npr. šala, pričanje priča ili komentiranje tijela, izgleda ili seksualnih aktivnosti) s ciljem da se dijete/mlada osoba osjeća nepoželjnom.

Sve veći broj djece dijeli seksualne slike sebe na internetu s drugom djecom. Online seksualno nasilje koje se ponavlja često se naziva online seksualno uznemiravanje, umjesto seksualnog cyber maltretiranja (Madigan, Rash i sur., 2017).

### *3.2.1. Vrijeđanje*

Pod vrijeđanjem se obično podrazumijevaju kratkotrajne rasprave između dviju ili više osoba, a koja uključuje nepristojan i vulgaran rječnik, uvrede, a ponekad i prijetnje. Ova vrsta nasilja se može odvijati putem panela za raspravu, chat soba, igrica, pomoću instant poruka ili putem elektroničke pošte. Najčešće se radi o javnom nasilju gdje osobe koje nisu uključene u raspravu mogu vidjeti svađu. Sadržaj koji počinitelj objavljuje uglavnom ima za cilj izazvati određene emocije i odgovore koji uključuju bijes, tugu, poniženje i sl. (Willard, 2007). Za ovaj je oblik nasilja karakteristično to što pojedini napadači traže ljude koji su entuzijastični oko određene teme s namjerom omalovažavanja njihovog izbora i mišljenja u vezi te teme, bez obzira na to što sami zapravo misle o njoj.

### *3.2.2. Uznemiravanje*

Uznemiravanje je pojam koji se odnosi na prijeteće radnje kojima je cilj prisiliti nekoga da bude u ponižavajućoj poziciji ili prisilnoj podređenosti dok počinitelj demonstrira svoju moć i dominaciju. Za uznemiravanje je karakteristično opetovano slanje uvredljivih, provokativnih, neprijateljskih poruka pojedincu ili grupi. Ono što razlikuje uznemiravanje od vrijeđanja jest činjenica da uznemiravanje traje puno duže (Willard, 2007). Osim toga, često se radi o tome da jedna strana napada drugu koja pokušava prekinuti komunikaciju.

Anonimnost koju pružaju društvene mreže je upitno za korisnike društvenih mreža.

Ranije je osoba mogla biti uznemiravana samo uživo, a danas bilo koja anonimna osoba može postati nasilnik i uznemiravati preko interneta.

### *3.2.3. Ogovaranje i klevetanje*

Ogovaranje i klevetanje je kategorija koja se odnosi na objavljivanje lažnih izjava na internetu kao da su točne s ciljem da se diskreditira ili ponizi određena osoba. Dakle, uključuje slanje ili objavljivanje uvredljivih i neistinitih informacija o drugoj osobi s namjerom ugrožavanja njene reputacije ili prijateljstva. Poseban oblik ove kategorije jesu *elektroničke knjige utisaka* čija je svrha ismijati ili poniziti drugu osobu, najčešće vršnjaka. Radi se o internetskim stranicama na kojima se nalaze imena školskih vršnjaka te bilo tko pored imena

može napisati komentar o toj osobi, a najčešće su komentari zlobni i nepristojni. (Zovkić, 2015, 6).

### *3.2.4. Lažno predstavljanje*

Lažno predstavljanje karakterizira kreiranje lažnog profila, hakiranje ili neovlašteno korištenje tuđeg online računa te slanje poruka, slika i drugih sadržaja u ime te osobe koje će izazvati neugodu ili će uništiti njen ugled i prijateljstva. U ekstremnim slučajevima, napadač može koristiti tuđi identitet te postavljati provokativne i uvredljive komentare u okviru tzv. grupne mržnje ili nekih drugih vrsta grupnih foruma, ostavljajući pri tome ime, adresu i broj telefona, kako bi ga osobe koje je navodno napao mogli kasnije pronaći (Zovkić, 2015, 6).

### *3.2.5. Nedozvoljeno priopćavanje*

Nedozvoljeno priopćavanje ili javno razotkrivanje (outing) se odnosi na situacije kada napadač šalje drugima ili javno objavljuje informacije koje mu je žrtva poslala u povjerenju. Može se raditi o razgovorima ili slikama koje žrtva ne želi podijeliti s drugima zbog neugode koju bi tada osjećala (Zovkić, 2015, 6). Ovakvo nasilje se često događa nakon prekida romantičnih ili prijateljskih odnosa (Zovkić, 2015, 6). Jedna strana šalje informacije o drugoj kako bi ju povrijedila, ponizila, osvetila joj se ili prijetila.

### *3.2.6. Obmanjivanje*

Obmanjivanje ima sličnosti sa nedozvoljenim priopćavanjem u smislu da je riječ o javnom objavljivanju privatnih informacija o drugoj osobi. Međutim, ono što razlikuje ove dvije kategorije je svrha i način na koji je osoba došla do tih informacija (Zovkić, 2015, 7). Dok se u prethodnoj kategoriji radi o dijeljenju informacija koje je napadač stekao dok su on i žrtva imali dobar odnos, u obmanjivanju je naglasak na prevarama koje netko koristi kako bi naveo drugu osobu da mu otkrije tajne ili informacije kojih se stidi te potom objavljuje i prosljeđuje te informacije drugim ljudima (Zovkić, 2015, 7).

### *3.2.7. Isključivanje*

Isključivanje je vezano uz označavanje pripadnosti vlastitoj ili vanjskoj grupi, a podrazumijeva namjerno isključivanje osobe iz neke *online* grupe ili zajednice. Ono se na

internetu može pojaviti u online igricama, grupnim blogovima i bilo kojim drugim stranicama koje su zaštićene lozinkom (Zovkić, 2015, 7). Također se može pojaviti i u kontekstu slanja instant poruka kroz naglašeno isključivanje nekoga s liste prijatelja. Za tinejdžere, isključivanje s liste prijatelja predstavlja krajnje odbijanje, a neki autori navode da osobe koje su žrtve online isključivanja pokazuju pad samopoštovanja te da se pridružuju i konformiraju novim, drugačijim grupama od onih kojima su prethodno pripadali (Zovkić, 2015, 7).

### *3.2.8. Uhođenje i proganjanje*

Uhođenje i proganjanje na internetu podrazumijeva tajno ili pak otvoreno, kontinuirano, ali neželjeno praćenje određene osobe, koje se može odnositi i na neprestano pokušavanje uspostavljanja i nastavljanja neželjenog kontakta (Willard, 2007). Za njega je karakteristično opetovano slanje štetnih poruka koje uključuju prijetnje te su zastrašujuće ili pretjerano uvredljive. Nadalje, izravno se proganjanje gotovo uvijek odvija putem privatnih kanala komunikacije. Ponekad će počinitelj koristiti anonimna sredstva za komunikaciju sa svrhom sakrivanja identiteta. Neizravno proganjanje uključuje komunikaciju s drugima s namjerom ocrnjivanja žrtve ili dovođenje žrtve u nesigurnu, opasnu situaciju (Zovkić, 2015, 8). Kraće rečeno ova vrsta uhođenja podrazumijeva lažne objave na web-stranicama, krađu identiteta osobe ili podataka, špijuniranje i praćenje osobnog kompjutora i korištenje interneta (Willard, 2007). Ponekad se prijetnje mogu prenijeti u fizičke prostore. Počinitelji nisu uvijek stranci; često su to bivši ili trenutni partneri ili nekadašnji prijatelji.

### *3.2.9. Veselo šamaranje*

Veselo šamaranje je naziv za fizički napad jedne osobe ili grupe ljudi na drugu osobu, bez nekog povoda, a sve s ciljem snimanja i slanja videa drugima, ili pak postavljanje takvog videa na Internet. Zlostavljači su najčešće tinejdžeri koji se opravdavaju šalom. Ipak, ovakvo nasilje uključuje i teže fizičke ozljede (Popović-Ćitić, 2009). Posljedice imaju karakteristike kaznenog djela.

## *3.3. Sigurnost podataka na društvenim mrežama*

Uz brzo rastuću tehnologiju, online društvene mreže su eksplodirale u popularnosti u posljednjih nekoliko godina. Informacije koje se dijele na društvenim mrežama i medijima šire se

vrlo brzo, gotovo trenutno, što napadačima čini privlačnim za dobivanje informacija. Napadač može zlonamjerno koristiti dijeljene informacije u nelegitimne svrhe. Rizici su još veći ako je ciljana skupina djeca ili mladi.

Budući da ljudi društvene mreže smatraju osobnim komunikacijskim alatom, važnost zaštite svojih informacija pohranjenih na tim društvenim mrežama često se uzima zdravo za gotovo. S vremenom ljudi stavljaju sve više informacija u različite oblike na društvene mreže što može dovesti do neviđenog pristupa informacijama o ljudima i poslovnim subjektima. Količina informacija pohranjenih na društvenim mrežama vrlo je primamljiva za protivnike čiji je cilj nekome naštetiti.

# 4. ZAŠTITA I SIGURNOST MLADIH NA INTERNETU

Internet može biti jako koristan za mlade ljude. Mogu ga koristiti za istraživanje i učenje, te aktivnosti koje se vežu za školske potrebe, komunikaciju s učiteljima ili svojim vršnjacima, ili za vlastita istraživanja koja im mogu pomoći u svakodnevnom životu. Međutim, za mlade ljude internetski pristup također nosi rizike, poput neprikladnog sadržaja, cyberbullyinga i internetskih grabežljivaca.

## *4.1. Zakonska regulativa sigurnosti*

U Republici Hrvatskoj postoji nekoliko zakona koji se tiču sigurnosti, osobnih podataka i elektroničkih komunikacija, a to su:

- Zakon o informacijskoj sigurnosti (NN 79/07)
- Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/2018-805)
- Zakon o elektroničkim komunikacijama (NN 72/17)

Zakonom o informacijskoj sigurnosti se utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za

donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti (Zakon o informacijskoj sigurnosti, čl. 1.).

Zakonom o provedbi Opće uredbe o zaštiti podataka se osigurava provedba Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Zakon o provedbi Opće uredbe o zaštiti podataka, čl. 1.).

Zahtjevi GDPR-a primjenjuju se na svaku državu članicu Europske unije, s ciljem stvaranja dosljednije zaštite potrošačkih i osobnih podataka u svim zemljama EU-a. Neki od ključnih zahtjeva za privatnost i zaštitu podataka GDPR-a uključuju:

- zahtijevanje suglasnosti subjekata za obradu podataka,
- anonimiziranje prikupljenih podataka radi zaštite privatnosti,
- pružanje obavijesti o povredi podataka,
- sigurno rukovanje prijenosom podataka preko granica,
- od određenih tvrtki zahtijeva se da imenuju službenika za zaštitu podataka koji će nadzirati usklađenost s GDPR-om.

GDPR ne predstavlja temeljnu promjenu za mnoga prava koja djeca imaju nad svojim osobnim podacima. Zakon o zaštiti podataka iz 1998. (Zakon iz 1998.) ne spominje izričito djecu, no njegove se odredbe primjenjuju na njih kao na pojedince za sebe. Na primjer, djeca imaju pravo zahtijevati kopiju svojih osobnih podataka prema oba zakona i imaju pravo zahtijevati da prestanete s obradom njihovih podataka. Za razliku od GDPR-a, Zakon iz 1998. ne zahtijeva izričito da se podaci o djeci zaštite i ne zahtijeva da obavijesti o privatnosti moraju biti jasne i dostupne djetetu ili prilagođene posebno za njih.

GDPR pruža mnoge mogućnosti za zaštitu djece, njihovo osnaživanje i dopuštanje da sudjeluju u svim vrstama procesa koji se na njih odnose. Međutim, stupanj u kojem se te mogućnosti mogu ostvariti ovisi o tome kako se odredbe provode u praksi. GDPR nudi nekoliko odredbi koje se odnose na djecu, bilo eksplicitno ili implicitno. Unatoč činjenici da neke važne odredbe ne spominju djecu, one se ipak smatraju posebno relevantnim za djecu.

Zakonom o elektroničkim komunikacijama se uređuje područje elektroničkih komunikacija, i to korištenje elektroničkih komunikacijskih mreža i pružanje elektroničkih komunikacijskih usluga, pružanje univerzalnih usluga te zaštita prava korisnika usluga, gradnja, postavljanje, održavanje i korištenje elektroničke komunikacijske infrastrukture i povezane opreme, uvjeti tržišnog natjecanja te prava i obveze sudionika na tržištu elektroničkih komunikacijskih mreža i usluga, adresiranje, numeriranje i upravljanje radiofrekvencijskim spektrom, digitalni radio i televizija, zaštita podataka i sigurnost elektroničkih komunikacija te obavljanje inspekcijskog i stručnog nadzora i kontrole u elektroničkim komunikacijama, kao i osnivanje nacionalnog regulatornog tijela za elektroničke komunikacije i poštanske usluge, njegovo ustrojstvo, djelokrug i nadležnosti te postupak donošenja odluka i rješavanja sporova u elektroničkim komunikacijama (Zakon o elektroničkim komunikacijama, Čl. 1.).

## *4.2. Zaštitne mjere*

Zaštitne mjere su svi postupci, procedure i mehanizmi kojima se štite resursi informacijskog sustava od prijetnji te se smanjuje njihova ranjivost, otkrivaju se neželjeni događaji i smanjuje se njihov učinak te se pospješuje oporavak (Vukelić ,2016).

Podjela zaštitnih mjera je prikazana Slikom 3.

**Slika 3.**

*Podjela zaštitnih mjera*


Izvor: Izrada autorice prema Vukelić, B., 2016.

Zaštita podataka je praksa zaštite digitalnih informacija od neovlaštenog pristupa, oštećenja ili krađe tijekom cijelog njihovog životnog ciklusa (Madigan, Rash i sur., 2017, 327). To je koncept koji obuhvaća svaki aspekt informacijske sigurnosti od fizičke sigurnosti hardvera i uređaja za pohranu do administrativnih kontrola i kontrola pristupa, kao i logičke sigurnosti softverskih aplikacija.

Zaštitne mjere proizlaze od osobnih podataka i njihove dostupnosti na internetu, kao primjerice broj mobitela ili e-mail adresa. Lozinke je potrebno čuvati za sebe, kada se radi o društvenim mrežama, lozinke je potrebno sačuvati samo za sebe. Najčešće tehnike koje se koriste

za zaštitu operativnih sustava uključuju korištenje antivirusnog softvera i drugih mjera zaštite krajnjih točaka, redovita ažuriranja zakrpa operativnog sustava, vatrozid za praćenje mrežnog prometa i provedbu sigurnog pristupa kroz najmanje privilegija i korisničke kontrole.

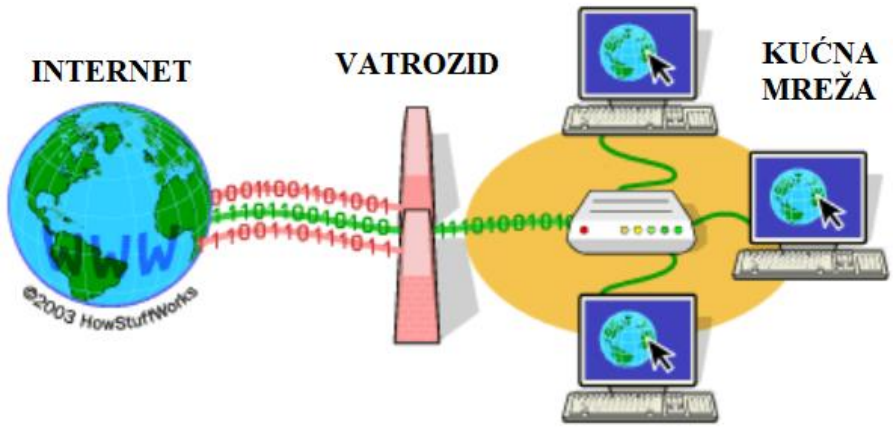
Izrazi zaštita podataka i privatnost podataka često se koriste naizmjenično, ali postoji važna razlika između njih (Livingstone, Carr, Byrne, 2015). Privatnost podataka definira tko ima pristup podacima, dok zaštita podataka pruža alate i pravila za stvarno ograničavanje pristupa podacima.

Vatrozid je jedna od zaštitnih mjera koja može pomoći u zaštiti računala i podataka upravljanjem mrežnim prometom. To čini blokiranjem neželjenog i neželjenog dolaznog mrežnog prometa. Vatrozid potvrđuje pristup procjenom ovog dolaznog prometa na bilo što zlonamjerno poput hakera i zlonamjernog softvera koji bi mogao zaraziti računalo. Najvažnija najbolja sigurnosna praksa s vatrozidom je da prema zadanim postavkama blokira sav promet. Zatim ga treba konfigurirati da dopušta samo određeni promet poznatim uslugama. Konfiguracija vatrozida je kritična, pa je znanje administratora vatrozida ključno (https://www.comodo.com/resources/home/how-firewalls-work.php).

Funkcije Vatrozida na mreži je prikazana na Slici 4.

**Slika 4.**

*Funkcije Vatrozida na mreži*




Izvor: Obrada autorice prema, Comodo Group, 2021.

Vatrozid je konfiguriran s popisom pravila koja se ponekad nazivaju politikama. Vatrozid koristi ovaj popis pravila kako bi odredio što učiniti s prometom nakon što stigne na vatrozid.

Vatrozid kontrolira sav promet između interneta i klijenta, što je vidljivo i na Slici 4.

Redovito ažuriranje softvera na računalu i drugim uređajima jedan je od najjednostavnijih zaštitnih mjera.

Operativni sustavi imaju mnogo ugrađenih funkcija za sprječavanje napada. Problem je, međutim, što se cyber prijetnje stalno mijenjaju. Zato davatelji operativnih sustava redovito nude ažuriranja operativnog sustava: kako bi bili u tijeku s promjenjivim prijetnjama od strane cyber kriminalaca.

Izraz sigurnost operativnog sustava se odnosi na postupke i mjere koje mogu osigurati povjerljivost, integritet i dostupnost operativnih sustava. Cilj sigurnosti operativnog sustava je zaštititi operativni sustav od raznih prijetnji, uključujući zlonamjerni softver kao što su crvi, trojanci i drugi virusi, pogrešne konfiguracije i udaljeni upadi (Antoliš, 2010).

Sigurnost operativnih sustava obično uključuje implementaciju kontrolnih tehnika koje mogu zaštititi imovinu od neovlaštene izmjene i brisanja ili krađe.

Antivirusni softver štiti vaš uređaj od virusa koji mogu uništiti podatke, usporiti ili srušiti uređaj ili omogućiti pošiljateljima neželjene pošte slanje e-pošte putem računa. Antivirusna zaštita skenira datoteke i dolaznu e-poštu na viruse, a zatim briše sve zlonamjerno. Potrebno je ažurirati antivirusni program kako biste se uređaj branio od bilo kojeg napada na njega. Većina antivirusnih softvera uključuje značajku za automatsko preuzimanje ažuriranja kada je korisnik na mreži. Također je potrebno provjeriti radi li softver kontinuirano, osobito ako se preuzmu datoteke s weba ili provjeravaju e-pošte. Potrebno je postaviti antivirusni softver da provjerava viruse svaki dan. Također je potrebno temeljito skenirati svoj sustav barem dva puta mjesečno (https://www.nibusinessinfo.co.uk/content/server-security).

### *4.3. Uloga roditelja i lokalne zajednice u zaštiti mladih na internetu*

Na globalnoj razini procjenjuje se da su 1/3 djece korisnici interneta i da su 1/3 korisnika interneta osobe mlađe od 18 godina (Livingstone, Carr, Byrne, 2015).

U 2017. godini polovica svjetskih stanovništvo koristilo internet; među dobnom skupinom od 15 do 24 godine taj se udio popeo na oko 2/3 (Livingstone, Carr, Byrne, 2015).

Roditelji trebaju podržati djecu i mlade kako bi mogli sigurno koristiti tehnologiju. Trebali bi imati uravnotežen pristup i prepoznati širok raspon prednosti koje Internet može pružiti. Roditelji su možda skloni usredotočiti se na mnoge pozitivne koristi koje se mogu steći na internetu, ali je važno da uzmu u obzir i cijene društvene koristi koje djeca mogu steći - igra i istraživanje osobnih interesa mogu biti ključni motivatori za korištenje interneta kada je riječ o mladima. Razumijevanje toga može pomoći roditeljima da se bolje uključe i podrže svoju djecu. Kako bi osigurali da djeca i mladi koriste internetske stranice sigurno i odgovorno, roditelji trebaju biti svjesni sljedećeg:

- upoznavanje s rizicima i prilikama s kojima se djeca i mladi mogu susresti na internetu, važno je biti u stanju prepoznati potencijalne prijetnje s kojima se djeca mogu suočiti, a pritom upamtiti da rizici ne mogu dovesti do štete,
- roditelji trebaju biti aktivno uključeni u ono što njihova djeca rade na mreži, vrstu sadržaja koji gledaju, dijele ili stvaraju, usluge, platforme i igre koje koriste te ljude s kojima se povezuju, roditeljima je uvijek od pomoći isprobati usluge koje njihova djeca koriste,
- roditelji bi se trebali upoznati s dobrim web stranicama i igrama za učenje i zabavu koje mogu koristiti sa svojom djecom, dobra web stranica ili igra imat će namjensku sigurnosnu stranicu s jasnim poveznicama, mehanizmima prijavljivanja i smjernicama za djecu i mlade ljude i njihove roditelje,
- roditelji se trebaju pobrinuti da dijete zna kada i gdje treba dobiti pomoć, potrebno je potaknuti stav da, ako dožive nešto uznemirujuće na internetu, o tome trebaju razgovarati s odraslom osobom od povjerenja,

- roditelji se trebaju pobrinuti da djeca imaju uravnoteženu digitalnu prehranu, tako da njihovo vrijeme na internetu bude dobro provedeno i sadrži mješavinu aktivnosti koja uključuje učenje, stvaranje i povezivanje na pozitivne načine,
- potrebno je naučiti djecu da ne dijele svoje pristupne lozinke s prijateljima ili braćom i sestrama,
- bez obzira na prijetnje, roditelji ne smiju pretpostavljati da svi na internetu ciljaju na njihovu djecu, generalno web stranice mogu biti sigurne i mogu pružiti prekrasno, kreativno društveno i obrazovno iskustvo (Livingstone, Carr, Byrne, 2015).

# 5. ZAKLJUČAK

Mladi mogu nesvjesno izložiti svoje obitelji internetskim prijetnjama, na primjer, slučajnim preuzimanjem zlonamjernog softvera koji bi cyber kriminalcima mogao omogućiti pristup bankovnom računu njihovih roditelja ili drugim osjetljivim informacijama. Zaštita djece na internetu stvar je svijesti. U današnjem svijetu gotova svaka osoba služi se internetom na kojem ostavlja velik broj vlastitih informacija, a sigurnost tih podataka uvelike ovisi i o edukaciji korisnika interneta kako podatke ne bi ostavljali na nesigurnim stranicama. Bitno je i znanje djelatnika tvrtki u poslovnom svijetu o korištenju informacijskih sustava te cjelokupna suradnja svih sudionika koji dolaze u doticaj s podatcima. Nasilje nije novi problem, no pojavom interneta zadobio je novu dimenziju. Takvo nasilje gotovo da nikada ne prestaje - dok se u fizičkim situacijama osoba koja trpi zlostavljanje uglavnom može maknuti od zlostavljača i pobjeći u „sigurnu zonu“ kod nasilja vršenog putem interneta takva mogućnost ne postoji. Žrtva je neprestano izložena napadima različitih vrsta i prisiljena ih je ponovno i ponovno proživljavati. Kod ovakve vrste nasilja golem problem predstavlja činjenica da ga društvo još uvijek ne smatra oblikom nasilja koje može imati ozbiljne posljedice te se nerijetko može čuti kako se ono nije dogodilo u „stvarnom svijetu“ i da su žrtve samo preosjetljive na situaciju koja uopće nije toliko ozbiljna. Zbog navedenoga ozbiljnost situacije postaje jasna tek kada je šteta već počinjena. Nasilje na mreži može se definirati kao namjerna upotreba online digitalnih uređaja kako bi se nanijela šteta ili nelagoda drugima. To uključuje uređaje kao što su mobilni telefoni, računala ili tableti i aktivnosti kao što su pozivi, tekstualne poruke/SMS, dijeljenje videozapisa, e-pošte, razmjenu trenutnih poruka, društvene mreže, sobe za razgovor i bilo koju drugu metodu koja se koristi za komunikaciju na internetu.

# LITERATURA


Antoliš, K.,et al, Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010.

Bedić, B.,Filipović, M. (2014):. "Klikni za sigurnost" – spriječim onasilje, gradimo kulturu mira i ne nasilja. Zagreb: Ambidekster Klub

Gómez-Diago, G. (2012): Cyberspace and Cyberculture (pp.58-60)

Gómez-Diago, G. (2012): Cyberspace and Cyberculture, In book: Encyclopedia of Gender in Media.Chapter: Cyberspace and Cyberculture

Hamidović, Haris. Mjesto i uloga cyber sigurnosti u razvoju modernih društava. // Sarajevski žurnal za društvena pitanja, vol 4, 1-2(2015). Str. 82. URL: https://www.researchgate.net/publication/302901758_Mjesto_i_uloga_cyber_sigurnosti_u_razvoju_modernih_drustava. Prikupljeno 12. Travnja 2022.

Kuleš, M. (2015): Internet i društveni mediji kao pokretači društvenih promjena. Osijek: Filozofski fakultet

Kuleš, M. (2015): Internet i društven imediji kao pokretači društvenih promjena. Osijek: Filozofski fakultet

Livingstone, S., Carr, J., and Byrne, J. (2015) One in three: The task for global internet governance in addressing children's rights. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights 16 DQ Insti

Lobe, B., Velicu, A., Staksrud, E., Chaudron, S. and Di Gioia, R., How children (10-18) experienced online risks during the Covid-19 lockdown - Spring 2020, EUR 30584 EN, Publications Office of the European Union, Luxembourg, 2021.

Madigan S, Ly A, Rash CL, Van Ouytsel J, Temple JR. Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis.JAMA Pediatr. 2018;172(4):327–335.

Spitzer, M. (2018). Digitalna demencija: kako mi i naša djeca silazimo s uma. Zagreb: Naklada Ljevak

Usp. Vuković, Hrvoje. Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. National security and the future, vol. 13, br. 3, 2012. Str.15. URL: https://hrcak.srce.hr/100728

Vukelić, B., (2016): Sigurnost informacijskih sustava; Veleučilište u Rijeci, https://www.veleri.hr/files/datotekep/nastavni_materijali/k_sigurnost_s2/Sigurnost_informacijskih_Vukelic.pdf. Pristupljeno 20. Travnja 2022.

Zovkić, D. (2015): Nasilje putem interneta, završni rad, Osijek: Filozofski fakultet Sveučilišta u Osijeku

Internetski izvori:

Comodo Group, (1. Travnja 2022). Što vatrozid radi? - Mrežni sigurnosni vatrozid: https://www.comodo.com/resources/home/how-firewalls-work.php. Pristupljeno 5. svibnja 2022.

Nibusiness info, (20. listopada 2021). Zaštita poslovanja na mreži: https://www.nibusinessinfo.co.uk/content/server-security. Pristupljeno 17. svibnja 2022.

Revizijska izvješća (20. Ožujka 2021). Kibersigurnost u EU-u i njegovim državama članicama: https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_HR.pdf. Pristupljeno 18. travnja 2022.

Social Media & User-Generated Content (28. tavnja 2022). Number of social network users worldwide from 2017 to 2025: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/. Pristupljeno 5. travnja 2022.

# PRILOZI I DODACI

**Popis slika:**



**Popis tablica:**



**Popis grafikona:**

## IZJAVA O IZVORNOSTI DIPLOMSKOG RADA

Izjavljujem da je moj diplomski rad izvorni rezultat mojeg rada te da se u izradi istog nisam koristila drugim izvorima osim onih koji su u njemu navedeni.

_____

(vlastoručni potpis studenta)