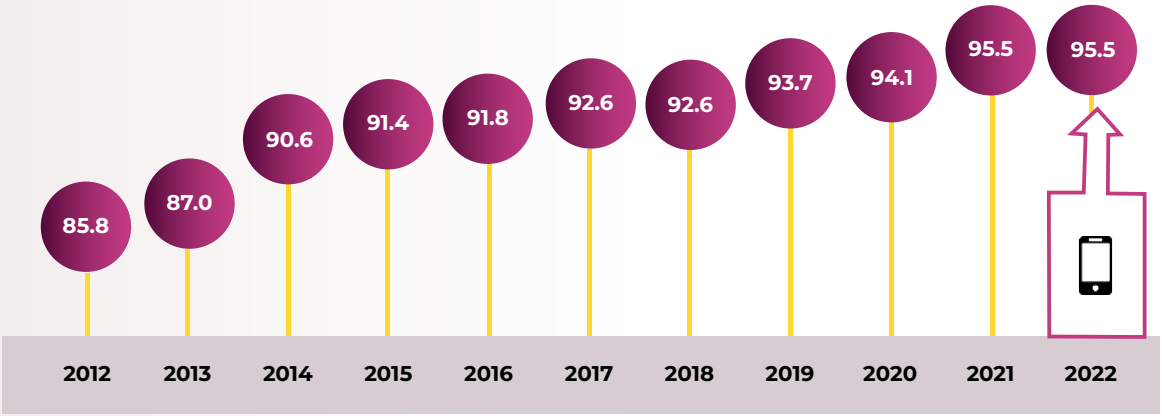
Bezbedno korišćenje aplikacija na mobilnim uređajima

Internet je danas široko rasprostranjen i dostupan svim kategorijama stanovništva, što korisnicima omogućava komunikaciju sa prijateljima, porodicom, i poslovnim saradnicima, korišćenje društvenih mreža, informisanje i mogućnost sticanja novih veština i znanja. Masovnost upotrebe interneta dovodi i do povećanja upotrebe mobilnih uređaja, poput pametnih telefona, tableta, laptopova kao i pametnih satova, a koji su postali jedna od osnovnih tehnologija koja se primenjuje kako u privatnom tako i u profesionalnom životu.

СРБ-ЦЕРТ

Istraživanje za 2021. i 2022. godinu, je pokazalo da 95,5% stanovništva u Republici Srbiji koristi mobilni telefon, dok je taj podatak za 2020. godinu je iznosio 94,1%[1].



Slika 1 - Upotreba mobilnog telefona (%)

Istovremeno, upotreba interneta i mobilnih uređaja, donosi brojne bezbednosne rizike. Na mobilnim uređajima nudi se instalacija brojnih aplikacija koje su na raspolaganju i koje omogućavaju veću produktivnost, bržu komunikaciju i razmenu informacija sa drugim ljudima, kao i više zabave. Upravo iz ovog razloga, potrebno je preduzeti sve mere prevencije u cilju sprečavanja prevara, a koje su sve zastupljenije.

Moguće zloupotrebe mobilnih aplikacija

Mobilne aplikacije mogu biti preuzete i instalirane kako iz prodavnica (*Play Store* i *App Store*), tako i putem linkova sa interneta. Instalacija aplikacija sa linkova se generalno smatra nebezbednom ukoliko niste upoznati sa detaljima i autorom aplikacije. Ovi linkovi se često distribuiraju uz pomoć fišing poruka.

Fišing (eng. phishing) je tip prevare koja ima za cilj prikupljanje i zloupotrebu poverljivih podataka korisnika, poput brojeva bankovnih računa, lozinki naloga na društvenim mrežama ili pristupa elektronskoj pošti. Žrtva ovog tipa sajber napada dobija poruku putem elektronske pošte, društvenih mreža, telefona ili SMS-a u kojoj se od nje zahteva da poseti link ili otvori dokument i upiše lične i poverljive podatke.

[1] *https://publikacije.stat.gov.rs/G2022/Pdf/G202216017.pdf*

Kao jedna od mogućih fišing prevara putem mobilnog uređaja, jeste kada napadač kontaktira potencijalnu žrtvu, upozorava je da mobilni uređaj zaražen i traži da se preduzme hitna akcija preuzimanja aplikacije za uklanjanje virusa sa telefona, a koja je zapravo maliciozna. Ovo su česti pokušaji prevare korisnika, koji se ogledaju u zastrašivanju i zahtevanju preduzimanja hitnih akcija od strane korisnika. Detaljnije o fišing napadima, može se pronaći na sledećem linku.

Pored distribucije malicioznih aplikacija uz pomoć linkova na internetu, maliciozne aplikacije se mogu preuzeti i na *Play Store* i *App Store*, iako se na ovim prodavnicama, pre objavljivanja, rade provere bezbednosti aplikacija.

Bez obzira na koji način su preuzete, ove aplikacije često zahtevaju pristup upravljanju pozivima i porukama na mobilnom uređaju čime dobijaju mogućnost da pozivaju i šalju SMS poruke prema međunarodnim brojevima, bez znanja korisnika, što dalje dovodi do uvećanja računa korisnika. Nažalost korisnici najčešće primete ovu aktivnost tek nakon dobijanja računa za telefon, kada je on značajno uvećan, te im kao jedina mogućnost ostaje da reklamiraju postojanje neželjenih poruka ili poziva kod telekomunikacionog operatora tražeći umanjenje iznosa na računu.

Do zloupotrebe dolazi na sledeći način:

- Instalacijom različitih aplikacija na mobilnim uređajima, od strane korisnika;
- Prilikom instalacije, korisnici, instaliranim aplikacijama dozvoljavaju opciju za upravljanje pozivima i porukama na mobilnom uređaju;
- Neke od navedenih aplikacija imaju funkcionalnost da pozivaju i šalju SMS poruke prema međunarodnim brojevima, bez znanja korisnika, što dovodi do uvećanja mesečnog računa korisnika;
- Ovakve, zlonamerne aplikacije, imaju mogućnost brisanja poslatih poruka i upućenih poziva iz evidencije SMS poruka i iz liste poziva, a u skladu sa dozvolama koje su dodeljene od strane korisnika. Na ovaj način korisniku se dodatno otežava da opazi generisanje neželjenih SMS poruka ili poziva prema međunarodnim brojevima.

Napadači koriste sve sofisticiranije načine za distribuciju zlonamernih mobilnih aplikacija, koje na prvi pogled, izgledaju kao da su legitimne, što može omogućiti napadačima potpunu kontrolu nad mobilnim uređajima ili podacima koji se nalaze na uređaju. Ovi tipovi prevare, dešavaju se u slučajevima kada korisnici neke od zlonamernih aplikacija instaliraju, tj. preuzimaju sa neproverenih platformi, pristupanjem nebezbednim linkovima od strane korisnika. Takođe, važno je napomenuti da u pojedinim slučajevima, zlonamerne aplikacije mogu biti dostupne i na poznatim platformama *Play Store* i *App Store*. Iz tih razloga, korisnicima se sugeriše da budu oprezni prilikom instaliranja aplikacija, čak i sa ovlašćenih platformi.

Preporuka korisnicima nakon realizovane prevare

Ukoliko je prevara realizovana, korisnicima se savetuje:

- da provere instalirane aplikacije na svom uređaju kao i dozvole koje su tim aplikacijama dodeljene;
- da instaliraju antivirus i antimalver programe (npr. Bitdefender, Norton, Kaspersky i druge) i pokrenu skeniranje uređaja;
- potražiti savet IT stručnjaka jer su zlonamerne aplikacije sve sofisticiranije i teško ih je samostalno detektovati;
- da ukoliko su detektovali malicioznu aplikaciju sa ovakvim dozvolama ili su instalirali aplikacije sa neproverenih linkova/platformi ove informacije dostave Nacionalnom CERT-u na dalju analizu;
- da mobilni uređaj vrate na fabrička podešavanja kako bi eventualne maliciozne aplikacije bile izbrisane.

Preporuke za bezbedno korišćenje i preuzimanje aplikacija na mobilnim uređajima

Preuzimanje bezbednih mobilnih aplikacija

Preporuka je da se mobilne aplikacije instaliraju putem ovlašćenih i proverenih platformi kao što su *Google Store* za *Android* uređaje ili *App Store* za *Apple* mobilne uređaje. Ovlašćene platforme kontinuirano obavljaju bezbednosnu proveru svih mobilnih aplikacija pre nego što ih učine dostupnim za preuzimanje. Iako nije moguće otkriti sve maliciozne mobilne aplikacije, na ovaj način se okruženje kontroliše i značajno umanjuje rizik od instalacije malicioznih aplikacija.

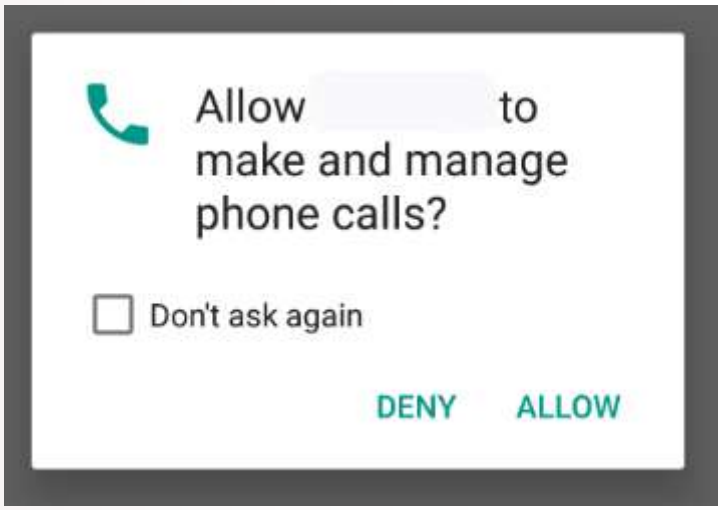
Slika 2 - Prodavnice Google Store i App Store

Važno je napomenuti da preuzimanje aplikacija sa ovlašćenih platformi, nije garancija da aplikacija nije maliciozna, stoga je bitno da korisnici detaljnije istraže aplikaciju pre preuzimanja, odnosno, da provere koliki vremenski period je aplikacija dostupna u okviru prodavnice, koliko je ljudi koristi, ko je proizvođač kao i recenzije i komentare drugih korisnika. Ukoliko korisniku, aplikacija nije neophodna ili je ne koristi duže vreme, preporuka je da se takve aplikacije ne instaliraju ili obrišu sa mobilnog uređaja.

Privatnost i dozvole

Nakon instaliranja aplikacije na mobilnom uređaju, aplikacije uglavnom traže dozvole za pristup drugim sistemima ili podacima kao što su lokacija, kontakti, mikrofon, lista poziva, poruke itd. Besplatne mobilne aplikacije prikupljaju podatke korisnika, kako bi se kasnije iskoristili za personalizovano oglašavanje. Međutim, davanjem ovih dozvola, korisnik može omogućiti autoru aplikacije da prati lokaciju, razmenjuje ili prodaje prikupljene informacije.

Na tržištu se nalazi veliki broj ovakvih aplikacija, pa je savet korisnicima da biraju one gde su zahtevi za pristup podacima, smisleni i ograničeni. Ukoliko korisnik smatra da su određene zahtevane dozvole neophodne za korišćenje aplikacije, takve dozvole treba omogućiti, u suprotnom, ove zahteve treba odbaciti.

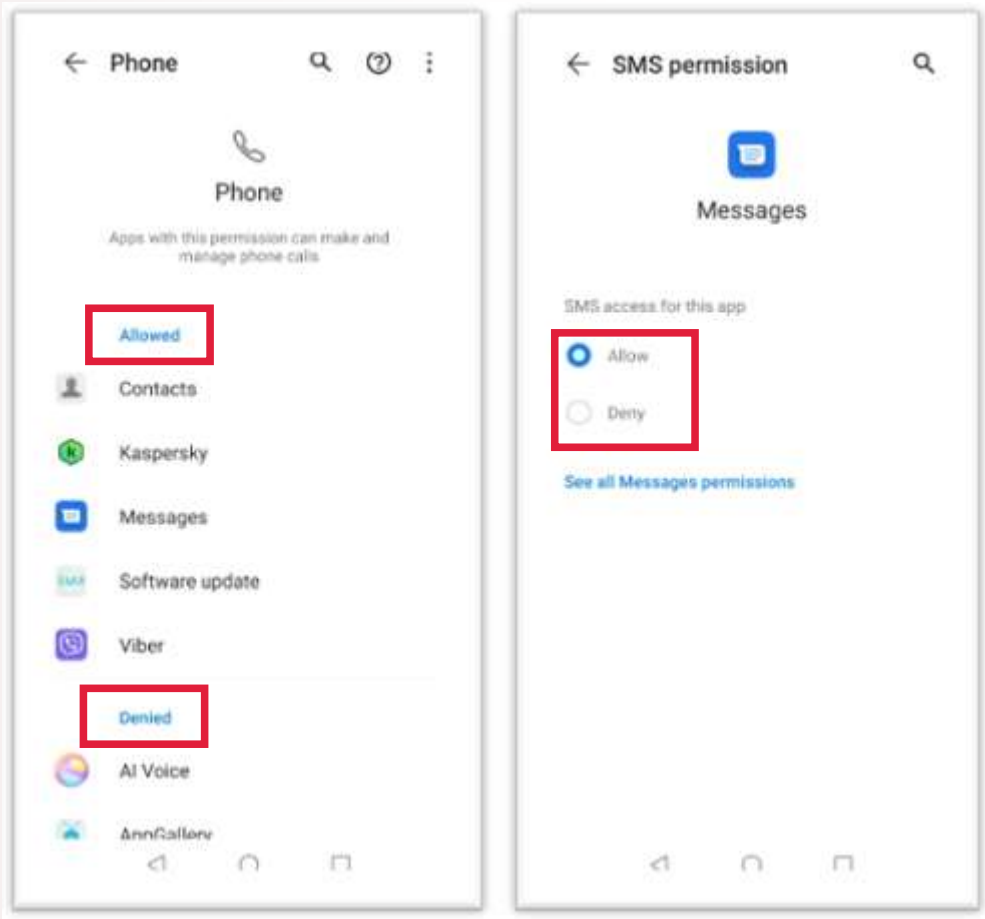


Slika 3 - Primer kada aplikacija traži dozvolu za upravljanje telefonskim pozivima

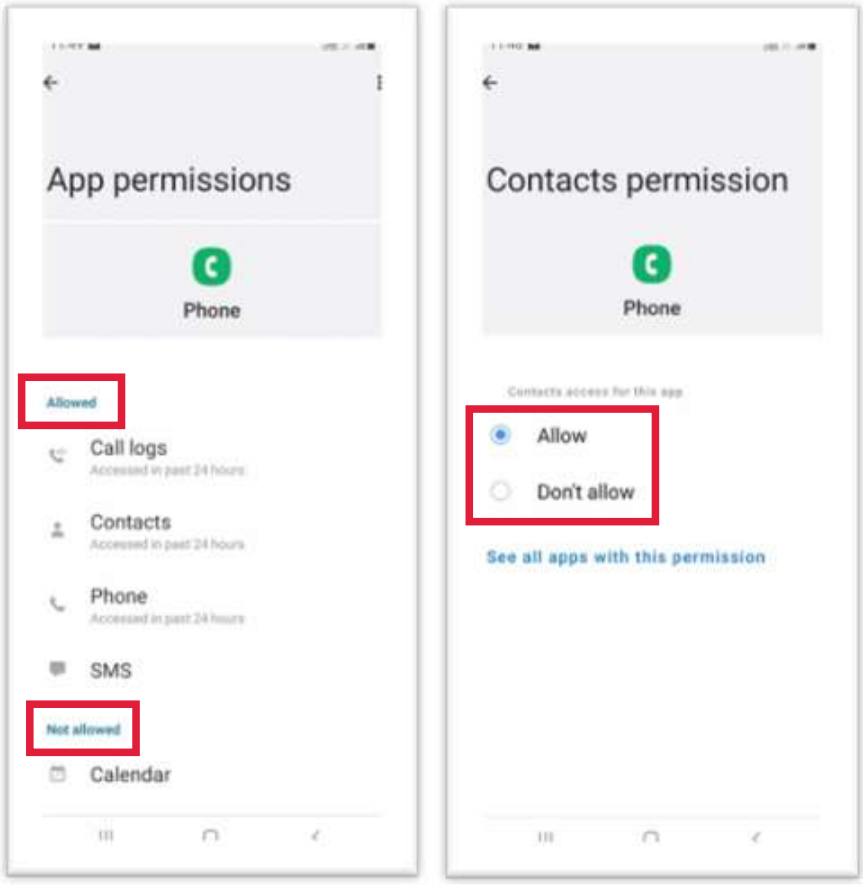
Često, instalirana aplikacija zahteva dozvole da bi aplikacija uopšte mogla da se koristi, a za koje korisnik smatra da su prevelike. U ovim slučajevima, preporuka je da korisnik instalira drugu alternativnu aplikaciju.

Kod aplikacija koje su već instalirane na mobilnom uređaju, potrebno je proveriti koje su dozvole dodeljene, i ukoliko nisu neophodne, te dozvole treba ukinuti/isključiti.

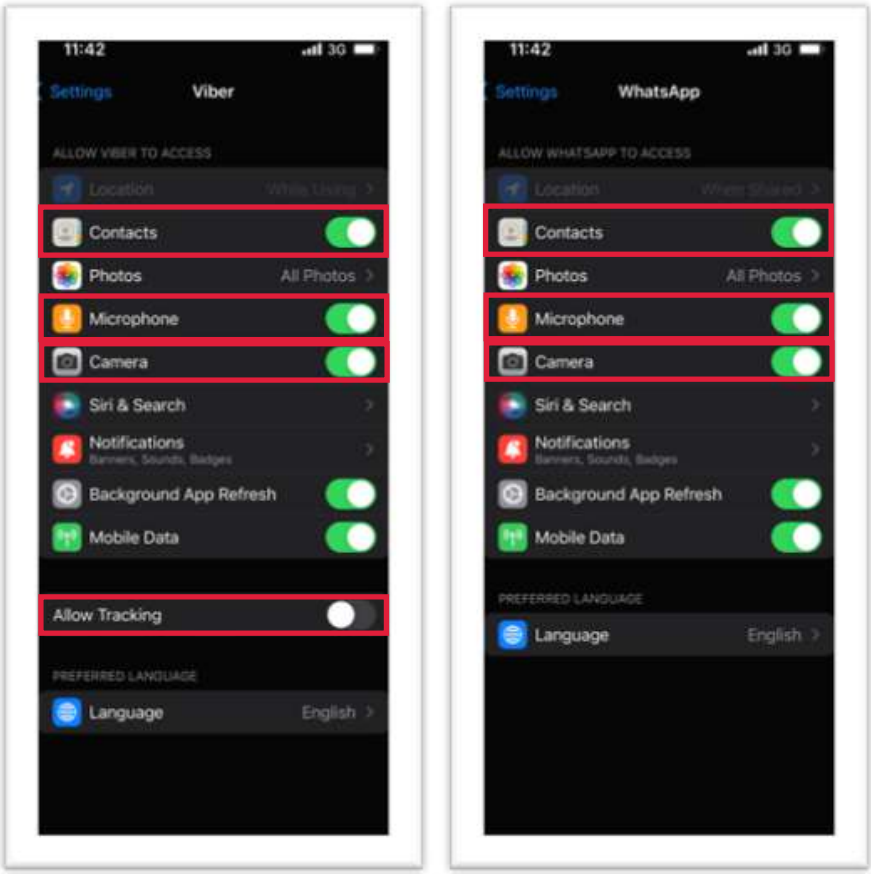
Korisnik može da ukine ili doda dozvole za svaku aplikaciju pojedinačno, biranjem opcije *podešavanja (settings) –> aplikacije (application) –>* odabrati instaliranu aplikaciju i pogledati koje dozvole su odabrane. Ovim dozvolama je moguće manipulisati u vidu „Enable/Disable" dugmetom ili biranjem opcije „*Allow/Deny*". Primeri za različite tipove mobilnih telefona se nalaze na sledećim slikama.



Slika 4 - Primer dozvola za pozive i poruke na Huawei mobilnom telefonu



Slika 5 - Primer dozvola za pozive na Samsung mobilnom telefonu



Slika 6 - Primer dozvola Viber i WhatsApp mobilnih aplikacija na iPhone mobilnom telefonu

Ažuriranje aplikacija

Redovno ažuriranje operativnih sistema, softvera i aplikacija pomaže u prevenciji da do bezbednosnih rizika uopšte dođe, s obzirom da je glavna svrha ažuriranja da dodaju bezbednosna unapređenja, poprave ili poboljšaju softver koji se koristi. Napadači kontinuirano traže i pronalaze bezbednosne propuste odnosno ranjivosti u aplikacijama, a zatim osmišljavaju načine za iskorišćavanje tih ranjivosti. Iz ovog razloga, preporuka je da korisnici redovno ažuriraju kako mobilne uređaje i operativne sisteme, tako i same mobilne aplikacije. Redovnim ažuriranjem mobilnih aplikacija, ispravljaju se ranjivosti koje su pronađene u okviru aplikacija i time se smanjuje mogućnost iskorišćavanja istih.

Preporuka je da se uključi automatsko ažuriranje za operativni sistem kao i za sve aplikacije koje imaju tu opciju jer napadači mogu koristiti uočene i poznate ranjivosti sistema ili aplikacija u toku sprovođenja napada. Redovnim ažuriranjem obezbeđuju se zakrpe za uočene ranjivosti, što za napadača otežava posao u izvođenju napada. U momentu kada se pojavi novo ažuriranje, automatski se preuzima i instalira, što čini aplikaciju ili mobilni uređaj bezbednijim za korišćenje. Prednost automatskog ažuriranja se ogleda i u tome, što ne zahteva nikakvu akciju korisnika.

Antivirus i antimalver programi

U današnje vreme, mobilne uređaje koristimo za svakodnevne aktivnosti, i podaci koji se nalaze u jednom takvom uređaju su raznovrsni, od bankarskih podataka, elektronskih poruka, dokumenata, kontakta i mnogi drugi. Naš telefon je zapravo mali džepni računar, stoga je potrebno čuvati podatke i zaštititi uređaj od brojnih bezbednosnih rizika. Kao jedan od boljih vidova prevencije i zaštite od bezbednosnih rizika, u kombinaciji sa prethodno navedenim, je korišćenje antivirus i antimalver programa na mobilnim uređajima. Mnogi antivirus provajderi nude zaštitu mobilnih uređaja. Postoje, pored verzija koje se plaćaju, i verzije koje su besplatne za korisnike i nude osnovni novo zaštite. Funkcija ovakvih programa je skeniranje mobilnih uređaja u cilju pronalaženja malicioznih aplikacija i fajlova, i u alarmiranju korisnika na potencijalne probleme na uređaju. Antivirus i antimalver programi imaju mogućnost da u realnom vremenu, otkriju ranjivost, upozore na potencijalno nebezbedne internet stranice koje korisnik želi da poseti, i na taj način umanji mogućnost od malicioznih aktivnosti od strane napadača. Određene antivirus aplikacije nude i preko osnovnog nivoa zaštite, kao što su blokiranje neželjenih poziva i poruka ili lociranje mobilnog uređaja u slučaju krađe.

Preporuke korisnicima mobilnih aplikacija na svojim uređajima su:

- Aplikacije instalirati sa proverenih i ovlašćenih platformi;
- Proveriti koje dozvole su dodeljene instaliranim aplikacijama, ukoliko su dopuštene dozvole slanja SMS poruka ili poziva, a nisu potrebne za funkcionisanje aplikacije iste treba ukinuti/isključiti;
- Ne uzvraćati pozive i ne slati SMS poruke ka inostranstvu ukoliko ne postoji jasna i nedvosmislena informacija o pošiljaocu;
- Ne učestvovati u nagradnim igrama ili kvizovima pre provere da se zaista radi o legitimnoj nagradnoj igri, odnosno kvizu.

U skladu sa navedenim, preporuke korisnicima mobilnih uređaja jesu primena pomenutih mera prevencije i zaštite, kako bi smanjili mogućnost prevara, koje se registruju u sve većem broju. Ukoliko do prevare ipak dođe, savet korisnicima je da se obrate svom telekomunikacionom operatoru i da prijave svoj problem Nacionalnom CERT-u, putem internet stranice (Prijavi incident) ili slanjem prijave putem imejla na adresu info@cert.rs. Informacije dostavljene Nacionalnom CERT-u ne utiču na proces reklamacije računa i koristiće se samo u svrhu sprečavanja dalje distribucije malicioznih aplikacija.

* https://mts.rs/Binary/1910/ouch-_serbian_june_2021_securely_using_mobile_apps.pdf
** https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/safety-and-security/using-apps-safely-and-securely
*** https://www.sans.org/newsletters/ouch/the-power-of-updating/
**** https://www.nlb.me/me/stanovnistvo/savjeti/7-pravila-za-bezbjedno-koriscenje-mobilnih-uredaja
***** https://uk.norton.com/internetsecurity-mobile-do-you-need-antivirus-protection-on-your-phone.html
****** https://publikacije.stat.gov.rs/G2022/Pdf/G202216017.pdf