

Безбедност корисника интернета у Србији

Фебруар
2022.



Садржај

О истраживању	3
01. Методологија истраживања	4
02. Увод, резиме и препоруке	6
03. Резултати и закључци истраживања	11
04. Додатак: Како користимо интернет	46

О истраживању

Теме којима се бавимо у истраживању су:

- **Како смо информисани о безбедносним ризицима приликом коришћења интернета**
- **Да ли нам је нарушена безбедност на интернету**
- **Како штитимо наше податке на интернету**

У додатку дајемо одговоре и на питања о коришћењу интернета (на којим уређајима, колико често, на који начин, које садржаје конзумирамо).

Истраживање је спровео Регистар националног интернет домена Србије (РНИДС). Припрема истраживања је реализована уз подршку Националног ЦЕРТ-а Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ).

01.

Методологија истраживања

Методологија истраживања

Истраживање о безбедности коришћења интернета у Србији реализовано је у два корака, јануара и фебруара 2022. године.

Први део истраживања спроведен је на национално репрезентативном узорку пунолетних становника Србије, методом телефонске анкете са 2000 испитаника. Циљ овог дела истраживања био је обезбедити квалитетан и репрезентативан узорак корисника интернета у Србији. Утврђено је да 74% становника Србије користи интернет.

Други део истраживања спроведен је методом онлајн панел истраживања на репрезентативном узорку од 1000 пунолетних становника Србије који користе интернет.

02.

Увод, резиме и препоруке

Увод

Развој телекомуникационе инфраструктуре допринео је да интернет стигне у свако село и сваку општину и да постане доступан свим категоријама становништва.

Број корисника интернета у Србији и њихов удео у укупној популацији повећава се из године у годину и он данас износи 74%. Пре десет година, 2012. године, интернет је користило мање од 50% становника.

И међу старијима од 60 година бележи се значајно повећање - 44,9% суграђана треће доби користи интернет.

Доступност интернета омогућила је комуникацију са рођацима и пријатељима и коришћење друштвених мрежа, информисање и могућност стицања нових вештина и знања свим категоријама становништва.

Истовремено, интернет, као добар слуга а зао господар, нуди нам бројне ризике коришћења. Безбедносни ризици коришћења интернета су значајни, али за већину испитаника они су разумљиви и прихватљиви.

Млади и старији од 60 година су две посебно осетљиве категорије становништва изложене ризицима на интернету. Млади, због недостатка животног искуства, а старији због недостатка дигиталног искуства.

74%

становника Србије
користи интернет

44,9%

становника Србије старијих од
60 година користи интернет

**Млади и старији од 60 година су
две посебно осетљиве категорије
становништва изложене ризицима
на интернету.**

Резиме

Највећи број анкетираних упознат је у основним цртама или има довољно информација о безбедносним ризицима, кумулативно 60-82%. Детаљно је, у зависности од наведеног ризика, упознато између 14 и 18 процената анкетираних. Ипак, ако ове податке ставимо у контекст информације да се 59% испитаника информише (пored осталих канала) и на друштвеним мрежама, не чуди закључак да информисаност о безбедносним ризицима приликом коришћења интернета често није у сагласности са одговорношћу за личну безбедност.

Интернет нуди информације, али нуди и бројне дезинформације, и веома је важно да корисници интернета у Србији добро разумеју који су релевантни извори информисања о безбедносним ризицима, али и да учине лични напор да унапреде своју безбедност на интернету.

Одговорност за заштиту од напада у дигиталном простору, корисници интернета у Србији приписују другима. Тек 14% корисника интернета у Србији препознаје своју одговорност за личну безбедност на интернету. Пружаоци интернет услуга (компаније које су власници друштвених мрежа и апликација за комуникацију) одговорни су за нашу безбедност, каже 40% грађана.

Истовремено, у готово истом проценту (43,8%, кумулативно) мисле да власници друштвених мрежа и интернет претраживача не брину уопште или не брину на задовољавајући начин о безбедности корисника интернета.

У том случају, логика налаже да би о безбедности на интернету требало да бринемо сами, међутим, тек 14% становника Србије, који користе интернет, препознаје своју одговорност за личну безбедност.

У вези тога, безбедност корисника интернета била би много више угрожена да сами уређаји (рачунари и мобилни телефони), оперативни системи и софтвери, друштвене мреже и апликације за комуникацију и рад, не обезбеђују корисницима интернета минимум безбедности – лозинку са великим и малим словима, бројевима и специјалним знацима или двостепену верификацију креираних налога, на пример.

14%

корисника интернета у Србији препознаје своју одговорност за личну безбедност на интернету

40%

анкетираних сматра да су пружаоци интернет услуга одговорни за нашу безбедност на интернету

43,8%

анкетираних мисле да власници друштвених мрежа и интернет претраживача не брину уопште или не на задовољавајући начин о безбедности корисника

Безбедност би била много више угрожена да сами уређаји, оперативни системи и софтвери, друштвене мреже и апликације за комуникацију и рад, не обезбеђују корисницима минимум безбедности.

Како сами штитимо своје податке на интернету?

За сада, ствари су овакве:



Рачунари чак 60% корисника интернета у Србији су бар једном заражени вирусом или неким другим малвером. Четвртина корисника интернета у Србији не зна да ли су били мета сувер напада.



Велики проценат, 14% корисника, каже да им је хакован налог на друштвеној мрежи.



11,1% анкетираних и даље не користи антивирус софтвер, а 4,7% не зна да ли га користи.



19,7% корисника интернета признаје да се бар једном "упецало" на е-поруку и кликнуло на линк који су добили од непознате особе. Још 11,9% не зна да ли је кликнуло или не.



Још увек велики број корисника интернета у Србији, чак 39%, својим рачунарима приступа директно, без лозинке или било које друге врсте идентификације.



72,6% старијих од 60 година не користи двостепену проверу идентитета.



12,8% корисника интернета узео је за коришћење USB када га пронађе на јавном месту и тако преузети огроман ризик од заражавања свог рачунара вирусом или малвером.



57,1% не зна одговор на питање да ли је безбеднији HTTPS или HTTP. 21% зна да је HTTPS безбеднији, 12% мисли да нема разлике. Ипак, 9,9% мисли да је HTTP безбеднији.

Препоруке

1. Информационо се квалитетније, из релевантних извора, поступајмо уз више личне одговорности и улажимо мало додатног напора да конкретним активностима сами за себе (и своје најближе) обезбедимо безбедније окружење на интернету.
2. Инсталирајмо антивирус софтвер, подесимо снажну лозинку за приступ рачунару и телефону или инсталирајмо апликацију која ће за нас креирати и чувати приступне податке апликацијама и сајтовима. Мењајмо лозинку довољно често и не дозволимо себи да исту лозинку користимо на различитим местима.
3. Не кликћимо на линкове у порукама које смо добили од непознатих особа. Немојмо никад да узимамо и користимо USB стикове који нису наши и не знамо шта се на њима налази.

03.

Резултати и закључци истраживања

Безбедносни ризик 1

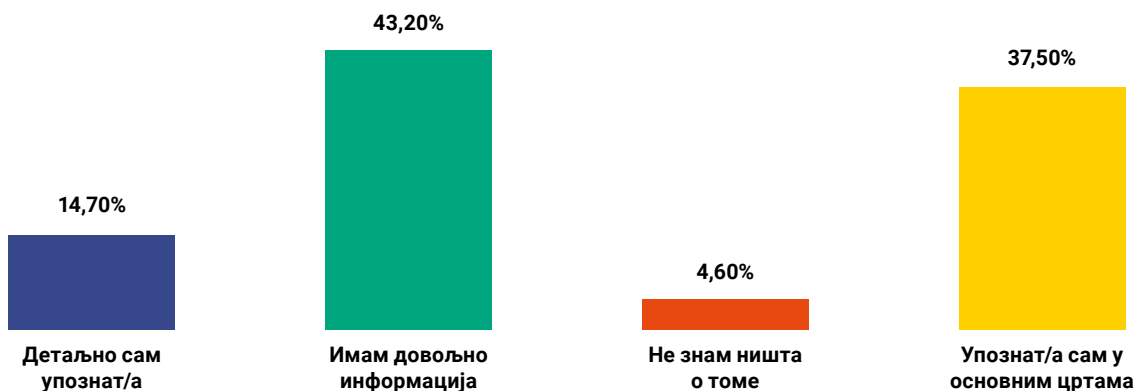


Рачунар заражен вирусом или неким другим малвером

95,4%

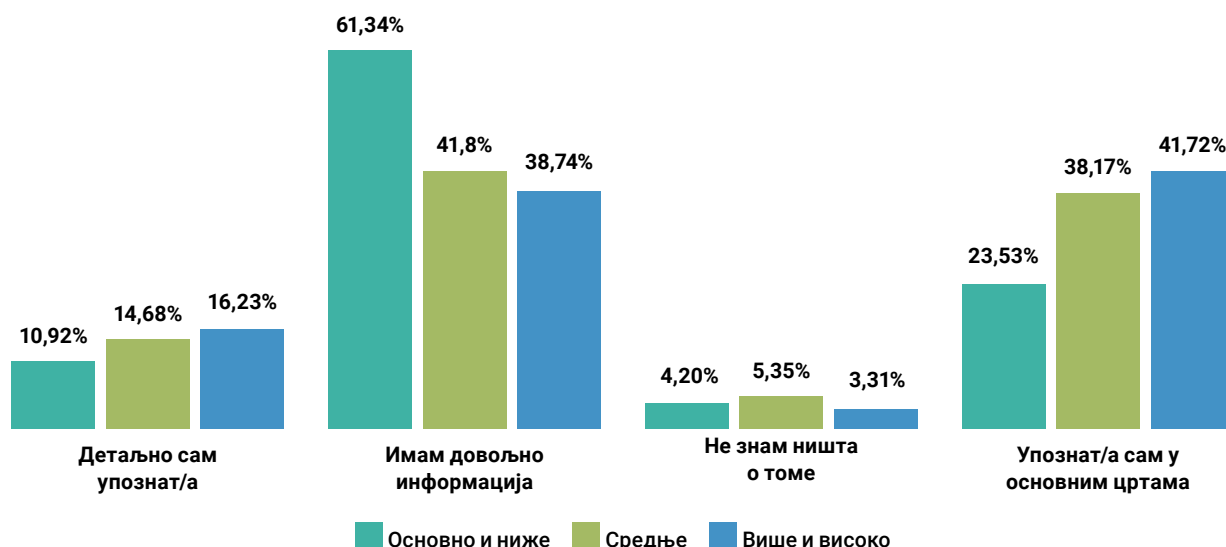
корисника препознаје овај безбедносни ризик.

Чак 95,4% корисника интернета препознаје безбедносни ризик да им рачунар буде заражен вирусом или неким другим малвером. О овом ризику 14,7% испитаника детаљно је упознато, а 43,2% има довољно информација. Велики број испитаника (37,5%) упознато је, тек, у основним цртама.



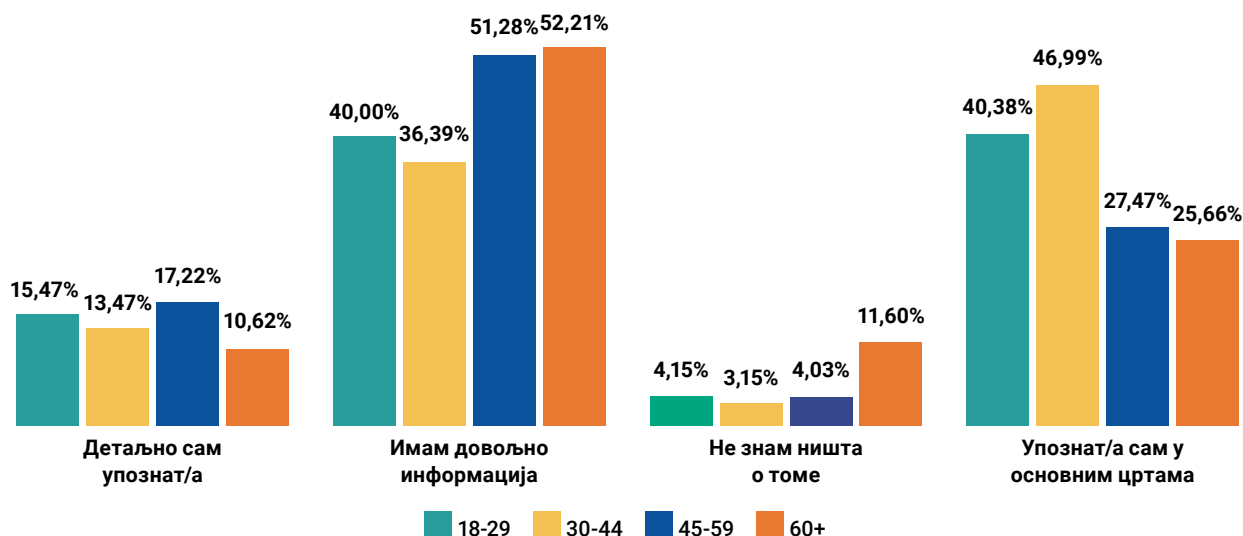
Укрштање по образовању

Становници Србије који имају завршену средњу школу/гимназију, по својим ставовима најближи су просеку. Грађани који имају основно и ниже образовање у мањој мери су детаљно упознати са наведеним безбедносним ризицима (10,9% наспрам просечне вредности од 14,7%) али је зато натпросечан проценат овог дела друштва одговорио да има довољно информација о поменутом безбедносном ризику (61,3% у односу на просечних 43,2%).



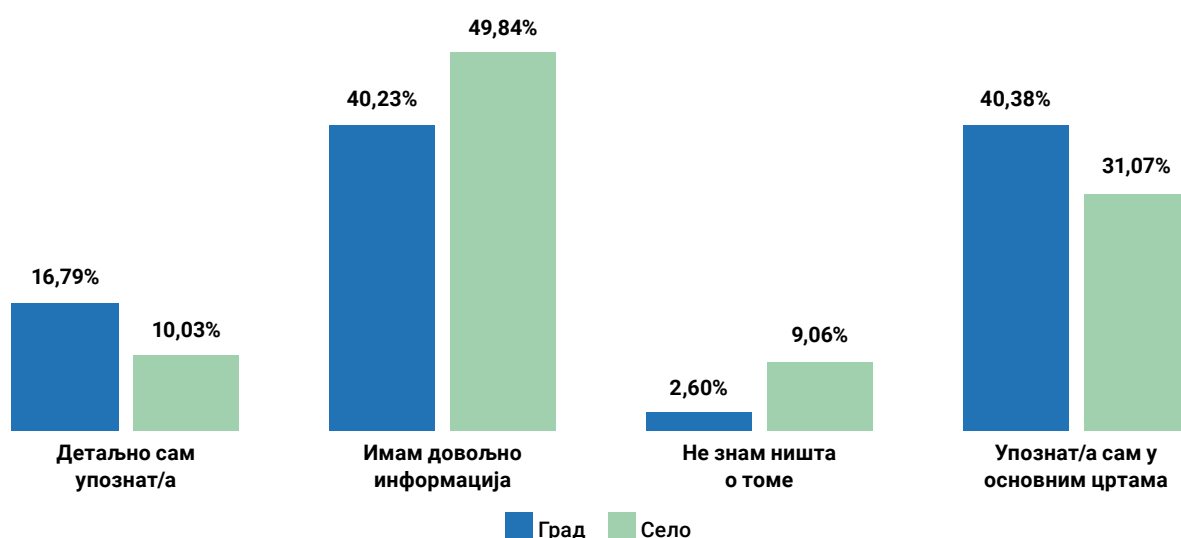
Укрштање по старости

Такође, припадници старије популација (60+) више од осталих мисле да имају довољно информација о безбедносним ризицима повезаним са заражавањем рачунара вирусом (52,2% у односу на просечних 43,2%) иако је испотпросечан број детаљно упознат (10,6%), а натпросечан број старијих суграђана (11,6%) не зна ништа о овом безбедносном ризику.



Укрштање по месту становања

Слична су запажања и када посматрамо укрштање према месту становања. Људи из руралних средина су у мањој мери детаљно упознати са безбедносним ризиком заражавања рачунара вирусом или неким другим малвером (10% у односу на просечних 14,7%), али истовремено у натпросечном броју тврде да имају довољно информација, и у значајно већем броју од људи који живе у урбаним срединама (49,8% наспрам 40,2%).



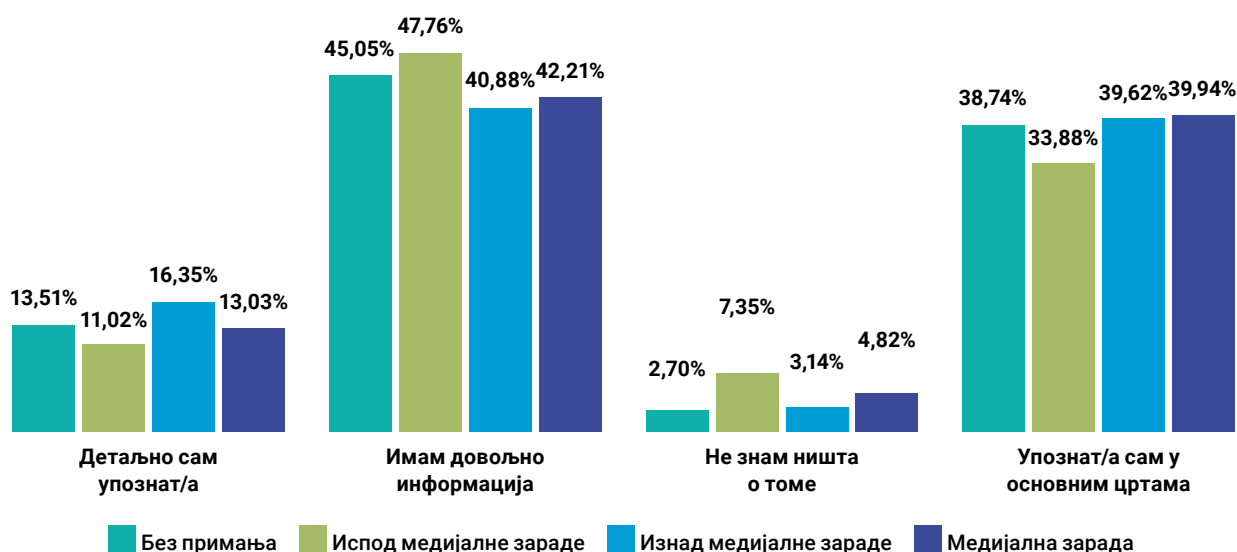
Као што смо већ нагласили, у последњих неколико година значајно је повећан број корисника интернета међу популацијом пензионера. Овим људима, који имају много више времена од радно способног становништва да претражују интернет и читају најразличитији садржај, отворио се један нови, непрегледни свет информација (и дезинформација). Стога не чуди њихов став да су информисани веома добро. Такође, ова категорија грађана много више проводи времена уз традиционалне медије, пре свега телевизију, па је број порука о теми безбедности, које на овај начин добијају, већа него код осталих категорија становништва.

У даљем тексту видећемо да перцепција информисаности о безбедносним ризицима често није у корелацији са личним деловањем да се безбедност обезбеди и унапреди.

Укрштање по висини зараде

Ако посматрамо висину зарада као демографску категорију, корисници интернета у Србији који имају натпросечну медијалну зараду, натпросечно су детаљно упознати о заражавању рачунара вирусом као безбедносним ризиком (16,3% наспрам просечних 14,7%).

Медијална нето зарада за децембар 2021. године износила је 53.349 динара, што значи да је 50% запослених остварило зараду до наведеног износа.



У категорији оних који имају зараду испод медијалне зараде преклапају се пензионери, дакле старији суграђани, и људи који имају ниже образовање и нижа примања. Такође, у категорији грађана без примања, која по својим ставовима у многоме предњачи у односу на остатак популације, велики део заузимају студенти или тек свршени студенти, који су и млади и имају високо образовање.

Сличне податке о ставовима различитих демографски одређених група - по полу, старости, образовању, висини зараде, добијамо и као одговоре о осталим ставовима о безбедности. Разлике су fine и резултати кореспондирају са закључцима који су изнети у опису првог наведеног безбедносног ризика - рачунар заражен вирусом или неким другим малвером.



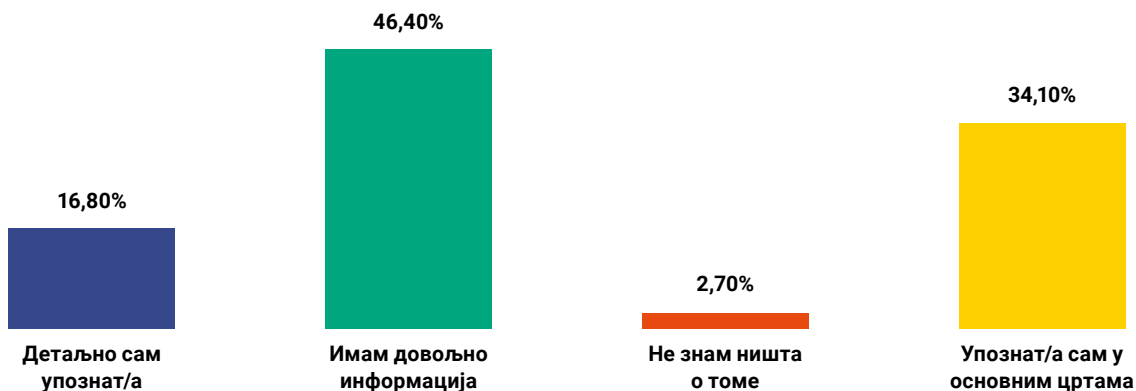
Превара (нпр. приликом електронске куповине)

63,2%

корисника
детаљно је
упознато или
има довољно
информација
о превари као
безбедносном
ризикy.

Превара на интернету је безбедносни ризик који укључује две стране - оног ко врши превару и оног ко је мета преваре. Због те своје сличности са понашањем у реалном, офлајн свету, корисници интернета у великој мери разумеју о коликој опасности је реч па је информисаност на високом нивоу.

Близу 2/3 корисника интернета у Србији (63,2%, кумулативно) детаљно је упознато или има довољно информација о превари као безбедносном ризику коришћења интернета.





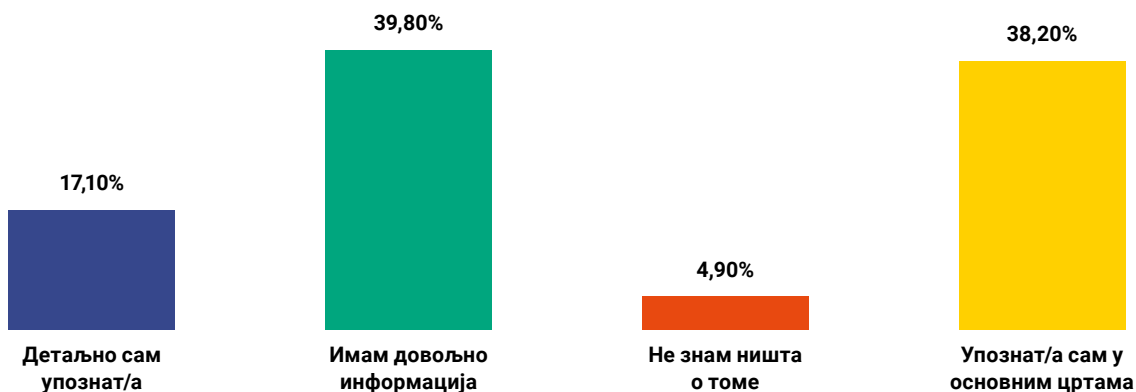
Крађа података (о идентитету, лозинкама, бројевима платних картица)

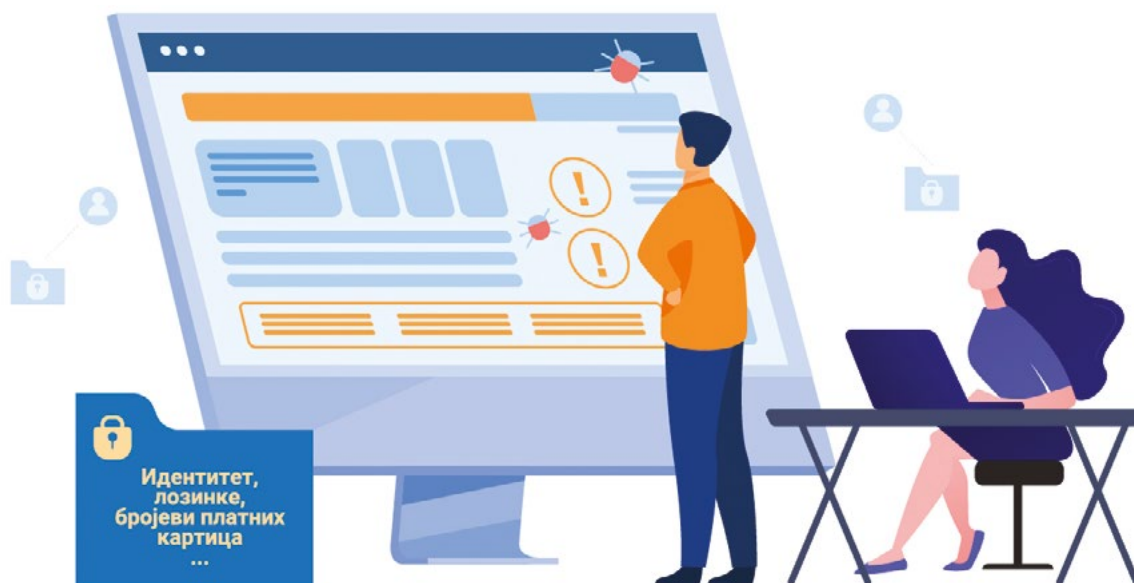
17,1%

корисника
детаљно је
упознато са
крађом података
као значајним
безбедносним
ризиком.

Број корисника интернета у Србији расте. Овом расту значајно доприносе старији суграђани. Такође, препознаје се значајан раст коришћења друштвених мрежа. Истовремено, подаци Народне банке Србије показују да је до краја 2021. године уручено више од 10 милиона платних картица, а број куповина путем интернета је у сталном порасту. Небезбедно коришћење података о идентитету може да доведе до озбиљних последица, до крађе идентитета или новца са картица.

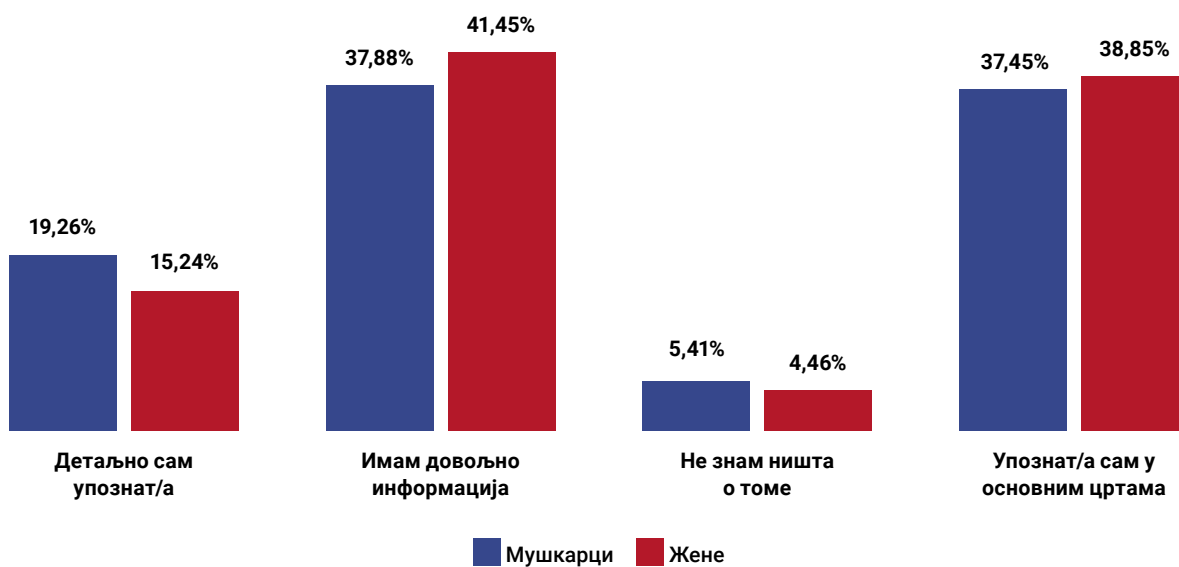
17,1% пунолетних грађана Србије који користе интернет детаљно је упознато са крађом података као значајним безбедоносним ризиком.





Укрштање по полу

Већи проценат мушкараца него жена не зна ништа о томе (5,4% наспрам 4,5%) али истовремено је и већи број мушкараца детаљно упознат са овим безбедносним ризиком (19,3% наспрам 15,2%).



Безбедносни ризик 4

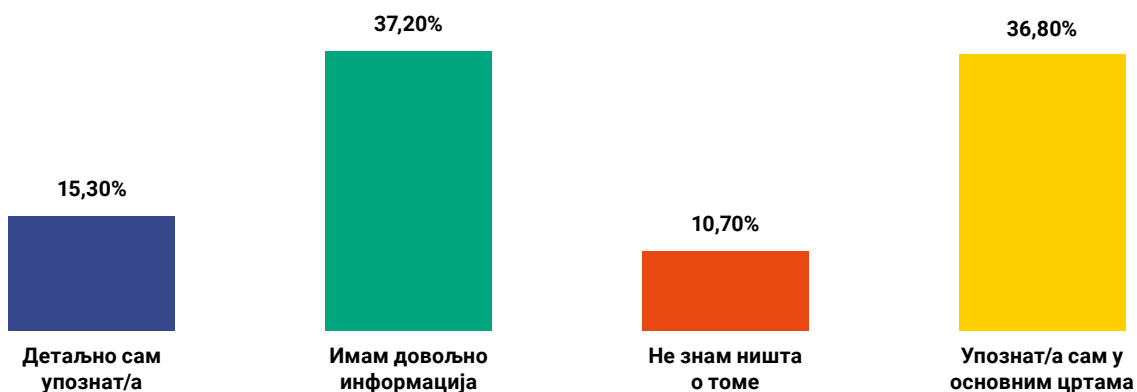


Хакован налог на друштвеној мрежи

89,3%

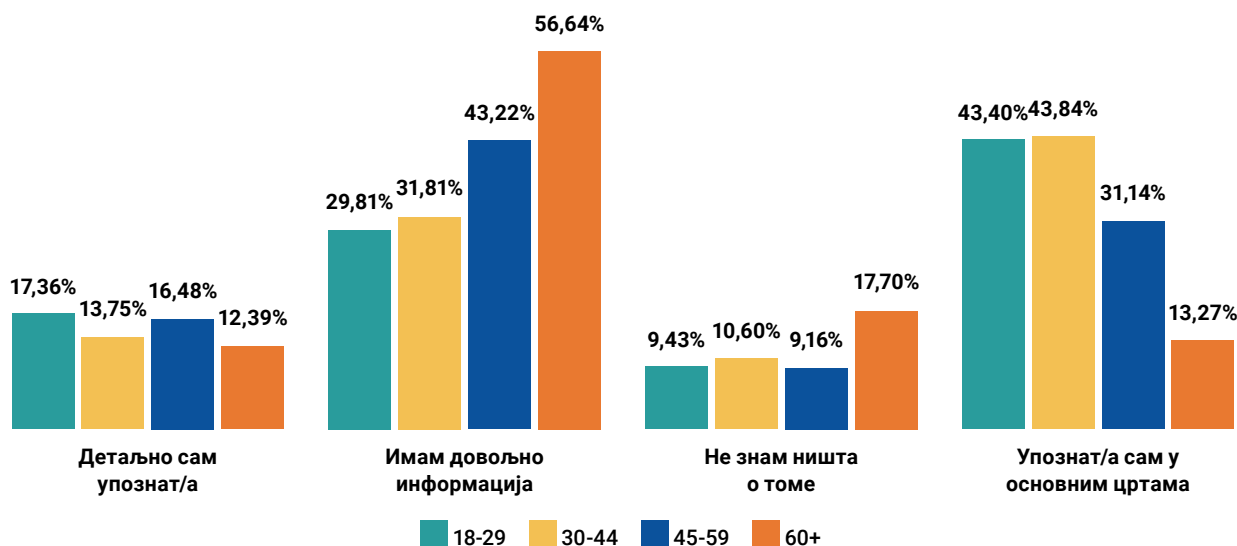
становника Србије
препознаје овај
безбедносни
ризик.

Овај безбедносни ризик препознаје препознаје 9 од 10 становника Србије. Готово 3/4 корисника интернета (74%, кумулативно) упознато је у основним цртама или има довољно информација о овом виду безбедносног ризика.



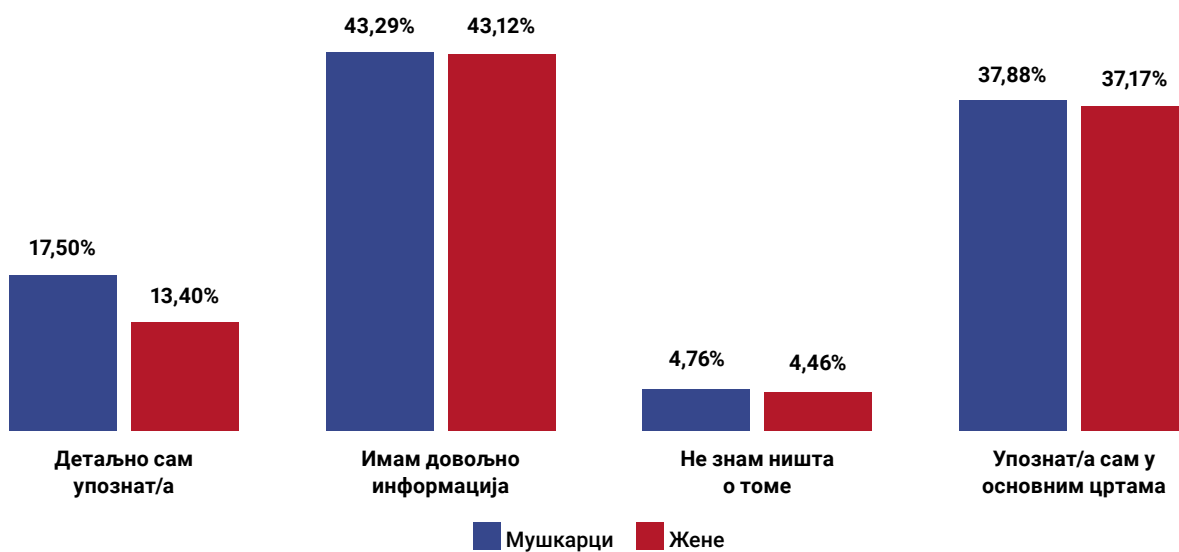
Укрштање по старости

Када је у питању хаковање налога на друштвеној мрежи, најмлађа популација (18-29 година) је најбоље упозната са овим ризиком (детаљно је упознато 17,4% младих наспрам 15,3%, колико износи просек).



Укрштање по полу

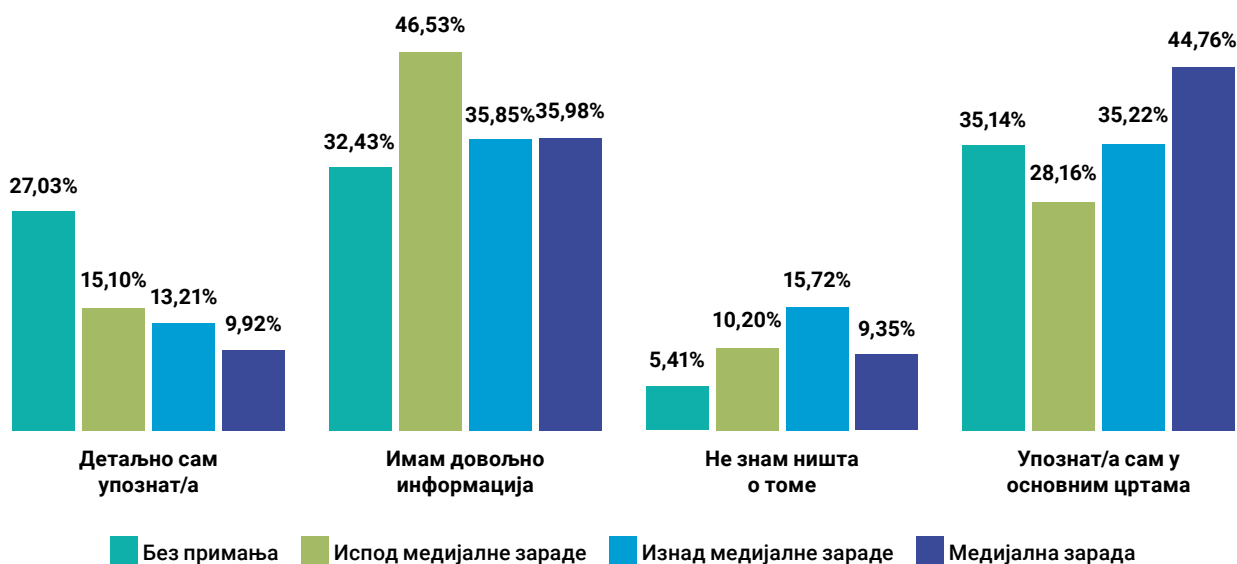
Мушкарци су мало детаљније информисани од жена (17,5% наспрам 13,4%).





Укрштање по висини примања

Они без примања, дакле студенти, и они који немају посао (и имају вишак слободног времена које проводе на друштвеним мрежама) у значајно већој мери су детаљно упознати о ризику хаковања налога на друштвеним мрежама. Чак 27% популације која спада у ову категорију износи овакав став, и то је готово дупло више од просека за целу популацију интернет корисника, који износи 15,3%.





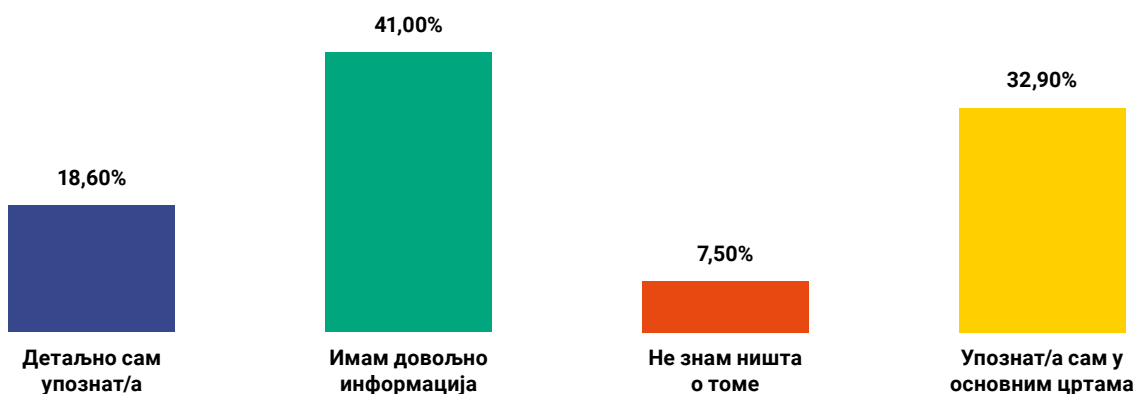
Злостављање на друштвеним мрежама и другим дигиталним платформама (cyber bullying)

59,6%

**испитаника
има довољно
информација
или је детаљно
упознато са овим
безбедносним
ризиком.**

Национална кампања, веома заступљена на телевизији, значајно је допринела информисаности грађана о злостављању на друштвеним мрежама. 59,6% испитаника, кумулативно, има довољно информација или је детаљно упознато са овим безбедносним ризиком.

Од свих поменутих безбедносних ризика, највећи број грађана је детаљно упознат баш са злостављањем на друштвеним мрежама (18,6%). Потпуно природно, о безбедности пре свега деце и младих, брину њихови родитељи, али и њихове баке и деке. Стога, иако ове две категорије нису, најчешће, угрожене на интернету, они су и даље веома важна циљна група за информисање о злостављању као безбедносном ризику коришћења интернета.





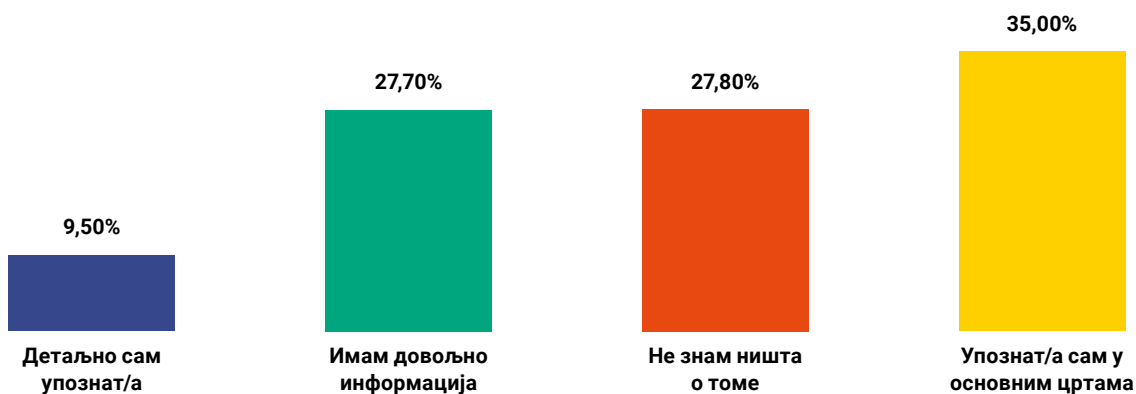
Безбедносни ризик 6

Преузимање интернет домена

27,8%

**испитаника
не зна ништа
о преузимању
интернет домена.**

За разлику од свих претходних безбедносних ризика, који су повезани са коришћењем интернета у приватне сврхе, преузимање интернет домена, као безбедносни ризик, скопчан је са коришћењем интернета у пословне сврхе. Стога, не чуди изузетно велики број испитаника који ништа не знају о томе (27,8%). Овом проценту можемо додати и трећину оних који су упознати са ризиком у основним цртама (35%).



РНИДС свим регистрантима .rs и .срб домена нуди чак три врсте заштите домена. Две основне врсте заштите, које задовољавају потребе највећег броја корисника, РНИДС не наплаћује.

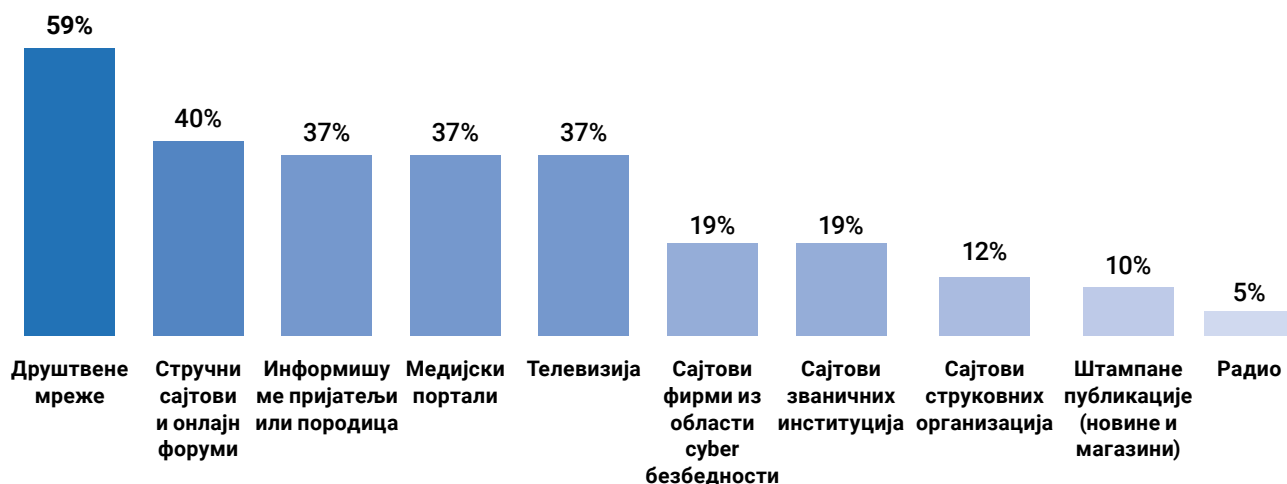
Годишње се изврши више стотина милиона успешних напада на домене, при чему се нападнути домени преусмеравају ка серверима и сервисима које контролише нападач. Захваљујући преусмеравању саобраћаја на лажни сајт идентичног изгледа, велики број корисника хакерима оставља своје креденцијале за приступ сервисима банака или другим сервисима за пословање на интернету. Притом, поред сајтова могу бити погођени и сервиси е-поште, као и сви други интернет сервиси повезани са "киднапованим" доменом, што често доводи до крађе осетљивих пословних и приватних података.

Ти напади су успешни углавном захваљујући небризи корисника домена и занемаривању безбедносних мера. Анализе након напада показале су да „киднаповани“ домени нису имали активну ниједну врсту заштите, а РНИДС свим регистрантима .rs и .срб домена нуди чак **три врсте заштите домена**. Две основне врсте заштите, које задовољавају потребе највећег броја корисника, РНИДС не наплаћује.

Где се информисете о дигиталној безбедности?

Корисници интернета се на најразличитије начине информисају о дигиталној безбедности и ризицима повезаним са коришћењем интернета.

Највећи број грађана, који користе интернет у Србији, информиса се на друштвеним мрежама, њих 59%. На стручним сајтовима и онлајн форумима информиса се 40% грађана. Следе медијски портали са 37%. Исти проценат корисника интернета информиса се преко телевизије, 37%. Телевизија је значајан медиј за преношење информације о дигиталној безбедности категорији становништва која, ипак, ређе користи интернет од просека, а то су старији од 60 година. Сајтови званичних институција (међу којима су МУП Републике Србије и Национални ЦЕРТ) место су информисања нешто мање од петине корисника интернета у Србији (19%).



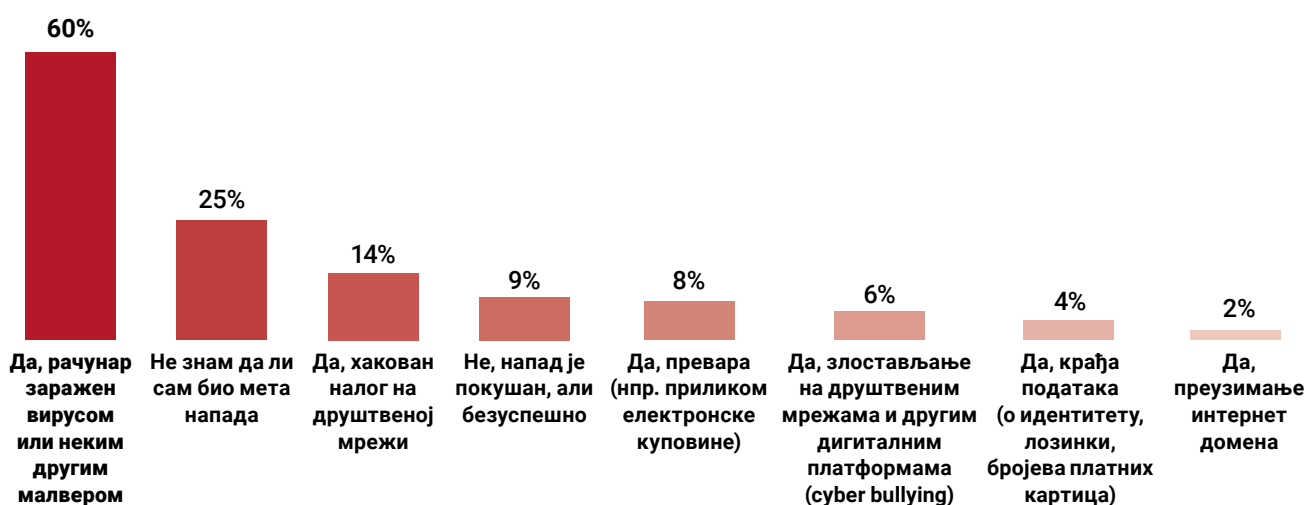
Да ли нам је нарушена безбедност на интернету?

— Да ли сте некад доживели неки од напада?

Четвртина корисника интернета у Србији (25%) не зна да ли је био мета cyber напада. Само 1 од 10 корисника (9%), био је, према свом мишљењу, жртва напада на интернету али напад није прошао.

Рачунари чак 60% корисника интернета у Србији су бар једном заражени вирусом или неким другим малвером. Велики проценат, 14% корисника, каже да им је хакован налог на друштвеној мрежи.

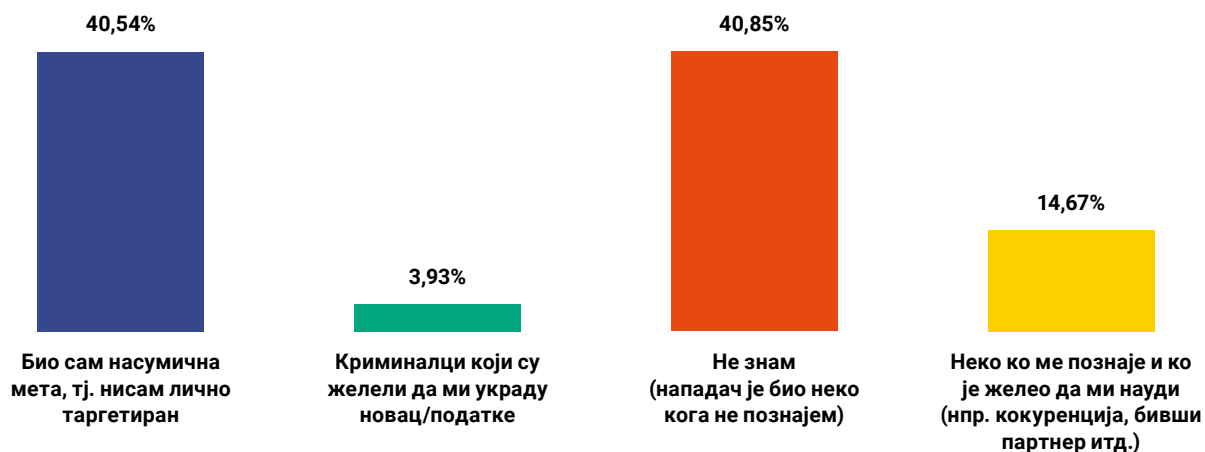
Рачунари чак **60%** корисника интернета су бар једном заражени вирусом или неким другим малвером.



— Ако сте доживели неки напад, шта мислите, ко је био нападач?

Готово исти број корисника интернета који су доживели напад, не зна ко је био нападач (40,85%) или мисле да су били насумична мета напада (40,54%). Ипак, 14,67% мисли да је нападач био неко ко их познаје и ко је желео да им науди (конкуренција, бивши партнер...). Мали број (3,93%) мисли да су напад извршили криминалци који су хтели да им изнуде новац или податке.

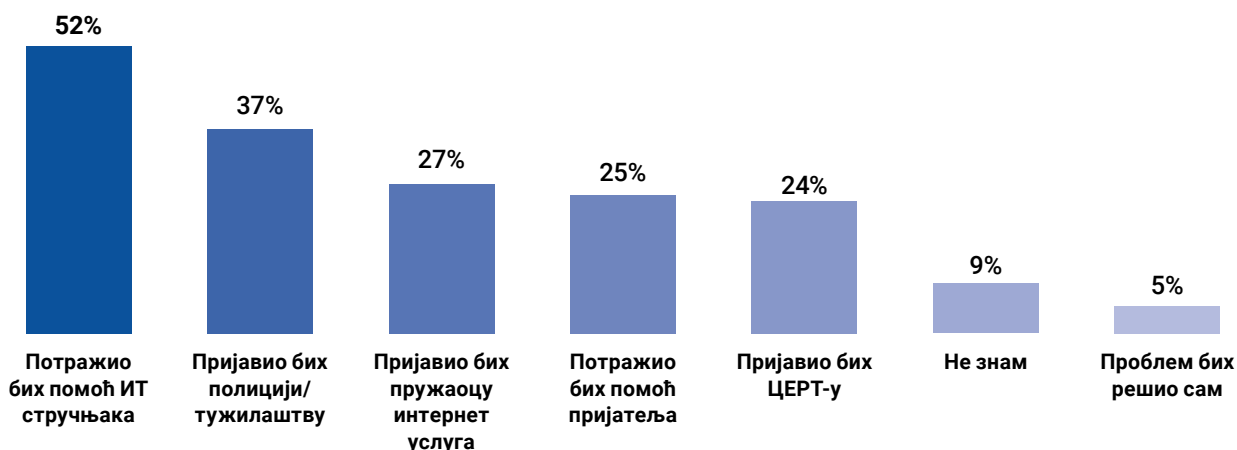
40,85% корисника интернета који су доживели напад не зна ко је био нападач.



— Шта бисте урадили у случају да постанете жртва напада?

Мало више од половине интернет корисника (52%) потражило би помоћ интернет стручњака. 37% би пријавило напад полицији или тужилаштву. 24% њих да би проблем интернет напада пријавило националном ЦЕРТ-у.

24% истраживаника
би проблем интернет
напада пријавило
националном
ЦЕРТ-у.

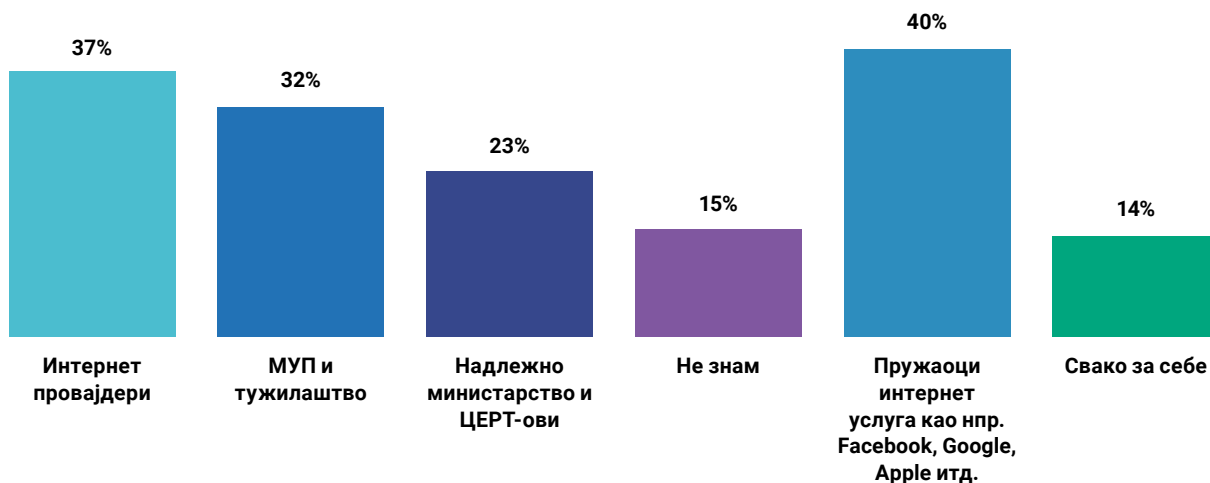


— Ко је одговоран за заштиту од напада у дигиталном простору?

Одговорност за заштиту од напада у дигиталном простору 2 од 5 интернет корисника у Србији приписује, пре свега, пружаоцима интернет услуга (компанијама које су власници друштвених мрежа и апликација за комуникацију). Корисницима су одговорни и интернет провајдери (37%) али и МУП и тужилаштво (32%).

Тек **14%**
корисника интернет
у Србији препознаје
своју одговорност за
личну безбедност на
интернету.

Мало мање од четвртине корисника интернета у Србији (23%) апострофира надлежна министарства и ЦЕРТ-ове као одговорне за њихову безбедност у дигиталном простору.



Како штитимо личне податке на интернету

Морамо пажљиво да сагледамо податак да тек 14% корисника интернета у Србији препознаје своју одговорност за личну безбедност на интернету.

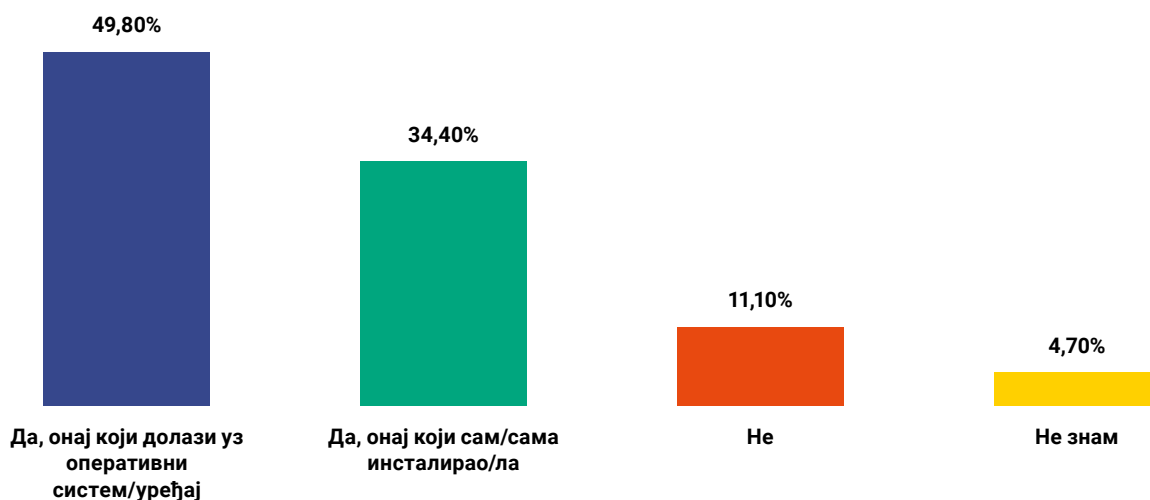
У вези тога, безбедност корисника интернета била би много више угрожена да сами уређаји (рачунари и мобилни телефони), оперативни системи и софтвери, друштвене мреже и апликације за комуникацију и рад, не обезбеђују корисницима интернета минимум безбедности.

Све већи број пружалаца услуга на интернету од својих корисника захтева да им лозинка садржи велика и мала слова, бројеве и специјалне знаке. Такође, многи од њих захтевају двостепену проверу идентитета, потврђивање е-мејл адреса као и повезивање мобилног броја телефона са интернет налогом ради заштите података корисника услуга.

— Да ли користите антивирус софтвер?

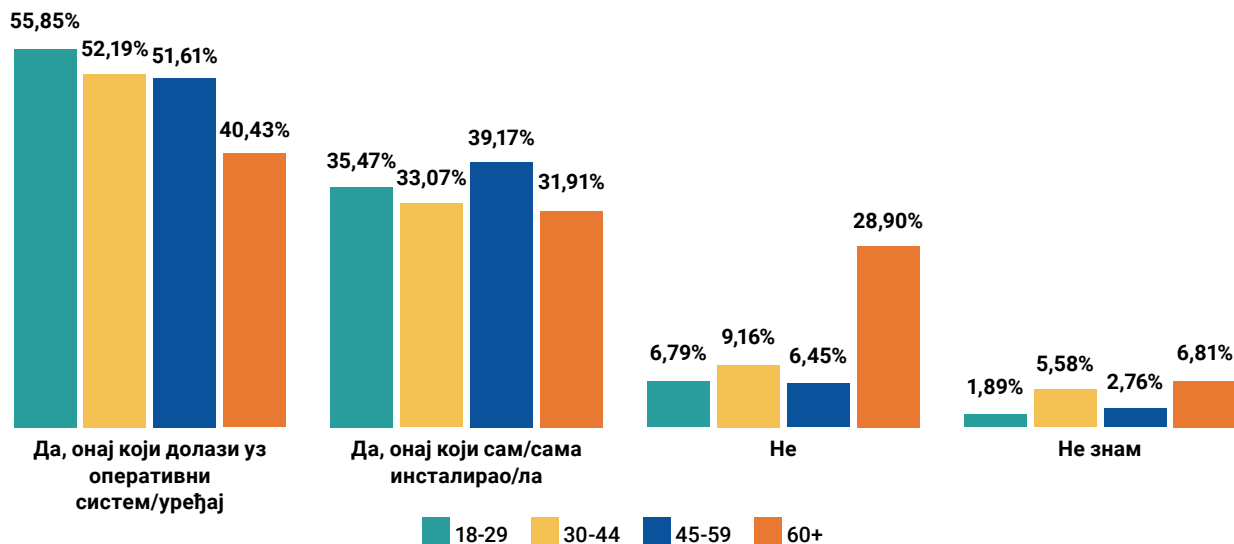
84,2% корисника интернета у Србији користи антивирус софтвер. Близу половине њих (49,8%) користи онај антивирус софтвер који долази уз оперативни систем. 11,1% корисника не користи антивирус софтвер, а 4,7% не зна да ли га користи.

84,2%
корисника интернета
у Србији користи
антивирус софтвер.



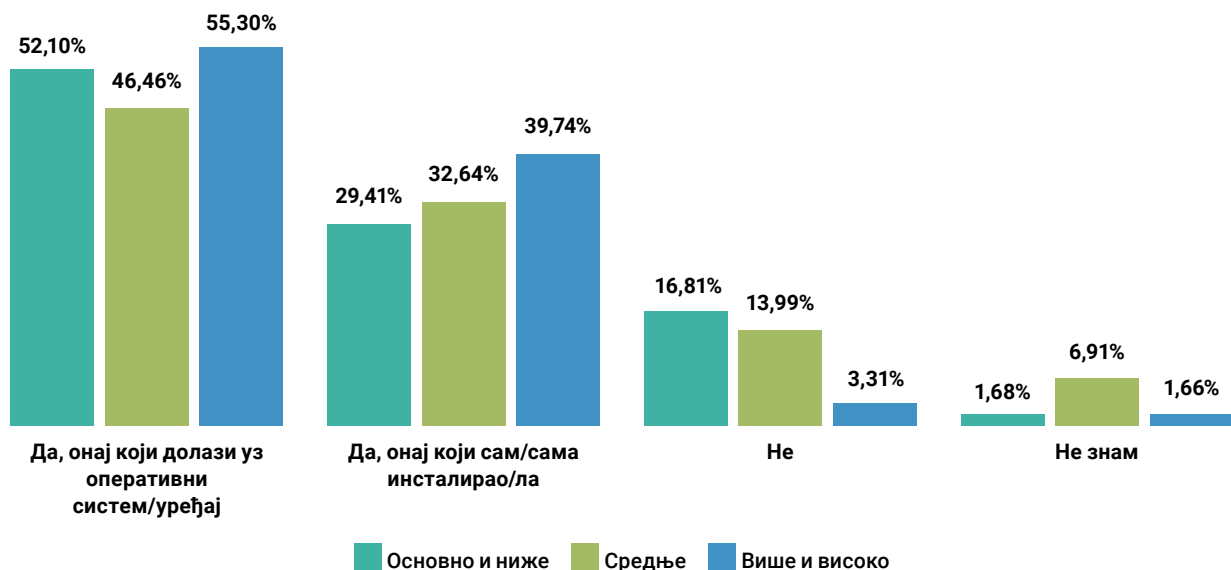
Укрштање по старости

Старији од 60 година у најмањој мери користе антивирус софтвер. Чак 28,9%, скоро три пута више од просека (11,1%), не користи антивирус софтвер.



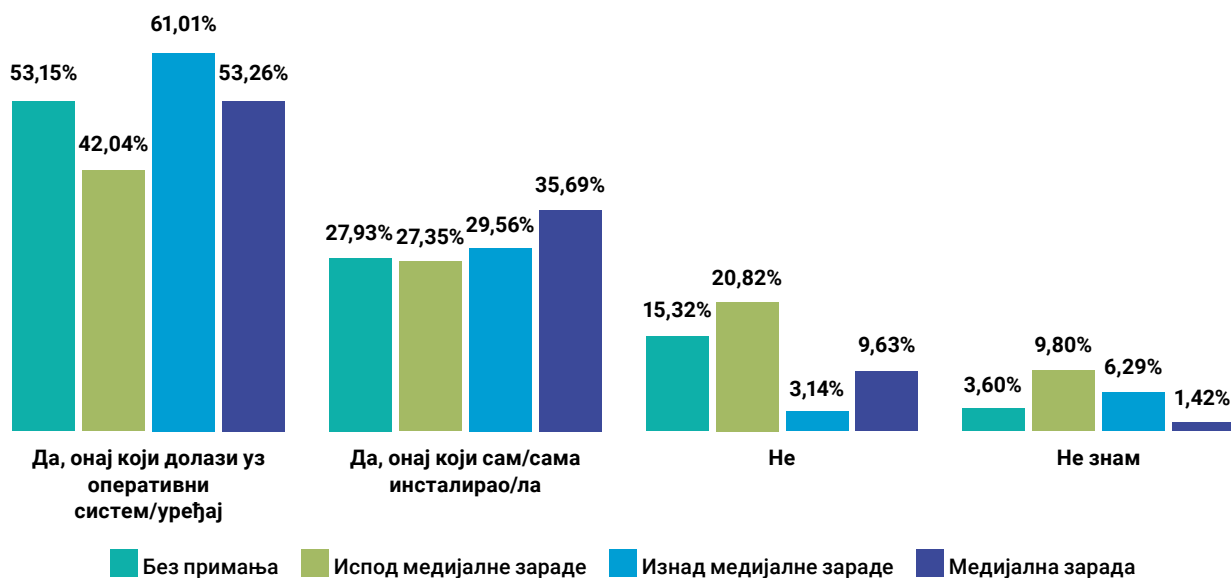
Укрштање по образовању

Антивирус софтвер у мањој мери користе грађани са најнижим степеном образовања (16,8%) у односу на просечних 11,1%.



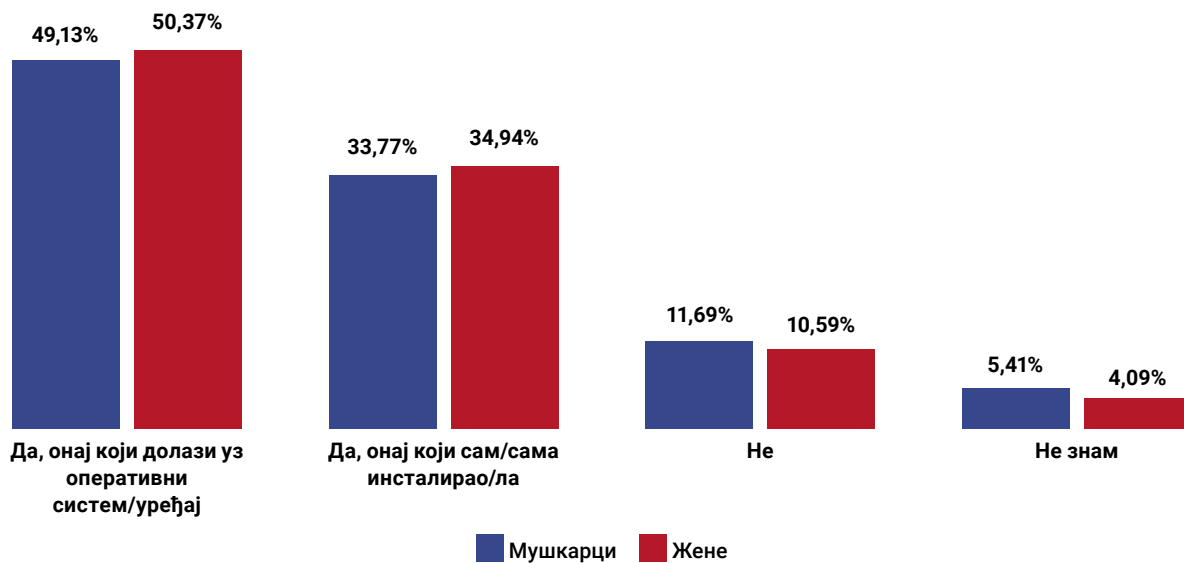
Укрштање по висини примања

Корисници чија су примања испод медијалне зараде у већој мери не користе антивирус софтвер (20,8%) али и не знају да ли га користе (9,8%).



Укрштање по полу

Жене и мушкарци готово подједнако користе антивирус софтвер.

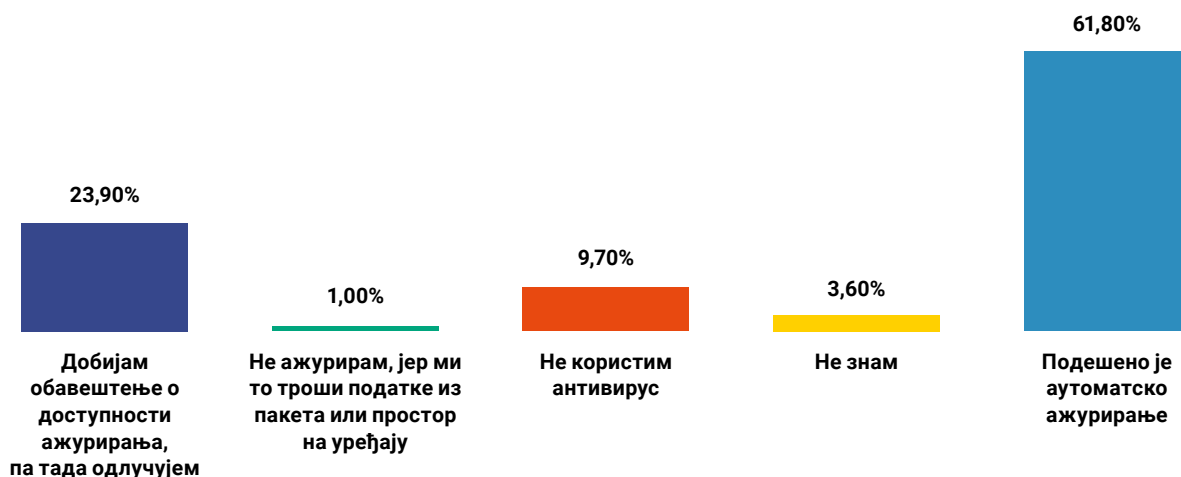


— Како ажурирате антивирус софтвер?

61,8% корисника ажурира антивирус софтвер јер им је подешено аутоматско ажурирање. Још 23,9% добија обавештење о ажурирању софтвера па одлучује да ли ће га ажурирати.

61,8%

корисника ажурира антивирус софтвер јер им је подешено аутоматско ажурирање.

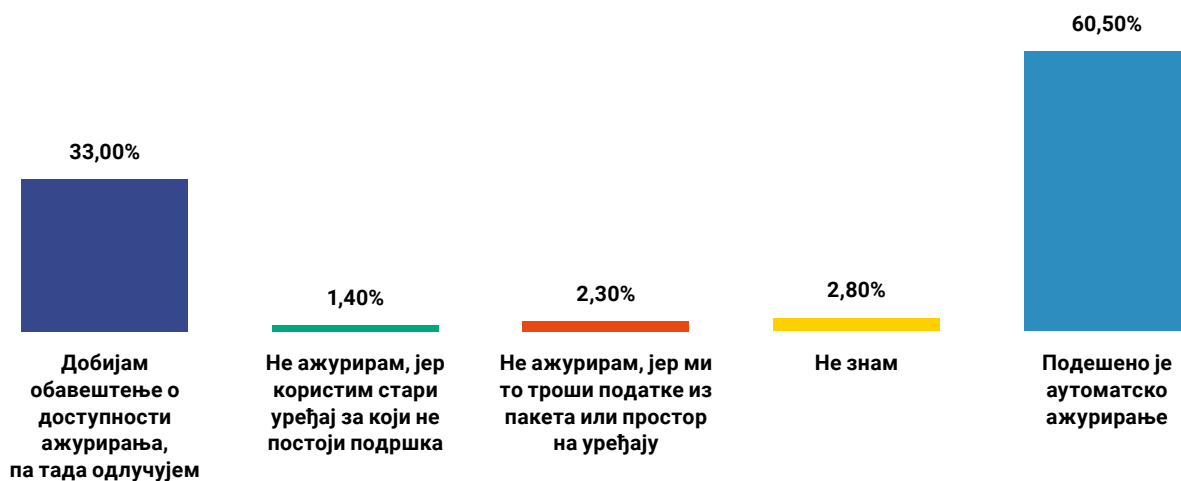


— Како ажурирате оперативни систем на својим рачунарима и мобилним уређајима?

И када је ажурирање оперативних система у питању, ситуација је слична. 60,5% њих је подесило аутоматско ажурирање и још 33% добија обавештење о доступности ажурирања па тада одлучује. Неки одлажу ажурирање због недостатка времена или недостатка простора у меморији.

60,5%

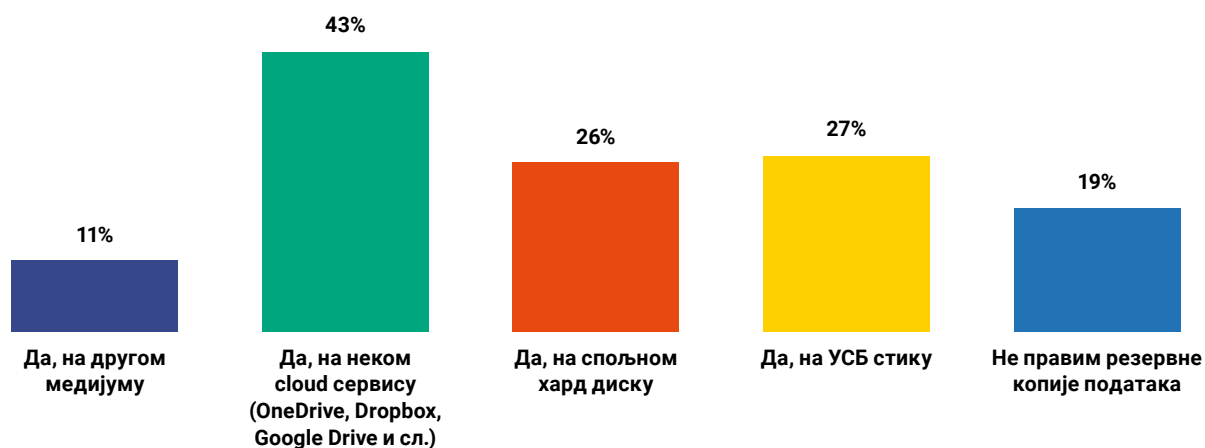
њих је подесило аутоматско ажурирање.



— Да ли правите резервне копије података/слика/докумената?

Петина корисника интернета у Србији (19%) не прави резервне копије. Од оних који их праве, највећи број користи cloud сервисе за ову активност, њих 43%.

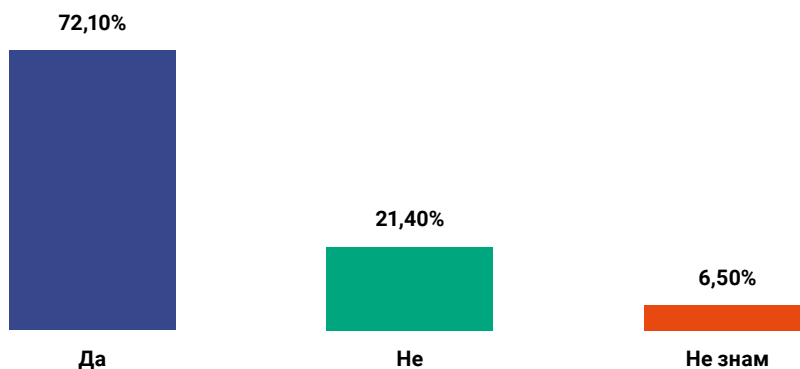
Петина
корисника интернета
у Србији (19%) не прави
резервне копије.



— Да ли при инсталацији апликација проверавате какав приступ подацима и функцијама уређаја апликација захтева?

Чак 72,1% пунолетних корисника интернета у Србији при инсталацији апликација проверава какав приступ подацима и функцијама уређаја апликација захтева. Пошто је ово изненађујуће велики број, неопходно је његово тумачење. Корисници од провајдера услуга добијају поруку коју треба да потврде, и наше је мишљење да највећи број грађана летимично прође погледом кроз садржај, и потврђује опције које од њих захтева апликација.

Чак **72,1%**
пунолетних корисника
при инсталацији
апликација
проверава какав
приступ подацима и
функцијама уређаја
апликација захтева.

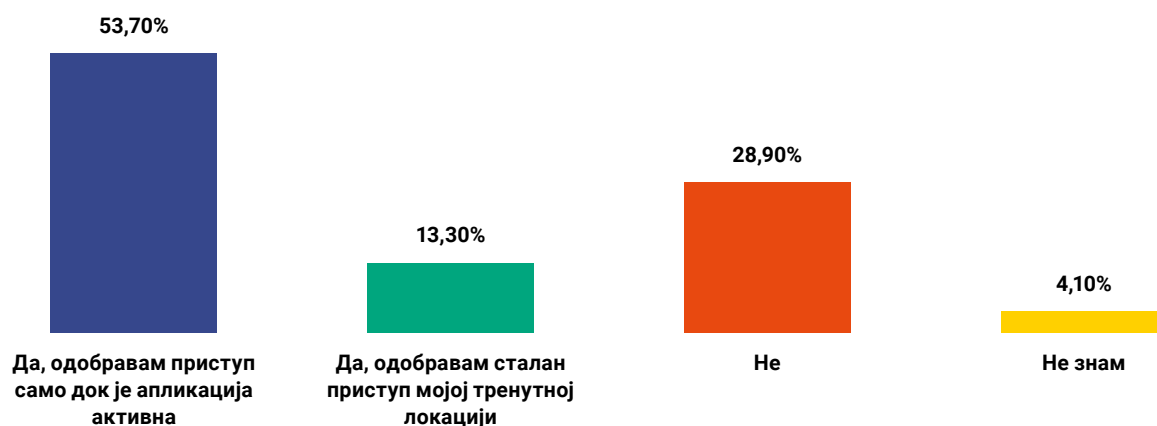


— Да ли одобравате апликацијама приступ вашој тренутној позицији/географској локацији?

67% корисника, кумулативно, одобрава апликацијама приступ тренутној позицији или географској локацији, стално или док се апликација користи. Чак 13,3% дозвољава апликацији да има сталан приступ њиховој тренутној локацији.

67%

одобрава приступ тренутној позицији или географској локацији, стално или док се апликација користи.



— Како приступате рачунару?

Још увек велики број корисника интернета у Србији, чак 39%, својим рачунарима приступа директно, без подешене лозинке или било које друге врсте идентификације.

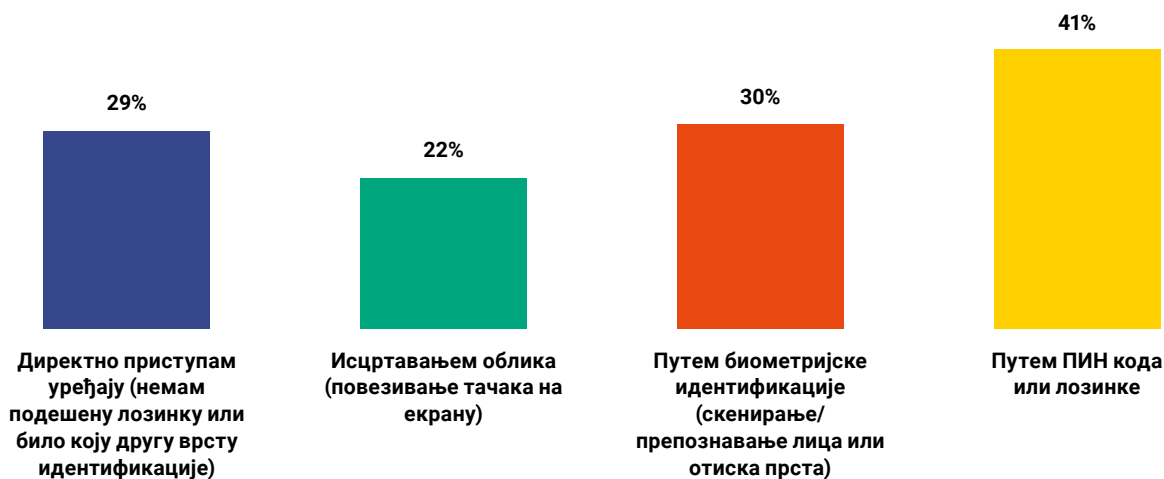
Чак **39%** корисника својим рачунарима приступа директно.



— Како приступате мобилном уређају?

Близу трећине корисника интернета на мобилном телефону (29%) приступа директно уређају, без лозинке или неке друге врсте идентификације. Они који приступају мобилном уређају коришћењем неке врсте заштите, најчешће то чине путем ПИН кода или лозинке (41%).

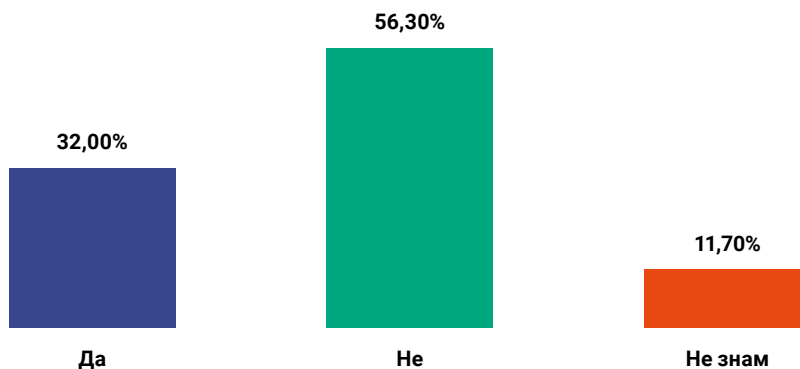
29%
корисника интернета на мобилном телефону приступа директно уређају, без лозинке или неке друге врсте идентификације.



— Да ли користите двофакторску (двостепену) проверу идентитета, ако имате ту опцију?

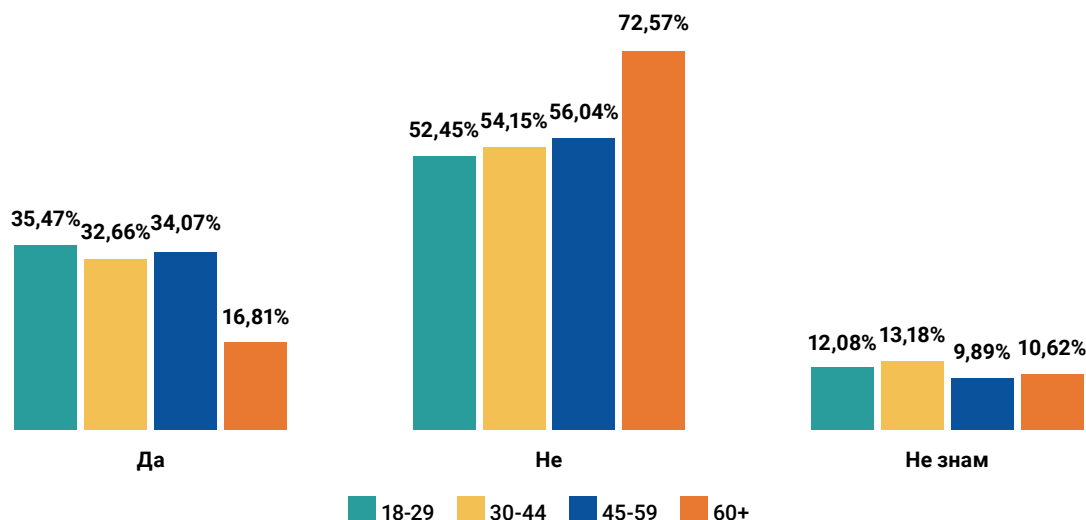
32% корисника интернета користи двофакторску/двостепену проверу идентитета. Велики број сајтова и мобилних апликација има обавезну двофакторску проверу идентитета па је и то разлог релативно великог процента.

32%
корисника интернета користи двофакторску/двостепену проверу идентитета.



Укрштање по старости

Најстарији суграђани у најмањој мери користе двофакторску проверу идентитета. 72,6% старијих од 60 година не користи ову врсту провере и то је 16,3 процентних поена више од просечних 56,3%.

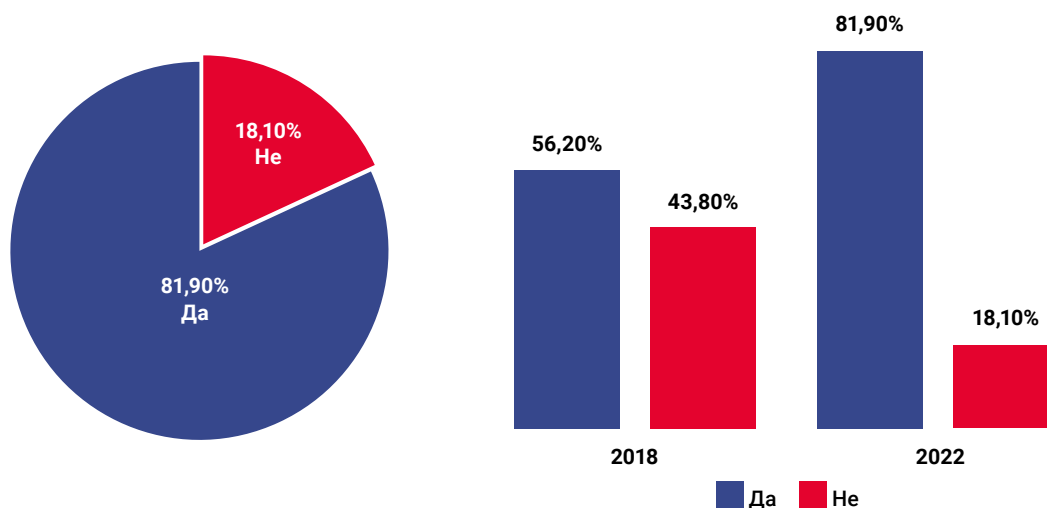


— Да ли ваше лозинке (за приступ рачунару, мобилном уређају, сајтовима и дигиталним сервисима) садрже специјалне знакове, бројеве, велика и мала слова?

Код чак 81,9% корисника интернета лозинке које користе садрже специјалне знаке.

Многи интернет сајтови и апликације захтевају од својих корисника да, када креирају налоге, обавезно, због сопствене заштите али и заштите самог сајта или апликације, морају да креирају лозинку која садржи специјалне знаке, велика и мала слова, бројеве, па је и то разлог овако великог процента и великог напретка у односу на период од пре 4 године.

Код чак **81,9%**
корисника лозинке
садрже специјалне
знаке.



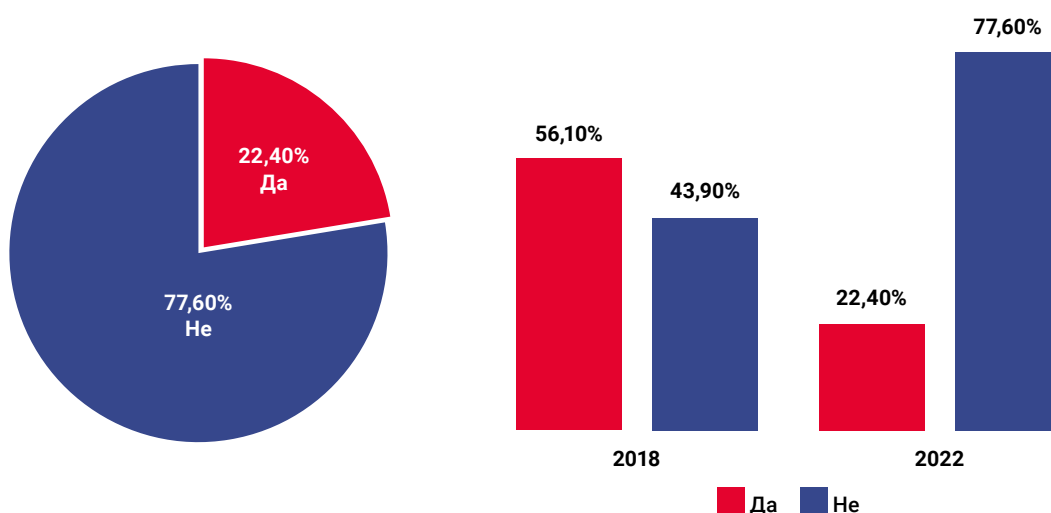
— Да ли ваше лозинке садрже неки од личних података као што су датум рођења, име кућног љубимца, година рођења и слично?

Три четвртине корисника интернета у Србији разумело је да може бити веома опасно користити лозинке које садрже неки од личних података, па их не користе.

У односу на 2018. годину, бележимо значајну промену у личном делању по питању безбедности, много мање грађана (22,40% у односу на претходних 56,1%) уписује личне податке у лозинке.

Три четвртине

корисника интернета у Србији не уписује личне податке у лозинке.



— Да ли користите различите лозинке за приступ сваком уређају, друштвеној мрежи, сајту или дигиталном сервису?

Мало више од пола корисника интернета у Србији (51,8%, кумулативно) користи свуда исту лозинку или користи исту лозинку на неким местима. 48,2% увек поставља различите лозинке.

51,8%

корисника користи свуда исту лозинку или користи исту лозинку на неким местима.



— Где чувате ваше лозинке?

Више од половине корисника памти лозинке (53,2%), а још 28,7% их записује на папиру. Тек 8,7% чува лозинке у оквиру веб читача или користи посебну апликацију за креирање и памћење лозинки.

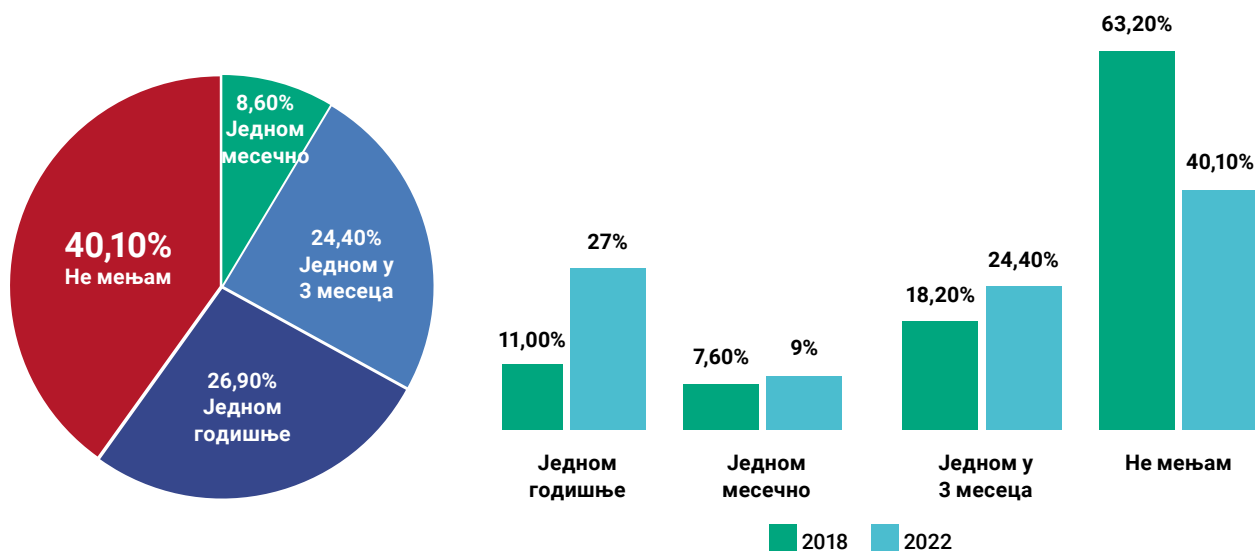
53,2%
корисника памти лозинке,
а **28,7%**
их још увек записује на папиру.



— Колико често мењате лозинку за приступ вашем рачунару или мобилном уређају?

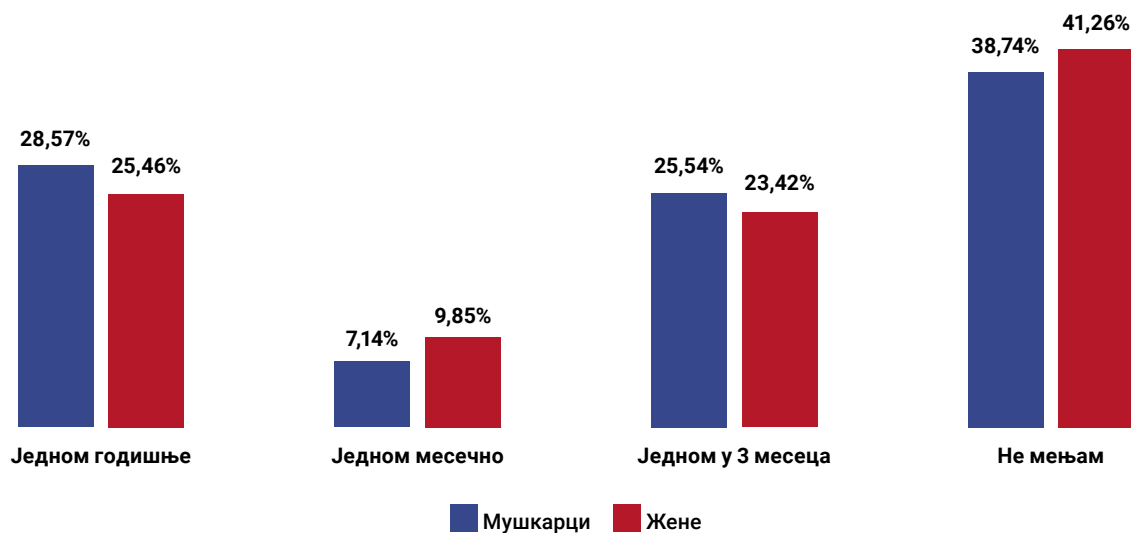
40,1% никад не мења лозинку на свом рачунару. Иако је и даље реч о веома великом броју грађана који на овај начин нарушавају своју дигиталну безбедност, у 2022. години, ипак, имамо значајно побољшање у односу на 2018. годину, када чак 63,2% корисника интернета никад није мењало своју лозинку.

40,1%
никад не мења лозинку
на свом рачунару.



Укрштање по полу

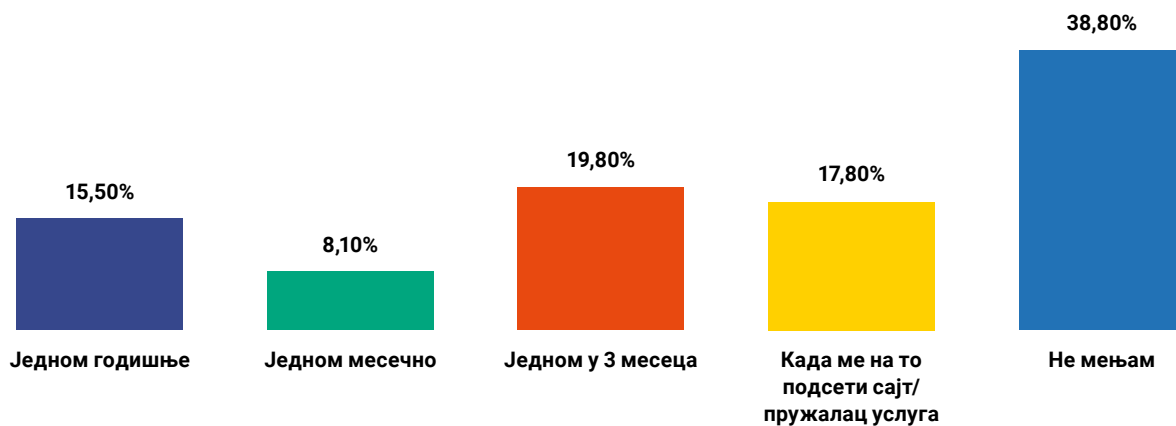
41,3% жена и 38,7% мушкараца никад не мења своју лозинку.



— Колико често мењате лозинку за приступ сајтовима и дигиталним услугама?

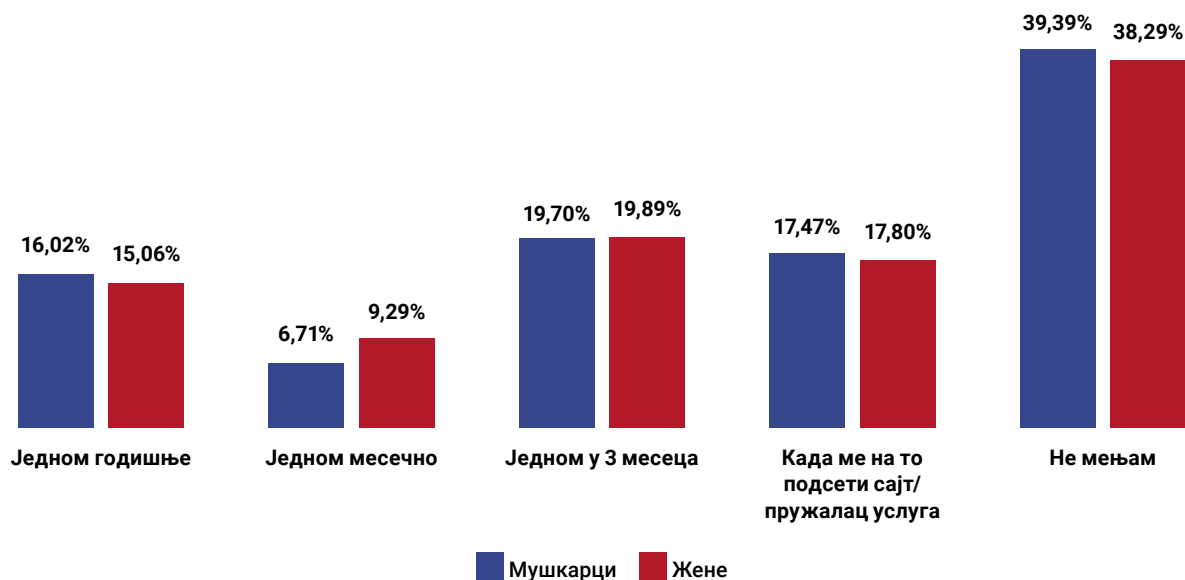
Слично одговору на претходно питање, 38,8% корисника интернета у Србији никад не мења лозинке за приступ сајтовима и дигиталним услугама.

38,8%
корисника никад не мења лозинке за приступ сајтовима и дигиталним услугама.



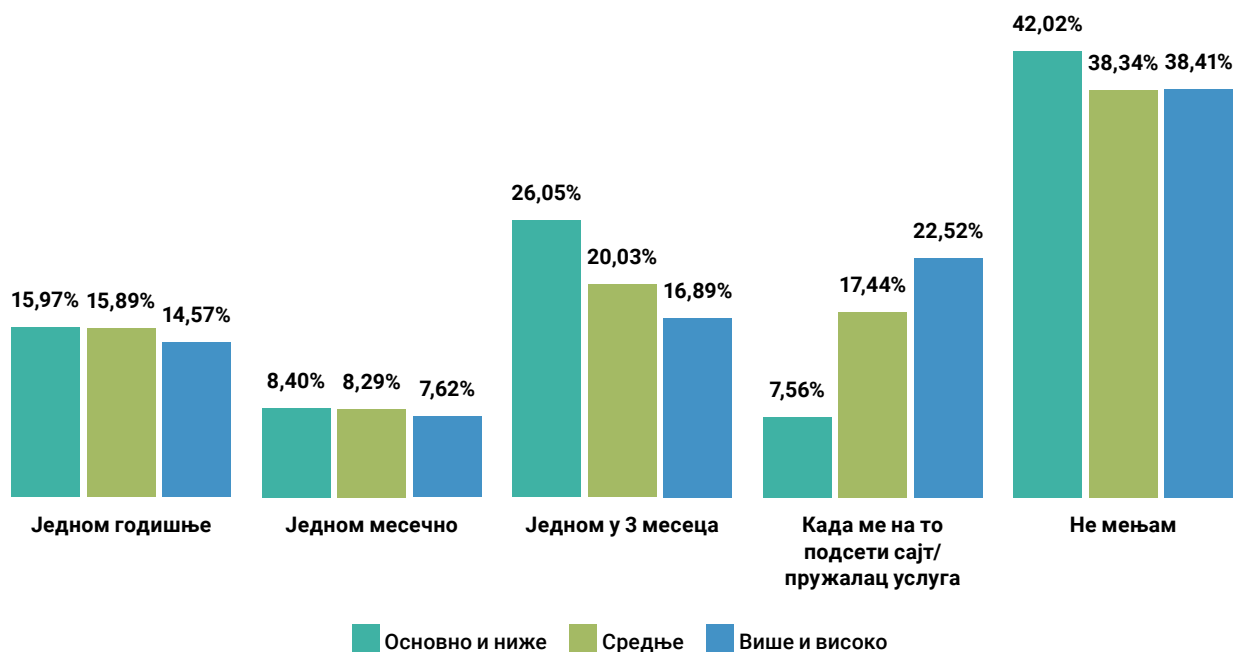
Укрштање по полу

Када је у питању промена ове врсте лозинки, мушкарци су за нијансу неодговорнији. 39,4% мушкараца, наспрам 38,3% жена, никада не мења лозинку за приступ сајтовима и дигиталним услугама.



Укрштање по образовању

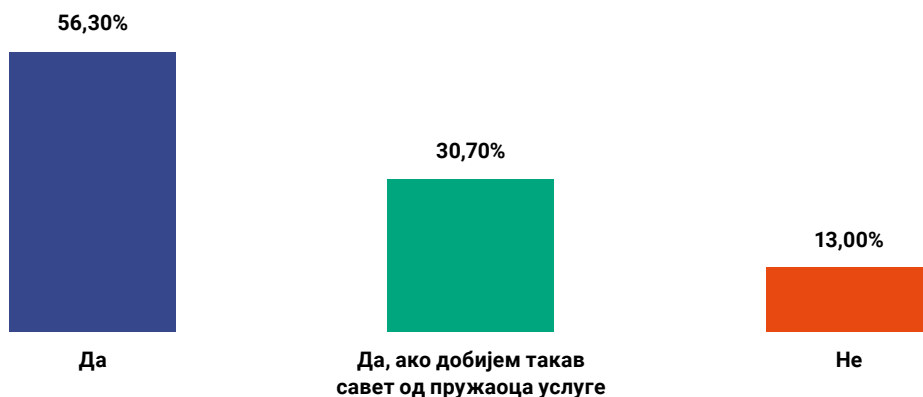
42% интернет корисника у Србији који имају основно и ниже образовање никада не мења лозинке на сајтовима и дигиталним сервисима и то је за 3,2 процентна поена више од просечне вредности.



— Да ли промените лозинку ако сазнате да је нападнута друштвена мрежа, сајт или дигитална услуга коју користите?

Чак 13% корисника интернета неће променити лозинку ни ако сазна да је нападнута друштвена мрежа, сајт или нека друга дигитална услуга коју користе. Још 30,7% корисника сачекаће савет од пружаоца услуге, па ће тек тада променити лозинку.

13%
корисника неће
променити лозинку ни
ако сазна за напад.



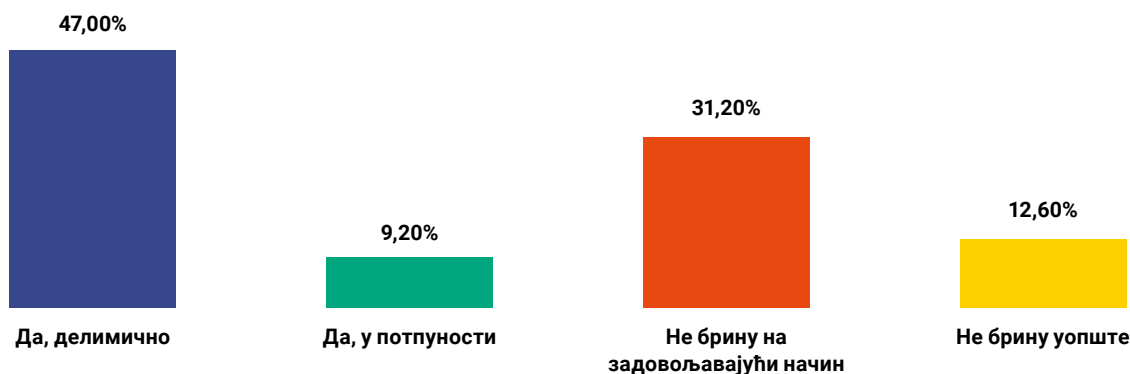
— Да ли верујете да се власници друштвених мрежа (ТикТок, Instagram итд.) и интернет претраживача (Google, Bing итд) брину о вашој безбедности на задовољавајући начин?

Иако одговорност за заштиту од напада у дигиталном простору 40% интернет корисника у Србији приписује, пре свега, пружаоцима интернет услуга (компанијама које су власници друштвених мрежа и апликација за комуникацију), у готово истом проценту (43,8%, кумулативно) мисле да власници друштвених мрежа и интернет претраживача не брину уопште или не брину на задовољавајући начин о безбедности корисника интернета.

14%
пунолетњих грађана
Србије који користе
интернет препознаје
своју одговорност за
личну безбедност.

47% мисли да само делимично брину, а тек 9,2% да у потпуности брину о безбедности корисника интернета.

У том случају, логика налаже да би о безбедности на интернету требало да бринемо сами, међутим, тек 14% пунолетњих грађана Србије који користе интернет препознаје своју одговорност за личну безбедност.



— Да ли сами подешаваате ниво заштите приватности на друштвеним мрежама и другим дигиталним платформама, или користите иницијална подешавања?

Трећина корисника интернета (32,1%) користи иницијална подешавања нивоа заштите приватности. Охрабрује податак да 2/3 корисника интернета сами подешавају приватност на друштвеним мрежама и дигиталним платформама.

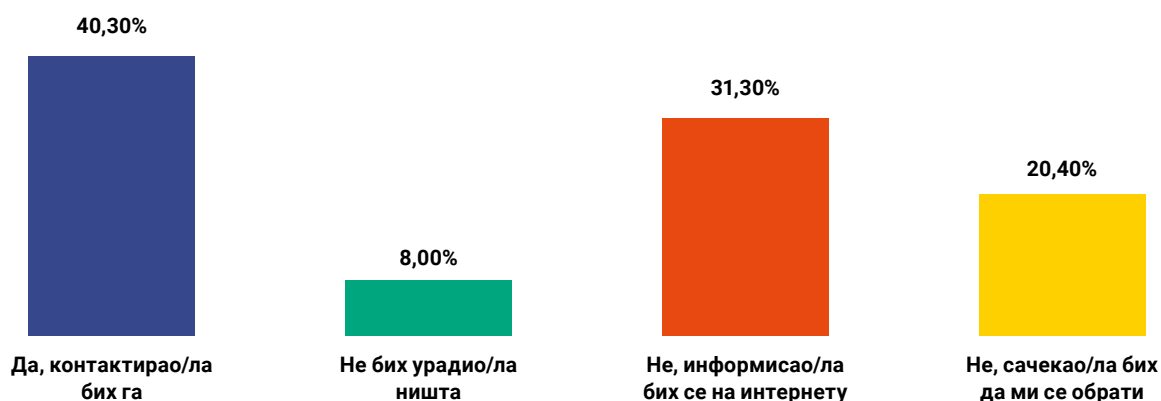


32,1%
корисника користи иницијална подешавања нивоа заштите приватности.

— Ако је ваш пружалац услуга нападнут, да ли бисте га контактирали да се информишете о томе шта се десило и да ли су ваши подаци угрожени?

Готово 60% корисника интернета не би се понашало проактивно у случају да је њихов пружалац услуга нападнут. Не би га контактирали да се информишу о нарушавању безбедности, сачекали би да им се он обрати или не би урадили ништа.

Готово **60%**
корисника се не би понашало проактивно у случају да је њихов пружалац услуга нападнут



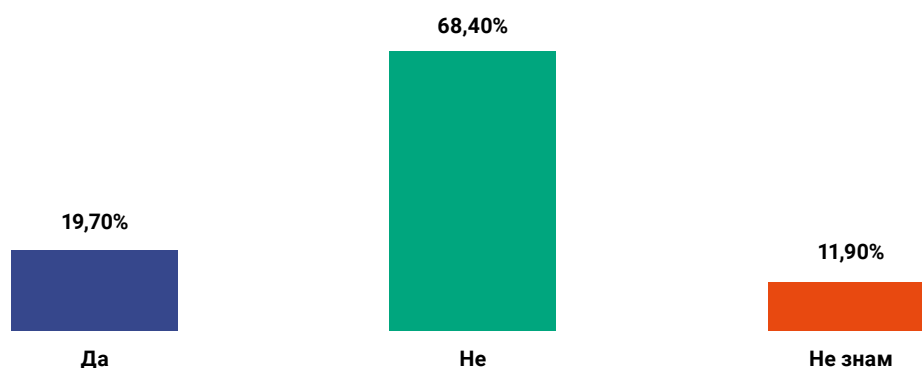
— Да ли сте некад одговорили на е-пошту или кликнули на линк у поруци, коју сте добили од непознате особе?

19,7% корисника интернета признаје да се бар једном "упецало" на е-поруку и кликнуло на линк који су добили од непознате особе. Још 11,9% не зна да ли је кликнуло или не.

2/3 пунолетних корисника интернета у Србији никад није кликнуло на линк који су од непознате особе добили у е-поруци.

19,7%

корисника признаје да се бар једном "упецало" на е-поруку и кликнуло на линк који су добили од непознате особе



— Да ли некада шаљете своје корисничко име, лозинку или број кредитне картице путем порука (нпр. е-пошта, SMS, Viber/WhatsApp/Messenger итд)?

Највећи број корисника интернета (89,2%) никада не шаље своје корисничко име, лозинку или број кредитне картице путем порука. Ипак, 10,8% шаље податке и на овај начин се не понаша безбедно.



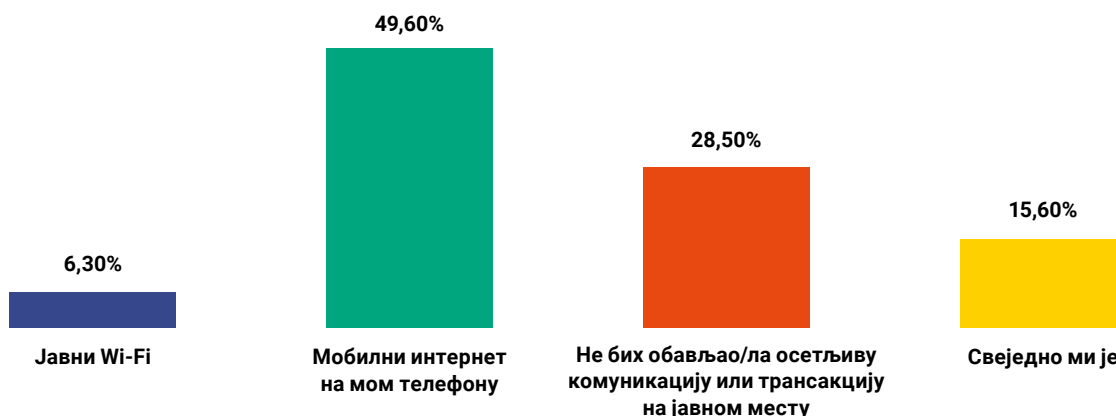
89,2%

корисника никада не шаље своје корисничко име, лозинку или број кредитне картице путем порука.

— Шта бисте радије користили за обављање осетљиве комуникације или онлајн трансакције (куповину, онлајн банкарство) на јавном месту (у ресторану, кафићу, на аеродрому)?

Близу половине корисника интернета у Србији (49,6%) за обављање осетљиве комуникације или онлајн трансакција (куповину, онлајн банкарство) на јавном месту (у ресторану, кафићу, на аеродрому) користило би мобилни интернет на свом телефону. **Још 28,5% не би обављало осетљиву комуникацију или трансакцију на јавном месту.**

49,6%
корисника би
користи́ло мобилни
интернет на свом
телефону.



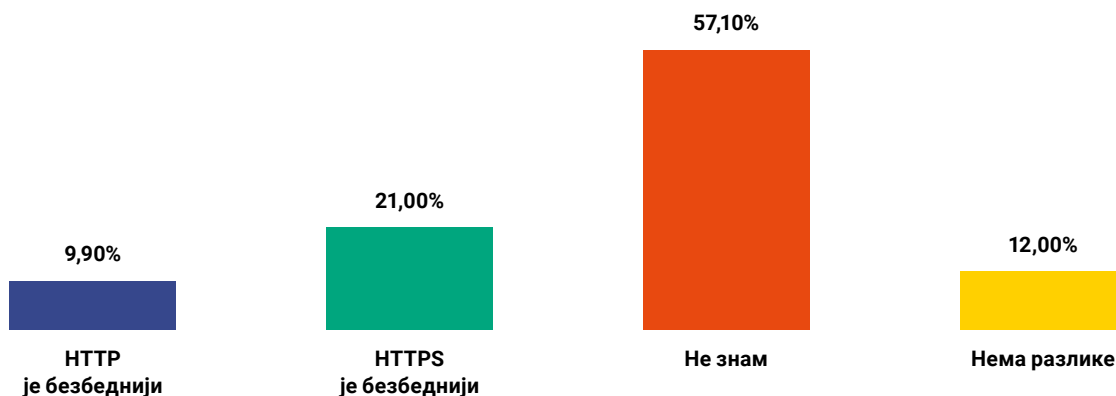
— Да ли је безбеднији сајт чија адреса почиње са HTTP или HTTPS?

57,1% не зна одговор на ово питање. Само 21% зна да је HTTPS безбеднији, 12% мисли да нема разлике, док 9,9% мисли да је HTTP безбеднији.

Само **21%**
испитаника зна да је
HTTPS безбеднији.

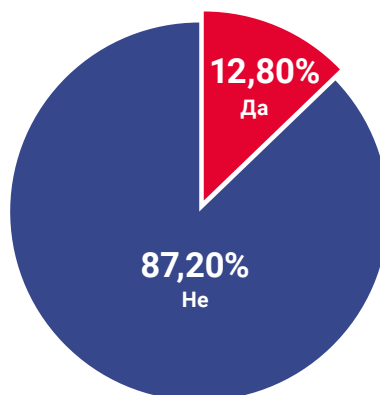
Разлика између HTTP и HTTPS је у томе да ли су подаци који се шаљу и примају шифровани. "S" у HTTPS-у значи Secure или безбедан. Дакле, ако веб-сајт који посетите користи HTTPS, то значи да се подаци који се шаљу и примају шифрују помоћу SSL-а (Secure Socket Layer).

Супротно томе, ако је веб-сајт користи HTTP, то значи да подаци који се шаљу и примају нису шифровани. Будући да идентитет власника сајта није тачно идентификован, хакери могу да експлоатишу и украду осетљиве информације из протока.



— Ако на јавном месту или у свом пословном окружењу пронађете USB стик који није ваш, да ли ћете га узети за коришћење?

87,2% корисника интернета неће узети USB стик. Ипак, њих 12,8% ће га узети када га пронађе на јавном месту. Ово је веома небезбедно понашање јер убацивањем USB стика у рачунар можемо унети опасне вирусе или друге малвере.

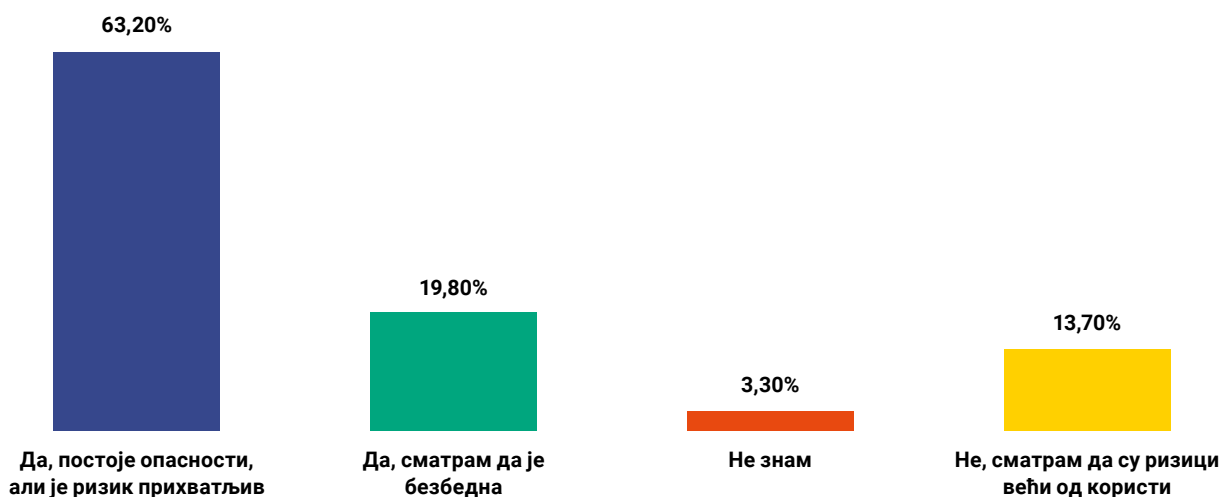


87,2%
корисника неће узети USB стик за коришћење када га пронађе на јавном месту.

— Да ли сматрате да је онлајн куповина безбедна?

Више од 4/5 корисника интернета (83%, кумулативно) сматра да је онлајн куповина безбедна, односно да постоје опасности, али да је ризик прихватљив.

83%
корисника у Србији сматра да је онлајн куповина довољно безбедна.



Укрштање по полу

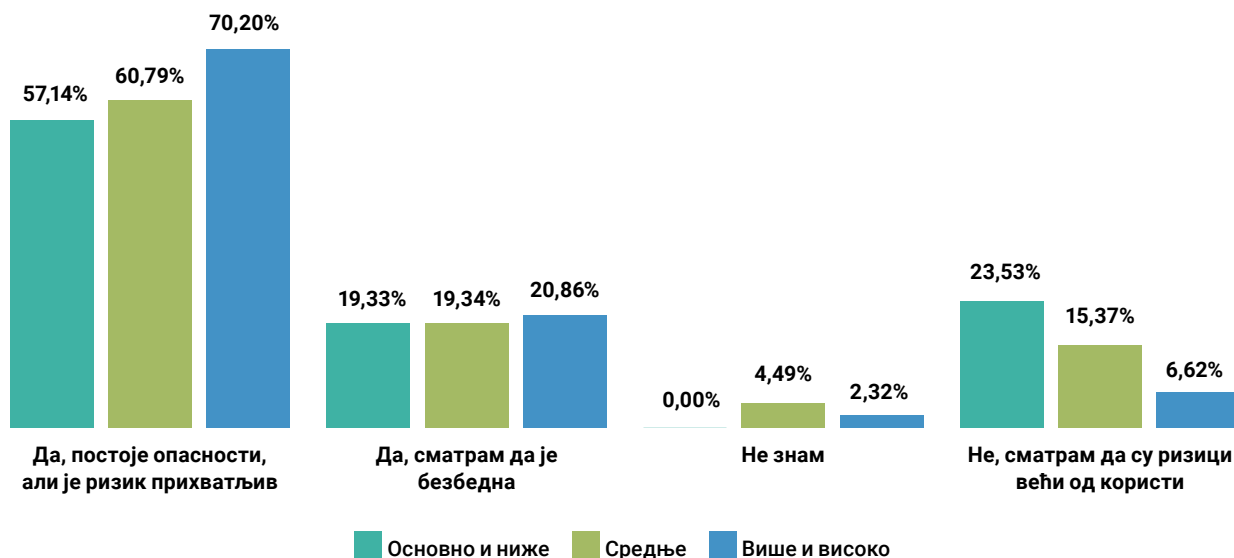
Већинском ставу грађана Србије да је онлајн куповина безбедна доприноси 65,6% жена које стоје иза становишта да постоје опасности, али да је ризик онлајн куповине прихватљив. 60,4% мушкараца дели њихов став.



Укрштање по образовању

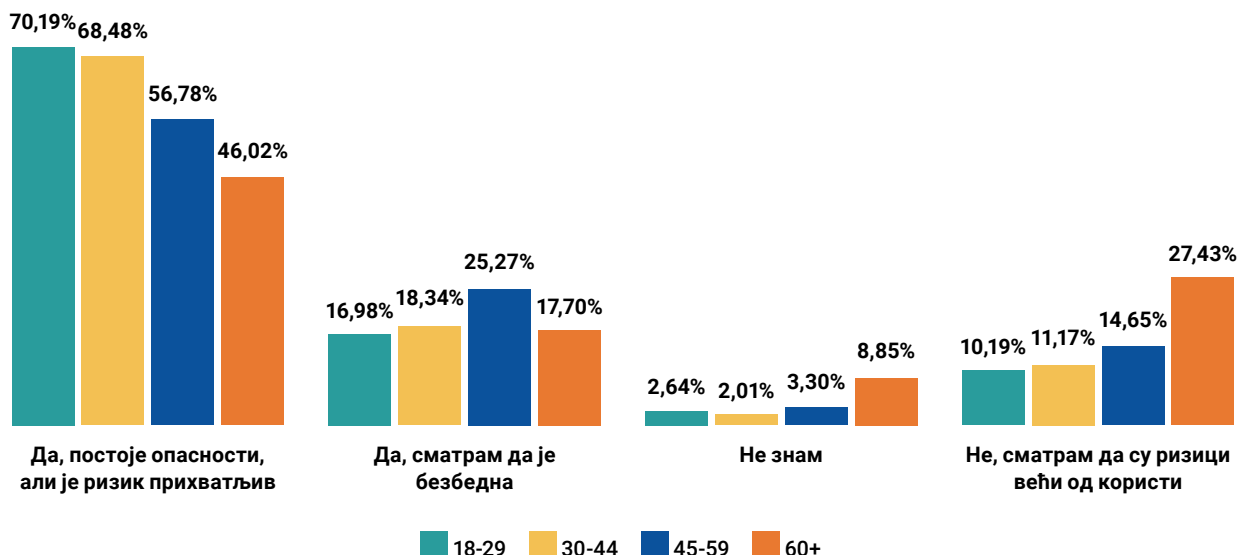
Мишљењу о безбедној куповини у великој мери доприносе високо образовани грађани Србије. Да је онлајн куповина безбедна или да је ризик за онлајн куповину прихватљив сматра збирно 91,6% високообразованих грађана Србије.

Значајно изнад просека (23,5% у односу на просечних 13,7%) корисника са основним и нижим образовањем сматра да су ризици онлајн куповине већи од користи и да, самим тим, онлајн куповина није безбедна.



Укрштање по старости

Овај проценат је још већи (27,4%) ако посматрамо став грађана старијих од 60 година. Међу најстаријим грађанима је највише оних који не знају да ли је онлајн куповина безбедна или не (8,8%).

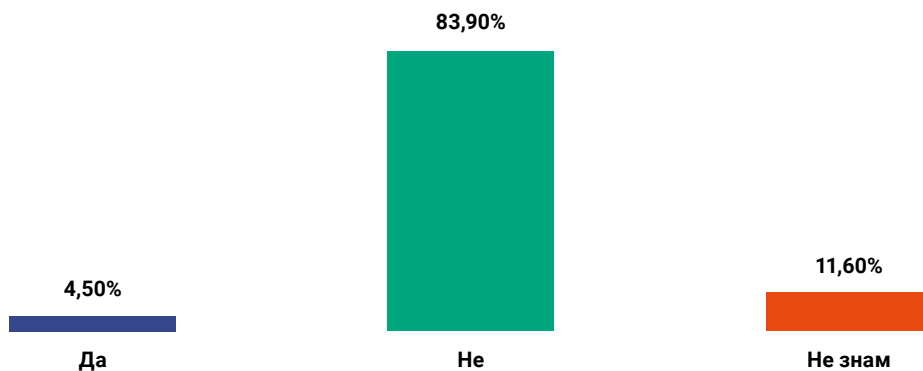


— Ако вам продавац накнадно тражи податке о картици, иако сте претходно договорили плаћање поузећем, да ли бисте му дали податке?

83,9% не би дало податке, док 11,6% корисника не зна да ли би их дали, а 4,5% корисника би дало податке.

83,9%

корисника интернета у Србији не би дало податке.



04.

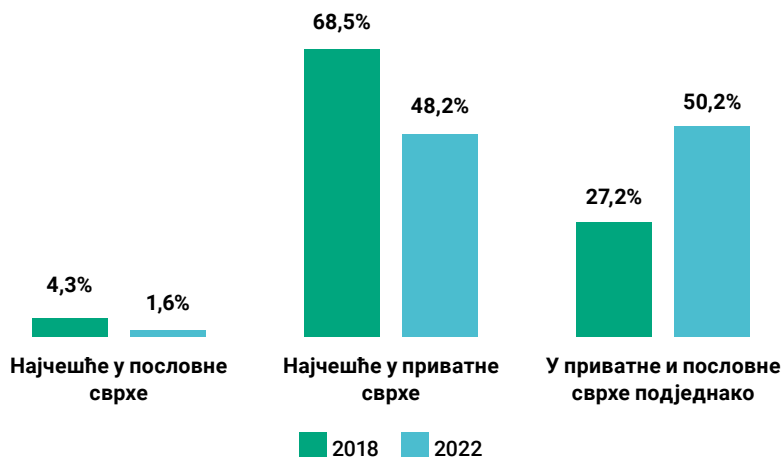
Додатак: Како користимо интернет

Како користимо интернет

У које сврхе најчешће користите интернет?

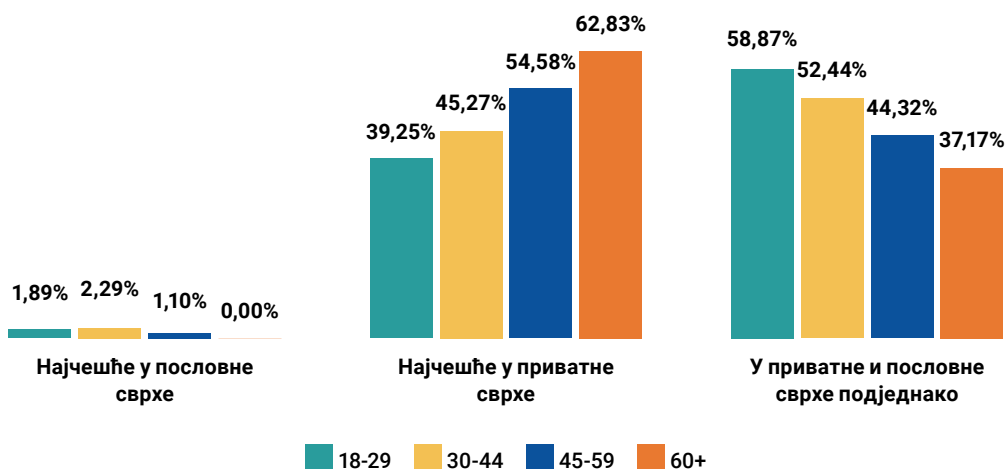
Од укупног броја испитаника, њих 50,2% најчешће користе интернет подједнако у приватне и пословне сврхе, док 48,2% интернет најчешће користи у приватне сврхе. Тек 1,6% корисника интернета у Србији каже да интернет најчешће користи у пословне сврхе.

Ако погледамо податке из 2018. године, примећујемо извесне промене у сврси коришћења интернета. Интернет се у већој мери користи равномерно у приватне и пословне сврхе (50,2% у 2022. години наспрам 27,2% 2018).



Укрштање по старости

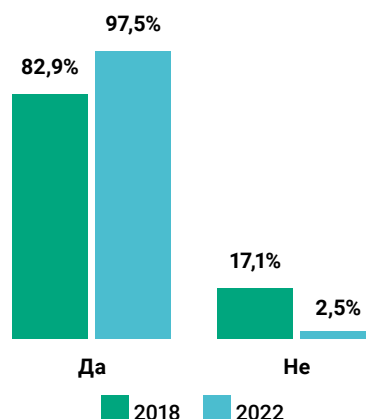
Испитаници старији од 60 година у већој мери користе интернет у приватне сврхе (62,83%) док млади (18-29 година) и радно активно становништво (30-44) користе интернет више од просека подједнако у приватне и пословне сврхе.



Да ли користите интернет на мобилном телефону?

Интернет на мобилном телефону користи 97,5% пунолетних корисника интернета у Србији. У последње четири године дошло је до повећања броја корисника интернета на мобилном телефону.

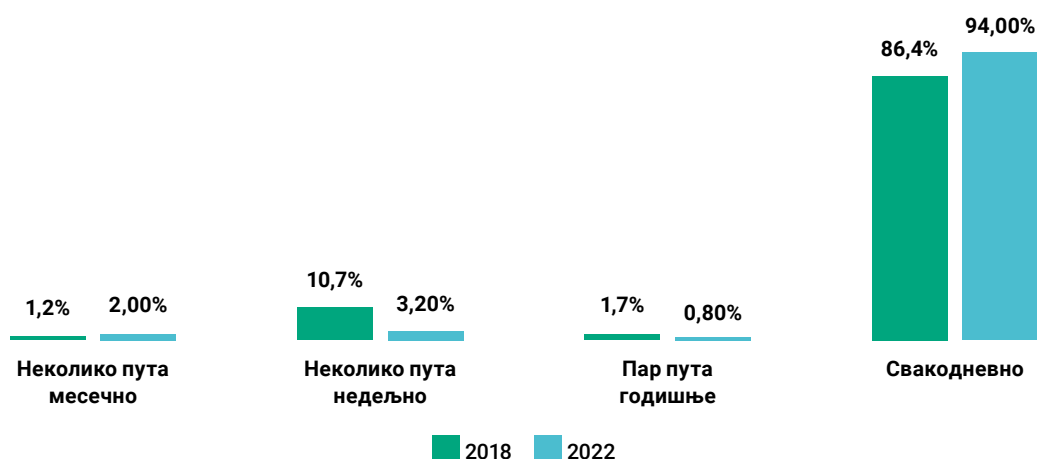
2018. године, мобилни телефон за приступ интернету користило је 82,9% становника Србије а данас је тај проценат 97,5%. Повећање од скоро 15 процентних поена резултат је значајног повећања корисника интернета у најстаријој популацији, али и развој интернет инфраструктуре.



Колико често сте, у просеку, користили интернет у приватне сврхе током протеклих годину дана?

94% анкетираних свакодневно користи интернет у приватне сврхе.

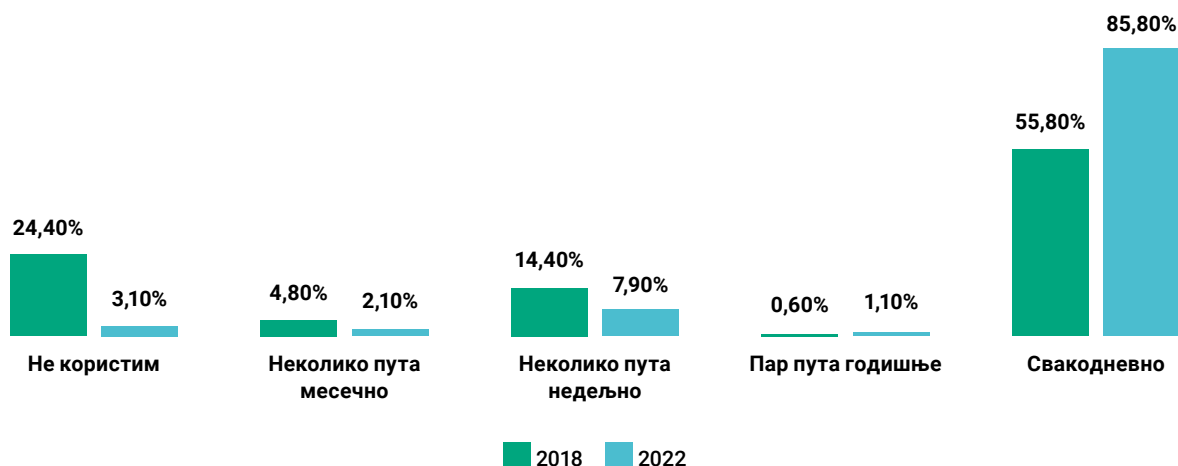
У односу на претходно мерење из 2018. године, ово је повећање од 7,7 процентних поена (94% у 2022. години у односу на 86,4% у 2018. години).



Колико често, у просеку, користите друштвене мреже на рачунару и мобилном телефону?

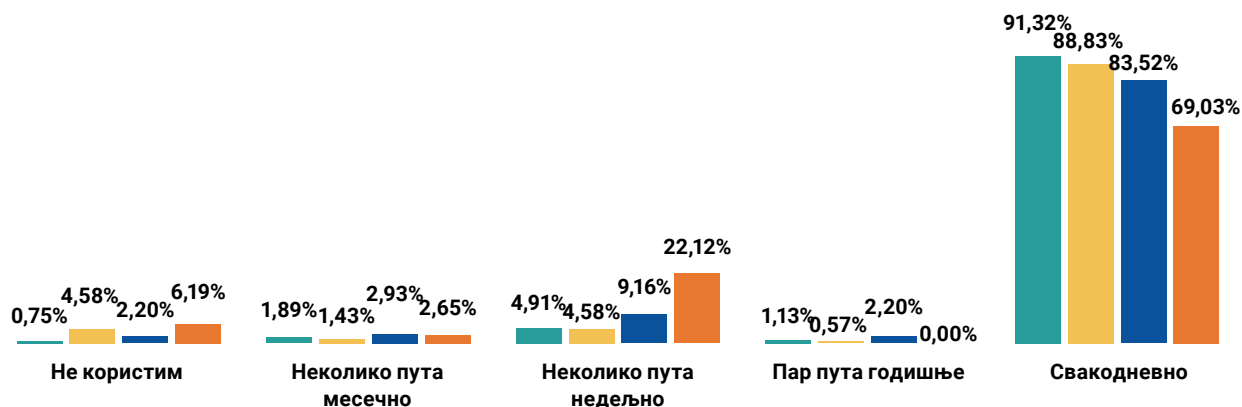
Свакодневно их користи 85,8% интернет корисника у Србији. У односу на 2018. годину, запажамо значајно повећање од 30 процентних поена. Истовремено, пре четири године близу

четвртина испитаника (24,4%) није користило друштвене мреже. Данас тек 3% пунолетних корисника интернета у Србији не користе друштвене мреже.



Укрштање по старости

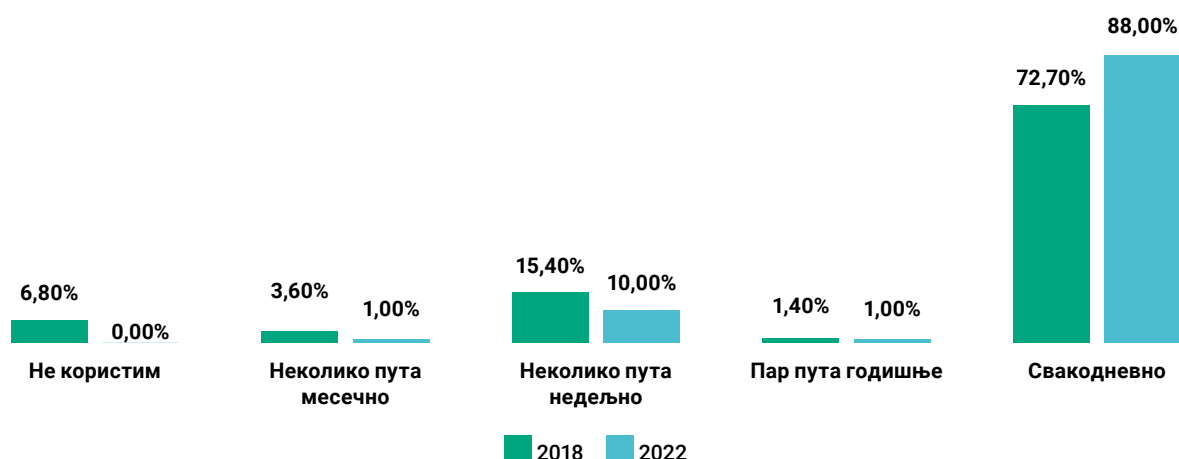
Последњих неколико година значајно је повећан број корисника интернета у популацији старијих од 60 година. Овај велики део становништва значајно доприноси увећању укупног процента оних који користе интернет. Ипак, припадници ове старосне групе у мањој мери користе интернет свакодневно (69%) а чешће од других користе интернет неколико пута недељно (22,1%).



Колико често, у просеку, користите сервисе за размену порука и комуникацију (е-пошту, Skype, Viber, WhatsApp, Messenger...)?

Повећање од 15,3 процентних поена бележи се и када је коришћење сервиса за размену порука у питању.

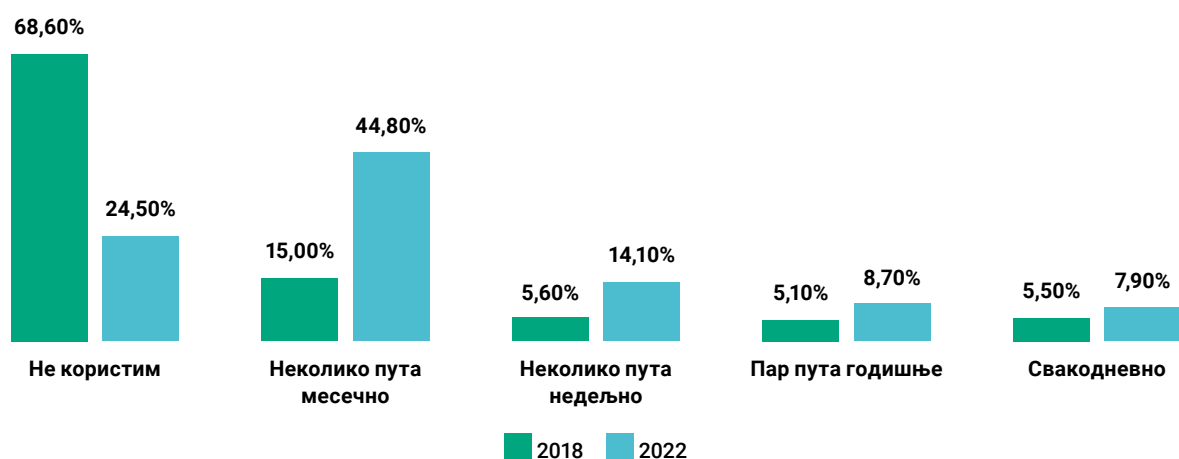
2018. године 72,7% корисника интернета свакодневно је за комуникацију користило сервисе за размену порука, док данас 88% њих свакодневно користи ове сервисе.



Колико често, у просеку, користите сервисе за плаћање преко интернета (апликације банака, PayPal...)?

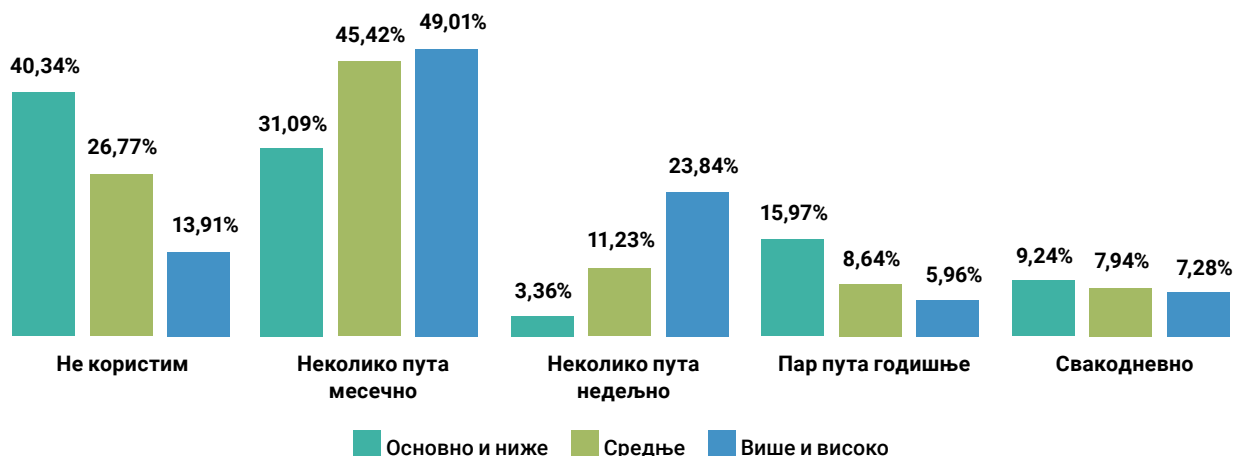
Дошло је до значајних промена у понашању када је коришћење сервиса за плаћање преко интернета у питању. Данас тек четвртина корисника интернета у Србији (24,5%) не користи сервисе за плаћање преко интернета. Највећи број анкетираних (њих 44,8%) неколико пута

месечно користи сервисе за плаћање преко интернета. Свакодневно ову врсту интернет услуге користи 7,9% испитаника. 2018. године, чак 68,6% пунолетних корисника интернета није користило сервисе за плаћање преко интернета (апликације банака, PayPal).



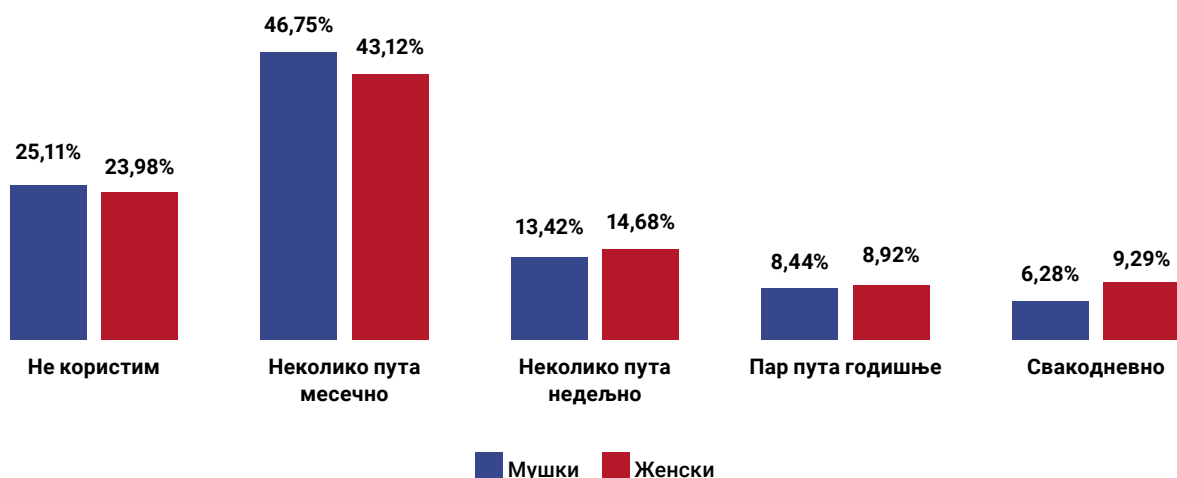
Укрштање по образовању

Становници Србије који имају основни и нижи ниво образовања у мањој мери користе сервисе за плаћање преко интернета. 40,3% испитаника са основним и нижим образовањем не користи ове сервисе. Анкетирани са вишим и високим образовањем више од просека користе сервисе за плаћање преко интернета. Тек 13,9% високообразованих не користи ове сервисе.



Укрштање по полу

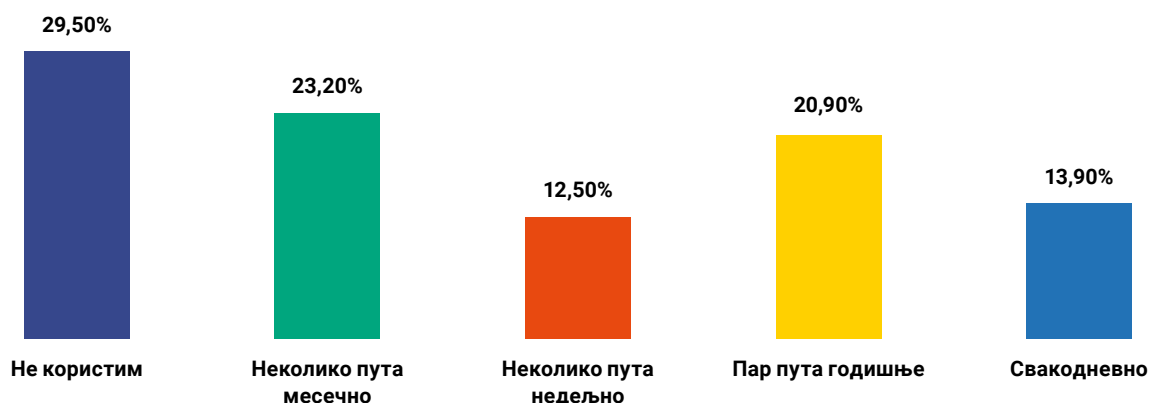
Приближан број мушкараца и жена користи сервисе за плаћање преко интернета. Жена је тек 1% више. Ипак, жене користе апликације за плаћање за нијансу чешће од мушкараца. 9,3% жена свакодневно користи сервисе за плаћање преко интернета наспрам 6,3% мушкараца.



Колико често, у просеку, користите cloud сервисе (Google Docs/Sheets, Dropbox, iCloud...)?

Cloud сервисе користи 70,5% испитаника. Од овог броја, највећи број има потребу за овом услугом неколико пута месечно (23,2%) и неколико пута годишње (20,9%).

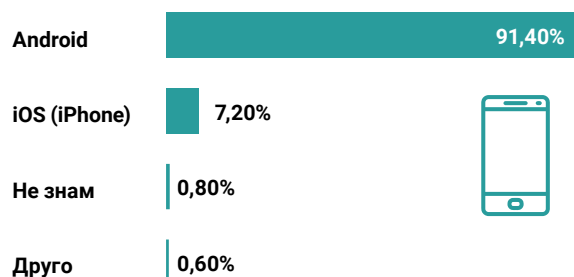
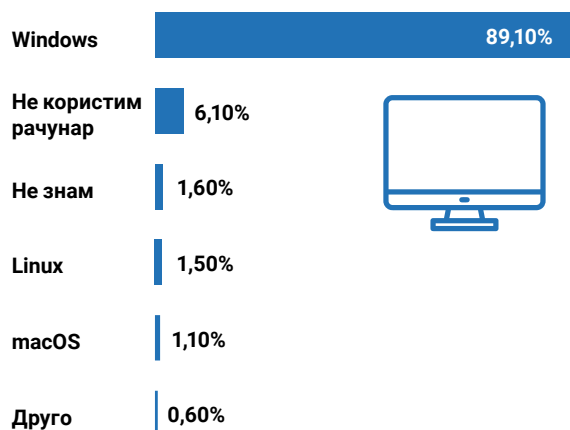
Свакодневно cloud сервисе користи тек 13,9% испитаника. 29,5% пунолетних корисника интернета не користи cloud сервисе.



Који оперативни систем имате на свом рачунару а који на мобилном телефону?

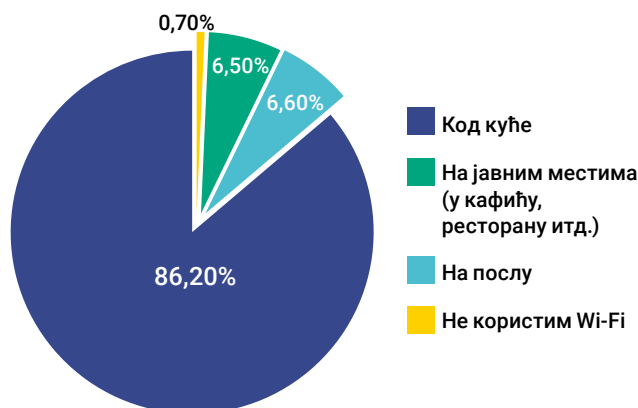
У Србији је Windows најкоришћенији оперативни систем на рачунарима (89,1%). Када је у питању коришћење мобилних телефона, чак 91,4% користи телефоне са Андроид оперативним системом. Последњих неколико година дошло је развоја пре свега кинеских брендова мобилних телефона чија је цена повољна и доступна најширем броју корисника, а то су Андроид телефони.

Истовремено, чак и у оквиру припејд пакета, уз скромну надокнаду корисници добијају могућност коришћења неограниченог интернета на апликацијама друштвених мрежа и сервиса за комуникацију (Viber, Facebook, Instagram...). Пошто је животни циклус андроид телефона процењен на дужину трајања уговорне обавезе, старији (родитељи и баке и деке) добијају често на поклон коришћене мобилне телефоне своје деце и унука, како би остали у контакту са њима.



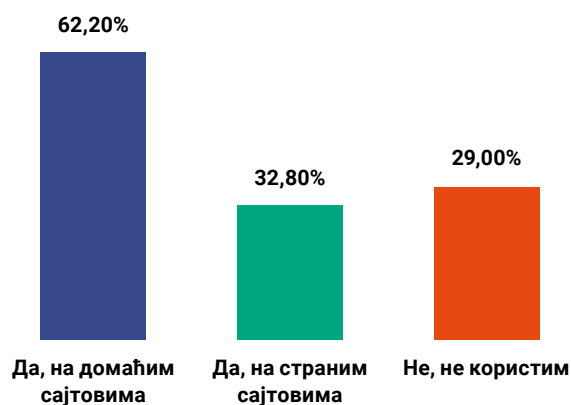
Где најчешће користите Wi-Fi за приступ интернету?

Wi-Fi мрежа за приступ интернету најчешће се користи код куће. 86,2% пунолетних корисника интернета у Србији на овај начин приступа интернету.



Да ли користите услуге електронске трговине?

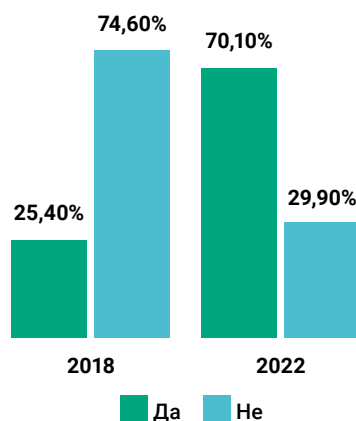
Услуге електронске трговине у Србији користи 67% пунолетних корисника интернета. Највећи број, њих (62,20%) ове услуге користи на домаћим веб-сајтовима, док их на страним сајтовима користи 32,80%. 29% корисника интернета не користи услуге електронске трговине.



Да ли користите услуге електронског/мобилног банкарства?

70,1% пунолетних корисника интернета у Србији користи услуге електронског/мобилног банкарства. Мало мање од трећине корисника (29,9%) не користи ове услуге.

У односу на 2018. годину када, када је тек четвртина испитаника користило услуге мобилног банкарства, ова врста услуга бележи значајан раст.



О нама

Фондација „Регистар националног интернет домена Србије” (РНИДС) управља регистром назива националних .rs и .срб домена и критичним деловима инфраструктуре за националне интернет домene, обезбеђујући њихово беспрекорно функционисање и несметану доступност из било које тачке интернета. РНИДС-у је управљање .rs и .срб доменима, уз подршку надлежног министарства Републике Србије, делегирао ICANN – организација одговорна за управљање глобалном адресном структуром интернета.

На наше интернет сервисе ослања се преко 50.000 предузећа. Ако би неки назив домена био недоступан, веб-страница на њему не би била видљива, онлајн сервис на њему не би радио, а његови корисници не би могли да размењују електронску пошту. Системи који подржавају .rs и .срб домene раде без прекида откако су наши национални домени постали видљиви на интернету.

Осим тога, РНИДС дефинише и правила која регулишу регистрацију назива националних домена, као и спорове у вези са њима.

Такође, РНИДС активно ради на едукацији и промовисању одговарајућег присуства на интернету. Знање које смо стекли током година делимо широм Србије кроз конференције и стручне скупове које организујемо, или на којима учествујемо, у сарадњи са представницима локалне интернет заједнице.



Фондација
"Регистар националног
интернет домена Србије"
(РНИДС)

rnids.rs | rnids.rs

Реализацију истраживања подржао:



РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ
И ПОШТАНСКЕ УСЛУГЕ

Истраживање реализовао:

plummark