Privatnost i sigurnosni aspekti uporabe mobilnih aplikacija

Jovanović, Milica

Sveučilište Jurja Dobrile u Puli

Fakultet ekonomije i turizma

„Dr. Mijo Mirković“

MILICA JOVANOVIĆ

PRIVATNOST I SIGURNOSNI ASPEKTI UPORABE MOBILNIH APLIKACIJA

Završni rad

Pula, rujan 2024.godine

Sveučilište Jurja Dobrile u Puli

Fakultet ekonomije i turizma

„Dr. Mijo Mirković“

MILICA JOVANOVIĆ

PRIVATNOST I SIGURNOSNI ASPEKTI UPORABE MOBILNIH APLIKACIJA

Završni rad

JMBAG:0303087778 / redovni student

Studijski smjer: Informatički menadžment

Predmet:Informatika

Mentor: Prof.dr.sc. Branimir Dukić

Sumentor: Izv. Prof.dr.sc. Danijela Rabar

Pula, rujan 2024.godina

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljeni način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj Završni rad pod nazivom

_____

_____

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____

Potpis

_____

SADRŽAJ

1. UVOD

U današnje je vrijeme gotovo nemoguće pronaći osobu koja ne posjeduje mobilni telefonski uređaj. Korištenje mobilnih telefonskih uređaja više ne predstavlja luksuz nego potrebu. U školi, na radnom mjestu, na ulici i drugim javnim mjestima moguće je vidjeti da većina osoba posjeduje mobilni telefonski uređaj. Mobilni telefoni imaju različite namjene. Od pojave prvih mobilnih uređaja do danas došlo je do značajnih promjena u digitalnoj tehnologiji i uporabi mobilnih telefonskih uređaja. Prvi mobilni telefoni bili su namijenjeni za obavljanje glasovne komunikacije. Kasnije je, uz glasovne komunikacijske mogućnosti, mobilnim telefonima dodana i mogućnost slanja kratkih tekstualnih poruka (engl. Short Message Service – SMS) i multimedijskih poruka (engl. Multimedia Messaging Service – MMS). Nakon toga je, u vrlo kratkom razdoblju, došlo do brzog rasta mogućnosti mobilnih telefona, posebice zbog integracije mobilnih telefona s tehnologijama za snimanje digitalnih slika i video sadržaja, zvuka, kao i s tehnologijom geografskog lociranja, odnosno pozicioniranja (engl. Global Positioning System – GPS), omogućavanja instalacije programskih aplikacija te uvođenja mogućnosti povezivanja mobilnih telefona na Internet i omogućavanja uporabe internetskih usluga namijenjenih korisnicima na mobilnim telefonima. Mobilni telefonski uređaji koji imaju sve navedene mogućnosti nazivaju se naprednim ili pametnim mobilnim telefonskim uređajima (engl. Smartphone). Pristup je Internetu s pametnim mobilnim telefonskim uređajima omogućio uporabu raznih programskih aplikacija među kojima su i one koje omogućavaju virtualno društveno umrežavanje što je značajno pridonijelo porastu obujma uporabe mobilnih telefona.

No, porast obujma uporabe mobilnih telefona privukao je pozornost onih koji iskorištavaju slabosti u mobilnoj telefonijskoj tehnologiji kako bi ostvarili svoje maliciozne nakane i kroz to ugrozili na različite načine korisnike mobilnih telefona. U pravilu se sve ugroze odnose na iskorištavanje, s jedne strane, nesavršenosti programske tehnologije koja se koristi u radu s mobilnim telefonima, a s druge strane, na iskorištavanju naivnosti i manjkavosti u znanjima korisnika mobilnih telefona. Iako se u biti ne radi o problemu iz domene malicioznih ugroza, u posljednje je vrijeme sve značajniji i veći problem privatnosti prilikom uporabe mobilnih telefona jer programske

aplikacije uporabom globalnog komunikacijskog sustava prikupljaju sve veći opseg osobnih podataka o korisniku i njegovu ponašanju, često bez korisnikova znanja.

Prikupljeni se podaci putem naprednih mobilnih telefona uobičajeno koriste za unaprjeđenje korisničkog iskustva prilikom uporabe programskih aplikacija putem pametnih telefonskih uređaja, ali i za istraživanja ponašanja korisnika pametnih telefonskih uređaja. Unaprjeđenje korisničkog iskustva predstavlja način na koji programske aplikacije, s obzirom na spremljene podatke o korisniku i njegovu ponašanju (interesi korisnika, vrijeme i mjesto pristupa, interakcije s aplikacijama i drugim korisnicima te drugo) olakšavaju i ubrzavaju uporabu same programske aplikacije korisniku te kroz nuđenje alternativnih i/ili dodatnih usluga korisniku.

Problem se privatnosti pojavljuje prije svega kada se podaci prikupljeni o korisniku učine javnim na način da se prodajom ili besplatno učine dostupnim drugim osobama koje mogu na različite načine iskoristiti prikupljene podatke. Jedan od uobičajenih načina narušavanja privatnosti je, bez znanja i pristanka korisnika, prodaja prikupljenih podataka o korisniku i njegovom ponašanju drugim poslovnim subjektima koji te podatke iskorištavaju za potrebe promocijskih kampanja. Pozitivnom zakonskom regulativom danas se prisiljava poslovne subjekte koji su u poziciji da prikupljaju podatke o korisniku pametnih mobilnih telefonskih uređaja i njegovu ponašanju, da za prikupljanje takvih podataka zatraže i dobiju privolu od samih korisnika, čega se poslovni subjekti, zbog potencijalno visokih kazni i pridržavaju. No, u biti glavni je problem privatnosti taj što korisnici nisu, najčešće zbog vlastite nonšalantnosti i neznanja, jer pažljivo ne pročitaju uvjete korištenja, potpuno upoznati s onim što prihvaćaju prilikom potvrde općih uvjeta uporabe programske aplikacije. Praktično nisu svjesni tko će i kako će se njihovi podaci koristiti.[1] Nažalost, nerijetko se događa da se podataka o korisnicima koje su prikupili poslovni subjekti, dokopaju oni koji te podatke nemaju namjeru koristiti u pozitivnom smislu, primjerice za unaprjeđenje iskustva korisnika prilikom uporabe programskih aplikacija, već oni čije su namjere maliciozne.

[1] Osnove privatnosti na Internetu, CERT.hr , https://www.cert.hr/wpcontent/uploads/2017/12/osnove_privatnosti_na_Internetu_0.pdf [15.5.2024]

Generalno se može konstatirati kako su korisnici pametnih mobilnih telefona izloženi raznim prijetnjama zlonamjernih programskih rješenja (virusi, crvi, trojanski konji...). Zbog generalno niske razine znanja često korisnici pametnih mobilnih telefona nisu svjesni prisutnosti zlonamjernih programa na svom pametnim telefonskim uređajima ni pristupa zaraženim programskim rješenjima putem Interneta. Zlonamjerna programska rješenja neprestano napreduju što otežava korisnicima prepoznavanje ugroženosti od malicioznih programskih rješenja. Zlonamjerna programska rješenja mogu korisniku nanijeti velike štete, od šteta financijske prirode, preko štete koje nastaju zbog krađe identiteta, do prijevara koje su posljedica naivnosti i neznanja korisnika pametnih telefonskih uređaja.

Zbog generalno sve češćih i globalno većih ugroza koje su rezultat djelovanja malicioznih programskih rješenja, kao i zbog sve većih problema koji su posljedica problema vezanih za privatnost prilikom uporabe pametnih mobilnih telefona, provedeno je istraživanje vezano za rizike privatnosti i sigurnosti korisnika prilikom uporabe pametnih mobilnih telefonskih uređaja, odnosno programskih aplikacija koje su uobičajeno instalirane na pametnim mobilnim telefonskim uređajima ili kojima se pristupa putem pametnih telefonskih uređaja uporabom Interneta. Rezultati istraživanja prikazani su u ovom završnom radu.

2.METODOLOGIJA ISTRAŽIVANJA

Usporedno s rastom popularnosti pametnih mobilnih telefonskih uređaja rastu i problemi koji su vezani za sigurnost od malicioznog koda kojim se ugrožava sigurnost uporabe ovih uređaja kao i problemi vezani za privatnost korisnika pametnih mobilnih telefonskih uređaja. Kako se radi o vrlo dinamičnom procesu kojemu globalno raste značaj, fokus je provedenog istraživanja usmjeren na rizike privatnosti i sigurnosti korisnika prilikom uporabe pametnih mobilnih telefonskih uređaja, odnosno programskih aplikacija koji su uobičajeno instalirane na pametnim mobilnim telefonskim uređajima ili kojima se pristupa putem pametnih telefonskih uređaja uporabom Interneta.

Sukladno prethodno navedenom postavljeno je sljedeće istraživačko pitanje: „Je li uporaba programskih aplikacija putem naprednih mobilnih telefonskih uređaja sigurna za korisnika?“. U tom je smislu planirano sagledati sljedeće aspekte sigurnosti uporabe pametnih mobilnih telefonskih uređaja:

1. aspekt sigurnosti uporabe programskih aplikacija putem pametnih mobilnih telefonskih uređaja i
2. aspekt privatnosti korisnikovih osobnih podataka prilikom uporabe pametnih mobilnih telefonskih uređaja.

Temeljem definiranog problema istraživanja te postavljenog istraživačkog pitanja definirani su sljedeći ciljevi istraživanja:

1. istražiti u sekundarnim, tercijarnim i kvartarnim izvorima informacija i znanja pojam i ulogu pametnih mobilnih telefona te mobilnih programskih aplikacija,
2. istražiti u sekundarnim, tercijarnim i kvartarnim izvorima informacija i znanja pojmove privatnosti i sigurnosti vezanih uz uporabu pametnih telefonskih uređaja.

3. istražiti u sekundarnim, tercijarnim i kvartarnim izvorima informacija i znanja temeljne vrste zlonamjernih prijetnji,
4. istražiti u sekundarnim, tercijarnim i kvartarnim izvorima informacija i znanja neke poznate sigurnosne incidente u Republici Hrvatskoj u 2023. godini,
5. istražiti u sekundarnim, tercijarnim i kvartarnim izvorima informacija i znanja optimalne načine zaštite korisnika pametnih mobilnih telefonskih uređaja,
6. istražiti u sekundarnim, tercijarnim i kvartarnim izvorima informacija i znanja Europske odredbe o zaštiti osobnih podatka,
7. istražiti u sekundarnim, tercijarnim i kvartarnim izvorima informacija i znanja razlike u rješavanju problema privatnosti i sigurnosti kod operacijskog sustava Android i operacijskog sustava IOS koji se koriste kod većine pametnih mobilnih telefonskih uređaja,
8. primarnim istraživanjem anketiranjem sagledati kakva su znanja i razumijevanja problema sigurnosti i privatnosti prilikom uporabe pametnih mobilnih telefonskih uređaja kod populacije stanovništva, osobito studenata Sveučilišta Jurja Dobrile u Puli,
9. kroz sintezu rezultata istraživanja izraditi prijedlog modela za osiguravanje privatnosti i sigurnosti uporabe programskih aplikacija putem pametnih mobilnih telefonskih uređaja.

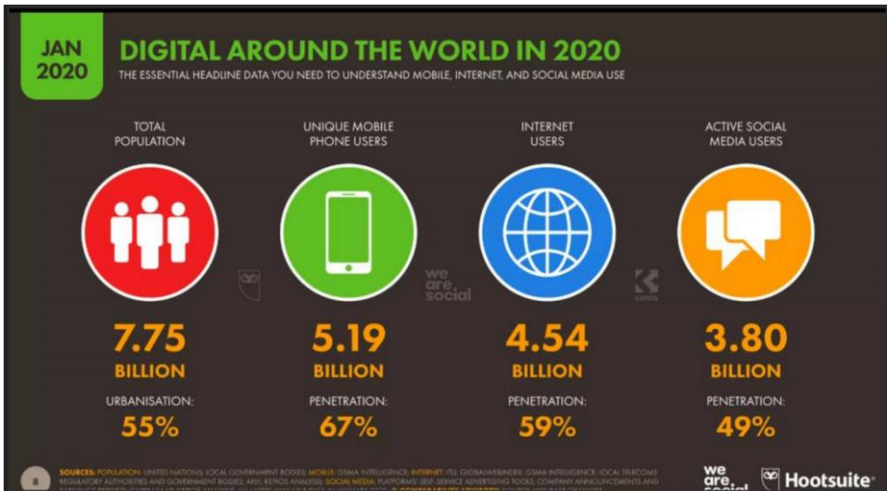
Provedeno se istraživanje koristilo metodom dedukcije jer se krenulo općenito od problema vezanih za sigurnost i privatnost kod uporabe pametnih mobilnih telefonskih uređaja, a završilo je primarnim istraživanjem kojim se sagledalo stanje vezano za problem razumijevanja sigurnosti i privatnosti kod stanovništva, a osobito kod studenata Sveučilišta Jurja Dobrile u Puli. Desk istraživanjima definirani su okviri za provođenje primarnih istraživanja anketiranjem. Prema tome, među korištenim znanstvenim istraživačkim metodama treba istaknuti kako se prilikom primarnih istraživanja koristila metoda istraživanja anketiranjem, podaci su obrađeni metodama deskriptivne statistike, a uz navedene metode korištene su metoda analize, metoda apstrahiranja, metoda klasifikacije, metoda generalizacije, metoda kauzalnog

zaključivanja, metoda sinteze, metoda deskriptivnog modeliranja, povijesna metoda, kao i druge znanstveno-istraživačke metode.

3.POJAM I ULOGA PAMETNIH MOBILNIH TELEFONA I PROGRAMSKE APLIKACIJE KOJE SE KORISTE PUTEM PAMETNIH MOBILNIH TELEFONA

Prema statističkim podatcima objavljenim na portalu Digital 2020., koji su prikazani na slici 1., 59% je svjetske populacije u mreži, odnosno koristi Internet. Od navedenog postotka više od polovice svjetskog stanovništva koristi društvene mreže. Više od 4.54 milijardi ljudi u svijetu koristi se Internetom, a od ukupnog broja korisnika Interneta 3.8 milijardi koristi društvene mreže. Prema navedenom je izvoru podataka prosječno porasla uporaba Interneta za 298 milijuna osoba u godinu dana od 2019. do 2020. godine. Nadalje, prema istom je izvoru 2020. godine u svijetu bilo oko 3.80 milijardi korisnika društvenih mreža, te se taj broj povećao u odnosu na 2019. godinu za više od 10%. Kada su u pitanju mobilni telefoni, prema istom izvoru je u 2020. godini mobilni telefon koristilo 5.19 milijardi ljudi. Broj korisnika mobilnih telefonskih uređaja od siječnja 2019. godine do siječnja 2020. godine povećao se za 124 milijuna.[2]

[2] Digital 2020, Global digital overview , https://datareportal.com/reports/digital-2020-global-digital-overview [3.5.2024] [3] Ibid.



Slika 1. Globalni prikaz uporabe mobilnih telefona i Interneta za 2020.godinu na portalu Digital 2020[3]

Izvor: Digital 2020, Global digital overview , https://datareportal.com/reports/digital-2020-global-digital-overview

Portal Digital 2020. iznosi podatke o prosječnoj dnevnoj uporabi Interneta, mobilnih telefonskih uređaja i društvenih mreža. Dnevna je uporaba Interneta prosječno u 2020. godini iznosila 6.43 sata po danu, uporaba društvenih mreža 2.24 sata po danu, gledanje televizije 3.18 sati po danu, slušanje glazbe preko streaming servisa 1.26 sati po danu i igranje videoigara 1.10 sati po danu.

Osim zabave i opuštanja Internet se koristi kako za obrazovne svrhe, tako i za posao. Veliki dio dnevnog vremena ljudi provode na Internetu. Globalno, 4.54 milijarde stanovnika koristi Internet što je otprilike 59% globalne populacije. Godišnje povećanje korisnika Interneta iznosi prosječno 7% odnosno 298 milijuna korisnika više od prethodne godine (2019.godine). Kako je vidljivo iz podataka objavljenih na portalu Digital 2020. broj Internet korisnika povećava se iz godine u godinu.[3]

[3] Ibid.

3.1. Mobilni telefoni

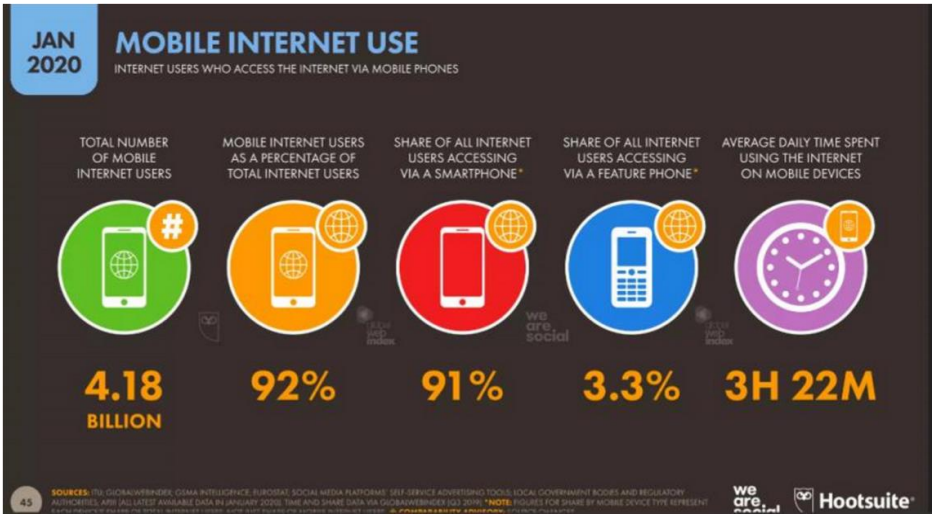
Danas je gotovo nemoguće zamisliti svakodnevni život bez uporabe pametnih telefona koje većina stanovništva posjeduje, što je vidljivo iz prethodno navedenih podataka s portala Digital 2020. Početak se izgradnje mreže za mobilnu telefoniju veže uz 1973. godinu. Prve mobilne mreže funkcionirale su na način koji je omogućavao da samo jedan korisnik može biti spojen na jednu baznu stanicu, a komunikacija je bila moguća samo u dometu bazne stanice. Značajan se pomak dogodio u 80-tim godinama prošlog stoljeća kada je omogućeno spajanje više korisnika istovremeno na jednu baznu stanicu kao i prijenos signala s jedne na drugu baznu stanicu sukladno promijeni prostorne pozicije mobilnog telefonskog uređaja.To je bilo razdoblje uporabe analognih komunikacija u prijenosu signala između mobilnog telefona i bazne stanice. Prva digitalna mreža GSM (engl. Global system for mobile communications) pokrenuta je u Finskoj 1991. godine, te se postupno proširila cijelom Europom. Značajke GSM-a su poboljšana kvaliteta zvuka i poziva, te dodatni servisi, odnosno mogućnost slanja SMS poruka. U Hrvatsku GSM dolazi 1995. godine.[4]

Primarna je funkcija klasičnog telefona glasovna komunikacija. Danas pametni telefoni posjeduju puno više funkcija, uz primarnu funkciju glasovne komunikacije, a to su funkcija slanja i primanja SMS poruka, geografsko lociranje, snimanje slikovnih i zvučnih zapisa, pohranjivanje i izvođenje programskih aplikacija te korištenja Interneta. Danas se pametni telefoni promatraju kao prijenosna mini računala s mogućnosti glasovne i SMS komunikacije. Kada je u pitanju razvitak GSM-a, tada se prve analogne bazne stanice koje su se koristile u 80-tim godinama prošlog stoljeća, ubrajaju u prvu generaciju GSM-a, odnosno u 1G mrežu.

Sljedeća, digitalna generacija baznih stanica označava se kao 2G mreža. Kroz godine su se digitalne bazne stanice poboljšale i u smislu obujma istodobnih korisnika i u smislu kvalitete i u smislu brzine prijenosa digitalnih signala, što je primjerice omogućilo brži prijenos podataka tako da 3G mrežu odlikuje mogućnost optimalnog prijenosa videozapisa. Četvrta generacija (4G i LTE) omogućila je znatno veću brzinu prijenosa podataka što daje primjerice mogućnost praćenja video sadržaja u realnom vremenu,

[4] Povijest mobilne telefonije: što se događalo u 40 godina?, Mob.hr, https://mob.hr/povijest-mobilnetelefonije-sto-se-dogadalo-u-40-godina/ [16.4.2023]

a najnovija 5G mreža omogućava diferencirane brzine prijenosa podataka u mobilnoj mreži, sukladno raspoloživim resursima i potrebama za resursima svakog pametnog mobilnog uređaja koji je pristupio baznoj stanici. Prema tome, 5G mreža je inteligentna bežična mreža koja optimizira resurse sukladno potrebama korisnika.[6] Prema portalu Digital 2020 podaci sa slike 2. prikazuju kako je ukupni broj mobilnih telefonskih uređaja povezanih Internetom u 2020. godini iznosio 4.18 milijarde. Od ukupnog broja uređaja (načina korištenja Interneta) 92% otpada na uporabu Interneta preko mobilnih telefonskih uređaja. Prosječno dnevna uporaba Interneta preko mobilnih telefonskih uređaja iznosi 3.22 sata. Nadalje, 91% Internet korisnika pristupa Internetu preko pametnih telefona.[7]



Slika 2 Uporaba Interneta putem mobilnih telefonskih uređaja prema portalu Digital 2020[5]

Izvor: : Digital 2020, Global digital overview, https://datareportal.com/reports/digital-2020-global-digital-overview

[5] Ibid.

3.2. Mobilne programske aplikacije

S obzirom na strojnu građu suvremenih pametnih mobilnih telefonskih uređaja, razvidno je da se radi o računalnim uređajima koje pogone procesori. Prema tome, kao i svi drugi računalni uređaji, tako su i pametni mobilni telefonski uređaji programirljivi uređaji.[6] Stoga je razumno da je sve veća uporaba pametnih mobilnih telefona potakla industriju koja se bavi razvojem programskih aplikacija (engl. Software) namijenjenih pokretanju na pametnim mobilnim telefonskim uređajima te njima srodnim tablet uređajima. Svrha je mobilnih programskih aplikacija pružanje sadržaja korisnicima ”na dohvat ruke”, sličnih onima koje korisnici upotrebljavaju na osobnim računalima.

Mobilne programske aplikacije svojim korisnicima omogućavaju i olakšavaju obavljanje osobnih, profesionalnih i obrazovnih zadataka, pristup bankovnim računima, lakše plaćanje, GPS navigaciju i drugo. Neke su mobilne programske aplikacije korisniku besplatno na raspolaganju, dok je za druge njihovu instalaciju ili pak uporabu putem Interneta potrebno platiti. Ono što je specifično za mobilne programske aplikacije, kada su u pitanju modeli naplate programskih aplikacija, to je da se radi o programskim rješenjima koja su cijenom značajno prihvatljivija no programska rješenja koja su namijenjena klasičnim računalnim uređajima.[7]

Koliko su mobilne programske aplikacije donijele koristi i učinile pametne mobilne telefonske uređaje korisnicima pristupačnim, toliko su s druge strane, otvorile vrata pristupu malicioznog koda kroz te aplikacije na mobilne telefonske uređaje. Maliciozni je programski kod u biti programski kod kao i svaki drugi, no njegova svrha nije dobrobit korisnika, već upravo suprotno. Zbog toga je potrebno da svaki korisnik bude upoznat s općim karakteristikama malicioznog koda kako bi znao zaštiti sebe,

---

[6] What's a smartphone processor and what does it do?, Cool Blue, https://www.coolblue.nl/en/advice/smartphone-processors.html [3.8.2024]

[7] Mobilne aplikacije. Što su, za što postoje i koje vrste postoje?, Pctown , https://pctown.co.nz/mobilneaplikacije-sto-su-za-sto-postoje-i-koje-vrste-postoje/#google_vignette [16.4.2024]

odnosno svoj mobilni telefonski uređaj od malicioznog koda i kako bi se u slučaju neposredne ugroze znao ponašati u smislu zaštite sebe te zaštite drugih kojima potencijalno taj programski kod može biti proslijeđen.

4.PRIVATNOST I SIGURNOST PRILIKOM UPORABE MOBILNIH TELEFONSKIH UREĐAJA

Generalno se može konstatirati kako privatnost predstavlja kontrolu neke osobe nad vlastitim osobnim podatcima, a sigurnost predstavlja postupke provedene u smislu zaštite programskih rješenja i podataka od zlonamjernog i/ili slučajnog uništenja ili izmjene.[8] Vezano za prikupljanje podataka na Web stranicama Google-a navodi sljedeće: „Podatke prikupljamo kako bismo svim svojim korisnicima pružali bolju uslugu. Na temelju njih možemo otkriti neke osnovne stvari, kao što je jezik kojim govorite, do onih složenijih, primjerice koji Vas oglasi najviše zanimaju, koje su Vam osobe najvažnije online ili koji bi Vam se videozapis na YouTubeu mogao svidjeti. Podaci koje Google prikuplja i način na koji ih upotrebljava ovisi o Vašoj uporabi naših usluga i načinu na koji upravljate kontrolama privatnosti. Kada niste prijavljeni na Google račun, podatke koje prikupljamo spremamo s jedinstvenim identifikatorima koji su povezani s preglednikom, aplikacijom ili uređajem koji upotrebljavate. Na taj način možemo zadržati Vaše postavke u sesijama pretraživanja, kao što je preferirani jezik ili prikazivanje više relevantnih rezultata pretraživanja ili oglasa na temelju Vaše aktivnosti. Kada ste prijavljeni, prikupljamo i podatke koje pohranjujemo na vaš Google račun i s njima postupamo kao s osobnim podacima.“ [9] Primjerice na platformi YouTube, koja je povezana s Google korisničkim računom, podaci koji se prikupljaju su:[13]

---

[8]Online privatnost i sigurnost, Europska komisija, https://digitalstrategy.ec.europa.eu/hr/policies/onlineprivacy [6.8.2024]

[9] Pravila o privatnosti, Google.com, https://policies.google.com/privacy?hl=hr [1.6.2024]

[13] Ibid.

- pojmove koje pretražuje korisnik,
- videozapise koji se pregledavaju,
- interakcija s oglasima, promidžba,
- podaci o glasovnoj i audio-aktivnosti,
- aktivnosti kupnje,
- drugi korisnici s kojima se dijeli sadržaj i komunikacija,
- aktivnost na Web lokacijama i aplikacijama treće strane unutar platforme Povijest pregleda na pregledniku.

Kao što je već navedeno, Google nije jedini poslovni subjekt koji prikuplja podatke o svojim korisnicima. Iskustvo ukazuje kako svaki ozbiljniji poslovni subjekt koji posjeduje vlastite Web stranice, sustavno prikuplja podatke o svojim korisnicima. Temeljem neformalno prikupljenih informacija, među korisnicima društvenih mreža postoji rasprostranjeni stav kako su danas društvene mreže izrazito aktivne u prikupljanju podataka o njihovim korisnicima. Takvi podaci se uobičajeno izravno ne zloupotrebljavaju od strane onih koji su podatke prikupili, no ti se podaci često prodaju trećim osobama među kojima se mogu naći i one osobe ili poslovni subjekti koji imaju maliciozne namjere vezane za uporabu podataka.

Kao što je već navedeno, osim problemima vezanim za privatnost, korisnici su Interneta izloženi sigurnosnim ugrozama, odnosno prijetnjama vezanim za posljedice djelovanja zlonamjernih programskih rješenja, kao što su ugroza funkcioniranja mobilnog telefonskog uređaja, mogućnost izmjene funkcionalnosti mobilnih programskih rješenja, krađe i/ili gubitka podatka ili pak izmjene sadržaja podataka.

5.ZLONAMJERNE PRIJETNJE NA PAMETNIM MOBILNIM TELEFONIMA

Zlonamjerna su se programska rješenja prvotno pojavila u računalnom svijetu i to u osamdesetim godinama prošlog stoljeća. Radilo se o zlonamjernim programima koji su distribuirani na različite načine, a čija je svrha bila ugroza računala na koje se programski kod instalirao. Maliciozni programski kod imao je različite načine djelovanja te širenja, stoga su se pojavili različiti nazivi za različite tipove zlonamjernog programskog koda, od računalnog crva, virusa pa sve do trojanskih konja. Zajednički naziv za sav takav maliciozni programski kod je Malware (engl. Malicious software).[10] U literaturi se može naći kako su najčešća tri razloga kreiranja Malware-a u svrhu zarade novca:[11]

- špijunaža - često se provodi pomoću Rootkit programa,
- slanje velikog broja „poruka“ – s velikog se broja računala šalju neželjene poruke (pošta) ili se pokušava iskoristit naivnost korisnika radi prijevara,
- neovlašten pristup računalu – špijuniranjem se pomoću tzv. spyware programa ili pak na neki drugi način (npr. socijalnim inženjeringom) pribavlja lozinka i pristupa se računalu što osigurava dolazak do niza bitnih podataka kao što su npr. brojevi bankovnih računa, lozinke i drugo.

Zlonamjerna se programska rješenja pokreću na računalnom sustavu korisnika bez korisnikova znanja i pristanka, te dovode do oštećenja programa, odnosno mijenjanja programskog koda kod zdravih programa. Osim već navedenih crva, virusa i trojanskih konja u praksi se uobičajeno susreću:[16]

- špijunski programi (engl. Spyware),
- oglašivački programi (engl. Adwere),

[10] Computer worm, Britannica, https://www.britannica.com/technology/computer-worm [7.8.2024]

[11] Conry-Murray, A., Weafer, V.: Sigurni na Internetu, Miš, Zagreb, 2005.,str. 2-50. [16] Ibid.

- kriminalni programi (engl. Crimeware)
- programi za udaljenu kontrolu i drugo.

5.1. Virusi

Računalni virusi se ubrajaju u skupinu zlonamjernog programskog koda, čija je značajna odlika sposobnost samostalnog umnožavanja, odnosno repliciranja vlastitog zlonamjernog (engl. Payload) programskog koda koji prilikom širenja na drugi računalni uređaj pronalaze program „žrtvu“ čiji će programski kod izmijeniti, mijenjaju izvorni programski kod programa „žrtve“ „inficirajući“ ga vlastitim malicioznim programskim kodom. Prema tome, virusi se samoumnožavaju (repliciraju) u drugim izvršnim datotekama (datotekama s programskim kodom) s kojima dolaze u kontakt. Virusi se najčešće s računalo na računalo prenose putem zaraženih izvršnih datoteka ili drugih datoteka koje mogu sadržavati programski kod (npr. PDF datoteka, DOCX datoteka, XLSX datoteka i drugo), poveznica (engl. Link), datoteka priloženih uz elektroničku poštu, USB stikova, računalnom mrežom i drugo. Kada korisnik pokrene zaraženu datoteku ili odabere poveznicu, virus se aktivira i započne replikaciju vlastitih kopija u datotekama računala domaćina (napadnutog računala) i time zaraženo računalo ne samo da je ugroženo zbog prisustva virusa već postaje potencijalni izvor za širenje zaraze.[12] Zbog opasnosti koje nose virusi, posebice u smislu gubitka ili zlouporabe podataka, došlo je do većeg razvitka tehnika kojima se putem programskih rješenja analizira, pronalazi i neutralizira programski kod u virusom zaraženim datotekama. Takva se programska rješenja, za sprječavanje spomenutih virusa, nazivaju antivirusna programska rješenja. Virusi u računalnim uređajima uobičajeno su "neprimjetni" za korisnika računalnog uređaja, te su korisnici uređaja izloženi zlonamjernom virusu bez njihova znanja.[13] Kako su mobilni telefonski uređaji u biti računala, njihove su datoteke podložne zarazi virusa.

[12] Conry-Murray A., Weafer V.: ibid, str. 50-53.

[13] Virusi, CERT.hr, https://www.cert.hr/virusi/ [datum pristupa:20.05.2024]

Kako bi se virusi razmnožili pokretanjem svojega koda, vežu se za izvršne datoteke programa ili za datoteke koje mogu izvršavati programski kod interpretiranjem. U tom slučaju tijekom pokretanja zaraženog programa, pokreće se istovremeno i izvršenje virusnog koda. S obzirom na način djelovanja virusa, virusi se dijele na dvije skupine. Nerezidentni se virusi nalaze samo unutar radne memorije (RAM) tijekom izvršenja programskog koda u koji je umetnut maliciozni programski kod, odnosno kada se učita i izvodi zaražena datoteka. Kada korisnik izađe iz programa, s brisanjem programa iz radne memorije briše se i virus. Nerezistentni virus je prema tome aktivan dok je aktivan u memoriji program koji je njegov nositelj. Prema tome, kod nerezistentnih virusa, uobičajeno se dio njihovog koda nalazi u zaraženim izvršnim datotekama ili datotekama koje mogu sadržavati programski kod koji se interpretira (.exe, .com, .docx, itd). Rezidentni virusi su vrsta virusa koji se nakon pokretanja programskog koda koji sadrži maliciozni kod, obično se radi o zaraženoj datoteci operacijskog sustava, postavi u radnu memoriju računala (RAM) te ostaju aktivni cijelo vrijeme u memoriji tijekom rada uređaja. Znači, završetkom rada programa putem kojeg se virus aktivirao i smjestio u radnu memoriju, programski se kod programa domaćina briše, dok programski kod virusa ostaje aktivan sve do gašenja računala kada se briše cjelokupan sadržaj radne memorije. U vremenu djelovanja virus tendira zaraziti ključne datoteke operacijskog sustava koje osiguravaju da će kod svakog pokretanja računala, kada se učitavaju datoteke operacijskog sustava i sam virus biti učitan i aktiviran. Prema tome, rezidentni virusi koriste mehanizme operacijskog sustava za svoje pokretanje, te se prilikom svakog pokretanja programske aplikacije pokreće i virusni programski kod.[14]

S obzirom na prethodno navedene informacije o virusima, njihovoj strukturi i načinima djelovanja, virusi se još dijele na tri osnovne vrste:

[14] Zlonamjerni programi-razlike, načini djelovanja, Hrvatska akademska i istraživačka mreža-CARNET,https://edutorij-admi api.carnet.hr/storage/extracted/2219325/html/433_zlonamjerni_programi__razlike_nacin_djelovanja.html [20.5.2024]

- boot sektor virusi – kopiraju svoj zlonamjerni kod u Master boot sektor i tako osiguravaju izvršenje zlonamjernog koda pri svakom pokretanju računalnog sustava,
- programski virusi – aktiviraju se pri izvršenju zaražene izvršne datoteke, najčešće s ekstenzijom .exe ili .com,
- makro virusi – virusi koji su napisani višim programskim makro jezikom, imaju mogućnost kopiranja i brisanja samih sebe, te mijenjanja dokumenata.

5.2. Crvi

Crvi predstavljaju skupinu zlonamjernih programa koji imaju svojstvo širenja svojih kopija, najčešće putem računalne mreže, na druge računalne uređaje. Crvi za razliku od virusa, ne zahtijevaju postojanje matične datoteke za svoj rad, odnosno datoteke koju će inficirati, nego su samostalni programi koji rade neovisno od drugih programa na računalnom uređaju domaćinu. Crvi se samoumnožavaju replikacijom polazne datoteke i prenose s jednog uređaja na drugi. Iako se u načelu crvi šire na način kao i virusi, kada korisnik odabere zaraženu datoteku ili poveznicu, oni su po svom djelovanju jednostavniji jer ne mijenjaju datoteke na računalu domaćinu već se postojećim datotekama na uređaju domaćinu dodaje i datoteka crva. Osim putem zaraženih poveznica i datoteka, crvi se uobičajeno distribuiraju putem Interneta i lokalnih mreža. Crv unutar računalnog uređaja koji je napadnut uobičajeno će utjecati na sigurnost računalnog uređaja domaćina. Takav računali sustav postaje „ranjiv“. Pojam “ranjiv sustav” prema Murray-u i Weafeer-u predstavlja manjak sigurnosti, tzv. pukotine, unutar operacijskih sustava računala i programskih aplikacija. Također, navedeni autori ističu kako takozvane pukotine ne sadrže dovoljnu razinu zaštite, te kroz te pukotine u zaštiti crvi mogu pristupiti ključnim dijelovima operacijskog sustava napadnutog računalnog uređaja i obaviti svoj maliciozni napad. Zaštita od crva zahtjeva ažurirane verzije programskih rješenja koje štite računalo od malicioznog programskog koda (tzv. antivirusni programi).[15]

[15] Conry-Murray A., Weafer V. : ibid.

Kao što je već navedeno, crvi se uobičajeno šire računalnim mrežama. U biti postoje dva osnovna načina širenja crva računalnim mrežama, a to su širenje bez interakcije korisnika i širenje putem socijalnog inženjeringa. Širenje se bez interakcije korisnika zbiva najčešće zbog nedostataka u sustavu sigurnosti (zaštite od malicioznog koda) na računalnom uređaju potencijalnog domaćina. Kada crv „preskoči“ sigurnosne provjere na računalu budućem domaćinu, pokreće proces vlastite instalacije na računalnom uređaju domaćinu, bez korisnikova znanja, te nakon pokretanja malicioznog programskog koda, crv će započeti ponovni proces pokušaja razmnožavanja na drugim računalnim uređajima putem računalne mreže tražeći računala s manjkavostima u sigurnosti. Drugi je način širenja crva putem tzv. socijalnog inženjeringa, što podrazumijeva interakciju s čovjekom, odnosno korisnikom, žrtvom napada. Crv se u tom slučaju korisniku predstavlja kao program koji može biti od koristi korisniku i traži od korisnika pristanak za njegovo pokretanje čime se eliminira utjecaj sigurnosnog podsustava računalnog sustava domaćina jer pristankom na njegovu instalaciju korisnik praktično sam daje dozvolu crvu da se instalira na njegovo računalo. U ovom slučaju crv iskorištava naivnost korisnika i njegovo neznanje.[16]

5.3. Špijunski programi

Špijunski programi (engl. Spyware), kao što im ime kaže su dizajnirani sa svrhom špijunaže aktivnosti korisnika. Radi se uobičajeno o programu koji je u obliku izvršnog programskog koda stoga je njihovo pokretanje i rad najčešće neprimjetno za korisnika. Prema tome špijunski programi čine skupinu nepoželjnih (zlonamjernih) programa koji uobičajeno prate aktivnosti korisnika na Internetu, Web mjesta koja posjećuje, sadržaje koji ga zanimaju i drugo. Osim praćenja aktivnosti korisnika, špijunski programi mogu dodavati i mijenjati skočne prozore (oglase) i postavke pretraživača, čime utječu na mogućnosti rada korisnika. Posebnu skupinu špijunskih programa čine programi koji

[16] O crvima, CERT.hr,https://www.cert.hr/crvi/ [20.5.2024]

[23] Conry-Murray A., Weafer V. : ibid.

prati aktivnosti odabira tipki na tipkovnici, odnosno prati što korisnik piše. Može se zaključiti kako špijunski programi koriste računalni sustav kao resurs koji omogućava skupljanje, korištenje i distribuciju privatnih informacija korisnika, te koji mogu uzrokovati promjene koje utječu na rad računalnog uređaja i privatnost i sigurnost korisnika.[23]

5.4. Oglašivački programi

Oglašivački programi (engl. Adware) predstavljaju podskup špijunskih programa koji uobičajeno nemaju mogućnost repliciranja (umnožavanja). Oglašivački se program uobičajeno implementira u internetski preglednik na način da korisniku predlaže ciljnu vrstu promocijskih oglasa, najčešće preko skočnih prozora (engl. Pop Up) tijekom pretraživanja Web stranice.

Oglašivački programi uobičajeno prate korisnikove interese tijekom pretraživanja Web prostora, te na temelju saznanja o interesu korisnika predlažu korisniku sadržaj za daljnje pretraživanje Web prostora. Osim što utječu na korisnikovo pretraživanje Web prostora prateći korisnikovu aktivnost, oglašivački programi mogu putem Interneta slati poslužiteljima informacije o korisnikovim navikama tijekom pretraživanja, kao i osobne informacije o korisniku kao što su dob, spol, lokacija i drugo. Ti podaci često se koriste za svrhe istraživanja tržišta, kao i za otkrivanje potencijalnih novih korisnika nekog proizvoda.

5.5. Trojanski konj

Trojanski je konj zlonamjerni program koji “zamaskiran” kao bezazlena aplikacija pokušava ući na računalo korisnika. Prema tome, trojanski se konj često prikazuje kao korisna programska aplikacija, te iskorištava naivnost korisnika koji daje dopuštenje trojanskom konju da se instalira na računalo koje u tom slučaju postaje domaćin. Trojanski se konj ne replicira samostalno već ga na svoje računalo mora „pustiti“ sam

korisnik.[17] Nakon instaliranja na korisnikovom računalu zadatak je trojanskog konja krađa lozinki i/ili otvaranje tzv. stražnjih vrata (engl. Back Door) koja omogućuju osobi koja stoji iza trojanskog konja ulaz na zaraženi računalni uređaj. Ulaz putem stražnjih vrata omogućavaju napadaču da putem računalne mreže pristupi zaraženom računalnom uređaju uporabom programa za udaljenu kontrolu bez korisnikova znanja te obavi željene maliciozne radnje (npr. krađu podataka). Prema tome, ako napadač ima mogućnost kontrole nad zaraženim računalnim uređajem, korisnikova privatnost i sigurnost su nezaštićeni. Također uređaj zaražen trojanskim konjem omogućava napadaču instalaciju drugih oblika zlonamjernih programa. Korisnici trebaju biti svjesni da se trojanski konj širi njihovim dopuštenjem, stoga ne trebaju preuzimati i pristati na instalaciju programa koji nisu iz pouzdanog izvora i za koje nisu sigurni što rade, otvarati privitke iz elektroničke pošte koja je stigla od nepoznatog izvora, kao i pristajati na ponude koje stižu putem Web stranica.[18]

5.6. Datoteke kolačića

Datoteke kolačića (engl. Cookies) formirane su na lokalnom računalu Web mjesta, a u njima se spremaju aktivnosti korisnika, a kroz to i korisnički interesi. U biti kolačići bi trebali biti pozitivna stvar jer programskoj aplikaciji Web mjesta pomažu u poboljšanju korisničkog iskustva. Prema tome, kolačići Web mjesta kao što su online časopisi, trgovine i slično najčešće su bezazleni za korisnika, no postoje i kolačići za praćenje (eng. Tracking cookies) koji spremaju informacije korisnika koje Web lokacije posjećuju i što je područje njihova interesa. Informacije iz takvih kolačića koriste oglašivači i poslovni subjekti koji se bave istraživanjem tržišta. Iako takvi kolačići korisnikovom uređaju neće načiniti štetu, oni utječu na privatnost jer se informacije dobivene putem kolačića koriste u oglašivačke svrhe što može iritirati korisnika prilikom pretraživanja Web prostora.[19]

---

[17] Virusi, računalni, Hrvatska enciklopedija, https://www.enciklopedija.hr/clanak/virus-racunalni [20.5.2024]

[18] Trojanski konji, CERT.hr, https://www.cert.hr/trojanski_konji/ [20.5.2024]

[19] Conry-Murray A, Weafer V. : ibid, str. 78-79.

5.7. Programi za udaljenu kontrolu

Programe za udaljenu kontrolu (engl. Rootkit) čini skup programa koji omogućuju pristup udaljenom računalu, odnosno procesima na računalu kojima nije dopušten pristup od strane neovlaštenih korisnika. Ovaj se skup programa često naziva i "špijunom u računalu". Naime, kada se program za udaljenu kontrolu instalira na računalu domaćina, on omogućava malicioznom korisniku da putem računalne mreže pristupa operacijskom sustavu računala domaćina kao administrator, što malicioznom korisniku napadaču daje potpunu kontrolu nad računalnim uređajem. Napadač praktično ima ovlasti u svakom trenutku izvršavati radnje koje želi na napadnutom uređaju i pokretati bilo koju operaciju i radnju na uređaju. Prema tome, namjena je programa za udaljenu kontrolu neovlašten pristup i zadržavanje razine kontrole zaraženog računalnog uređaja, te prikrivanje vlastitih i stranih datoteka i procesa koji se koriste u procesu obavljanja zlonamjernih aktivnosti na računalnom uređaju.[20] Korisnici ovu vrstu zlonamjernog programskog koda najčešće instaliraju slučajno na vlastito računalo. Uređaj se može zaraziti programom za udaljenu kontorlu na sljedeće načine:[21]

- na aplikacijskoj razini - najčešće trojanski konji,
- na razini sistemskih biblioteka – program za udaljenu kontrolu napada biblioteke operacijskog sustava i mijenja njihov izvršni kod u radnoj memoriji,
- na razini operacijskog sustava - unutar jezgre operacijskog sustava,
- na razini upravitelja virtualnim sadržajem,
- na razini ugrađenih programa u strojni podsustav (engl. Hardware).

Najčešće se napad na računalne uređaje odvija na način da se program za udaljenu kontrolu ugradi u jezgru operacijskog sustava (OS). U tom slučaju program za udaljenu

[20] Razvoj naprednih tehnika za izradu malwerea/rootkita, FOI, https://security.foi.hr/wiki/index.php/Razvoj_naprednih_tehnika_za_izradu_malwarea/rootkita.html [20.5.2024]

[21] Ibid.

kontrolu može mijenjati (modificirati) operacijski sustav te prilikom izvođenja malicioznih operacija prikrivati se dajući lažne povratne informacije korisniku.[22]

Razlika je između programa za udaljenu kontrolu i drugih zlonamjernih programa (npr. virusa i crva) ta da su programi za udaljenu kontrolu načinjeni tako da nisu vidljivi unutar korisničkog sučelja. Programi se za udaljenu kontrolu pretežno koriste u zlonamjerne svrhe, no postoje programi za udaljenu kontrolu koji imaju korisnu svrhu. Primjer za to su programi koji omogućavaju nadzor i upravljanje nad udaljenim računalima osobama koje su zadužene za sigurnost i održavanje računalnih sustava u poslovnim subjektima.[23]

5.8. Računalne prijevare

Pod računalnom se prijevarom podrazumijeva napad na korisnika Interneta pri kojim se lažnim ponudama dovodi korisnika u zabludu. Primjeri računalne prijevare su kupovina i plaćanje proizvoda na lažnoj Web stranici trgovca koja je u biti načinjena da bi se prevario korisnik.

Često se za pokušaje prijevare koristi elektronička pošta gdje se unutar poruke navodi korisnik da učini plaćanje radi dobivanja protu usluge (npr. dobiti će veliki iznos novaca na ime ostavštine preminulog rođaka u inozemstvu, no prvo mora platiti odvjetničke troškove). Osim navedenog, čest je slučaj potražnje i krađe osobnih podataka korisnika putem elektroničke pošte (npr. banka traži osobne podatke radi produljenja trajanja tekućeg računa). U slučajeve računalne prijevare spadaju krađa identiteta, muljaže (engl. Scam), pecanje (engl. Phishing), odnosno neželjena pošta (engl. Spam). Sve

[22] O Rootkit softveru, CERT.hr, https://www.cert.hr/rootkitovi/ [20.5.2024]

[23] Koja je razlika između Rootkita i zlonamjernog softvera, Objašnjeno.hr, https://objasnjeno.com/koja-jerazlika-izmedu-rootkita-i-zlonamjernog-softvera/ [20.5.2024]

računalne prijevare koriste naivnost i neznanje korisnika i ubrajaju se u kategoriju socijalnog inženjeringa.[24]

5.8.1. Neželjena poruka

Neželjene poruke čini skupina poruka sa svrhom izvješćivanja korisnika o stvarima koje ga (ne) zanimaju. Svaka poruka upućena korisniku, a on je ne očekuje, je neželjena poruka. No neželjene poruke se mogu u startu diferencirati na bezazlene oglašivačke poruke te na poruke koje su s malicioznom pozadinom i koje ciljaju u krajnjoj liniji na zaradu temeljem lakomislenosti korisnika. Neželjene se poruke, odnosno ponude uobičajeno šalju korisnicima putem elektroničke pošte. S obzirom da su tijekom vremena neželjene poruke postale vrlo velik problem, razvijeni su sustavi zaštite od neželjenih poruka (pošte) koji diferenciraju prave poruke od neželjenih prema pošiljatelju te prema sadržaju poruke. Takva programska rješenja sumnjive poruke odvajaju u zasebnu mapu unutar programa klijenta elektroničke pošte koji se okvirno naziva „neželjena pošta“ (engl. Junk Mail). Dvije su najčešće vrste neželjene pošte koje su malicioznog karaktera: muljaže i pecanje.[33]

Kreatori malicioznih neželjenih poruka ciljaju da putem poruke korisniku ponude primamljive sadržaje ciljajući na osnovne ljudske želje, kao što je želja za zaradom, želja za seksualnošću ili nekim drugim pripadanjem i slično. Kad je u pitanju zarada, onda se radi o ponudama jeftinih hipotekarnih kredita, kada je u pitanju seksualnost nude se pornografski sadržaj, kada je u pitanju ljepota, nude se proizvodi za poboljšavanje izgleda kao što su tablete za mršavljenje, razne kreme protiv bora, strija i slično, serumi za rast kose i drugo. Maliciozne se neželjene poruke uobičajeno “kamufliraju” u ponude slične ponudama legalnih marketinških agencija koje promoviraju proizvode. Neželjenim se porukama ponekad služe i poslovni subjekti koji nemaju maliciozne nakane, za potrebe oglašavanja, jer se radi o gotovo besplatnom obliku oglašavanja. Zbog takvih je slučajeva korisnicima teško razlikovati maliciozne

[24] Računalne prijevare, e-Građani, https://gov.hr/hr/racunalne-prijevare/1234 [2.9.2024] [33] Conry-Murray A., Weafer V. : ibid.

od nemalicioznih neželjenih poruka. Mnoge zemlje su predvidjele kazne za slanje neželjenih poruka, tako da se poslovni subjekti sve rjeđe odlučuju za ovakav oblik promocije.[25]

5.8.2. Prijevara neželjenom porukom putem muljaže

Muljažu čini maliciozna poruka čiji je sadržaj lažan, a čiji je cilj nekoga nagovoriti na davanje osobnih podataka ili na uplatu novca. Poznat je primjer muljaže s nigerijskom naftom unutar koje pošiljatelj elektroničke poruke tvrdi da posjeduje milijune dolara koje pokušava prenijeti iz Afrike, te obećava da će prenijeti dio novca primatelju poruke ako mu pošalje određenu svotu novca, izjašnjavajući se da je novac potreban za svrhu naknada. Pošiljatelj od primatelja traži bankovni broj računa, te dobivši te informacije, pošiljatelj je u mogućnosti zloupotrebljavati primateljev bankovni račun. Muljaže su prilično uspješan oblik prijevare jer iskorištavaju lakovjernost ljudi. Ovim se oblikom računalne prijevare bave pojedinci, ali i grupe ljudi i organizacije. Neki su od uobičajenih oblika muljaže nagradne igre (npr. ”sretni ste dobitnik osvojili ste 1000 eura”), oglasi za posao s “nerealnom” zaradom i savršenim uvjetima rada.[26]

5.8.3. Prijevara neželjenom porukom putem pecanja

Pecanje se koristi za krađu identiteta korisnika. U slučaju pecanja uobičajeno kreator poruke za pecanje šalje korisniku elektroničku poštu pretvarajući se da je banka ili neka druga organizacija koja upućuje korisnika da u e-mailu pošiljatelju poruke dostavi vlastite tajne podatke ili da na Web stranicama te institucije načini prijavu, dajući poveznicu na stranicu koja je izgledom identična stanici stvarne banke ili financijske institucije, no Web adresa je uobičajeno slična, ali se razlikuje u jednom ili par slova

[25] Ibid.

[26] Scam i Phishing? Što su i kako se zaštititi?, Plaviured.hr, https://plaviured.hr/vodici/scam-phishing-sto-sezastititi/ [2.6.2024]

kako bi se neoprezan korisnik „upecao“. Primjerice, PayPal i eBay su često korišteni kao krinke kreatora poruka pecanja. Maliciozne neželjene poruke pecanja najčešće od korisnika traže hitno ažuriranje podataka, bankovnih podataka, korisničkog imena i lozinki. [27] Najčešći je cilj računalne prijevare pecanjem financijska korist. Osim putem e-maila poruke namijenjene pecanju distribuiraju i platforme Whatsapp, platforme Viber te putem drugih platformi.[28]

Vrste su poruka za pecanje:[39]

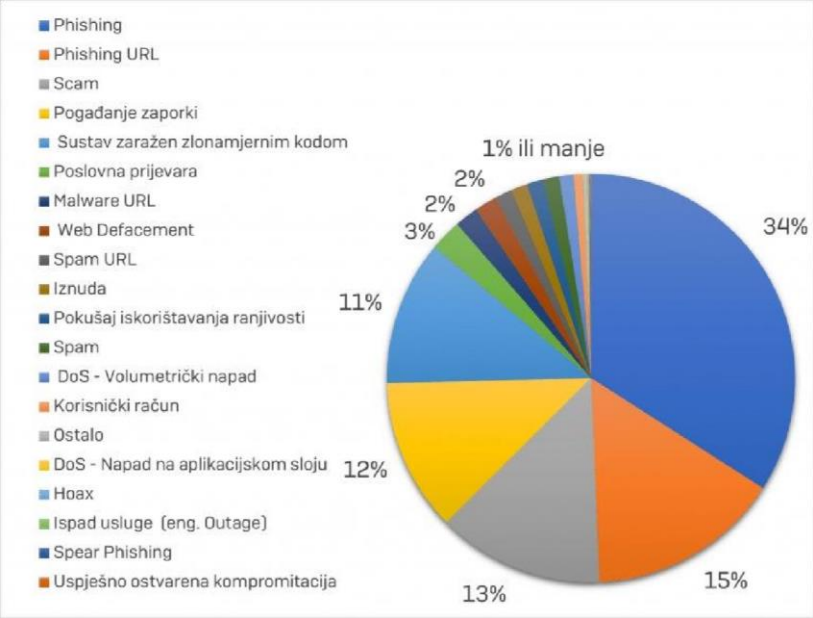
- jednostavni zahtjev - pošiljatelj se lažno predstavlja kao institucija, te u odgovoru na pošiljateljevu poruku traži od korisnika upis osobnih podataka,
- zlonamjerne poveznice - putem e-pošte pošiljatelj šalje korisniku poveznicu koja odabirom vodi na zlonamjernu Web stranicu. Zlonamjerne stranice se od ispravnih (legitimnih) stranica mogu razlikovati u jednom slovu ili znaku u Web adresi,
- zlonamjerna Web stranica - često pomoću “krinke” izgleda kao legitimna Web stranica neke institucije, banke, internetske trgovine, a napadači skupljaju osobne podatke korisnika u cilju ostvarivanja financijske koristi i ostalih zlonamjernih radnji,
- zlonamjerni skočni prozori na legitimnim stranicama - najčešće sadrže polja za upis osobnih podataka,
- hvatanje otvorenih kartica (engl. Tabnabbing) – iskorištava situaciju kada korisnik ima otvoreno više kartica u Web pregledniku da jednu od neaktivnih kartica (engl. Tab) osvježi s sadržajem zlonamjerne Web stranice.

[27] Phishing napadi – kako ih prepoznati i zaštititi se, azop, https://azop.hr/phishing-napadi-kako-ih-prepoznati-izastititi-se/ [7.9.2024]

[28] Phishing, Techtarget , https://www.techtarget.com/searchsecurity/definition/phishing [2.6.2024] [39] Ibid.

6.PRIMJER SIGURNOSNIH INCIDENATA U REPUBLICI HRVATSKOJ ZA 2023. GODINU

Prema istraživanju CERT-a u 2023. godini: „U Hrvatskoj se bilježi smanjenje broja računalnosigurnosnih incidenata za 4,63 posto u odnosu na 2022.godinu. Nadalje, došlo je do porasta incidenata zlonamjernih softvera. Napadi zasnovani na novim tehnikama, poslužili su za lakše iskorištavanje građana, odnosno financijske koristi. Na udaru se našao povrat poreza, razne subvencije za troškove stanovanja, te prelazak na euro valutu."[29] Slika 3. prikazuje prethodno navedene tvrdnje. Krađa identiteta pecanjem i muljaže su najzastupljeniji oblici računalnih prijevara u Republici Hrvatskoj u 2023. godini.



Slika 3 Prikaz sigurnosnih incidenata u RH za 2023.godinu

Izvor: Godišnji izvještaj rada, CERT.hr , https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2023godinu/

[29] Godišnji izvještaj rada, CERT.hr , https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2023godinu/ [datum pristupa:20.04.2024]

7.NAČINI ZAŠTITE PRIVATNOSTI KORISNIKA TE NAČINI ZAŠTITE KORISNIKA OD MALICIOZNIH NAPADA

Kao što je već navedeno korisnici su Interneta, kao i mobilnih programskih aplikacija, pod učestalim rizikom od ugroze njihove privatnosti i pod učestalim rizikom od malicioznih napada bilo u vidu malicioznog programskog koda ili u vidu malicioznih pokušaja prevare. Kako bi se korisnika zaštitilo od ugroze privatnosti i malicioznih napada u praksi se koriste programska rješenja koja štite računalne uređaje, pa prema tome i mobilne telefonske uređaje, od navedenih oblika ugroza. Među osnovna programska rješenja za zaštitu privatnosti i sigurnosti korisnika od malicioznih napada ubrajaju se programska rješenja koja se generalno nazivaju vatrozid (engl. Firewall) te tzv. antivirusni programi koji u biti ne štite samo od virusa već i drugih malicioznih programskih napada.

Vatrozid se može definirati kao programsko, odnosno strojno-programsko rješenje koje se postavlja između vanjske računalne mreže (Interneta) i lokalne mreže ili samog računalnog uređaja, a čiji je primarni zadatak nadzor mrežnog prometa kako bi se odstranio i/ili spriječio prodor potencijalnog ili stvarnog prometa podataka s malicioznim sadržajem. Prema tome, vatrozid je program koji filtrira i regulira komunikacijske tijekove između globalne mreže i lokalne mreže, odnosno računalnog uređaja. U tom se smislu provjerava promet koji dolazi putem Web servisa, elektroničke pošte, baza podataka, te drugih oblika komunikacije putem globalne računalne mreže. Kako bi se zaštitila korisnikova sigurnost i privatnost potrebno je redovito ažuriranje programskog sustava vatrozida. Vatrozid traži dopuštenje svake promjene na uređaju (instaliranje aplikacija, programa itd.) na način da blokira sav promet i dobre i loše programe, te je potrebno dopuštenje korisnika za obavljanje bilo koje radnje koja može omogućiti ugrozu podacima koji dolaze putem globalne računalne mreže..[30]

[30] Conry-Murray A., Weafer V.: ibid, str. 27-44.

Antivirusni su programi koristan alati za otkrivanje zlonamjernog programskog koda. Načelno antivirusni programi rade na principu detekcije virusa i drugih malicioznih programa ili dijelova programskog koda na način da uspoređuju programski kod koji se pokreće na računalnom uređaju s onim iz vlastite baze podataka, koja sadrži bitna obilježja programskog koda poznatih malicioznih programskih rješenja te u slučaju otkrivanja malicioznog programskog koda pokušava taj programski kod odstraniti iz zaražene datoteke, a ako je ta radnja nemoguća blokira pokretanje zaraženog programskog rješenja. Suvremeni antivirusni programi koriste se i tehnikama strojnog učenja (umjetne inteligencije) kako bi poboljšali detekciju i predikcijom spriječili djelovanje malicioznog programskog koda i prije no što je on službeno otkriven i ažuriran, odnosno zapisan u bazi podataka antivirusnog programa. Glavna je mana ovih programa ta što u slučajevima pojave novog malicioznog programskog koda moguće je da i uz ugrađenu umjetnu inteligenciju u antivirusno rješenje, antivirusni program ne prepozna maliciozni programski kod. Da bi se smanjili rizici od malicioznog koda i drugih oblika ugroze u praksi se kombinira uporaba antivirusnog programa s vatrozidom.[31]

Prema preporukama portala Duplico.IO kako bi se zaštitila korisnikova privatnost i sigurnost na Internetu bitno je:[32]

- korištenje snažnih lozinki za korisničke račune (dodavanje velikog i malog slova, brojeva i znakova unutar lozinke),
- oprez pri dijeljenju osobnih podataka,
- zaštita internetske veze virtualnom privatnom mrežom (engl. Virtual Private Network), predstavlja skrivanje privatnih internetskih mreža (engl. IP address),
- redovito ažuriranje programa,

[31] Ibid.

[32] Sigurnost na Internetu: 5 pravila kako zaštititi privatne podatke, Duplico.IO, https://duplico.io/sigurnost-nainternetu-5-pravila-kako-zastititi-privatne-podatke/ [3.6.2024]

- oprez pri uporabi internetskih tražilica i preglednika, novo uvedena je mogućnost anonimnog pretraživanja tražilice tijekom kojega platforma ne prati korisnikovu aktivnost,
- oprez prilikom preuzimanja datoteka i odabira poveznica (engl. Link),
- kritičko pregledavanje raznih ponuda (često neželjenu poštu), te ne nasjedanje na sumnjive ponude.

8.EUROPSKA ODREDBA O ZAŠTITI OSOBNIH PODATKA

Kada su u pitanju Europske direktive osobni su podaci korisnika: korisnikovo ime i prezime, ulica i broj stanovanja, mjesto stanovanja, e-mail adrese, broj telefona, broj identifikacijskih dokumenata, internetska adresa, oznake kolačića Web stanica, podaci o medicinskoj skrbi osobe (liječnika). Kako bi se pospješilo i smanjilo dovođenje korisnika u probleme glede privatnosti i sigurnosti, Europsko vijeće donijelo je odluku o zaštiti podataka korisnika aplikacija u Europskoj Uniji. Prema odredbi Europskog vijeća za zaštitu podataka, zaštita osobnih podataka korisnika postaje temeljno pravo.[33] Europska Unija je donijela, potpisivanjem ugovora u Lisabonu 2007. godine, temeljno pravo o zaštiti podataka. Naime, ovaj se dokument temelji na Povelji Europske Unije o temeljnim ljudskim pravima, kojom je određeno, u 8.članku povelje, da svaki korisnik (osoba) ima pravo na zaštitu svojih osobnih podataka, te pristup prikupljenim podacima i pravo na izmjenu (ispravljanje) podataka.[34] Slika 3. zorno prikazuje elemente te uredbe.

[33] Zaštita podataka u EU, Vijeće Europse unije, https://www.consilium.europa.eu/hr/policies/data-protection/ [22.4.2024]

[34] Povelja o temeljnim pravima Europse unije Vijeće, Europse unije, https://fra.europa.eu/hr/eucharter/title/title-ii-freedoms [22.4.2024]

Slika 4. Uredba Europske Unije o zaštiti osobnih podataka[35]

Izvor: Prikaz uredbe o zaštiti podataka , EU vijeće, https://fra.europa.eu/hr/eu-charter/title/title-ii-freedoms

Kako je iz slike 4. vidljivo, za svaku obradu podataka od treće stane (osobe koja nije vlasnik podataka) potreban je jasan razlog i pristanak za obradu podataka od osobe o čijim se osobnim podacima radi. Ova odredba onemogućava trećim stranama pristup korisničkim podatcima za svoje svrhe. Korisnik ima pravo na obavijest u slučaju ako su njegovi osobni podaci ugroženi. Ova odredba znači olakšan i smanjen obujam mogućih nepoželjnih događaja za vlasnika podataka (krađe, neovlaštena uporaba).

[35] Prikaz uredbe o zaštiti podataka , EU vijeće, https://fra.europa.eu/hr/eu-charter/title/title-ii-freedoms [22.4.2024]

9.NAJVAŽNIJI OPERACIJSKI SUSTAVI ZA PAMETNE MOBILNE TELEFONSKE UREĐAJE

Operacijski sustav (engl. Operating System - OS) čini skupina programa koja je poveznica između strojnog dijela i korisničkih programa te između strojnog dijela i korisnika, stoga, operacijski sustavi omogućavaju korisniku uporabu računalnog uređaja. Paljenjem se računala prvo pokreće operacijski sustav. Svrha je operacijskog sustava upravljanje radom svih sklopova računala kao i vanjskih uređaja spojenih na računalni uređaj. Suvremeni su operacijski sustavi korisnički orijentirani. Korisnički orijentiran operacijski sustav je tako dizajniran da korisniku uporabu računalnog uređaja učini lakšom. Različiti operacijski sustavi mobilnih telefonskih uređaja imaju jedinstvene značajke i dizajn.[36]

Danas su najkorišteniji operacijski sustavi mobilnih telefonskih uređaja iOS i Android. Oba operacijska sustava dostupna su na tržištu od 2007. godine. Godine 2009. na globalnom tržištu dominirao je operativni sustav Symbian. Symbian je bio operacijski sustav tada popularnih Nokia telefona. S vremenom je došlo do slabljenja popularnosti Symbian operacijskog sustava, te su Andorid i iOS zauzeli prvo mjesto popularnosti na globalnom tržištu. Od tada, u usporedbi s drugim operacijskim sustavima, Android i iOS operacijski sustavi za pametne mobilne telefonske uređaje i tablet računala, broje većinu korisnika na globalnom tržištu. Razlika je između iOS i Android operacijskih sustava u tome što iOS operacijski sustav, proizvođača Apple, ima manju fleksibilnost i ranjivost sustava, zbog zatvorenog programskog koda, dok je Android operacijski sustav otvorenog programskog koda i stoga je ranjiviji od iOS operacijskog sustava. Otvoren programski kod podrazumijeva javnu objavu izvornog programskog koda što olakšava s jedne strane razvoj programskih aplikacija, ali i pruža mogućnost lakšeg

---

[36] Uloga operacijskog sustava u radu računalnog sustava, različiti operacijski sustavi za različite digitalne uređaje, Carnet.hr, https://edutorij-admin-api.carnet.hr/storage/extracted/c4e1aebf-48e0-4d92-b6a90716a4e1c740/html/405_uloga_operacijskog_sustava_u_radu_racunalnoga_sustava_razliciti_operacijski_sus tavi_za_razlicite_digitalne_uredaje.html [9.6.2024]

[48] Ibid.

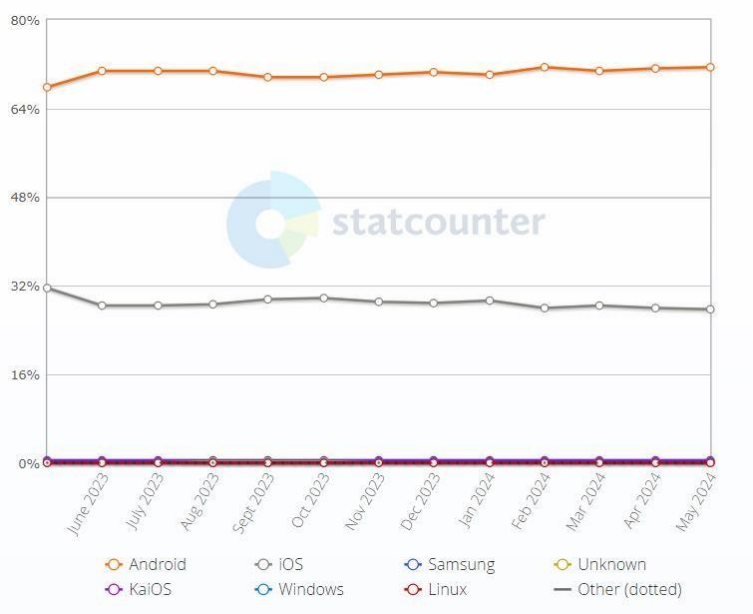
pronalaska manjkavosti u kodu koji mogu iskoristiti oni koji kreiraju maliciozni programski kod.[48]

Novi podaci za svibanj 2024. godine pokazuju tržišnom udjele mobilnih operacijskih sustava globalno prema portalu Statcounter:[37]

3. Android 71.5%,
4. iOS 27.73%,
5. Samsung 0.38%,
6. Windows 0.02%.

Andorid operacijski sustav drži prvo mjesto na svjetskom tržištu najviše korištenih mobilnih operacijskih sustava. Apple-ov iOS zauzima drugo mjesto. Navedeni su podaci prikazani na grafu 1.

[37] Mobile Operating System Market Share Worldwide, Statcounter, https://gs.statcounter.com/os-marketshare/mobile/worldwide [8.6.2024]



Graf 1. Tržišni udio operacijskih sustava za mobilne telefonske uređaje

Izvor: Mobile Operating System Market Share Worldwide, Statcounter, https://gs.statcounter.com/os-marketshare/mobile/worldwide

Portal Statcounter objavljuje također statističke podatke za Republiku Hrvatsku. U Republici Hrvatskoj također najkorišteniji mobilni operacijski sustav je Android, koji broji 78,09% udjela, te iOS koji broji 20,71% udjela u ukupnom broju mobilnih operacijskih sustava Republike Hrvatske.[38]

S obzirom na popularnost mobilnih telefona i rasprostranjenost mobilnih telefonskih programskih aplikacija napadači traže prilike za krađu podatka korisnika, prevare korisnika i za izvlačenje financijske koristi. Napadačima se otvaraju šanse zbog propusta mrežnih trgovina za mobilne aplikacije kao i manjkavosti u programskom kodu kako mobilnih programskih aplikacija tako i operacijskih sustava namijenjenih mobilnim telefonskim uređajima.[39]

[38] Mobile Operating System Market Share Croatia, ibid.
[39] Markota, K.: Svjesnost korisnika o čimbenicima rizika prilikom korištenja mobilnih aplikacija, završni rad, Sveučilište Josipa Juraja Strossmayera u Osijeku, fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Osijek, 2018., str. 3-4.

9.1. Sigurnost i privatnost Andoroid operacijskog sustava

Android je operacijski sustav tvrtke Google. Prema Markoti Android operacijski sustav sadrži nekoliko servisa namijenjenih za sigurnost, a to su:[40]

- protuvirusna zaštita i provjera aplikacija,
- zaštita od mrežnih i aplikacijskih prijetnji,
- sigurno pregledavanje mrežnih stranica,
- upravitelj Android uređaja
- pametno zaključavanje uređaja.

Primjerice, kako bi se povećala sigurnost operacijskog sustava Android Google je 2017. godine poboljšao enkripciju podataka i uveo veći broj sigurnosnih zakrpa u svoj operacijski sustav. Uz to, računalstvo u oblaku (engl. Cloud Computing) Andorid operacijskog sustava pruža veću sigurnost korisničkih podataka jer se korisnički podaci kopiraju u oblak i time se smanjuje mogućnost gubitka podataka. Opciju sigurne mreže (engl. Safety Net) Google je uveo 2013. godine. Ova opcija štiti od mrežnih i programskih prijetnji, te pospješuje zaštitu u oblaku. Zbog sve većih je prijetnji od krađe identiteta i zlonamjernih napada Google već 2005. godine uveo provjere mrežnih stranica.[41]

9.2. Sigurnost i privatnost iOS operacijskog sustava

Prema Markoti: “Sustav sigurnosti na Appleovim uređajima konstruiran je tako da su programska podrška i sklopovlje osigurani kroz ključne komponente svakog iOS uređaja”[42]. Apple je za svoje uređaje osigurao zaštitu korisnika na principu koji

[40] Ibid, str. 6.

[41] Ibid, str. 6-7.

[42] Ibid, str. 4.

podrazumijeva da je svaki korak od paljenja do instaliranja novih (vanjskih) programskih aplikacija nadziran. Apple-ovi iTunes alati zaduženi su za nadopune zaštite te za programsku podršku iOS operacijskom sustavu. Nadogradnja se iOS operacijskog sustava obavlja na način da se mobilni telefonski uređaj spaja na iTunes koji se nalazi na Apple-ovom poslužitelju, a poslužitelj šalje mobilnom telefonskom uređaju kriptirane podatke u vidu instalacijskog paketa. Keychain Services se koristi za spremanje sigurnosnih podataka, odnosno spremanje ključeva, lozinki, certifikata. Podatci se šifriraju (kriptografska funkcija) i spremaju (pohrana podataka u datoteke) u biblioteku CommonCrypto koja sadrži razne kriptografske algoritme. Certificate, Key and Trust Service također koriste biblioteku CommonCrypto i upravljaju certifikatima i nizovima ključeva (engl. Keychain), šifriranjem i potpisivanjem podataka. Zadnje sigurnosno sučelje predstavlja Randomization Services dio koji je zadužen za kreiranje slučajnih brojeva.[43]

Još neke bitne značajke sigurnosti iOS operacijskog sustava su:[44]

- promjena lozinke,
- omogućavanje ili neomogućavanje provjere ID preko dodira prsta i prepoznavanja lica,
- dodavanje ili brisanje otiska prsta,
- ponovno postavljanje ID putem prepoznavanja lica te
- brisanje cijelog sadržaja i postavki.

[43] Sigurnost operacijskog susrava iOS, Cis.hr, https://www.cis.hr/files/dokumenti/CIS-DOC-2011-09-024.pdf [12.6.2024]

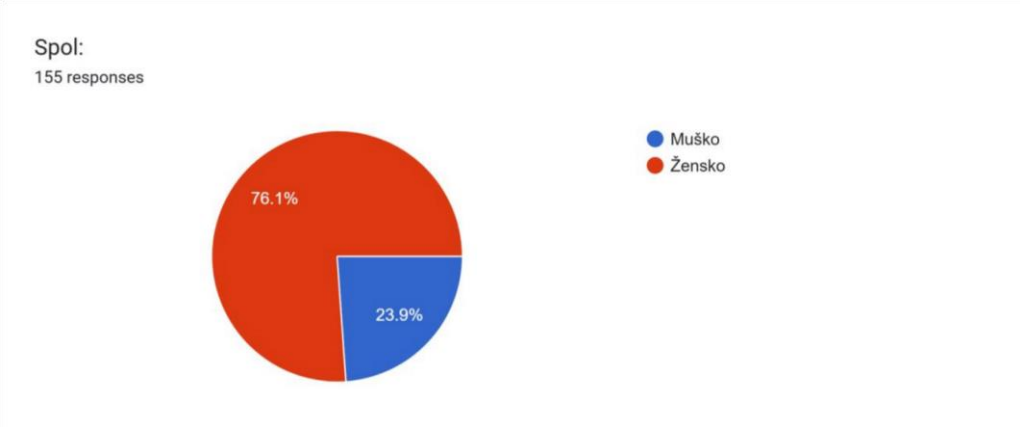
[44] Markota K.: ibid.

10. REZULTATI PRIMARNOG ISTRAŽIVANJA

Primarno je istraživanje provedeno prikupljanjem podataka od strane ispitanika vezano uz korisnička znanja o opasnostima glede privatnosti i sigurnosti podataka korisnika. Uzorak su činili ispitanici različitih dobnih granica. Upitnik je načinjen uporabom Web aplikacije Google obrasci. Kako bi se prikupio tražen broj ispitanika upitnik je proslijeđen putem društvenih mreža (Facebook, Instagram, WhatsApp, Viber) u razne grupe korisnika, te u grupe studenata. Prikupljeno je ukupno 155 ispitanika raznih dobnih granica.

Provedeni je upitnik sastavljen od dvije skupine pitanja. Prvu su skupinu činila demografska pitanja. Drugom su se skupinom pitanja ispitivala znanja i stavovi ispitanika vezani za sigurnost i privatnost vezanu uz uporabu mobilnih telefonskih uređaja. Ispitivanje je provedeno anonimno.

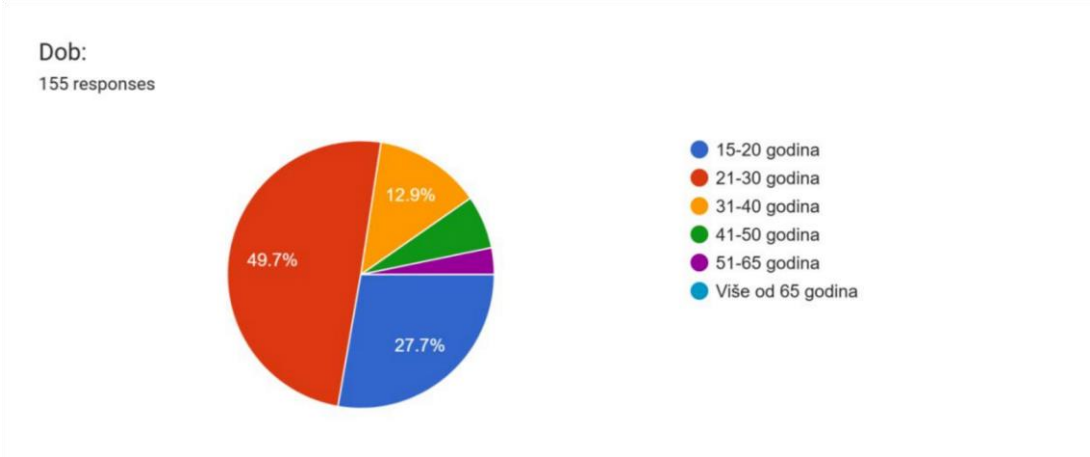
Prvo se pitanje iz upitnika odnosilo na spol ispitanika. Distribucija je odgovora na prvo pitanje prikazana grafom 2.



Graf 2. Struktura ispitanika prema spolu

Izvor: anketni upitnik

Kako je iz grafa 2. vidljivo, od ukupno 155 ispitanika, ženskih je ispitanika 76,1%, odnosno 118 osoba, dok je 23,9% muških ispitanika, odnosno 37 ispitanika. Grafom 3. prikazana je struktura ispitanika prema dobi.

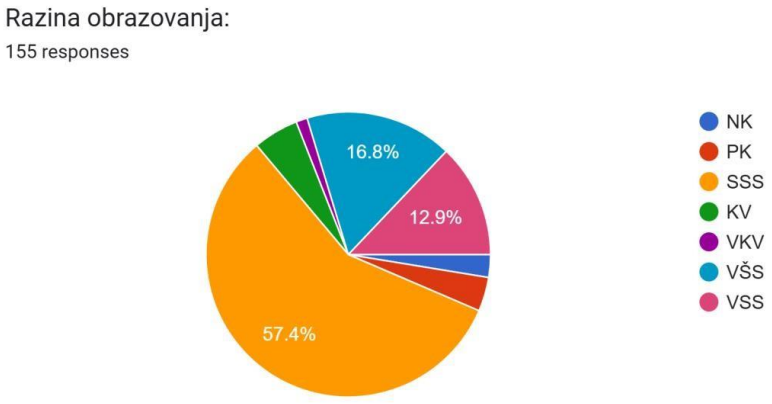


Graf 3. Struktura ispitanika prema dobi

Izvor: anketni upitnik

Kao što je iz grafa 3. vidljivo u strukturi ispitanika prevladavaju mladi ispitanici, posebice oni između 21. i 30.(49.7%) godine života. Najveći broj ispitanika su studenti ekonomskog fakulteta.

Strukturu ispitanika prema obrazovanju prikazuje graf 4.



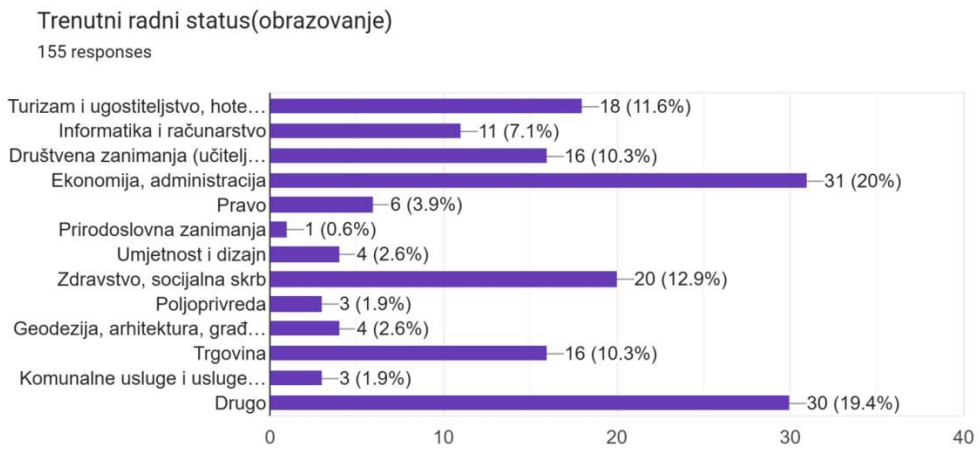
Graf 4. Struktura ispitanika prema razini obrazovanja

Izvor: anketni upitnik

Kao što je vidljivo prema grafu 4. više od polovine ispitanika (57.4%) je navelo SSS (srednju stručnu spremu) kao svoju razinu obrazovanja. VŠS (višu školsku spremu) je navelo 16.8% ispitanika. Najveći je broj ispitanika srednje stručne spreme jer je u strukturi ispitanika najveći broj studenata.

Ispitivalo se i mjesto stanovanja. Najviše je ispitanika odgovorilo da stanuju u gradu (67.7%).
Nadalje, ispitivalo se rade li ispitanici ili ne. U strukturi ispitanika 78 osoba je odgovorilo da je zaposleno, 78 osoba nezaposleno i 2 osobe su u mirovini.

Također, ispitivao se i radni status ispitanika,te obrazovanje ispitanika koji trenutno nisu u radnom statusu (zaposleni), što je prikazano grafom 5.

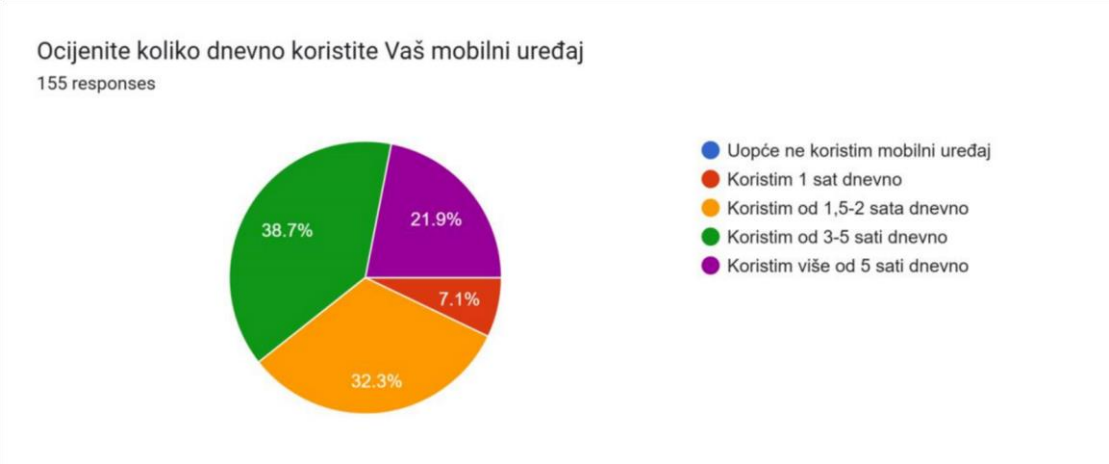


Graf 5. Struktura ispitanika prema radnom statusu ili obrazovanju

Izvor: anketni upitnik

Kako je vidljivo iz grafa 6. većina ispitanika radi ili se obrazuje u polju ekonomije i administracije.

Nadalje, istraživanja su dala odgovor na postavljeno pitanje: „Koliko sati dnevno koristite svoj mobilni telefonski uređaj?”. Rezultati distribucije odgovora na ovo pitanje prikazani su na grafu 6.

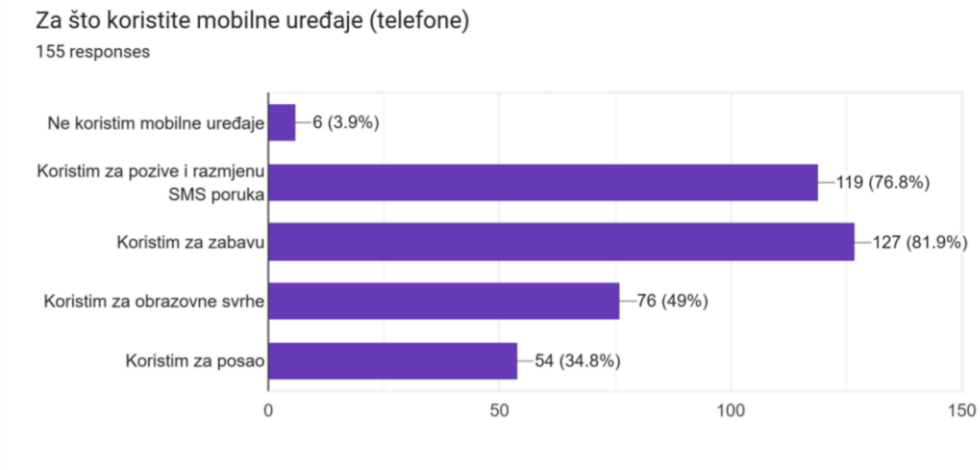


Graf 6. Struktura odgovora ispitanika vezana za dnevnu uporabu mobilnih telefonskih uređaja

Izvor: anketni upitnik

S obzirom na navedeno postavljeno pitanje o dnevnoj uporabi mobilnih telefona, odgovori prikazani grafon 6. prikazuju da većina ispitanika (32.3%) koristi mobilni telefonski uređaj između 1.5 i 2 sata dnevno, te 38.7% ispitanika koristi mobilni telefon između 3 i 5 sati dnevno. Svi ispitanici anketnog upitnika koriste mobilni telefonski uređaj svakodnevno.

Distribucija odgovora ispitanika na pitanje o svrsi uporabe mobilnog telefona prikazuje graf 7.



Graf 7. Distribucija odgovora ispitanika o svrsi uporabe mobilnih telefonskih uređaja

Izvor: anketni upitnik

Iz grafa 7. je vidljivo da se najučestalije mobilni telefoni koriste za zabavu i razgovore, odnosno razmjenu SMS poruka, nešto manje za obrazovne svrhe te posao. Ovakva se distribucija odgovora može objasniti strukturom ispitanika u kojoj je najveći broj ispitanika iz populacije mlađe životne dobi. Nadalje se istraživala dnevna uporaba popularnih programskih aplikacija na mobilnim telefonima od strane ispitanika. Struktura je prikazana tablicom 1.

	Ne koristim	Po potrebi (par puta tjedno, ne svaki dan)	Koristim 30 minuta dnevno	1-2 sata dnevno	2-4 sata dnevno	Više od 5 sati dnevno
WhatsApp	19	44	40	32	16	4
Viber	33	66	33	16	7	0
Gmail	10	113	22	6	4	0
Google karte (Maps)	25	110	15	5	0	0
Instagram	18	15	46	52	20	4
Facebook	40	51	35	20	8	0
YouTube	17	42	39	32	17	8
Snapchat	77	19	29	15	12	3
Twitter (X)	119	13	14	7	2	0
TikTok	61	20	24	22	21	7
Amazon shopping, Temu, e Bay	73	62	15	3	2	0
Bolt, Glovo dostava	92	47	12	2	2	0
Booking, Airbnb	106	34	9	3	3	0
Microsoft 365 alati	68	52	21	7	5	2
Pinterest	78	53	14	8	2	0

Tablica 1. Struktura odgovora ispitanika o dnevnoj uporabi programskih aplikacija i alata na mobilnim telefonima

Izvor: anketni upitnik

Kako je iz tablice 1. vidljivo, najučestalije se koriste programske aplikacije za komunikaciju, kao i programske aplikacije za društveno umrežavanje.

Nakon pitanja o učestalosti uporabe mobilnih aplikacija, slijedilo je pitanje o operacijskom sustavu mobilnog telefonskog uređaja. Svaki ispitanik koji koristi mobilni telefonski uređaj, trebao je odabrati koji operacijski sustav koristi. Prema dobivenim rezultatima 60.6% (94 ispitanika) koristi Android operacijski sustav, te 39.4% (61 korisnik) koristi iOS operacijski sustav.

U skupini pitanja kojima se provjeravalo znanje ispitanika vezano za sigurnost uporabe mobilnih telefona postavljeno je pitanje: „Virusi, crvi, trojanski konji nazivaju se Malware?". Najviše je ispitanika na ovo pitanje odgovorilo da ne zna. Nadalje, pitano je ispitanike prate li kolačići (engl. Cookies) korisnikovu aktivnost na Web stranicama. Većina je ispitanika odgovorila potvrdno, odnosno točno. Po pitanju sigurnosti operacijskih sustava, ispitanici su za Android operacijski sustav i iOS operacijski sustav većinom odgovorili da nisu sigurni operacijski sustavi. Nadalje, pojam „pecanje" (engl. Phishing) većini ispitanika nije bio poznat, dok je pojam „muljaže" (engl. Scam) većini ispitanika bio poznat pojam. Na kraju opet je ponovljeno prvo pitanje vezano uz maliciozne napade (engl. Malware), većina ispitanika nije znala odgovor. Na pitanje vezano uz pojavu zlonamjernog programskog koda na mobilnom telefonskom uređaju većina je ispitanika odgovorila da nikada na njihov uređaj nije došao zlonamjerni programski kod.

Sljedećom se skupinom pitanja željelo utvrditi znanje ispitanika o sigurnosti izvršenja određenih radnji na mobilnom telefonskom uređaju. Na pitanje o pohrani lokacije, adrese stanovanja, e-mail adresa, broja telefona i upisivanja bankovnih podataka unutar Web-a i aplikacija većina je ispitanika dala odgovor da nije sigurno. Pitanje vezano za sigurnost pohrane podataka u računalnom oblaku (engl. Cloud) te pitanje sigurnosti uporabe mikrofona i kamere rezultiralo je odgovorima iz kojih se vidi kako većina ispitanika ne zna je li sigurno. Korisnici općenito nisu upoznati u potpunosti kako računalni oblak funkcionira i gdje njihove fotografije i informacije ostaju, te tko ih može upotrijebiti. S obzirom da većina ispitanika koristi društvene mreže postavljeno je pitanje koje traži mišljenje ispitanika o sigurnosti uporabe popularnih društvenih mreža:

Facebooka, Instagrama i TikToka. Glede sigurnosti za Instagram platformu većina ispitanika je dala ocjenu 3. O sigurnosti Facebook-a i TikTok-a većina ispitanika nije znalo odgovor. Naposljetku postavljeno je pitanje što ispitanici misle o sigurnosti pretraživanja Interneta i odabira promidžbenih stranica na Web-u te o iskočnim (engl. Pop-Up) prozorima. Glede pretraživanja Interneta, većina ispitanika nije bila sigurna je li u tom slučaju njihova sigurnost ugrožena. Što se tiče odabira promidžbenih programa i iskočnih prozora većina ispitanika smatra da to uopće nije sigurna aktivnost. Pitanja i dobiveni odgovori prikazani su u tablici 2.

	Ne znam	Uopće nije sigurno	2	3	4	Potpuno sigurno
Pohrana podataka vaše lokacije unutar aplikacija	32	46	36	29	7	5
Upisivanje bankovnih podataka u aplikacijama/ na Web-u	29	61	28	22	10	5
Uporabu mikrofona i kamere tokom uspostave poziva i videopoziva	34	31	26	30	22	12
Upisivanje adrese stanovanja, e-mail adresa i broja telefona na Internetu	29	50	32	29	11	4
Pohrana informacija i fotografija na Cloudu (Oblak)	34	30	30	23	24	14
Uporaba društvenih						

mreža	28	33	33	33	20	8
Uporaba Facebooka	35	32	30	35	17	6
Uporaba Instagrama	31	32	29	40	17	6
Uporaba TikToka-a	40	35	29	27	18	6
Pretraživanje Interneta (internetskih pretraživača)	33	31	34	29	18	10
Odabir promidžbenih sadržaja na web stranicama i skočnim prozorima (pop-up)	38	48	37	19	9	4

Tablica 2. Struktura odgovora ispitanika o sigurnosti izvršavanja radnji na mobilnom telefonu

Izvor: anketni upitnik

Generalno gledano, dobiveni rezultati provedenog primarnog istraživanja ukazuju kako korisnici u značajnom obujmu koriste mobilne telefonske uređaje, najviše za komunikaciju i društveno umrežavanje, no slabo poznaju tehnologiju kojom se služe, posebice s aspekta sigurnosti i privatnosti uporabe ove tehnologije. Dobiveni rezultati primarnim istraživanjem upućuju na potrebu osvješćivanja postojanja ovog problema te na potrebu sustavnog pristupa obrazovanja ljudi kada su u pitanju sigurnost i privatnost prilikom uporabe mobilnih telefonskih uređaja.

11.ZAKLJUČAK

Evidentno je kako se informacijsko-komunikacijska tehnologija u posljednjih tridesetak godina izrazito brzo razvija. Ona je postala pokretač cjelokupnog društvenog razvitka tako da je pod njenim utjecajem došlo do velikih promjena u načinu funkcioniranja kako pojedinaca tako i društva u cjelini. Također je evidentno da se društvo u mnogim svojim segmentima nedovoljno brzo mijenja i ne uvažava promjene koje donosi suvremena informacijsko-komunikacijska tehnologija. Primjerice, iskustveno se može konstatirati kako sustavan pristup reformi obrazovnog sustava koji bi prihvatio promjene i koncentrirao se na pripremu ljudi za sustavno prihvaćanje i uporabu novih tehnologije u Republici Hrvatskoj nije načinjen, a vjerojatno niti u većini svijeta. To dovodi do kaotičnog stanja koje otvara mogućnost nepravilne, odnosno nesigurne uporabe suvremenih informacijsko-komunikacijskih tehnologija, osobito pametnih mobilnih telefonskih uređaja, koji su danas neizostavni pratitelj gotovo svake osobe. Prema tome, usporedno s rastom popularnosti pametnih mobilnih telefonskih uređaja rastu i problemi koji su vezani za sigurnost od malicioznog koda kojim se ugrožava sigurnost uporabe ovih uređaja kao i problemi vezani za privatnost korisnika pametnih mobilnih telefonskih uređaja. Kako se radi o vrlo dinamičnom procesu kojemu globalno raste značaj, fokus je provedenog istraživanja, čiji su rezultati prikazani u ovom radu, bio je usmjeren na rizike privatnosti i sigurnosti korisnika prilikom uporabe pametnih mobilnih telefonskih uređaja, odnosno programskih aplikacija koji su uobičajeno instalirane na pametnim mobilnim telefonskim uređajima ili kojima se pristupa putem pametnih telefonskih uređaja uporabom Interneta.

Iz rezultata dobivenih provedenim istraživanjima sekundarnih, tercijarnih i kvartarnih izvora informacija i znanja vidljiv je s jedne strane rast obujma uporabe pametnih mobilnih telefonskih uređaja te pripadajućih programskih aplikacija, kako u svijetu tako i u Republici Hrvatskoj te s druge strane širok spektar ugroza, bilo u domeni sigurnosti, bilo u domeni privatnosti uporabe pametnih mobilnih telefonskih uređaja. Temeljem provedenih primarnih istraživanja anketiranjem, u kojima je sudjelovala pretežito mlađa, obrazovno aktivna populacija ispitanika, koja vrlo intenzivno koristi suvremenu mobilnu telefonsku tehnologiju, posebice za potrebe komunikacije i društvenog

umrežavanja, može se zaključiti kako su znanja vezana za sigurnu uporabu navedene tehnologije izrazito niska što objektivno otvara vrata uspjehu onih koji čine napore vezane za ugrozu sigurnosti i privatnosti korisnika naprednih mobilnih telefonskih uređaja.

Slijedom rezultata dobivenih provedenim istraživanjima, može se zaključiti kako je potrebno sustavno pristupiti problemu obrazovanja ljudi za uporabu suvremene pametne mobilne telefonske tehnologije. To podrazumijeva uvođenje obuke za stjecanje znanja i vještina vezanih za uporabu suvremene mobilne pametne telefonske tehnologije u planove i programe svih razina obrazovanja, kao i otvaranje tečajeva na kojima bi se mogla, u okviru cjeloživotnog obrazovanja, nadopunjavati znanja i vještine vezane za uporabu suvremene pametne mobilne telefonske tehnologije. Upravo na sadržaje predmeta koji bi se bavili znanjima i vještinama potrebnim za sigurno i optimalno korištenje suvremene pametne mobilne tehnologije, trebala bi se usmjeriti daljnja istraživanja. Također, ovakva bi se istraživanja trebala provoditi permanentno kako bi se sustavno pratila znanja stanovništva vezana za sigurnost i privatnost uporabe pametnih mobilnih telefona. Prema tome, permanentno obrazovanje vezano za uporabu pametnih mobilnih telefona, kao i permanentno (periodično) istraživanje znanja veznih za sigurnu uporabu suvremene pametne mobilne telefonske tehnologije predstavlja put i načelan model za osiguranje privatnosti i sigurnosti korisnika prilikom uporabe pametnih mobilnih telefona.

11. LITERATURA

1. Computer worm, Britannica, https://www.britannica.com/technology/computer-worm [7.8.2024]
2. Conry-Murray, A., Weafer, V.: Sigurni na Internetu, Miš, Zagreb, 2005.
3. Digital 2020, Global digital overview , https://datareportal.com/reports/digital-2020global-digital-overview [3.5.2024]
4. Godišnji izvještaj rada, CERT.hr , https://www.cert.hr/godisnji-izvjestaj-radanacionalnog-cert-a-za-2023-godinu/ [datum pristupa:20.04.2024]
5. Koja je razlika između Rootkita i zlonamjernog softvera, Objašnjeno.hr, https://objasnjeno.com/koja-je-razlika-izmedu-rootkita-i-zlonamjernog-softvera/ [20.5.2024]
6. Markota, K.: Svjesnost korisnika o čimbenicima rizika prilikom korištenja mobilnih aplikacija, završni rad, Sveučilište Josipa Juraja Strossmayera u Osijeku, fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Osijek, 2018.
7. Mobile Operating System Market Share Croatia, Statcounter, https://gs.statcounter.com/os-market-share/mobile/croatia [8.6.2024]
8. Mobilne aplikacije. Što su, za što postoje i koje vrste postoje?, Pctown , https://pctown.co.nz/mobilne-aplikacije-sto-su-za-sto-postoje-i-koje-vrstepostoje/#google_vignette [16.4.2024]
9. Mobilni telefoni, Enciklopedija.cc, https://enciklopedija.cc/index.php/Mobilni_telefon [16.4.2023]
10. crvima, CERT.hr, https://www.cert.hr/crvi/ [20.5.2024]
11. Rootkit softveru, CERT.hr, https://www.cert.hr/rootkitovi/ [20.5.2024]
12. Online privatnost i sigurnost, Europsak komisija, https://digitalstrategy.ec.europa.eu/hr/policies/online-privacy [6.8.2024]

13. Osnove privatnosti na Internetu, CERT.hr , https://www.cert.hr/wpcontent/uploads/2017/12/osnove_privatnosti_na_Internetu_0.pdf [15.5.2024]
14. Phishing napadi – kako ih prepoznati i zaštititi se, azop, https://azop.hr/phishing-napadikako-ih-prepoznati-i-zastititi-se/ [7.9.2024]
15. Phishing, Techtarget , https://www.techtarget.com/searchsecurity/definition/phishing [2.6.2024]
16. Povelja o temeljnim pravima Europse unije Vijeće, Europse unije, https://fra.europa.eu/hr/eu-charter/title/title-ii-freedoms [22.4.2024]
17. Povijest mobilne telefonije: što se događalo u 40 godina?, Mob.hr, https://mob.hr/povijest-mobilne-telefonije-sto-se-dogadalo-u-40-godina/ [16.4.2023]
18. Pravila o privatnosti, Google.com, https://policies.google.com/privacy?hl=hr [1.6.2024]
19. Prikaz uredbe o zaštiti podataka , EU vijeće, https://fra.europa.eu/hr/eu-charter/title/titleii-freedoms [22.4.2024]
20. Računalne prijevare, e-Građani, https://gov.hr/hr/racunalne-prijevare/1234 [2.9.2024]
21. Razvoj naprednih tehnika za izradu malwerea/rootkita, FOI, https://security.foi.hr/wiki/index.php/Razvoj_naprednih_tehnika_za_izradu_malwarea/r ootkita.html [20.5.2024]
22. Scam i Phishing? Što su i kako se zaštititi?, Plaviured.hr, https://plaviured.hr/vodici/scam-phishing-sto-se-zastititi/ [2.6.2024]
23. Sigurnost na Internetu: 5 pravila kako zaštititi privatne podatke, Duplico.IO, https://duplico.io/sigurnost-na-internetu-5-pravila-kako-zastititi-privatne-podatke/ [3.6.2024]
24. Sigurnost operacijskog susrava iOS, Cis.hr, https://www.cis.hr/files/dokumenti/CISDOC-2011-09-024.pdf [12.6.2024]
25. Trojanski konji, CERT.hr, https://www.cert.hr/trojanski_konji/ [20.5.2024]

26. Uloga operacijskog sustava u radu računalnog sustava, različiti operacijski sustavi za različite digitalne uređaje, Carnet.hr, https://edutorij-adminapi.carnet.hr/storage/extracted/c4e1aebf-48e0-4d92-b6a9-0716a4e1c740/html/405_uloga_operacijskog_sustava_u_radu_racunalnoga_sustava_raz liciti_operacijski_sustavi_za_razlicite_digitalne_uredaje.html [9.6.2024]
27. Virusi, CERT.hr, https://www.cert.hr/virusi/ [datum pristupa:20.05.2024]
28. Virusi, računalni, Hrvatska enciklopedija, https://www.enciklopedija.hr/clanak/virusracunalni [20.5.2024]
29. What's a smartphone processor and what does it do?, Cool Blue, https://www.coolblue.nl/en/advice/smartphone-processors.html [3.8.2024]
30. Zaštita podataka u EU, Vijeće Europse unije, https://www.consilium.europa.eu/hr/policies/data-protection/ [22.4.2024]
31. Zlonamjerni programi-razlike, načini djelovanja, Hrvatska akademska i istraživačka mreža-CARNET, https://edutorij-adminapi.carnet.hr/storage/extracted/2219325/html/433_zlonamjerni_programi__razlike_nacin_djelovanja.html [20.5.2024]

POPIS SLIKA

POPIS TABLICA

POPIS GRAFOVA

SAŽETAK

Usporedno s rastom popularnosti pametnih mobilnih telefonskih uređaja rastu i problemi koji su vezani za sigurnost od malicioznog koda kao i problemi vezani za privatnost korisnika pametnih mobilnih telefonskih uređaja. Kako se radi o vrlo dinamičnom procesu kojemu globalno raste značaj, fokus je provedenog istraživanja bio usmjeren na rizike privatnosti i sigurnosti korisnika prilikom upotrebe pametnih mobilnih telefonskih uređaja, odnosno programskih aplikacija koji su uobičajeno instalirane na pametnim mobilnim telefonskim uređajima ili kojima se pristupa putem pametnih telefonskih uređaja upotrebom Interneta. Rezultati istraživanja ukazuju kako su znanja vezana za sigurnu upotrebu navedene tehnologije, osobito kod mlađe populacije koja intenzivno korisni pametne mobilne telefonske uređaje izrazito niska što objektivno otvara vrata uspjehu onih koji čine napore vezane za ugrozu sigurnosti i privatnosti korisnika pametnih mobilnih telefonskih uređaja. Sukladno je tome potrebno sustavno pristupiti problemu obrazovanja ljudi za upotrebu suvremene pametne mobilne telefonske tehnologije. To podrazumijeva uvođenje obuke za stjecanje znanja i vještina vezanih za upotrebu suvremene mobilne pametne telefonske tehnologije u planove i programe svih razina obrazovanja, kao i otvaranje tečajeva na kojima bi se mogla, u okviru cjeloživotnog obrazovanja, nadopunjavati znanja i vještine vezane za upotrebu suvremene pametne mobilne telefonske tehnologije. Prema tome, permanentno obrazovanje vezano za upotrebu pametnih mobilnih telefona, kao i permanentno (periodično) istraživanje znanja veznih za sigurnu upotrebu suvremene pametne mobilne telefonske tehnologije predstavlja put i načelan model za osiguranje privatnosti i sigurnosti korisnika prilikom upotrebe pametnih mobilnih telefona.

Ključne riječi: pametni mobilni telefonski uređaji, mobilne programske aplikacije, privatnost korisnika na Internetu, računalna sigurnost korisnika

SUMMARY

Parallel to the growth in popularity of smart mobile phone devices, problems related to security from malicious code(Malware) as well as problems related to the privacy of smart mobile phone users are also growing. As it is a very dynamic process whose importance is growing globally, the focus of the conducted research was on the privacy and security risks of users when using smart mobile phone devices, software applications that are usually installed on smart mobile phone devices or accessed via smart phone devices. devices using the Internet. The results of the research indicate that the knowledge related to the safe use of the mentioned technology, especially among the younger population who intensively use smart mobile phone devices, is extremely low, which objectively opens the door to the success of those who make efforts related to the threat to the security and privacy of users of smart mobile phone devices. Accordingly, it is necessary to systematically approach the problem of educating people to use modern smart mobile phone technology. This implies the introduction of training for the acquisition of knowledge and skills related to the use of modern mobile smart phone technology in plans and programs of all levels of education, as well as the opening of courses where, within the framework of lifelong education, knowledge and skills related to the use of modern smart mobile phones could be supplemented telephone technology. Therefore, permanent education related to the use of smart mobile phones, as well as permanent (periodic) knowledge research related to the safe use of modern smart mobile phone technology represents a path and a principled model for ensuring the privacy and security of users when using smart mobile phones.

Keywords: smart mobile phone devices, mobile software applications, user privacy on the Internet, user computer security