САЈБЕР КУЛТУРА У СРБИЈИ 2023.

СРБ-ЦЕРТ

Увод

У извештају Републичког завода за статистику о употреби информационо-комуникационих технологија у Републици Србији у 2023. години наводи се да је интернет, у последња три месеца, користило 85,4% лица. С друге стране интернет је ради тражења информација у сврху учења (аудио-визуелни материјали, онлајн софтвер за учење, електронски уџбеници...) користило 25,7% грађана, док је 7,6% испитаника проверило безбедност веб странице на којој су оставили личне податке. Шта нам ово показује?

Људски фактор се већ дуго сматра кључним фактором информационе безбедности. За људе се често каже да су најслабија карика у ланцу, међутим људи су заправо прва линија одбране од сајбер напада. Од нашег знања и вештина зависи безбедност уређаја које користимо, организације у којој радимо, али и нације уопште, и у ову врсту знања и вештина је потребно континуирано и стратешки улагати. Досадашњи напори да се потреба за сталним учењем адекватно разуме имали су ограничен резултат.

Ово истраживање има за циљ развој ефикасне добре праксе и унапређење сајбер отпорности. Резултати истраживања ће нам показати какав приступ је прихватљив за грађане Србије и како се жељена добра пракса може имплементирати. Наш задатак је да унапредимо разумевање сајбер културе и њен утицај на дигитализацију на националном нивоу.

Тренутни образовни систем нас не припрема за комплексне дигиталне ризике у које се подразумева да треба да „ускочимо“. У циљу стварања сајбер отпорне Србије неопходан је холистички приступ. Истраживање показује да је неопходно унапредити обухват и квалитет сајбер едукације, и унапредити националну сајбер хигијену.

Ово истраживање треба да покаже ниво знања, вештина и навика у односу на прво истраживање које је спроведено 2020. године.

Потреба за мерењем информационе безбедности у Србији

Због све веће жеље корисника да приступе информацијама и друштвеним мрежама у било које време и на било ком месту, приступ интернету и свеопшта повезаност постали су неизоставни део нашег свакодневног живота. Безбедност корисника, свест и разумевање потенцијалних ризика добили су суштински значај због сталне изложености сложеним врстама сајбер претњи, као што су крађа идентитета, уцењивање, прикупљање података о личности, заражавање малвером или сајбер насиље. У том смислу, веома је важно развити свест грађана о безбедносним ризицима и доступним мерама заштите.
Национална Стратегија развоја информационог друштва и информационе безбедности за период 2021.-2026. године као жељене промене дефинише између осталог дигитализовану јавну управу која ефикасно и транспарентно пружа услуге грађанима и привреди, као и

информационо безбедно окружење у коме постоји довољан ниво свести о ризицима, али и предностима које нове технологије пружају грађанима, јавној управи и привреди. Општи циљ Стратегије је развијено информационо друштво и електронска управа у служби грађана и привреде и унапређена информациона безбедност грађана, јавне управе и привреде.

Успостављање модерне легислативе и благовремено усклађивање са прописима ЕУ несумњиво указује да надлежно министарство настоји да информациона безбедност иде у корак са дигитализацијом. Регулаторни оквир омогућава успостављање мреже релевантних институција на националном нивоу, утврђивање обавезних мера заштите и њихово стално унапређење кроз обавезне годишње провере безбедности ИКТ система од посебног значаја. Овај оквир, поред ИКТ система од посебног значаја, укључује и информациону безбедност грађана, па се може закључити да свеобухватан приступ омогућава унапређење сајбер отпорности и умањење ризика од инцидената, односно постизање вишег нивоа информационе безбедности.

Један од најважнијих задатака безбедног и сигурног информационог друштва је да припреми грађане да своје савремене друштвене потребе ускладе са будућим изазовима у личном и професионалном животу. Ти кључни изазови су везани за све већу зависност од дигиталних технологија која би требало да прати унапређење свести о значају информационе безбедности. На креирање сигурног и безбедног информационог друштва велики утицај има људски фактор, пре свега знање, свест и перцепција ризика корисника. Због тога је потребно да знамо више о сајбер култури на националном и организационом нивоу. Национални ЦЕРТ настоји да развије националну метрику сајбер културе, која ће омогућити поуздано разумевање односа српског друштва према неизбежној дигитализацији.

Овим истраживањем настојимо да утврдимо критичне обрасце понашања корисника, ставове, навике, знање корисника о информационој безбедности, каква је потреба и могућност за јачање свести о информационој безбедности, као и спремност српског друштва да унапређује навике, знање и вештине. Сврха истраживања је идентификовање, предлагање и спровођење одговарајућих мера заштите, у циљу промоције безбедније сајбер културе корисника. Поред тога, настојимо да пронађемо начине за креирање адекватног програма обуке за кориснике интернета у Србији.

Дубље разумевање сајбер културе је веома значајно јер је повезано са неким од најважнијих питања развоја. Сајбер безбедан грађанин је од кључног значаја за успешну дигитализацију на националном нивоу. Не само да дигитализација омогућава привреди брзо и ефикасно коришћење информационих технологија и података, и омогућава грађанима различите користи дигиталног доба, већ представља основ економског развоја.

Национална сајбер култура

Од свих особина које разликују нације, култура је један од најдоминантнијих. Националне културе нас обликују ко смо као група и како се ми као појединци позиционирамо у свету. Другим речима речено, национална култура је фактор уједињавања међу грађанима и односи се на наше дубоко задржане вредности у вези са оним што сматрамо нормалним насупрот ненормалним, сигурним у односу на опасне, и рационално насупрот ирационалном. Национална култура нуди скуп вредности на основу којих се успоставља компас или оријентир на основу кога знамо "како нешто радимо". Национална култура садржи систем заједничких вредности, склоности, и понашања група становништва које се веома разликују међу државама. Ове културне вредности и норме се уче у раној фази живота, и преносе се формално (у школи, на радном месту, у слободно време итд.) и неформално кроз интеракцију са пријатељима, родитељима, браћом и сестрама, родбином и другима. Као резултат тога, националне културе су дубоко укорењене у свима нама и трају генерацијама.

Ипак, национална култура није једноставан и прецизан појам, и њен формат није такав да "једна величина одговара свима". Национална култура је састављена од више субкултура у којима фактори као што су старост, географија, интересовања, област фокуса и пол имају своју улогу. Информациона безбедност је једна таква субкултура. Данас се сасвим сигурно може рећи да је информациона безбедност важна за скоро свакога од нас, сразмерно степену дигитализације друштва у коме живимо. Другим речима: Све нације имају своју сајбер културу. Сви пишемо на рачунарима, скоро да не скидамо поглед са својих паметних телефона, купујемо намирнице и гардеробу преко интернета, плаћамо рачуне или користимо неку од еУслуга јавне управе.

Међутим, сајбер култура је до сада сматрана делом организационе културе, која је вид бриге за предузећа и индустрије. Последица тога је да је сајбер култура третирана као средство за организациону ефикасност и успех. Ипак, организациона култура се разликује од националне културе на најосновнијем нивоу: национална култура се бави заједничким вредностима и нормама, док се организациона култура бави заједничком праксом.

Организациона култура заснива се на различитим упутствима која чине организациону праксу не само у смислу стручног усавршавања и оспособљавања запослених, али се заснива и на нормама и развијеној пракси коју запослени треба да следе. Уколико запослени не поступе у складу са овим принципима ризикују губитак посла.
Ово свакако не умањује значај организационе сајбер културе, већ указује на разлику у односу на националну сајбер културу.

[1] *Uchendu, Nurse, Bada and Furnell. (2021). Developing a cyber security culture: Current practices and future needs, Computers & Security Journal*
[2] https://www.cert.rs/files/shares/Sajber%20Kultura%20Ratel%20web%20V0.5.6.pdf

Сајбер култура је веома комплексна област о којој се недовољно зна. Због недовољног познавања сајбер културе веома је сложено идентификовање свих индикатора који имају утицаја на ову област. Да ли старост има утицаја? Величина предузећа или организације? Или врста делатности има значајан утицај?

За потребе овог истраживања коришћени су индикатори из норвешког модела које смо модификовали у складу са нашим потребама. Истраживање је спроведено на општој популацији грађана, а поузданост индикатора је заснована на томе да сви једнако разумеју питања и да је значење појмова коришћених у одговорима за све једнако. Индикатори су поуздани и за коришћење у различитим секторима или предузећима. Иако обиман, овај сет индикатора је стандардизован и омогућиће нам да креирамо основе сајбер културе и извршимо поређење међу секторима, предузећима и групама популације.

Квантитативно истраживање спровела је агенција Smart+ Research[3], истраживачком техником *CAWI (Computer Aided Web Interviewing)* са циљем да се испита национална сајбер култура у Србији, што подразумева процењивање ставова, знања, навика и понашања грађана Србије у вези са коришћењем рачунара, мобилних уређаја и интернета. У складу са тим, циљ нам је да проучавамо и анализирамо ове социо-техничке елементе и истражимо свест о информационој безбедности српских корисника интернета.
Питања из упитника се односе на уже области интересовања и пружају кључне почетне показатеље неопходне за даљу евалуацију.

Питања и истраживања

Ово истраживање фокусира се на националну сајбер културу и њен утицај на дигитализацију јавног и приватног сектора. У том смислу формулисана су следећа питања:

- Шта карактерише сајбер културу у Србији?
- Колики је утицај едукације о информационој безбедности на понашање или свест свих грађана Србије?
- Како се грађани односе и како реагују на сајбер ризике?
- Колики је степен одговорности појединаца за безбедност сајбер простора?

[3] Агенција Smart+ Research

Да бисмо што једноставније приказали резултате истраживања одговоре на питања смо конципирали кроз четири поглавља:

- *Национална сајбер култура у Србији*
- *Компетенције, знање и учење*
- *Перцепција или схватање ризика*
- *Модели понашања*

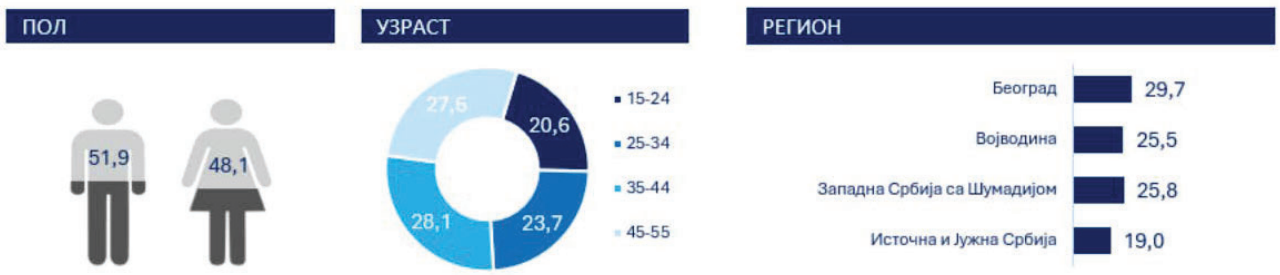
Процена знања

Новина у односу на истраживање из 2020.године је процена знања о информационој безбедности и тест препознавања фишинга који су испитаници решавали.
На основу питања из истраживања развијен је сет индикатора, питања, која могу да обезбеде релевантне податке, адекватне за даљу анализу.

Демографска структура

Истраживање је спроведено на национално репрезентативном узорку за онлајн популацију према полу, узрасту (18-54 год.) и региону у којем живе, док се друге демографске варијабле као што су радни статус или образовање узимају по случају.

Репрезентативни узорак од 1250 испитаника гарантује минималну статистичку грешку од ±2.7% на интервалу поузданости од 95%, односно максималну статистичку грешку ±6.2% на интервалу поузданости од 95% за најмању јединицу узорка (најстарија старосна група – *45-54* година).



База: 925
Запослени

Национална сајбер култура у Србији

Све културе успостављају равнотежу између појединачног и колективног, појединачног закључивања и схватања, и колективних норми и стандарда. Ми заправо нисмо у потпуности само појединци, али нисмо само ни део већег колектива. Конципирање сајбер културе упућује на факторе који не само да чине сајбер културу као целину, већ упућује и на важне дилеме и изазове сајбер културе који су њени градивни елементи.

Имајући све ово у виду, издвојено је 8 важних показатеља сајбер културе онако како их ми видимо. То су:

1. Колективизам

Културе су по дефиницији колективне чине их и развијају појединци, али и њиховом развоју и обликовању култура доприноси. Културе указују на карактеристике одређених група људи, као што су њихове социјалне навике, ставови, вредности и приоритети, и захтевају одређену солидарност међу члановима групе или заједнице. То значи да је за трајање и опстанак културама неопходна лојалност и солидарност међу појединцима. Појединци се морају сами идентификовати као део групе, доприносити и придржавати се експлицитних и имплицитних норми понашања.

Колективизам не значи блискост већ значи да појединац зна своје место у друштву. Издвајањем колективизма желимо да укажемо на однос појединца према колективу. Приликом утврђивања овог односа указујемо на две теме: Прво, у ком степену појединци виде себе (ако уопште виде) као део већег "Сајбер колектива". И друго, да ли појединачно понашање обликовано колективним нормама и понашањем.

Већина интернет популације Србије (62%) сматра да би требало да буде могуће остати анониман на интернету, док само 11% сматра да анонимност не би требало да буде могућа, Свега трећина особа прихвата да њене активности буду надгледане уколико би то допринело безбедности на интернету. **Лична безбедност се и даље не доводи у везу са безбедношћу других - две трећине испитаних сматра да интернет неће бити безбеднији чак и ако је њихов рачунар/телефон безбедан.**

2. Управљање и контрола

У односу на колективизам, управљање је колективни појам који се односи на питања уређења и регулисања колектива. Дакле, питање управљања односи се на ставове корисника о управљању и контроли информационо-комуникационих технологија (ИКТ). Овде је веома важно питање надзора: Ко је одговоран за одређивање прихватљиве употребе ИКТ-а где би се те црвене линије морале повлачити и како их се грађани придржавају?

Постављањем питања управљања, желимо да скренемо пажњу на то ко је одговоран за нашу сигурност на мрежи. У контексту безбедности, увек постоји питање како успоставити равнотежу између индивидуалне слободе и колективне сигурности. "Сви" желе слободу и "сви" истовремено желе да буду безбедни. Који ниво надзора је прихватљив када је у питању појединачна сигурност? Како постићи овај баланс сајбер култури?

У односу на податке из 2020. године, уочава се пораст оних који верују да ће им криминалистичке службе помоћи ако буду жртве сајбер криминала и присутан је за нијансу позитивнији став о надгледању онлајн активности. Овај став је израженији код особа са нижим знањем о сајбер безбедности.

3. Поверење

Поверење је камен темељац свих одрживих демократија. Демократија се заснива на низу различитих облика поверења: међу грађанима, грађана и владе, између владиних институција, различитих области пословања, запослених и послодавца, итд. Другим речима, поверење је предуслов за економско благостање, стабилност и раст сваке демократске државе. Поверење је у области информационе безбедности од великог значаја, с обзиром да је све већи степен националног раста везан за дигитализацију.

Јавној управи је за ефикасно и вршење власти у складу са законом, као и одржавање стабилности, поред утврђене надлежности неопходно и поверење грађана. То подразумева да се властима даје надлежност како за спровођење политика са којима се грађани не слажу, тако и када спроводе политике које су грађанима непознате или нове.

Процес дигитализације скоро подједнако зависи и од рањивости и поверења. Сам процес подстичу власти у скоро свим државама, а узимајући у обзир тренутни развој технологија процес дигитализације нашег друштва је неизбежан.

Грађани се подстичу да користе нове технолошке алате, али се истовремено и упућују да их користе кроз различите еУслуге.

Упућивање грађана да услуге управе користе електронским путем свакако смањује папирологију и користи бирократији, али претпоставља поверење од стране грађана. Електронске услуге морају бити безбедне, јер би компромитовање безбедности утицало на грађане на начин да неће посећивати интернет странице и користити еУслуге, односно изгубити поверење у управу.

Неопходни типови поверења се нарочито огледају у примеру електронске трговине, која постаје све учесталији начин трговине. Када купујемо преко интернета остављамо наше податке као што су подаци о кредитној картици, као и друге личне податке, а при томе верујемо да се нашим подацима пажљиво рукује. Ипак, постало је јасно да Google, Apple као и већина других компанија ове податке користе како би профилисали своје кориснике. Профилисање се користи као маркетиншки алат за циљано оглашавање и пласирање производа компанија. Ово сазнање нам намеће питање да ли ће куповина књиге преко Амазона довести до пласирања наших података другим компанијама које ће нас одредити као циљаног купца и рекламирати нам њихове производе?

Циљано оглашавање је друга страна новчића дигитализације и поверења. Циљано оглашавање за многе представља кршење поверења, које за резултат има сазнање да интернет странице податке које смо приморани да оставимо користе зарад стицања добити. То доводи до недостатка поверења, и представља потенцијалну претњу процесу дигитализације.

Није било већих промена у индикаторима поверења у односу на истраживање из 2020. године.

4. Схватање ризика

Компетенције, учење и ризик су чврсто повезани. На пример, студије су показале пораст такозваног „ризичног понашања“ међу појединцима који имају висок ниво стручности или вештине опажања. Отуда је вероватније да ће људи који имају одређено знање и вештине у области информационе безбедности проценити да су способни да контролишу претњу и да могу преузети више ризика[4].

У студији *Kathryn Parsons, Agata McCormac, Marcus Butavicius* и *Lael Ferguson* из аустралијске организације за одбрану, науку и технологију ризик се истиче као кључни фактор у формирању понашања. Студија је утврдила да појединци имају нереални оптимизам и сматрају да имају ризик под контролом “. Установљено је да уколико појединац сматра да има под контролом активности које предузима на личном рачунару, онда је безбедносни ризик мањи. Стога, појединци потцењују шансу да ће непоштовање безбедносних политика довести до озбиљних последица. То значи да је вероватније да ће се појединци одлучити на ризично понашање“[5].

Скоро сваки други корисник сматра да се излаже ризицима када је на интернету, а сваки пети се уздржава од коришћења онлајн услуга због претњи. Нешто више од половине (53%) интернет популације у Србији саопштава да је добро обавештено о онлајн претњама, док 15% сматра да то није случај. Ни у индикаторима схватања ризика није било већих промена у односу на истраживање из 2020. године.

[4] Parsons, McCormac et al. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment*
[5] Kreuter, M.W., & Strecher, V. (1995). *Changing inaccurate perceptions of health risk: Results from a randomised trial. Health Psychology, 14, 55–63*

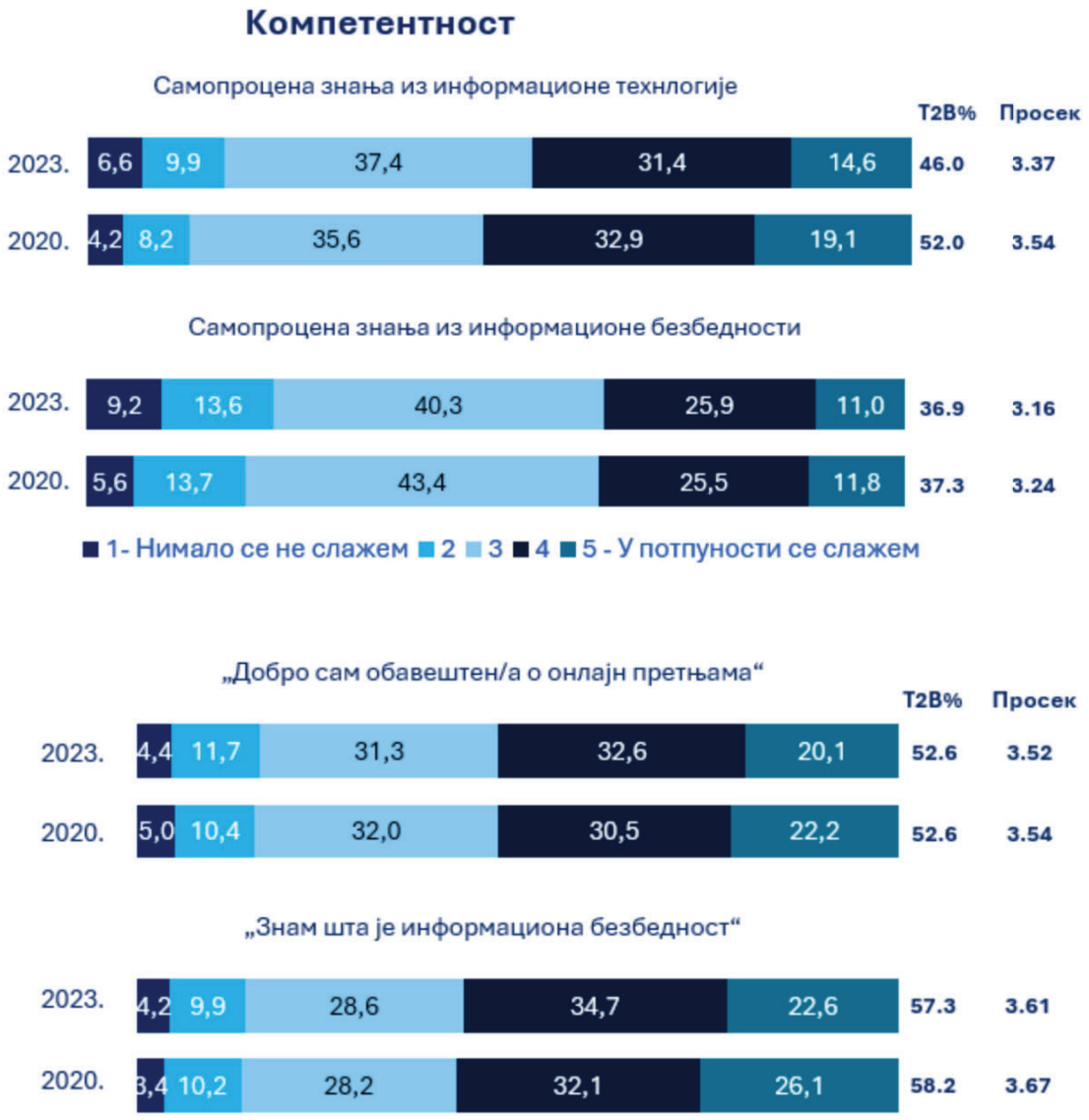
5. Технолошки оптимизам и дигитализација

Дигитализација не само да подстиче пословно окружење да паметно користе информационе технологије и податке, већ и обезбеђује корист коју грађани имају од дигиталног развоја, и доприноси економском расту. Чињеница је да је дигитализација један од сегмената развоја друштва, али је наша тенденција да скренемо пажњу на став грађана према овој друштвеној тенденцији. Другим речима: Ваш став према дигитализацији утиче на то како се односите према технологији. Безбедан сајбер грађанин је највећи успех националне дигитализације. Неповерење у дигиталне услуге и страх од сајбер криминала су неки од изазова са којима се људи суочавају у процесу дигитализације. Стога, морамо разумети динамику развоја сајбер културе, односно начин на који утиче на дигитализацију у компанијама, секторима и на националном нивоу.

Став према употреби нових технологија је и даље доминантно позитиван, али је нешто негативнији него пре три године. До благог смањења је дошло и у погледу интересовања за информационе технологије.

6. Компетентност

Грађани су за скоро све услуге усмерени да користе ИКТ без обзира да ли им то чини задовољство или не, од социјалних услуга и плаћања пореза до комуникације и дељења фотографија. Ово подразумева да грађани морају развити сет дигиталних вештина које их чини способним да буду део модерног друштва. Грађани Србије морају развити основне дигиталне вештине. Питање је: Где и како се стичу ове вештине? Парадокс је што већина земаља „гура“ своје грађане да користе интернет, док развој наших друштава зависи од свеобухватног процеса дигитализације. Ипак, основни сет дигиталних вештина се врло ретко учи у школама, па се до њега долази углавном кроз неформално образовање.



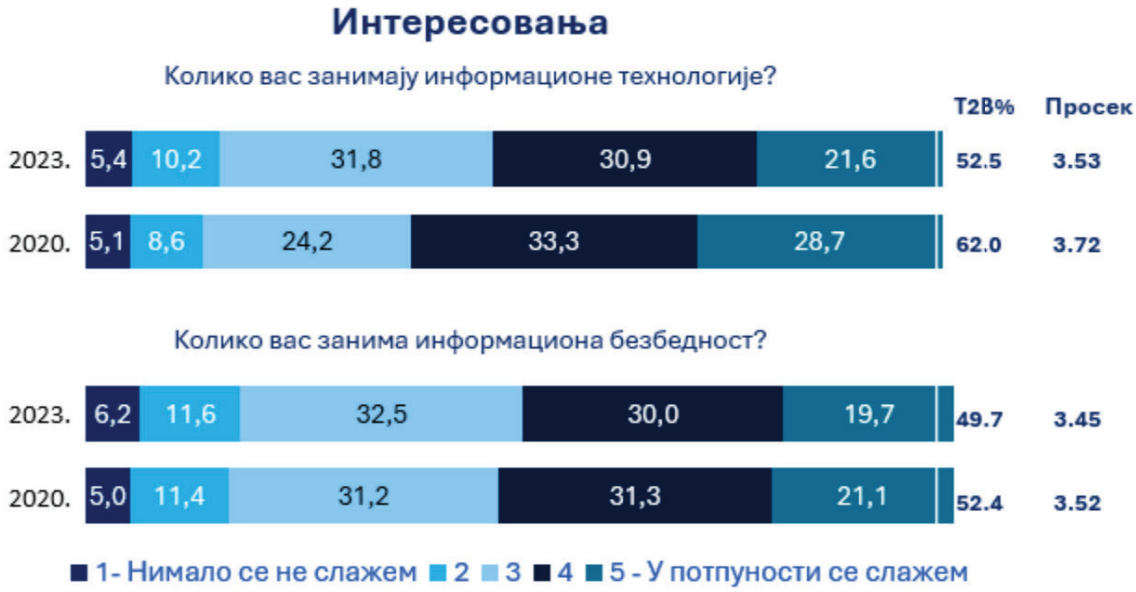
Када процењују своје знање из информационих технологија и информационе безбедности најчешће себи дају оцену 3 (на скали 1-5). Своје знање из информационе безбедности процењују као лошије него знање из информационих технологија. Више од половине сматра да зна шта је информациона безбедност (58%), док 13% сматра да не зна шта је информациона безбедност.

Резултати истраживања су нешто лошији у односу на истраживање из 2020. године.

7. Интересовања

У друштву које се све више дигитализује може се закључити да грађани који су заинтересовани за коришћење ИКТ имају предност у односу на грађане којима ово интересовање недостаје. Интересовања обликују наше ставове, вештине и знање, круг сарадника, као и круг оних од којих учимо. Интересовање развија свест, радозналост и представља основ у учењу. Ово води до питања да ли људи заинтересовани за ИКТ брже уче од оних којима недостаје такво интересовање.

Чини се да управо због тога интересовање може бити одлучујуће у дигитализованом друштву. До благог смањења је дошло и у погледу интересовања за информационе технологије.

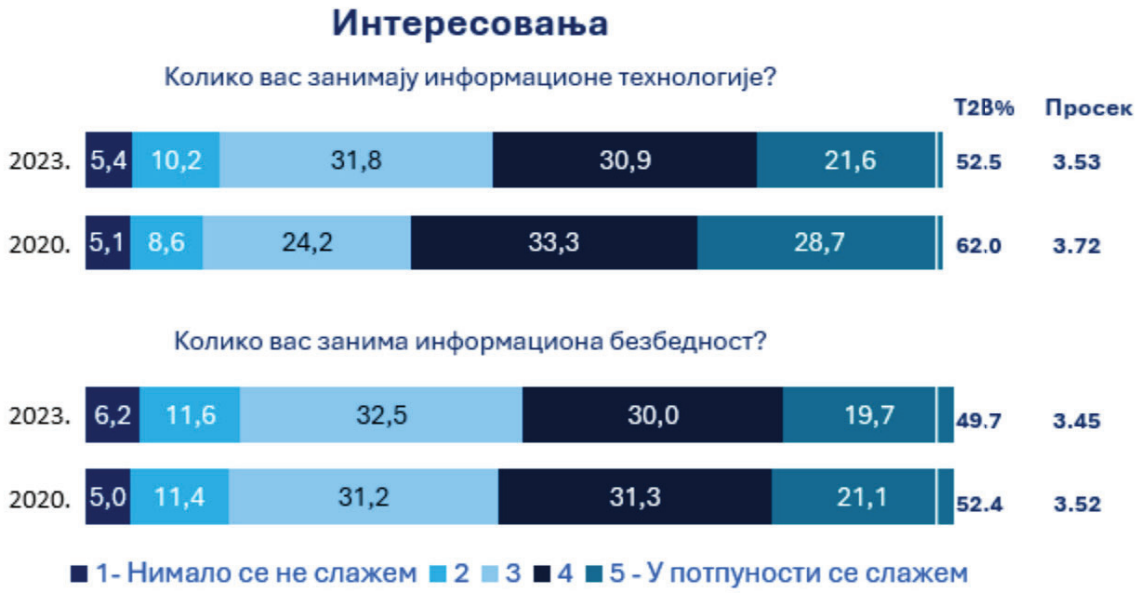


8. Понашање

Већина студија о сајбер култури је усмерена на понашање. Ово не треба да чуди јер наши поступци нису само најлакши за мерење већ имају конкретан утицај на информациону безбедност и дигитализацију друштва. У информационој безбедности постоје одређене врсте понашања која се охрабрују, док се на друге грађани упозоравају. Надлежни органи и експерти дају савете који представљају стандард понашања грађана. Међутим, брзи развој технологије води ка томе да се и стандард „најбоља пракса“ брзо мења, те да је неопходан сталан развој вештина и савета. Једна обука или курс није довољан, јер се једном стечено знање у појединим областима врло брзо сматра превазиђеним. Континуирано и планско унапређивање стандарда понашања је пресудно за развој информационе безбедности.
Ипак постоје понашања на које увек подстичемо грађане: не делити своје лозинке са другима; креирање резервних копија својих података и редовно ажурирање софтвера. Грађани се подстичу на ове кораке како би се умањили безбедносни ризици од губитка информација или смањити могућност манипулације информацијама, односно вероватноћа да ће бити жртве напада или високотехнолошког криминала.

Дакле, мерење образаца понашања српске сајбер културе, подразумева две ствари: прво, желимо да створимо слику понашања грађана Србије у контексту информационе безбедности, и друго, желимо да видимо у којој мери се грађани придржавају „најбоље праксе“.
Ови резултати говоре о томе како се грађани Србије позиционирају у односу на свет.

Компетенције, знање и учење

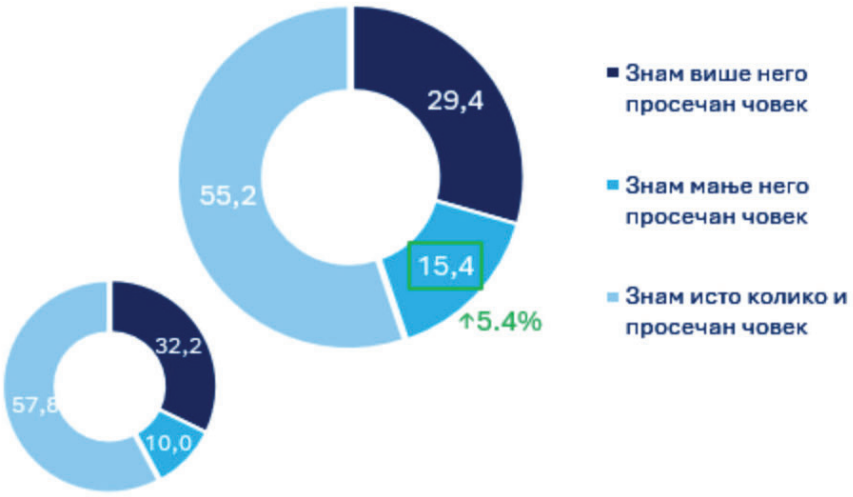


Технолошки напредак у области информационе безбедности је изузетан, међутим, напредак технологије сам по себи не значи стварање безбедног окружења. Примена комплексне енкрипције и безбеднији оперативни системи и програми отежавају нападачима реализацију напада. Број онлајн превара, као и кривичних дела високотехнолошког криминала је у порасту, па се стиче утисак да мете напада нису наши рачунари, већ ми сами.

Ризици од употребе информационих технологија се константно мењају и постају све комплекснији. С повећањем зависности друштва од технологије сваки појединац у друштву добија све више одговорности. Очекујемо да грађани разумеју ризике повезане са њиховим активностима на интернету, а то значи да имају знање о претњама које се константно и динамично мењају, као и новим технологијама и њиховим рањивостима. Од грађана се очекује безбедно и сигурно понашање на интернету, што ствара велику одговорност за појединце од којих се очекује да разумеју и поштују правила безбедног понашања на интернету. Многе компаније организују кампање подизања свести о значају информационе безбедности или обуке, али се врло мало или уопште не баве проценом ефикасности ових облика едукације. Незапослени или запослени у компанијама које не организују едукације, мање или више су препуштени систему образовања, неформалном начину преноса знања или самима себи.

Неопходно је дубље разумевање начина на који се формирају компетенције и знање. Како учимо о информационој безбедности? Да ли едукација о информационој безбедности заиста утиче на формирање образаца понашања?

Процена познавања информационе безбедности у односу на друге



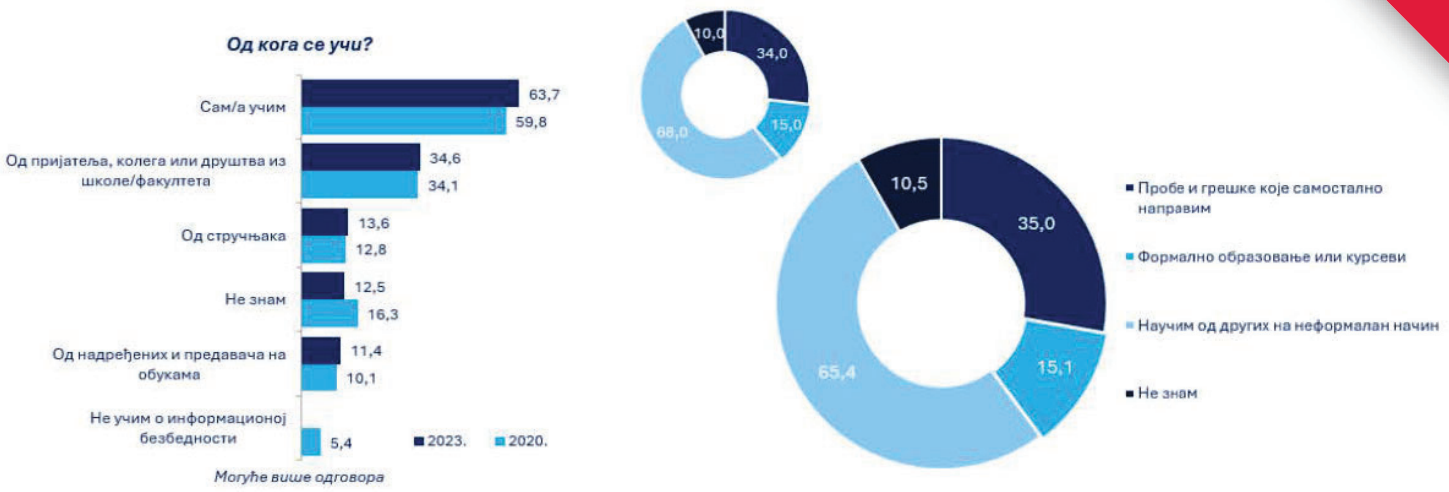
Нешто више од половине интернет корисника у Србији сматра да з**на о информационој безбедности исто колико и просечна особа.** Око 15% има **утисак да заостаје за другима,** а тај проценат корисника интернета је у односу на претходни талас истраживања порастао за 5%. Млади до 24 године теже да процењују своје знање као лошије од просека у односу на старије.

Тек **сваки други корисник** интернета сматра да зна да **разликује безбедно од небезбедног** понашања на интернету и њих је 7% мање него у претходном мерењу. Такође, чак 4**0% оних који показују ниско знање** на тесту о сајбер безбедности с**матра да зна да успешно разликује безбедно од небезбедног,** док исто тврди тек **57% оних који заиста имају високо знање** о безбедности.

Када дефинишу информациону безбедност својим речима, корисници најчешће дају одговоре који се тичу безбедности личних података и сигурност података од злоупотребе. Нису запажене упечатљиве промене у односу на претходни талас истраживања. У односу на 2020. годину повећан је проценат оних за које је информациона безбедност везана за заштиту база, ИКТ система и других података (+6%), као и оних који увиђају важност информисаности о интернет безбедности (+3%) као аспекта саме информационе безбедности.

Начини и извори знања уз помоћ којих интернет популација у Србији учи о информационој безбедности, идентични су онима из 2020. године. О информационој безбедности интернет корисници најчешће уче сами (64%), или од пријатеља, колега или друштва из школе, са факултета (35%). Релативно мали проценат наводи да учи од стручњака (14%) или на обукама (11%). Особе са највишим знањем о информационој безбедности су више училе из сваког од наведених извора.

Највећи број нешто научи о информационој безбедности од других, на неформалан начин (65%), скоро упола мање то чини на основу сопствених проба/грешака, док најмање особа помиње формално образовање/курсеве. Чињеница да се информације о информационој безбедности у великој мери шире на неформалан начин је са једне стране могуће тумачити оптимистично (у смислу да је довољно обучити један део популације који ће своје знање спонтано пренети другима), али у исто време указује на ризик, јер се на овај начин могу ширити и дезинформације.



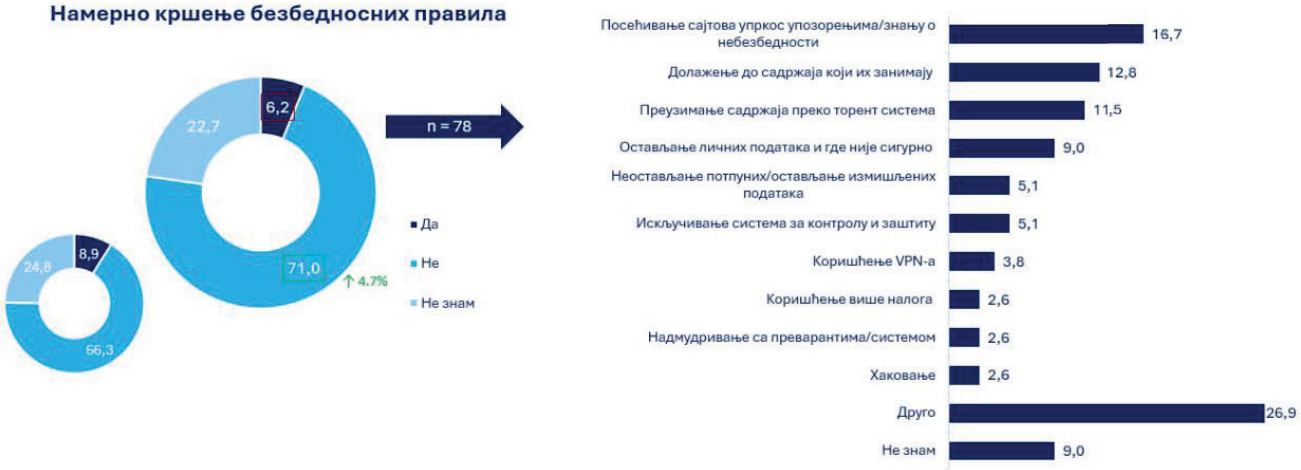
Схватање ризика

Схватање ризика заузима посебно место у нашем истраживању јер свако коришћење интернета подразумева и одређене дилеме о безбедности. Претње се могу манифестовати на много начина, а ми не успевамо да разумемо у потпуности сложени дигитални ланац догађаја који нас могу учинити рањивим. Да ли треба да отворимо прилог из имејла? Да ли ће вас придржавање правилима безбедног понашања учинити мање или више изложеним сајбер криминалцима? Да ли правилно процењујете ризик повезан са вашим активностима на интернету?

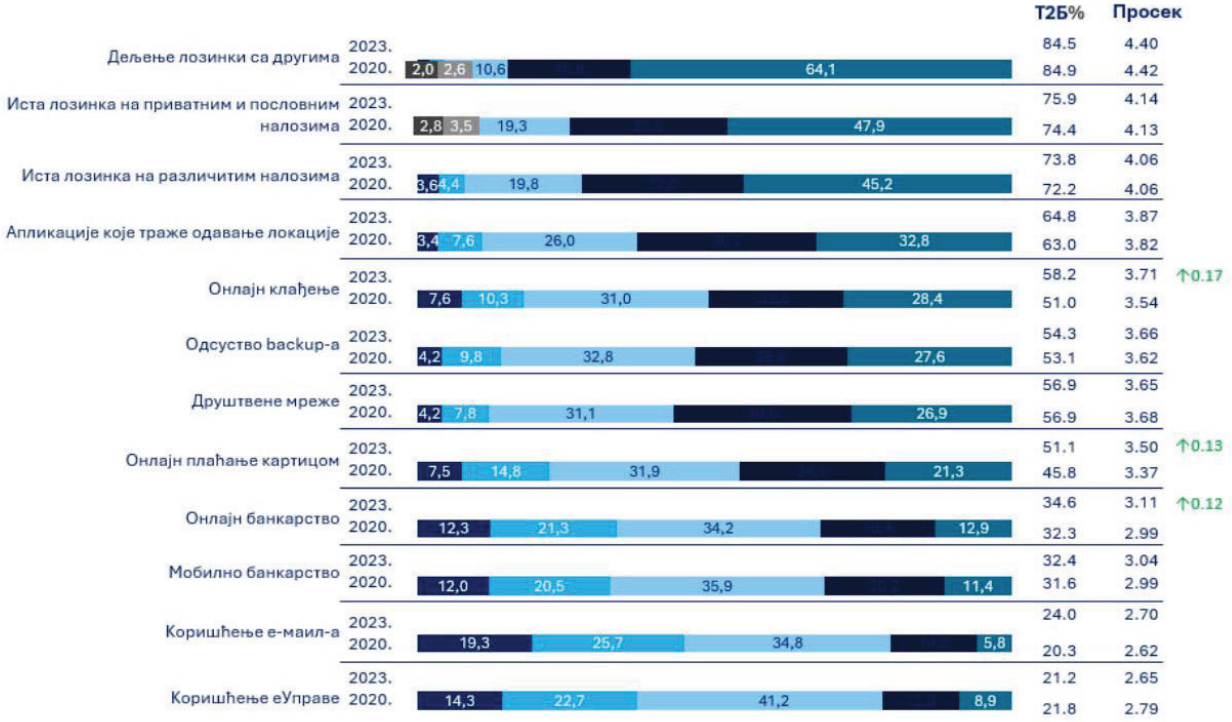
Експерти информационе безбедности сматрају да грађани немају довољно сазнања о безбедносним ризицима или да су наивни и да нису свесни својих поступака. Врло често се у последње време сајбер напади објашњавају са „људски фактор“. Људи бивају „оптужени“ због погрешних избора и тумачења безбедносног ризика својих поступака. Управо се због спречавања будућих инцидената све чешће организују обуке и спроводе кампање за подизање свести о значају информационе безбедности.

Ризици, посебно сложени, садрже значајан „људски елемент“, врло често су у већој мери засновани на личном расуђивању него на научном прорачуну. На процену ризика може утицати велики број фактора, од којих се сваки мења из дана у дан или од ситуације до ситуације. Чињенице и сазнања могу имати велику улогу у процени ризика, као и искуство, колико „ризично“ се осећамо у том тренутку или тог дана или да ли смо генерално особа која ризикује или не. Шта су фактори који утичу на процену ризика и шта чинимо у ризичним ситуацијама? Ако нам је циљ да побољшамо процене ризика, како би то требало да учинимо? У нашем истраживању се бавимо различитим аспектима перцепције ризика, и који фактори који су у корелацији са перцепцијом ризика.

У односу на 2020. годину, дошло је до малог смањења у броју интернет корисника у Србији који **намерно крше** безбедносна правила. Намерно кршење правила најчешће подразумева: **посећивање ризичних сајтова, долажење до садржаја који им је потребан** без обзира на последице и **преузимање садржаја преко торента.** Међу онима који крше правила чешћи су **мушкарци,** као и они **са вишим знањем** о безбедности на интернету.



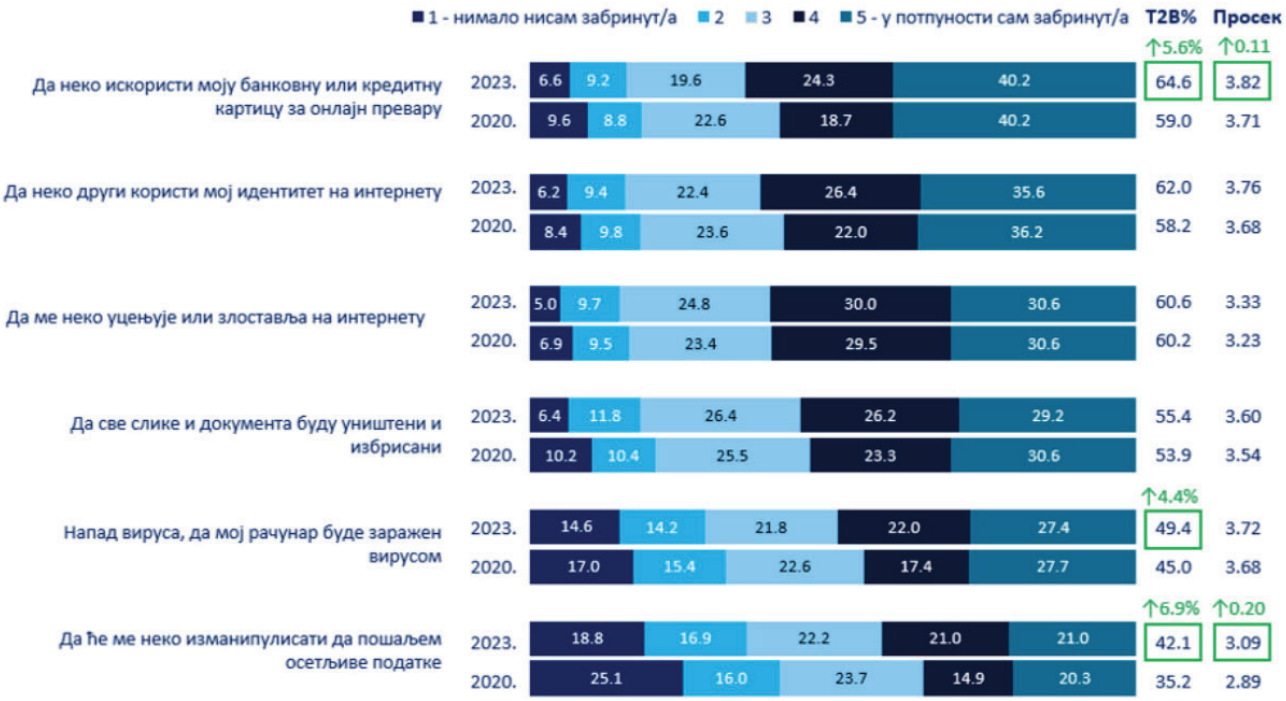
Оцене ризичности активности на интернету су сличног ранга и ове године. Као **најризичније** се и сада издвајају **активности везане за лозинке,** попут дељења лозинки са другима, коришћења исте лозинке на различитим, као и приватним и пословним налозима, док је као **најмање ризично оцењено коришћење еУправе и имејла.** Онлајн услуге као што су клађење, плаћање картицом и банкарство ове године су оцењене као нешто ризичније. Они с**а више знања о сајбер безбедности** су опрезнији и свеснији претњи. Најмлађа популација има најмање свести о ризику које носе одређене активности.



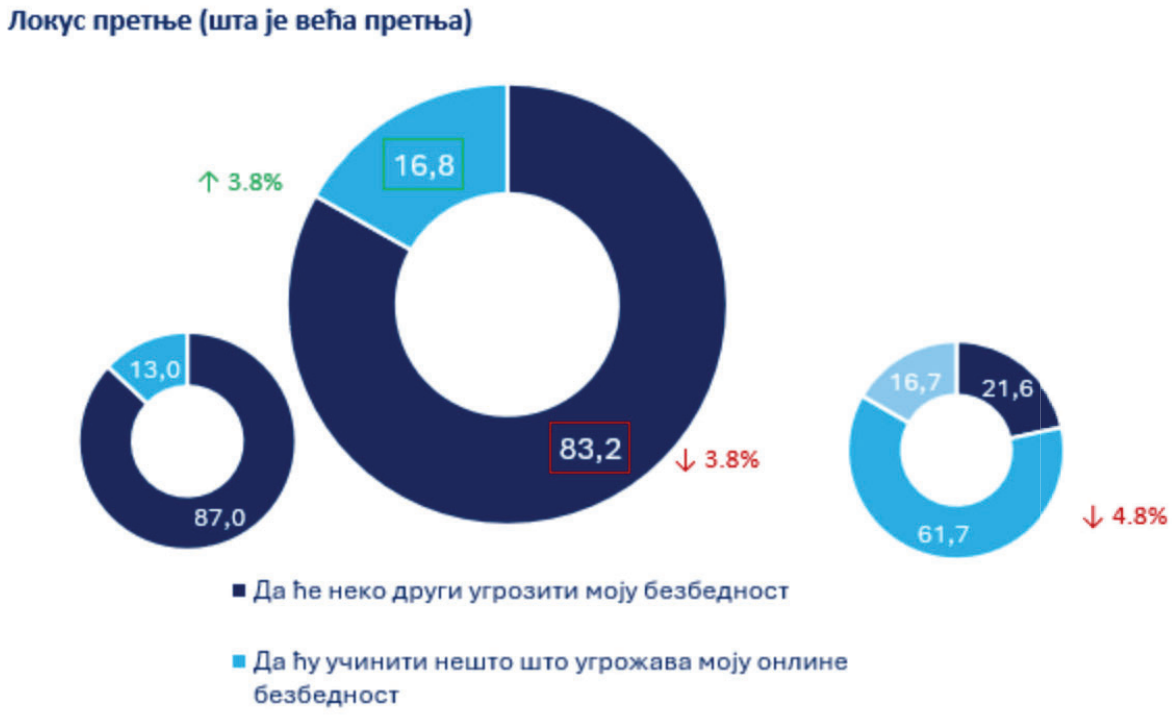
Ризичност неопрезног коришћења лозинке, али и онлајн клађење и одсуство резервних копија као знатно **мање** ризичним оцењују они који кажу да **не могу да процене шта је безбедно.** Са друге стране, интернет корисници, **сигурни у то шта је безбедно, онлајн плаћања картицом, банкарство, мобилно банкарство, коришћење имејла и еУправе** оцењују као **мање ризично** од оних који нису сигурни или не знају да разликују безбедно од небезбедног.

Висок проценат (62%) интернет популације у Србији је значајно забринут да ће неко други користити њихов идентитет на интернету, искористити њихову банковну картицу у онлајн превари, или да ће им рачунар бити заражен вирусом.

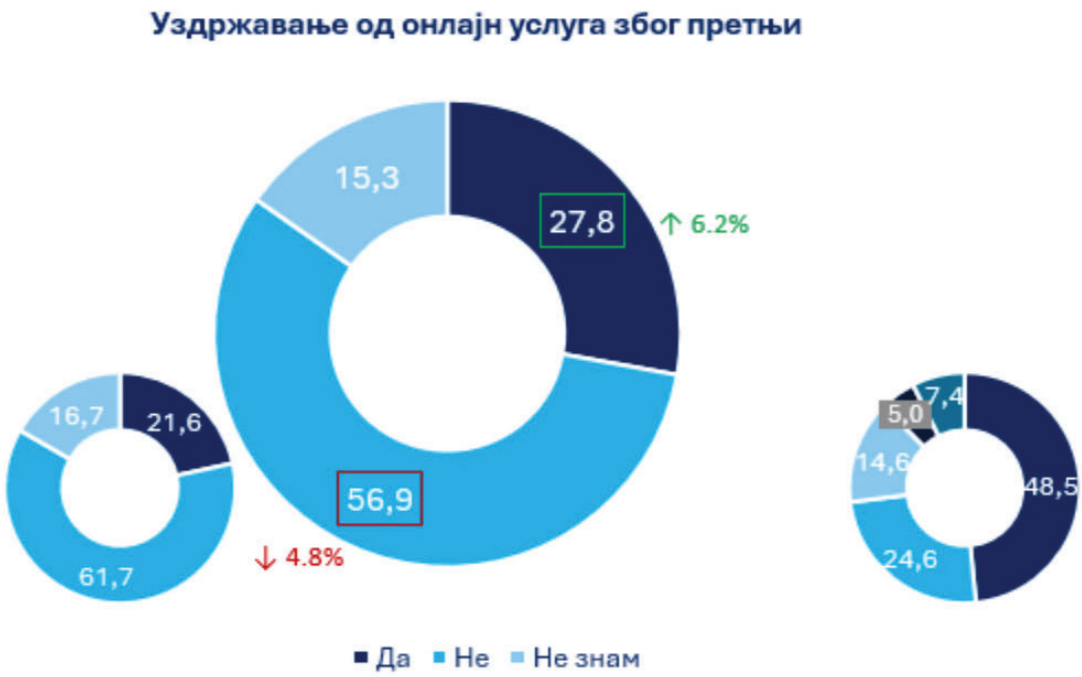
Забринутост поводом различитих негативних исхода је висока. Попут резултата у претходном таласу, **највећа забринутост** међу корисницима интернета и ове године, чак у још већој мери, тиче се **злоупотребе њихове банковне или кредитне картице** (65%). Одмах затим следи и **крађа идентитета на интернету** (62%), као и забринутост због могућег **напада вируса** (61%). **Најмање су забринути** да ће их неко изманипулисати да **пошаљу осетљиве податке,** али чак и ову забринутост изражава 42% интернет популације, што није занемарљив број. Женска интернет популација показује виши ниво забринутости за скоро сваки од сценарија.



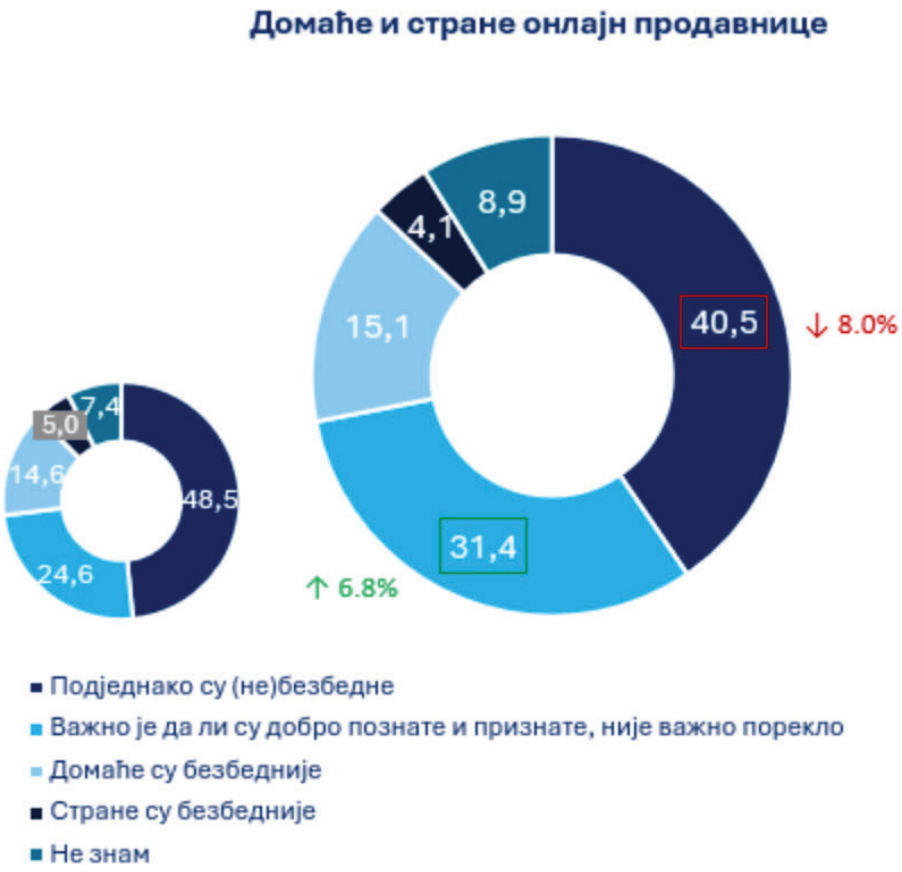
И ове године већина интернет корисника у Србији сматра **већом претњом** могућност да **их неко други на интернету угрози (83%),** него да сопственим поступцима угрозе своју безбедност (17%)..



Као последица сајбер претњи, 28% онлајн популације у Србији се уздржава од коришћења онлајн услуга, што је за 6% више у односу на претходно истраживање.



Већина и даље не прави разлику између страних и домаћих онлајн продавница по питању безбедности. Скоро **свака трећа особа** сматра да је једино **битно да ли су продавнице добро познате,** без обзира на порекло, **док 15% сматра домаће онлајн продавнице безбеднијим.**



Скоро половина интернет популације се **нашла у некој од ситуација** нарушавања информационе безбедности **(46%).** Најчешћи случај и даље је инфицирање **рачунара вирусом (40%),** иако се битно мањи проценат (-17%) онлајн популације сусрео се овим проблемом у односу на 2020. годину. Близу **8%** је било **жртва онлајн преваре, 5%** искусило је **крађу онлајн идентитета,** док је **4%** оних који су **злостављани или уцењивани** на интернету.

Искуство са компјутерским вирусима чешће су имале **старије узрасне групе,** као и они **вишег образовања и знања о безбедности на интернету.** Ове категорије становништва су вероватно успешније у идентификацији напада вирусом, те су због тога бројнији међу онима који препознају да су имали овај проблем.

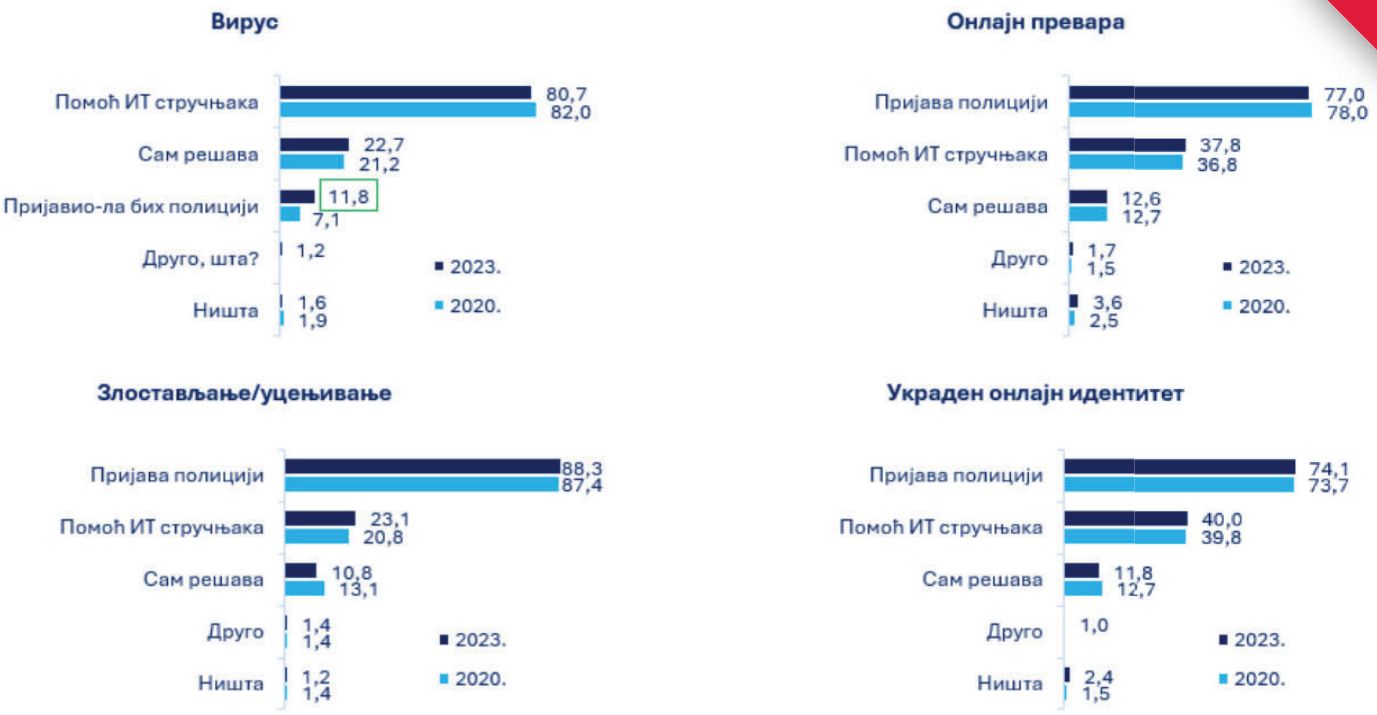
Ц5: Да ли сте можда били у следећим ситуацијама?
Јединица %

Самостално решавање је и даље најчешће решење за све ситуације нарушене безбедности, осим када долази до **инфицирања компјутерским вирусом,** где је обраћање **ИТ стручњацима** (57%) нешто чешће од самосталног решавања (46%).

И у овом таласу **помоћ полиције потражило је тек око 24% особа** у случајевима онлајн превара и злостављања/уцењивања на интернету.

Решења за хипотетички постављене проблеме бирана су у сличним размерама као и претходне године. И даље постоји значајна дискрепанца између стварних и хипотетичких решења. Наиме, за разлику од стварних ситуација, **самостално решавање** је, у скоро свим хипотетичким случајевима, **најређе бирана опција.** Такође, **помоћ ИТ стручњака** у ситуацији напада вируса интернет популација у Србији види се као **хипотетичко решење (81%) чешће од онога колико се овом решењу заиста прибегава (57%).**

Скоро **90%** у ситуацији злостављања или уцењивања, односно преко **70%** испитаника у осталим ситуацијама (онлајн превара, украден идентитет) као хипотетичко решење види **обраћање полицији,** док је **у реалности** проценат оних који проблем заиста и пријаве полицији и **два до четири пута нижи.**



Модели понашања

Модели понашања и навика у информационој безбедности били су предмет истраживања и процена у различитим областима пословања и временским размацима. Већина напора у овој области спроводи се у предузећима, а за циљ имају наметање безбедног понашања које ће спречити сајбер инциденте и допринети пословању компаније.

Без обзира да ли се примењује ISO/IEC 27001/27002, Закон о информационој безбедности или било који интерни оквир или политика информационе безбедности јединствени циљ је поставити стандарде безбедног понашања и спровођење контрола над поштовањем стандарда.

Ови стандарди су веома корисни за компаније или организације, али нису нужно корисни за све делове друштва, па тако нису дизајнирани да се користе као смернице за породице, у учионици у средњој школи или у дому за старе. Ипак, сви смо део дигиталног друштва и сви ми учествујемо у националној сајбер култури.

Стандарде и одређене обрасце понашања утврђују и стимулишу експерти информационе безбедности. Иако се обрасци понашања могу сматрати обавезним, временом ће се мењати као и претње и начини коришћења технологије.
За наше истраживање изабрали смо основне принципе безбедног понашања који се примењују, како у личној тако и пословној употреби интернета. То су контрола идентитета и заштита, безбедно понашање на интернету, редовно ажурирање оперативног система, заштита података и коришћење безбедносног софтвера.

На крају крајева, настојимо да се сви грађани понашају безбедно и да сви заједно допринесемо безбедном информационом друштву. Свакако, ово значи да је потребно да сви будемо боље информисани о начинима на које можемо остварити допринос и охрабрити друге да развију безбедне навике. Ипак, утврдили смо да је едукација у информационој безбедности најпогоднији начин за постизање овог циља. Али да ли то функционише на начин на који ми то настојимо? Који фактори утичу на безбедне навике?

Већина онлајн популације користи **антивирус програм на свом рачунару (70%),** мада у мањој мери него пре три године (за 11%). Број људи који користе Firewall је и даље низак – испитаници највероватније нису свесни постојања ове врсте заштите на својим рачунарима. Нешто **више од половине аутоматски ажурира софтвер,** док око **четвртина** њих то ради **ручно,** онда када ажурирање постане доступно. Проценат оних који **немају навике које се тичу ажурирања** се повећао и сада износи **16%.** У исто време приметан је пад у проценту особа са аутоматски подешеним ажурирањем.

Дошло је до пада у броју особа које креирају/користе лозинке на безбедан начин. **Различите лозинке** за већину онлајн услуга користи мало више **од половине** корисника интернета, што је за чак 17% мање у односу на претходни талас истраживања. Близу половине се труди да **креира јаке лозинке,** али је и овај проценат знатно нижи (за 33%). **Исту лозинку за све** налоге користи **17%** интернет популације у Србији, док само 12% користи апликацију за управљање лозинкама.

Сваки трећи корисник интернета у Србији прави резервне копије важних података бар једном месечно. Чешћа навика је да се **резервне копије праве ређе од једном месечно** (36%) и овај проценат је нешто виши него у претходном таласу истраживања. Са друге стране, **скоро трећина онлајн популације никад не прави резервне копије** или не зна колико често их прави, и међу њима је више оних са ниским знањем о сајбер безбедности и нижим образовањем.

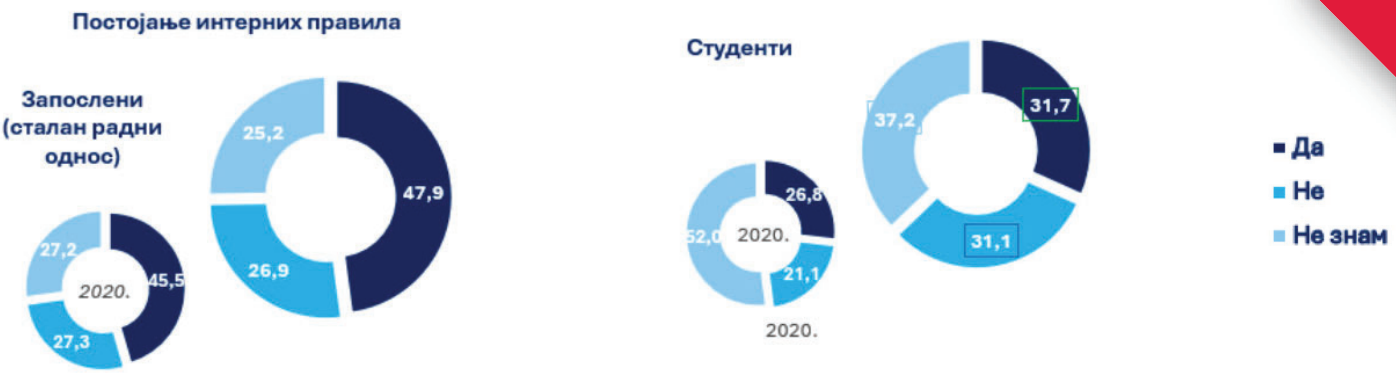
Близу **30% никада не проверава безбедност интернет страница.** Ипак, чини се да је овај проценат потцењен, јер само 46% тврди да зна како да провери безбедност одређене интернет странице.

Девет од десет испитаника **би нашло неки начин да сачува битне податке** са старог рачунара, од којих би већина пребацила све податке на друго место и обрисала све са старог рачунара (68%). Сваки десети корисник интернета **не би знао и/или не би урадио ништа са подацима пре продаје/бацања старог рачунара.**

Проценти који говоре о вештинама коришћења интернета нешто су нижи него 2020. године. **Око 80%** онлајн популације **зна да блокира нежељене поруке, избрише сајт из историје прегледања и промени опције о својим информацијама на друштвеним мрежама.**
Мањи број онлајн корисника у Србији зна и како да пронађе и**нформације о безбедности интернет странице** (46%), док **5%** њих не зна да уради **ништа од наведеног.**

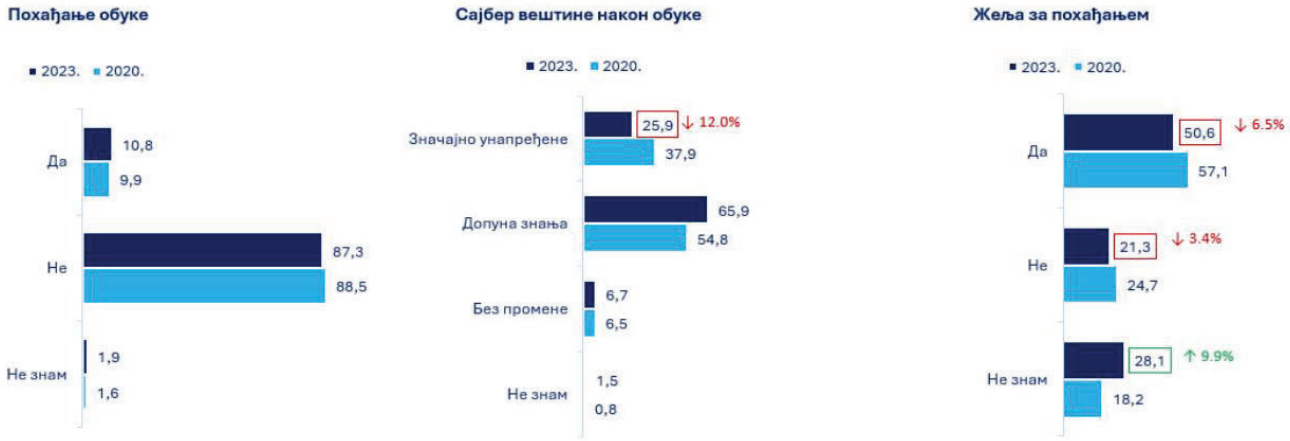
Постојање интерних правила о информационој безбедности у пословном окружењу остаје непромењено у односу на истраживање из 2020. године, док су студенти у већој мери обавештени о томе да ли оваква правила било постоје или не постоје.

Дошло је до **пооштравања правила која се тичу коришћења личних рачунара на послу/школи** – за близу половину интернет популације ово није дозвољено. Већина и даље сматра да је **једнако важно водити рачуна о информационој безбедности и на послу/школи/факултету и код куће.**



Тек с**вака десета особа је похађала неку врсту обуке о информационој безбедности** у претходне 2 године и ту се чешће ради о Београђанима и високообразованом становништву. Приметно је да су они који су похађали обуку постизали већа постигнућа на тесту знања о сајбер безбедности. Најчешћи исход након обуке је допуна знања (2/3 оних који су прошли кроз обуку), док је код сваке четврте особе дошло до значајног унапређења вештина.

Свака друга особа има жељу за похађањем обука о информационој безбедности. У односу на претходни талас истраживања, већи је број не знам одговора - може се закључити да спремност за похађање обука о информационој безбедности код 28% зависи од фактора као што су садржај/формат обуке.



Истраживање је обухватило и питање о префериранim изворима, односно начинима информисања о безбедности у сајбер простору. Кратки едукативни видео материјали су најпривлачнији формат за добијање информација о безбедности у сајбер простору. И други формати попут обуке на послу, информативног мејла, подкаста и онлајн тренинга су процењени као привлачни (око 1/3 интернет популације). У популацији најмлађих и оних са нижим нивоом знања има нешто више незаинтересованих за додатно информисање (20%).

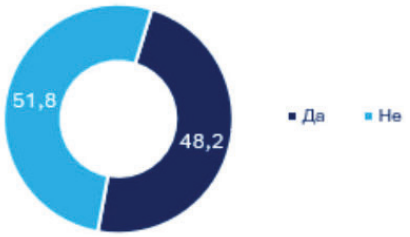
Постоји заинтересованост за разне теме везане за област безбедности у сајбер простору – 87% има жељу да нешто сазна о овој теми. Највеће интересовање се односи на праксе које се тичу заштите личних података и генерално савета како се заштитити, безбедно користити интернет, препознати нападе и преваре и слично.

Приближно сваки други испитаник је упознат са појмом двофакторске аутентификације. Четири од пет испитаника који су чули за 2FA тврде да је и користе (39% укупног узорка).

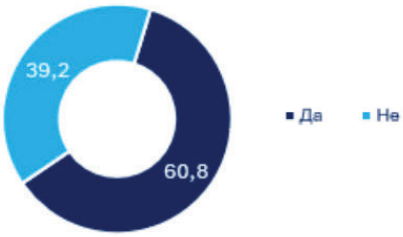
Док је познатост VPN-а већа (60%), знатно је мањи број оних који је користе (21% укупног узорка).

Главни разлози за употребу VPN-а су прописи на радном месту, очување безбедности и приватности на интернету и приступ садржају којем се иначе не би могло приступити.

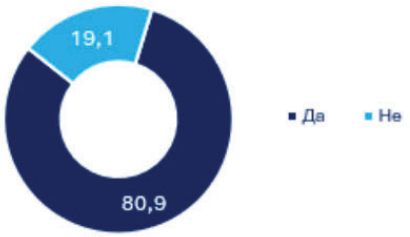
Двофакторска аутентификација
Познатост



VPN
Познатост



Двофакторска аутентификација
Употреба

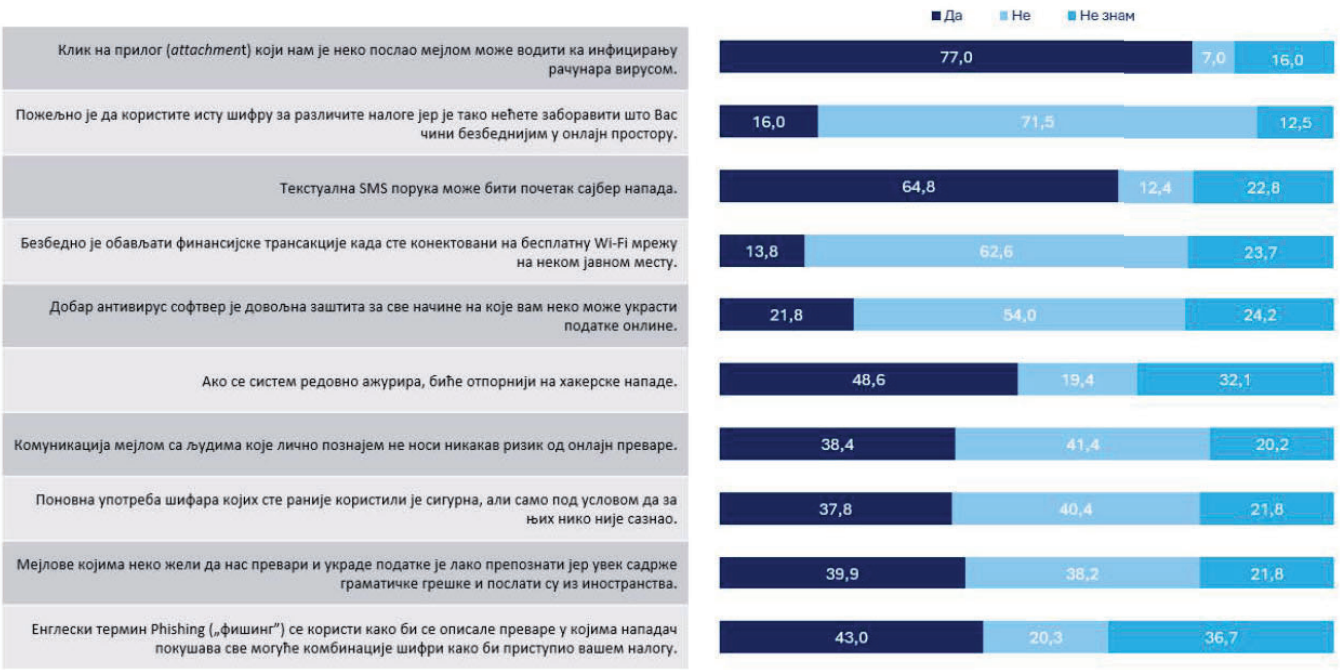


VPN
Употреба

Разлози за употребу VPN-а

Процена знања и препознавања фишинга

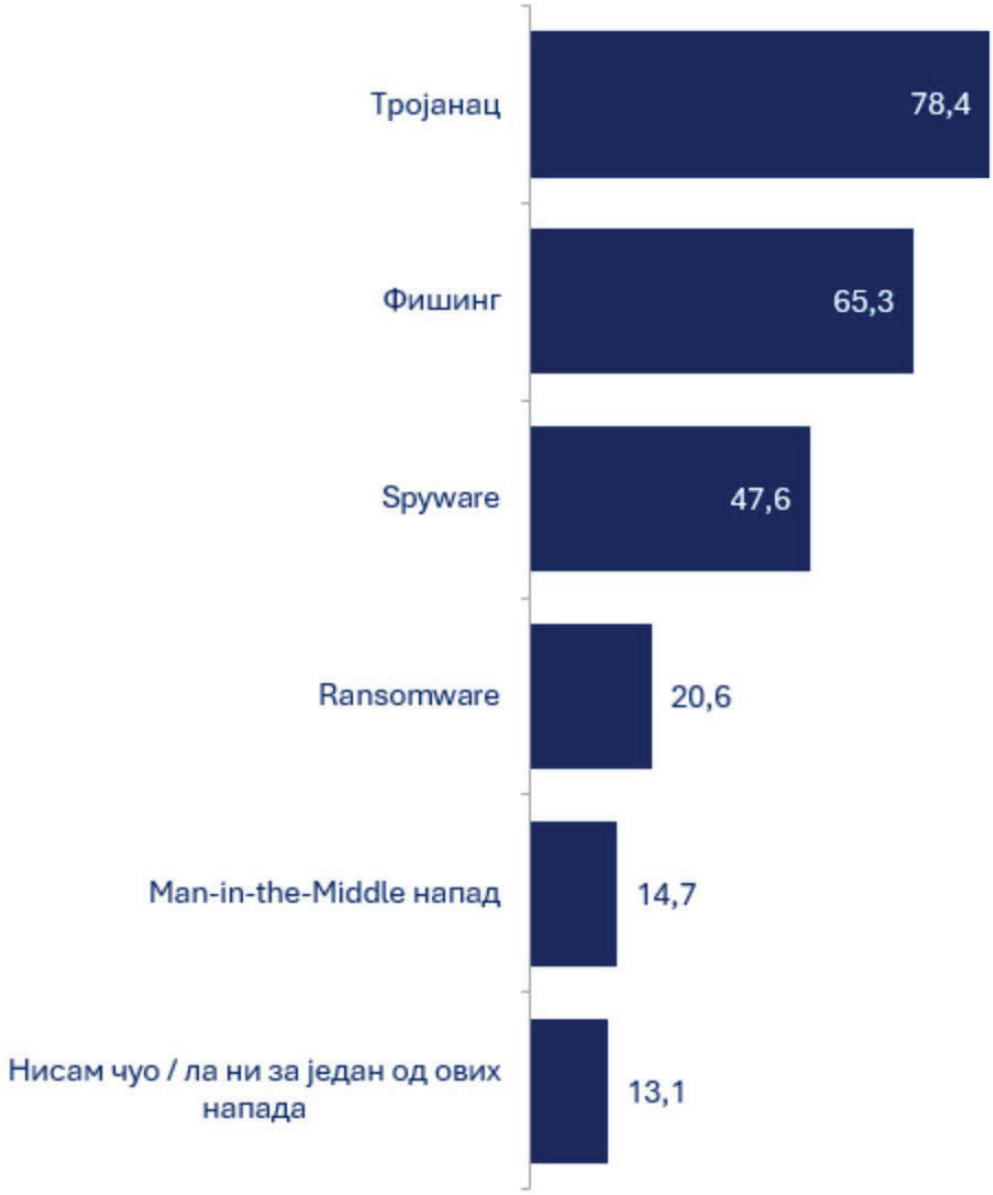
Одговори на неке од основних теза информационе безбедности указују на завидно знање испитаника иако има одговора који указују да је потребно подробније упознавање са терминима који су опште познати, као што је нпр. фишинг.



Упознатост са различитим врстама сајбер напада

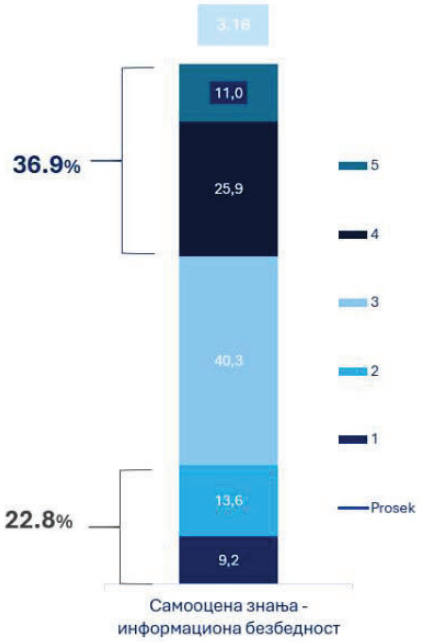
Интернет популацији у Србији су најпознатији тројанац и фишинг напад, док је близу половине чуло за Spyware. Ransomware и Man-in-the-Middle напади су мање познати.
Са друге стране, подаци са теста знања јасно показују да термин фишинг није довољно познат – само 20% успева да направи разлику између фишинга и Brute force напада (последња теза). Из тог разлога, иако су испитаници чули за ову врсту напада, не треба претпоставити да исправно повезују термин са његовим тачним значењем.

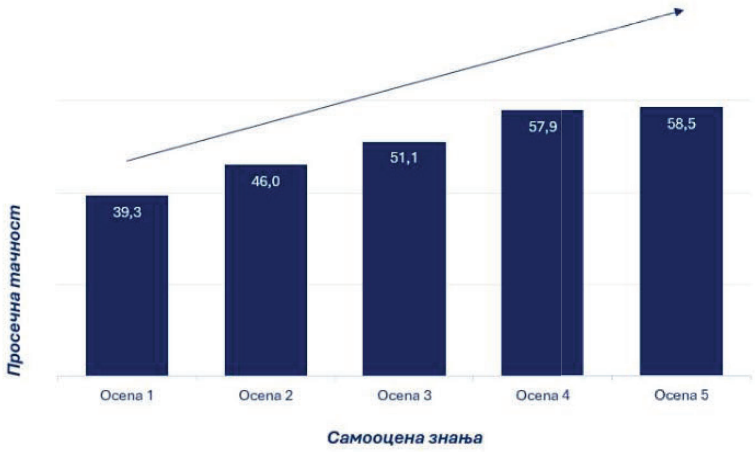
Занимљиво је да иако је низак проценат испитаника чуо за MITM нападе, а чак 63% је свесно опасности коју носи коришћење јавне отворене Wi-Fi мреже.



Препознавање фишинга

Пре отпочињања теста за препознавање фишинга спроведена је самооцена знања. Постоји позитивна повезаност између самооцене знања из информационе безбедности и постигнућа на тесту знања (они који своје знање о информационој безбедности процењују као веће, заиста и постижу више скорове на тесту знања). Ипак, чак и они који своје знање процењују највишим оценама у просеку решавају око 60% теста знања.





Испитаници су имали 6 примера које је требало да процене и одговоре да ли се ради о фишинг поруци или не.

Интернет популација у Србији је у просеку тачно решила 68% фишинг задатака, тј. у просеку се тачно препознаје 4 од 6 приказаних фишинг покушаја.

Само 8.2% је остварило савршен учинак, тј. направило тачну дистинкцију свих фишинг мејлова/порука од оних које то нису. Разлике у успешности препознавања нису нарочито изражене – жене, старији, високообразовани и они са вишим знањем из поља сајбер безбедности су били за нијансу успешнији.

Када су у питању очигледни покушаји преваре са лошим преводом текста и мало уложеног труда, већина испитаника није имала проблем да их успешно детектује као покушај фишинга. Исто тако, од помоћи је било и познавање уобичајених процедура (нпр. процедура доставе поште). Пажња се обраћа и на необичне мејл адресе пошиљаоца/страни број телефона.

Проблем настаје када је покушај преваре добро замаскиран тако да наликује порукама које би се могле добити од институције за коју се лажно представљају. Посебно занемарен елемент је податак да је мејл послат ка undisclosed recipients – овај податак се не користи као знак да је нешто потенцијално сумњиво.

Релативно често се као начин препознавања наводио општи утисак сумњивости, што може указивати на то да ови испитаници не умеју да детектују, тј. нису упознати са знацима за којима треба да трагају како би са већом вероватноћом донели суд о валидности мејла.

Такође, упечатљив је висок број лажних узбуна за мејл од непознате особе, линк у мејлу, приватна адреса са које се мејл шаље и субјективни доживљај необичности текста навели су испитанике да погрешно препознају овај мејл као покушај преваре. Са једне стране ово говори о сензитивности и сумњичавост испитаника на непознате садржаје која се може показати и корисном. Са друге, говори о немогућности да се пажња усмери на знаке који би дефинитивно указали на то да се ради о покушају фишинга.

Закључци и препоруке за стратешко планирање

Разумевање нивоа свести о безбедности, перцепције и културе корисника у аспектима везаним за безбедност је кључна за развој одговарајућих и ефикасних мера заштите како за кориснике интернета тако и за критичну информациону инфраструктуру. Ово разумевање постаје императив у земљама са повећаном интеграцијом информационо-комуникационих технологија (ИКТ), као што је Србија.

Приступ интернету, медији и еКуповина

Нису уочене битне разлике у начину приступа интернету у односу на период од пре 3 године, паметни телефони и даље представљају најчешћи начин приступа онлајн свету. Најупадљивија разлика односи се на коришћење друштвених мрежа, где је **Tik Tok остварио двоцифрен раст** па га сада користи скоро 2/5 интернет популације у Србији. Ова мрежа има посебну популарност међу особама узраста 15-24 година, али је користи и узрасна група старости 25-34 година. Запажене су минорне разлике које се тичу личних података који се остављају на друштвеним мрежама - нешто је мање оних који остављају податке попут послодавца/школе, личне фотографије и датума рођења. **Мобилно банкарство и електронска трговина на домаћим сајтовима су у двоцифреном порасту те их сада користи 68%, односно 60% интернет популације у Србији.** Благ пораст показује и електронска трговина на страним сајтовима (37%).

Национална сајбер култура у Србији

Промене у односу на претходни талас истраживања су видљиве **само на неколико индикатора.** Иако је став према употреби нових технологија и даље претежно позитиван (74%), он је за нијансу негативнији него пре 3 године. Друга промена тиче се нешто већег ослањања на криминалистичке службе у случају сајбер криминала и већег прихватања надгледања онлајн активности како би се остварила већа безбедност на интернету. Ипак, ова повећања су блага и представљају став са којим се слаже мањина интернет популације у Србији (тек нешто више од сваке треће особе). Већина корисника интернета и даље не прави везу између безбедности интернета и безбедности сопственог уређаја.

Компетенције, знање и учење

Самооцене знања из информационих технологија и информационе безбедности су нешто лошије у односу на претходну годину. Такође, више је особа које своје знање процењује као исподпросечно (15%), где се најчешће ради о младима узраста 15-25 година.
Нису уочене разлике у начину на који се учи о информационој безбедности - и даље су најчешће у питању самостално учење, самосталне пробе и грешке и неформално стицање знања од других људи.

Схватање ризика

Као најризичније активности су и у овом таласу процењене оне које се тичу лоших пракси руковања лозинкама (дељење лозинки, коришћење истих лозинки).
Са тим у вези, руковање лозинкама је на нижем нивоу у односу на претходни талас истраживања - мање интернет корисника настоји да креира јаке лозинке (80%) и мање је оних који користе различите лозинке за различите услуге (53%). Употреба апликација за управљање лозинкама и даље није заживела (12%).

Само половина корисника интернета у Србији је сигурна да разликује безбедно од небезбедног у сајбер простору, што је за 7% мање у односу на период од пре 3 године. Присутна је свест по питању различитих претњи по информациону безбедност, од злоупотребе банковних картица (65%) до манупулације која би водила откривању поверљивих података (42%). Као и у претходном периоду, постоји крупна дискрепанца по питању поступања у стварним и хипотетичким ситуацијама нарушавања сајбер безбедности - у хипотетичким ситуацијама се чешће бира умешаност полиције него што је то случај у реалним ситуацијама.

И у овом таласу помоћ полиције потражило је тек око 24% особа у случајевима онлајн превара и злостављања/уцењивања на интернету.

Модели понашања

Проценат особа које немају навике које се тичу ажурирања се повећао и сада износи 16%, док се са друге стране смањио број оних којима је ажурирање подешено на аутоматско. На тесту знања, нешто више од половине корисника интернета није знало да ли редовно ажурирање система води ка већој отпорности од хакерских напада.

Само 46% тврди да зна да пронађе податак о сигурности неке странице на интернету. Сваки трећи корисник интернета у Србији прави резервне копије важних података бар једном месечно. Чешћа навика је да се резервне копије праве ређе од једном месечно (36%) и овај проценат је нешто виши него у претходном таласу истраживања.

Постоји заинтересованост за разне теме везане за област безбедности у сајбер простору – 87% има жељу да сазна више о овој теми. Заинтересованост за обуке је и даље висока (51%). Кратки едукативни видеи се сматрају најпривлачнијим форматом за информисање.

Тест препознавања фишинга

Интернет популација у Србији је у просеку тачно решила 68% фишинг задатака, тј. у просеку се тачно препознаје 4 од 6 приказаних фишинг покушаја.
Када су у питању очигледни покушаји преваре са лошим преводом текста и мало уложеног труда, већина испитаника није имала проблем да их успешно детектује. Проблем настаје када је покушај преваре добро замаскиран тако да наликује порукама које би се заиста могле добити од институције испред које се лажно представља и када је потребно ослонити се и на специфичније знаке који указују да се ради о превари.

Сматрамо да би креирање националног програма за подизање свести о значају информационе безбедности обезбедило свеобухватан приступ обукама и другим начинима ширења знања, гарантовало њихов квалитет и спречило ширење дезинформација. Дефинисање нивоа квалитета појединачних активности може се постићи коришћењем међународних стандарда за креирање програма и обука, као и креирањем индикатора, циљева, начина евалуације за сваку од дефинисаних активности. Овакав приступ обезбедио би надлежним институцијама важан основ за креирање сопствених планова за подизање свести о значају информационе безбедности и њихово спровођење.

Овакав програм треба да обухвати најважније теме, као што су јачање вештина креирања копија резервних података, коришћења анти-вирусних софтвера, начина креирања јаких лозинки и коришћење апликација за управљање лозинкама које би се обрађивале и кроз интерне обуке запослених и на тај начин значајно утицати на унапређење знања и понашања корисника. Спровођење интерних обука запослених из области информационе безбедности би требало да обухвати и познавање интерних правила и процедура и омогући запосленима да искажу своје мишљење о правилима за која сматрају да их ограничавају у свакодневном раду, али и укажу на обавезу запослених да се понашају у складу са њима у циљу очувања безбедности ИКТ система послодавца.

Имајући у виду резултате истраживања верујемо да би стратешка имплементација препорука дала позитивне резултате у кратком року. Безбедно понашање корисника у сајбер простору један је од важних предуслова за развој информационог друштва и максималног искоришћавања потенцијала нових технологија. Истраживање српске националне сајбер културе отвара бројне могућности за даља истраживања и представља добар основ за планирање начина за унапређење знања и понашања у области информационе безбедности.

Литература

1. The Norwegian Cyber security culture, Bjarte Nakmedal & Hanne Eggen Røislien, 2016
2. Култура сајбер простора, Ива Ненић, 2004
3. Introducing Cyberculture, David Silver, 2000
4. Утицај националне културе на процес управљања организационим променама, Илић Ђурђијана, Андрејић Марко, Јаношевић Миљојко, Илић Слађана, ВОЈНО ДЕЛО, 7/2019
5. An Ontology for a National Cyber-Security Culture Environment N. Gcaza, R. von Solms and J. van Vuuren, Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)