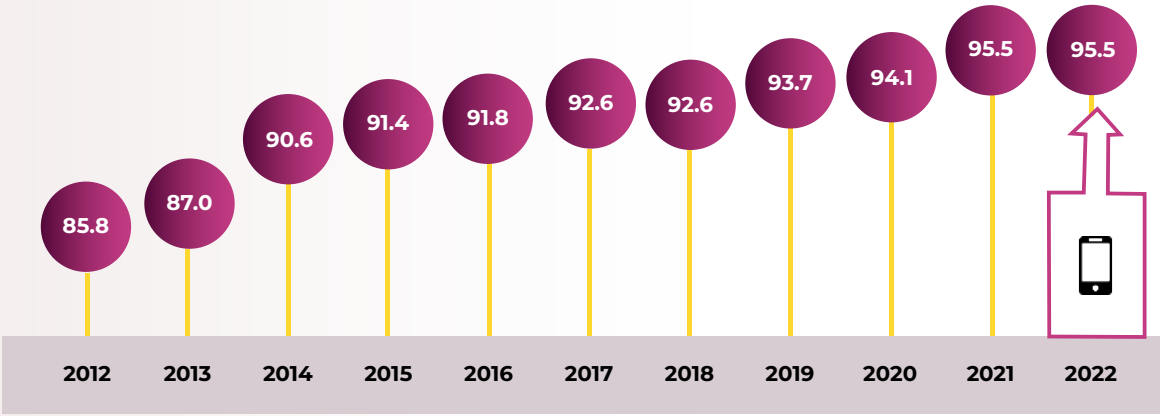
Безбедно коришћење апликација на мобилним уређајима

Интернет је данас широко распрострањен и доступан свим категоријама становништва, што корисницима омогућава комуникацију са пријатељима, породицом, и пословним сарадницима, коришћење друштвених мрежа, информисање и могућност стицања нових вештина и знања. Масовност употребе интернета доводи и до повећања употребе мобилних уређаја, попут паметних телефона, таблета, лаптопова као и паметних сатова, а који су постали једна од основних технологија која се примењује како у приватном тако и у професионалном животу.

СРБ-ЦЕРТ

Истраживање за 2021. и 2022. годину, је показало да 95,5% становништва у Републици Србији користи мобилни телефон, док је тај податак за 2020. годину је износио 94,1%.[1]



Слика 1 - Употреба мобилног телефона (%)

Истовремено, употреба интернета и мобилних уређаја, доноси бројне безбедносне ризике. На мобилним уређајима нуди се инсталација бројних апликација које су на располагању и које омогућавају већу продуктивност, бржу комуникацију и размену информација са другим људима, као и више забаве. Управо из овог разлога, потребно је предузети све мере превенције у циљу спречавања превара, а које су све заступљеније.

Могуће злоупотребе мобилних апликација

Мобилне апликације могу бити преузете и инсталиране како из продавница (*Play Store* и *App Store*), тако и путем линкова са интернета. Инсталација апликација са линкова се генерално сматра небезбедном уколико нисте упознати са детаљима и аутором апликације. Ови линкови се често дистрибуирају уз помоћ фишинг порука.

Фишинг (енг. phishing) је тип преваре која има за циљ прикупљање и злоупотребу поверљивих података корисника, попут бројева банковних рачуна, лозинки налога на друштвеним мрежама или приступа електронској пошти. Жртва овог типа сајбер напада добија поруку путем електронске поште, друштвених мрежа, телефона или СМС-а у којој се од ње захтева да посети линк или отвори документ и упише личне и поверљиве податке.

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

Као једна од могућих фишинг превара путем мобилног уређаја, јесте када нападач контактира потенцијалну жртву, упозорава је да мобилни уређај заражен и тражи да се предузме хитна акција преузимања апликације за уклањање вируса са телефона, а која је заправо малициозна. Ово су чести покушаји преваре корисника, који се огледају у застрашивању и захтевању предузимања хитних акција од стране корисника. Детаљније о фишинг нападима, може се пронаћи на следећем линку.

Поред дистрибуције малициозних апликација уз помоћ линкова на интернету, малициозне апликације се могу преузети и на *Play Store* и *App Store*, иако се на овим продавницама, пре објављивања, раде провере безбедности апликација.

Без обзира на који начин су преузете, ове апликације често захтевају приступ управљању позивима и порукама на мобилном уређају чиме добијају могућност да позивају и шаљу СМС поруке према међународним бројевима, без знања корисника, што даље доводи до увећања рачуна корисника. Нажалост корисници најчешће примете ову активност тек након добијања рачуна за телефон, када је он значајно увећан, те им као једина могућност остаје да рекламирају постојање нежељених порука или позива код телекомуникационог оператора тражећи умањење износа на рачуну.

До злоупотребе долази на следећи начин:

- Инсталацијом различитих апликација на мобилним уређајима, од стране корисника;
- Приликом инсталације, корисници, инсталираним апликацијама дозвољавају опцију за управљање позивима и порукама на мобилном уређају;
- Неке од наведених апликација имају функционалност да позивају и шаљу SMS поруке према међународним бројевима, без знања корисника, што доводи до увећања месечног рачуна корисника;
- Овакве, злонамерне апликације, имају могућност брисања послатих порука и упућених позива из евиденције SMS порука и из листе позива, а у складу са дозволама које су додељене од стране корисника. На овај начин кориснику се додатно отежава да опази генерисање нежељених SMS порука или позива према међународним бројевима.

Нападачи користе све софистицираније начине за дистрибуцију злонамерних мобилних апликација, које на први поглед, изгледају као да су легитимне, што може омогућити нападачима потпуну контролу над мобилним уређајима или подацима који се налазе на уређају. Ови типови преваре, дешавају се у случајевима када корисници неке од злонамерних апликација инсталирају, тј. преузимају са непроверених платформи, приступањем небезбедним линковима од стране корисника. Такође, важно је напоменути да у појединим случајевима, злонамерне апликације могу бити доступне и на познатим платформама *Play Store* и *App Store*. Из тих разлога, корисницима се сугерише да буду опрезни приликом инсталирања апликација, чак и са овлашћених платформи.

Препорука корисницима након реализоване преваре

Уколико је превара реализована, корисницима се саветује:

- да провере инсталиране апликације на свом уређају као и дозволе које су тим апликацијама додељене;
- да инсталирају антивирус и антималвер програме (нпр. Bitdefender, Norton, Kaspersky и друге) и покрену скенирање уређаја;
- потражити савет ИТ стручњака јер су злонамерне апликације све софистицираније и тешко их је самостално детектовати;
- да уколико су детектовали малициозну апликацију са оваквим дозволама или су инсталирали апликације са непроверених линкова/платформи ове информације доставе Националном ЦЕРТ-у на даљу анализу;
- да мобилни уређај врате на фабричка подешавања како би евентуалне малициозне апликације биле избрисане.

Препоруке за безбедно коришћење и преузимање апликација на мобилним уређајима

Преузимање безбедних мобилних апликација

Препорука је да се мобилне апликације инсталирају путем овлашћених и проверених платформи као што су Google Store за Android уређаје или App Stor e за Apple мобилне уређаје. Овлашћене платформе континуирано обављају безбедносну проверу свих мобилних апликација пре него што их учине доступним за преузимање. Иако није могуће открити све малициозне мобилне апликације, на овај начин се окружење контролише и значајно умањује ризик од инсталације малициозних апликација.

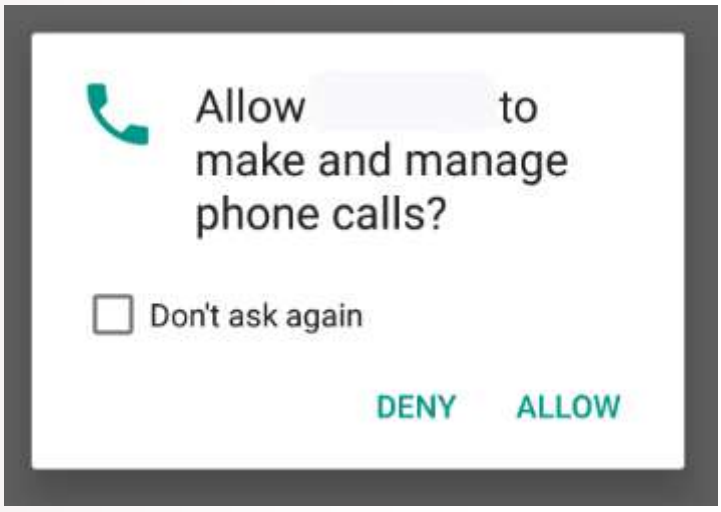
Слика 2 - Продавнице Google Store и App Store

Важно је напоменути да преузимање апликација са овлашћених платформи, није гаранција да апликација није малициозна, стога је битно да корисници детаљније истраже апликацију пре преузимања, односно, да провере колики временски период је апликација доступна у оквиру продавнице, колико је људи користи, ко је произвођач као и рецензије и коментаре других корисника. Уколико кориснику, апликација није неопходна или је не користи дуже време, препорука је да се такве апликације не инсталирају или обришу са мобилног уређаја.

Приватност и дозволе

Након инсталирања апликације на мобилном уређају, апликације углавном траже дозволе за приступ другим системима или подацима као што су локација, контакти, микрофон, листа позива, поруке итд. Бесплатне мобилне апликације прикупљају податке корисника, како би се касније искористили за персонализовано оглашавање. Међутим, давањем ових дозвола, корисник може омогућити аутору апликације да прати локацију, размењује или продаје прикупљене информације.

На тржишту се налази велики број оваквих апликација, па је савет корисницима да бирају оне где су захтеви за приступ подацима, смислени и ограничени. Уколико корисник сматра да су одређене захтеване дозволе неопходне за коришћење апликације, такве дозволе треба омогућити, у супротном, ове захтеве треба одбацити.

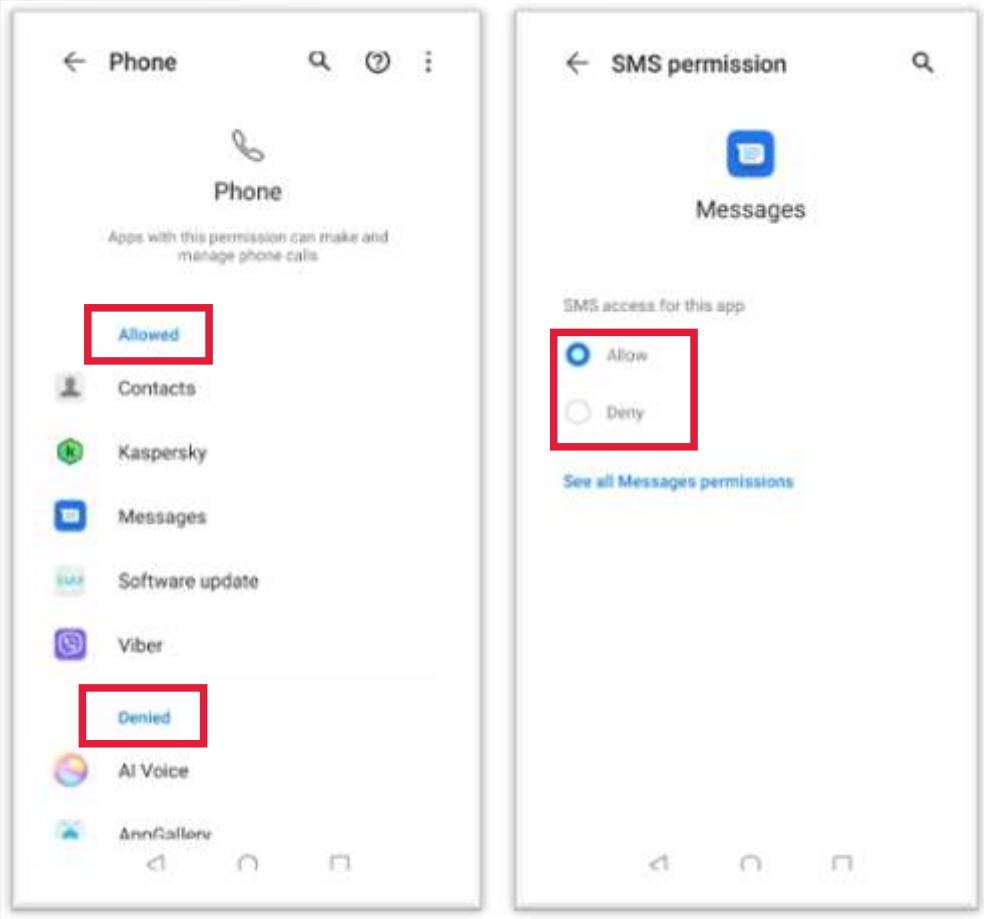


Слика 3 - Пример када апликација тражи дозволу за управљање телефонским позивима

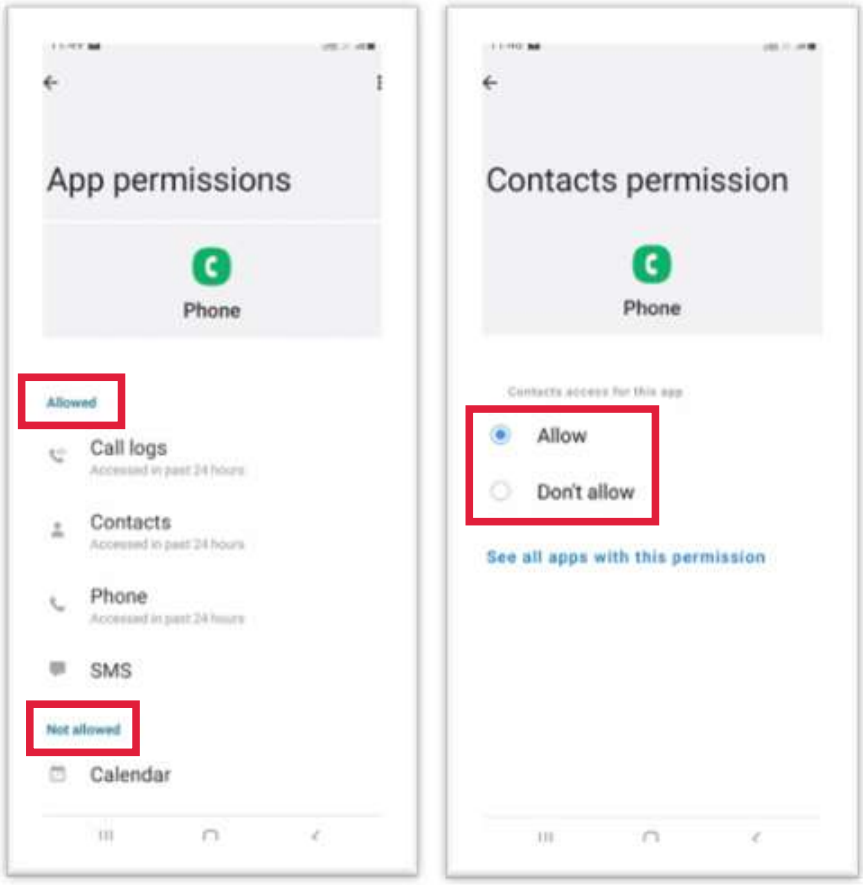
Често, инсталирана апликација захтева дозволе да би апликација уопште могла да се користи, а за које корисник сматра да су превелике. У овим случајевима, препорука је да корисник инсталира другу алтернативну апликацију.

Код апликација које су већ инсталиране на мобилном уређају, потребно је проверити које су дозволе додељене, и уколико нису неопходне, те дозволе треба укинути/искључити.

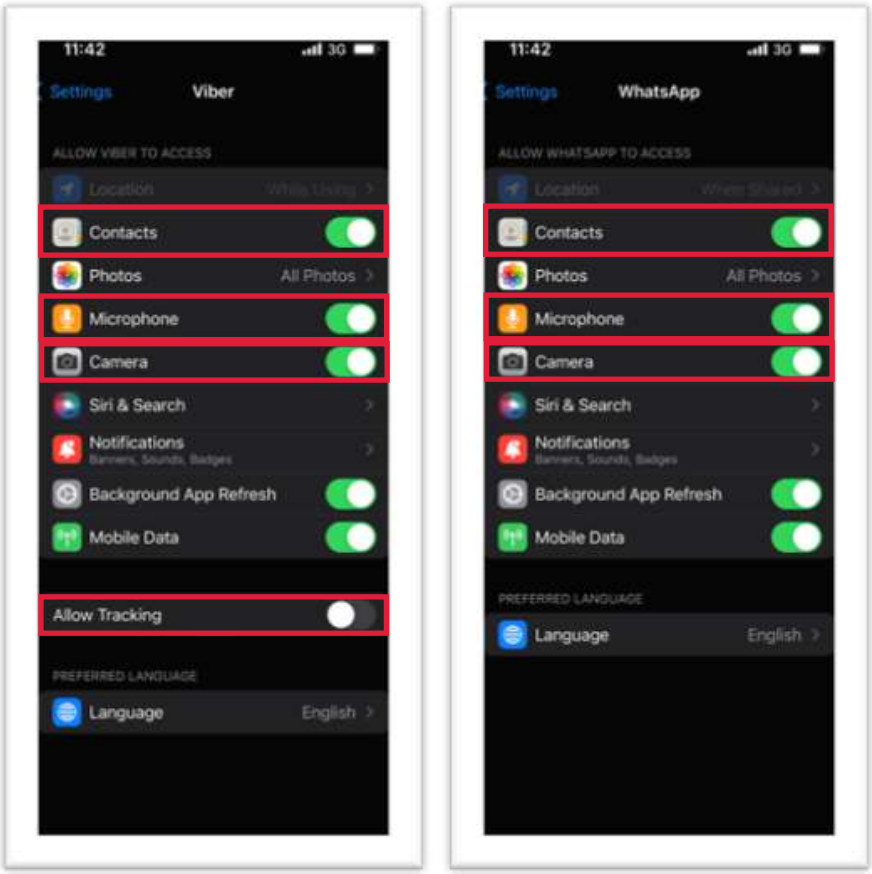
Корисник може да укине или дода дозволе за сваку апликацију појединачно, бирањем опције *подешавања* (*settings*) –> *апликације* (*application*) –> одабрати инсталирану апликацију и погледати које дозволе су одабране. Овим дозволама је могуће манипулисати у виду „*Enable/Disable*“ дугметом или бирањем опције „*Allow/Deny*“. Примери за различите типове мобилних телефона се налазе на следећим сликама.



Слика 4 - Пример дозвола за позиве и поруке на Huawei мобилном телефону



Слика 5 - Пример дозвола за позиве на Samsung мобилном телефону



Слика 6 - Пример дозвола Viber и WhatsApp мобилних апликација на iPhone мобилном телефону

Ажурирање апликација

Редовно ажурирање оперативних система, софтвера и апликација помаже у превенцији да до безбедносних ризика уопште дође, с обзиром да је главна сврха ажурирања да додају безбедносна унапређења, поправе или побољшају софтвер који се користи. Нападачи континуирано траже и проналазе безбедносне пропусте односно рањивости у апликацијама, а затим осмишљавају начине за искоришћавање тих рањивости. Из овог разлога, препорука је да корисници редовно ажурирају како мобилне уређаје и оперативне системе, тако и саме мобилне апликације. Редовним ажурирањем мобилних апликација, исправљају се рањивости које су пронађене у оквиру апликација и тиме се смањује могућност искоришћавања истих.

Препорука је да се укључи аутоматско ажурирање за оперативни систем као и за све апликације које имају ту опцију јер нападачи могу користити уочене и познате рањивости система или апликација у току спровођења напада. Редовним ажурирањем обезбеђују се закрпе за уочене рањивости, што за нападача отежава посао у извођењу напада. У моменту када се појави ново ажурирање, аутоматски се преузима и инсталира, што чини апликацију или мобилни уређај безбеднијим за коришћење. Предност аутоматског ажурирања се огледа и у томе, што не захтева никакву акцију корисника.

Антивирус и антималвер програми

У данашње време, мобилне уређаје користимо за свакодневне активности, и подаци који се налазе у једном таквом уређају су разноврсни, од банкарских података, електронских порука, докумената, контакта и многи други. Наш телефон је заправо мали џепни рачунар, стога је потребно чувати податке и заштитити уређај од бројних безбедносних ризика. Као један од бољих видова превенције и заштите од безбедносних ризика, у комбинацији са претходно наведеним, је коришћење антивирус и антималвер програма на мобилним уређајима. Многи антивирус провајдери нуде заштиту мобилних уређаја. Постоје, поред верзија које се плаћају, и верзије које су бесплатне за кориснике и нуде основни ново заштите. Функција оваквих програма је скенирање мобилних уређаја у циљу проналажења малициозних апликација и фајлова, и у алармирању корисника на потенцијалне проблеме на уређају. Антивирус и антималвер програми имају могућност да у реалном времену, открију рањивост, упозоре на потенцијално небезбедне интернет странице које корисник жели да посети, и на тај начин умањи могућност од малициозних активности од стране нападача. Одређене антивирус апликације нуде и преко основног нивоа заштите, као што су блокирање нежељених позива и порука или лоцирање мобилног уређаја у случају крађе.

Препоруке корисницима мобилних апликација на својим уређајима су:

- Апликације инсталирати са проверених и овлашћених платформи;
- Проверити које дозволе су додељене инсталираним апликацијама, уколико су допуштене дозволе слања SMS порука или позива, а нису потребне за функционисање апликације исте треба укинути/искључити;
- Не узвраћати позиве и не слати SMS поруке ка иностранству уколико не постоји јасна и недвосмислена информација о пошиљаоцу;
- Не учествовати у наградним играма или квизовима пре провере да се заиста ради о легитимној наградној игри, односно квизу.

У складу са наведеним, препоруке корисницима мобилних уређаја јесу примена поменутих мера превенције и заштите, како би смањили могућност превара, које се региструју у све већем броју. Уколико до преваре ипак дође, савет корисницима је да се обрате свом телекомуникационом оператору и да пријаве свој проблем Националном ЦЕРТ-у, путем интернет странице (Пријави инцидент) или слањем пријаве путем имејла на адресу info@cert.rs. Информације достављене Националном ЦЕРТ-у не утичу на процес рекламације рачуна и користиће се само у сврху спречавања даље дистрибуције малициозних апликација.

* 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