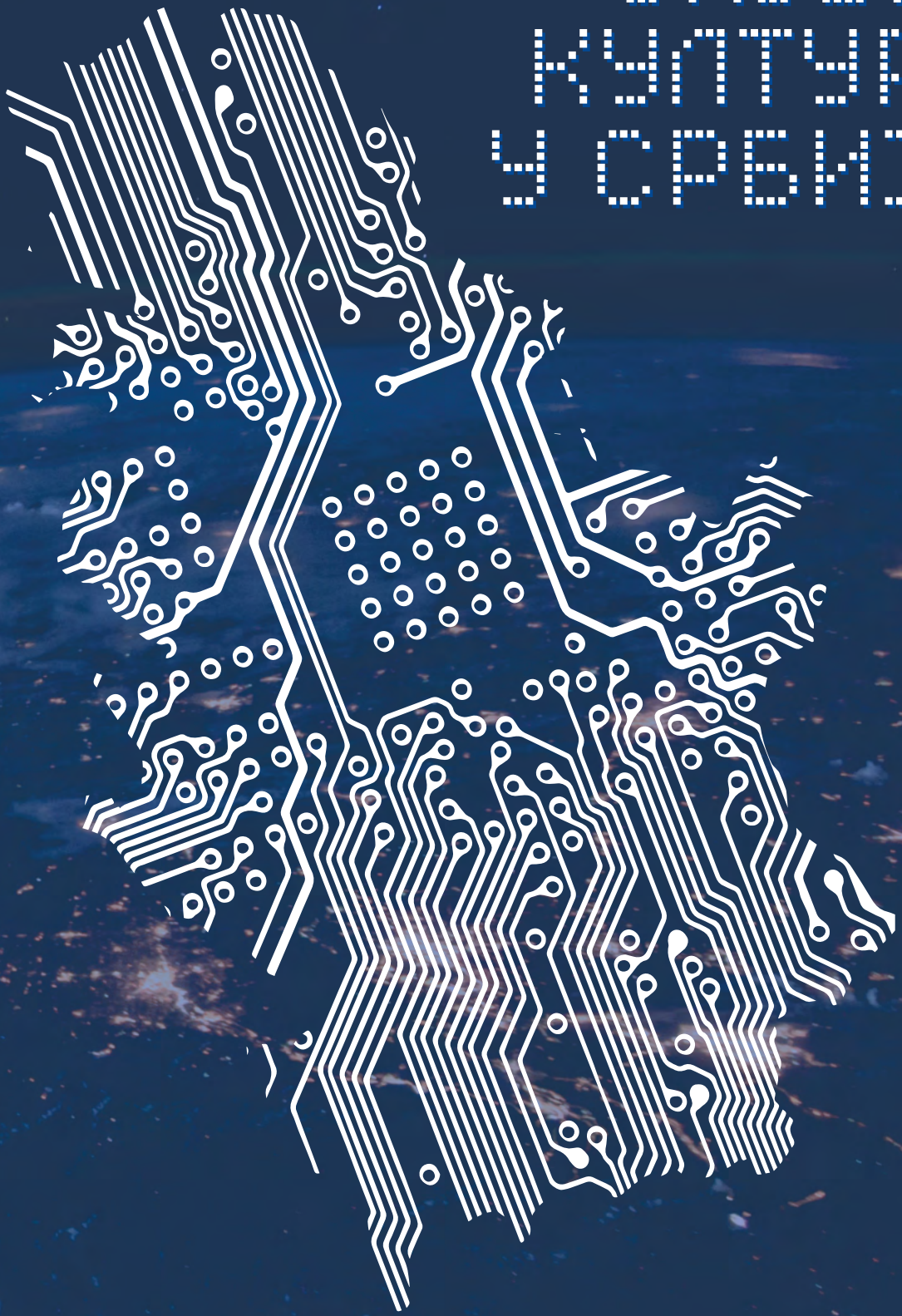
САЈБЕР КУЛТУРА У СРБИЈИ



РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

Децембар, 2020. година

Национални ЦЕРТ Републике Србије

www.cert.rs

Садржај

Увод

Регулаторна агенција за електронске комуникације и поштанске услуге (РАТЕЛ) је Законом о информационој безбедности, препозната као један од најзначајнијих субјеката у области информационе безбедности, па је овим Законом добила у надлежност и обављање послова Националног ЦЕРТ-а. Захваљујући свеукупном квалитету рада наше Агенције у пољу регулације тржишта телекомуникација и поштанских услуга утврђена је ова изузетно значајна, одговорна и престижна улога кључног чиниоца у области информационе безбедности у Републици Србији.

Информациона безбедност је аспект безбедности који се односи на безбедност података, уређаја, мрежа, информационих система организација и појединаца, односно на безбедносне ризике повезане са употребом информационо-комуникационих технологија. Ова област је у нашој земљи уређена у складу са прописима Европске уније, односно Директивом ЕУ о мрежној и информационој безбедности која је, као и наш Закон о информационој безбедности, ступила на снагу 2016. године.

Истраживање о сајбер култури у Србији спроведено је у циљу подизања свести о значају информационе безбедности и унапређењу знања, навика и понашања свих корисника интернета у нашој земљи.

Потреба за мерењем информационе безбедности

Наше друштво пролази кроз динамичан процес дигитализације у приватном и јавном сектору. Развој еУправе и спектра услуга које су нам доступне преко интернета се свакодневно увећава. Пандемија вируса COVID-19 суочила нас је са значајем дигитализације и електронских услуга управе на начин који није био ни замислив. У врло кратком периоду суочили смо се са другачијим условима живота и рада, мерама здравствене заштите које су упућивале на смањење кретања, самоизолацију, рад и учење од куће, што је подразумевало употребу информационо-комуникационих технологија свих грађана у значајно већем обиму. У таквим околностима постало је више него јасно да је даљи развој дигитализације и еУслуга у нашој земљи неопходан.

Дигитализација се све више везује за економију, па се и за државе у којима дигитализација није на високом нивоу развоја сматра да пролазе кроз дигиталну транзицију. Експанзија дигиталне економије је омогућила значајне приходе у буџетима дигитално развијених држава. Дигитализација, као облик трансформације и напретка друштва, има потенцијал за остваривање економског раста и напретка кроз националну и глобалну трговину и ефикасније јавне услуге. Свакако, овај потенцијал има своја ограничења и појаве које га угрожавају као што је високотехнолошки криминал.

Наша држава последњих година улаже изузетан напор како би се процес дигитализације спроводио темпом који одговара приликама у нашем друштву. Многе западне земље су достигле изузетно висок ниво развоја, а Норвешка, чији модел користимо у овом истраживању, је пета земља по дигитализацији у свету. Треба имати на уму да овај спорији напредак у односу на западне земље треба искористити управо применом њихових искустава и на тај начин настојати да информациона безбедност иде у корак са развојем дигитализације. Наша држава је препознала информациону безбедност као једну од шест

приоритетних области развоја информационог друштва и даје велики значај безбедном коришћењу еУслуга.

Национална Стратегија развоја информационе безбедности за период 2017–2020. године утврђује принципе развоја информационе безбедности, приоритетне области и стратешке циљеве. Информациона безбедност Републике Србије дефинисана је као кључни део свеобухватне националне безбедности која се заснива на информационој безбедности институција, снага, људи, система, процеса, информација и вредности које су од значаја за безбедност и одбрану земље.

Проактивна улога наше државе у доношењу Закона о информационој безбедности и усклађивања са прописима ЕУ, нарочито НИС Директивом, несумњив је знак настојања да информациона безбедност иде у корак са дигитализацијом. Проактивним деловањем и успостављањем читаве организације релевантних институција на националном нивоу, утврђивањем јединствене листе обавезних мера заштите и начела којима се треба руководити, сталним унапређењем и провером функционисања ИКТ система од посебног значаја Влада, односно Министарство трговине, туризма и телекомуникација настоји да формира адекватан ниво читавог система информационе безбедности.

Свакако, јасно је да се безбедно дигитално окружење не може креирати само на техничком нивоу, односно улагањем у информационе технологије. Сваки грађанин, запослени, студент, пензионер суочен је са друштвом које се убрзано технички развија, а упоредо са њим се развија и стално мења и дијапазон безбедносних претњи. Начин на који перципирамо дигиталне ризике, наше понашање, вештине и знање о заштити дигиталног окружења од круцијалног је значаја за развој информационог друштва. У најгорем случају, недостатак свести, вештина и знања могу довести до нежељеног развоја ситуације у којој нема жеље за употребом информационих технологија. Друштво у коме постоји страх од еУслуга ће исте избегавати или их неће ни користити. Уколико нема поверења у јавни сектор, односно да може да обезбеди сигурност наших личних података грађани ће пружити отпор свим тенденцијама и покушајима дигитализације. Управо зато треба да знамо више о сајбер култури, односно о нивоу разумевања информационе безбедности у нашем друштву, а кроз развијање начина за њено мерење. На овај начин спознаћемо ефекте развоја информационе безбедности и дигитализације уопште. Дубље разумевање сајбер културе је од великог значаја јер дотиче нека од најважнијих питања развоја. Сајбер безбедан грађанин је од фундаменталног значаја за успешну дигитализацију на националном нивоу.

Национална култура

Под националном културом подразумева се скуп претпоставки, веровања и вредности које су прихватили припадници једне националне заједнице и који битно одређује њихово разумевање света и понашања у њему. У културним традицијама социјалне организације народа то су обичаји, систем управљања, односи међу људима. Национална култура је, генерално, не само врховни израз индивидуалних вредности и колективног духа једног народа, већ и моћно оружје у рукама оних који знају да културне вредности промовишу и штите. Култура подразумева традицију, која је предуслов за постојање једне нације, и коначно, државе. Национална култура је важан фактор који опредељује и индивидуалне вредности и понашање појединца.

Претпоставке, вредности и норме националне културе су у највећој мери подсвесног карактера. Оне дефинишу ставове о природи људског карактера – да ли су људи по природи добри или лоши, вредни или лењи, променљиви или непроменљиви. Претпоставке дефинишу и однос људи према природи тј. да ли људи могу бити у хармонији са природом и да ли могу овладати природом. Национална култура дефинише и односе међу људима: да ли су једнаки, да ли би требало да буду једнаки са другима или моћнији од других, однос појединца и колектива. Људи ове односе и претпоставке не уважавају довољно све док не дођу у сусрет са културом која се разликује од њихове и тек тада постају свесни различитости својих и туђих ставова и претпоставки.[1]

Један од највећих истраживача националне културе и њених димензија је холандски аутор Герт Хофстед (*Geert Hofstede*). Аутор јединственог приступа инжењера који је постао антрополог, своје прво истраживање спровео је крајем 70-их година у филијалама мултинационалне компаније IBM у 40 светских земаља. То испитивање је дефинисано кроз 4 димензије на основу којих се разликују националне културе у свету. Током 90-их година је модел проширен тако да од тада садржи 6 димензија, а истраживање које је доступно на интернету[2] обухвата 76 држава међу којима је и наша земља. Мерење димензија културе карактерише чињеница да нема апсолутног стандарда, већ да мерења настају упоређивањем нација, односно њихових разлика.

1. Индивидуализам-колективизам

Ова димензија указује на одговорност за сопствену судбину, индивидуализам подразумева да је сваки појединац одговоран за себе, а колективизам да је за судбину сваког појединца одговоран колектив. Индивидуализам не значи егоизам, већ да се очекују индивидуални избори и одлуке. Колективизам не значи блискост, већ да појединац разуме своје место у друштву. У индивидуалистичком друштву су везе између појединаца лабаве, од сваког се очекује да води рачуна о себи и својој ужој породици. У колективистичком друштву су чланови од рођења део јаких група као што је шира породица, сеоска заједница и томе слично. Код колективизма је у решавању задатака међусобни однос на првом месту, док је код индивидуализма задатак на првом месту, а међусобни однос на другом месту. За друштва које карактерише колективизам заступљен је „високи контекст комуникације" већина ствари је очигледна и комуникација је краћа, док код индивидуализма заступљен „низак концепт комуникације" у коме постоји потреба за прецизним објашњењима. Резултати мерења изражени су 0–100, они ближи 0 су карактеристични за колективна друштва, док су резултати ближи 100 карактеристични за индивидуална друштва.

2. Дистанца моћи - висока и ниска

Ова димензија показује степен у којем припадници једне националне културе сматрају нормалним и очекиваним да моћ буде неравномерно распоређена односно да у друштву има врло моћних појединаца и група као и оних који уопште немају моћ. Индекс дистанце моћи дефинисан је 0–100, а резултати ближи 0 значе ниску дистанцу моћи, док резултати ближи 100 значе високу дистанцу моћи. Код култура са виском дистанцом моћи осећај је да су надређени супериорна бића, другачија врста људи, најважнија особина која

1 Утицај националне културе на процес управљања организационим променама, Илић Ђурђијана, Андрејић Марко ОРЦИД, Јаношевић Миљојко, Илић Слађана, ВОЈНО ДЕЛО, 7/2019

2 https://www.hofstede-insights.com/

се у васпитању деце преноси је поштовање. Код култура са ниском дистанцом моћи постоји хијерархија, али надређени нису супериорни и њихов положај се може променити, а најважнија особина која се преноси у васпитању деце је независност.

3. Мушке - женске вредности

Кроз ову димензију врши се идентификовање степена друштвене прихватљивости употребе силе. Код култура у којима преовлађују тзв. „мушке" вредности цене се постигнућа, успех, резултати, агресивност, кондиција, док су „женске" вредности: међуљудски односи, квалитет живота, равнотежа, склад, брига о средини и цене се толеранција, нежност, љубав, топлина, страст. У друштву које карактеришу мушке вредности посао је јасан изговор да се запостави породица, док у друштву које карактеришу женске вредности људи покушавају да пронађу равнотежу између посла и породице. Резултати мерења изражени су 0–100, а они ближи 0 карактеристични су за друштво са женским вредностима, док су резултати ближи 100 карактеристични за друштво са мушким вредностима.

4. Избегавање неизвесности

Ова димензија указује на степен угрожености чланова друштва у неизвесним, нејасним или променљивим околностима, односно друштвене толеранције на неизвесност и двосмисленост. Избегавање неизвесности није везано за избегавање ризика или поштовање правила већ је везано за анксиозност и неповерење при суочавању са непознатим у жељи да се имају сталне навике и ритуали и сазна истина. У друштву у којем је карактеристично избегавање неизвесности заступљен је већи стрес и анксиозност, док је у друштву које прихвата неизвесност мање стреса и анксиозности. Потреба за правилима и њиховим поштовањем, чак и када нису практична карактеристични су за друштво које избегава неизвесност, као и да је оно што је другачије опасно, док у друштву које прихвата неизвесност нема правила чак и обавезна правила се крше, и оно што је другачије сматра се занимљивим. Технолошке иновације се у друштву које избегава неизвесност прихватају споро и пажљиво, као што су на пример модерни информациони системи. Индекс избегавања неизвесности изражен је 0–100, а резултати ближи 0 карактеристични су за друштво слабог избегавања неизвесности, док су резултати ближи 100 карактеристични за снажно избегавање неизвесности.

5. Дугорочна - краткорочна орјентација

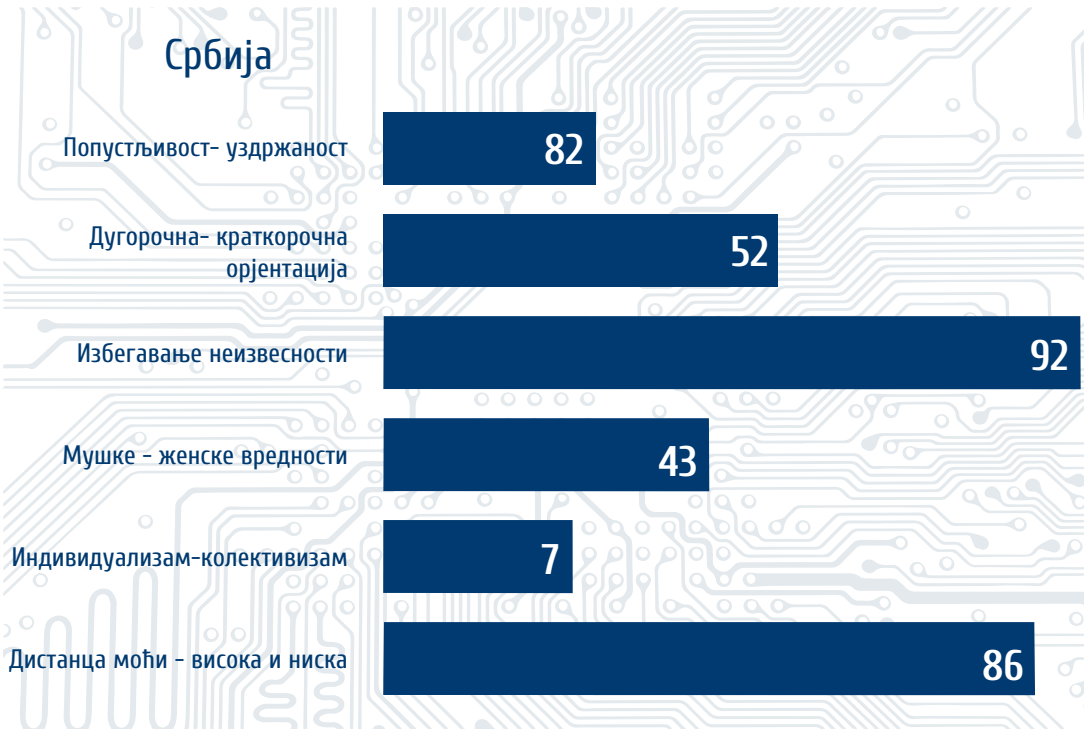
Дугорочна орјентација постоји у друштву практичних појединаца, орјентисаних ка будућим наградама, упорности, штедњи и навикавању на промене. Краткорочна оријентација је окренута ка прошлости и традиционалним вредностима, као што су национални понос, поштовање традиције и испуњавање социјалних обавеза. Друштво дугорочне орјентације карактерише скромност, релативитет доброг и лошег, те да се временом добро и лоше могу променити, док је за краткорочну орјентацију друштва карактеристична потрага за позитивним информацијама о себи, као и да су добро и лоше увек исти. Друштво

дугорочне орјентације је отворено за учење од других земаља, док је за краткорочну орјентацију карактеристичан национални понос. Индекс дугорочне орјентације је изражен резултатима 0–100, 0 значи краткорочну орјентацију, 100 дугорочну орјентацију.

6. Попустљивост - уздржаност

Ова димензија односи се углавном на субјективни осећај среће и контроле над животом људи. Попустљива друштва омогућавају релативно слободно задовољење природних и основних људских жеља које воде уживању у животу и забави. Уздржана друштва потискују потребе и регулисана су стриктним друштвеним нормама. У попустљивом друштву људи се осећају срећнијим и здравијим, док се у уздржаним друштвима људи осећају мање срећним и мање здравим иако је објективно највероватније да су подједнако здрави. У попустљивим друштвима људи имају утисак контроле над животом, да су господари сопственог живота, док у уздржаним друштвима људи имају утисак да оно што им се дешава не зависи од њиховог чињења већ зависи од других фактора. Попустљива друштва имају етику разоноде, више оптимизма и позитивног понашања, док уздржана друштва имају етику рада, више песимизма и цинизма. Индекс задовољства изражен је 0–100, а резултати ближи 0 карактеристични су за уздржана друштва, док су резултати ближи 100 карактеристични за попустљива друштва.

Овим истраживањем је утврђено да је српска национална култура има јединствену комбинацију високе дистанце моћи, високог избегавања неизвесности, колективизма, женске вредности, краткорочне орјентације и уздржаности.



Појам сајбер културе

Креирање начина мерења сајбер културе је изазов за многе државе и организације које се баве информационом безбедношћу. У креирању начина мерења коришћен је норвешки модел и метод истраживања. Главни изазов је уопште концепт мерења сам по себи. Разлог за ово је што је појам сајбер културе прво развијен у пословном окружењу и као такав је од стране стручњака у области информационе безбедности распрострањен на цело друштво и тренутно представља једну од најактуелнијих глобалних тема.

На самом почетку суочили смо се са два велика изазова први, како уопште превести овај појам „*cyber security culture*" и како га дефинисати. Сам појам сајбер културе није нов, али се чини да нема јединственог схватања овог појма, осим да се односи на „нешто што има везе са понашањем у сајбер простору".

Други, како утврдити овај концепт тако да буде примењив и на пословном и на националном нивоу. На пословном нивоу постоји начин да се запослени едукују, на начин на који то није могуће извести за грађане на националном нивоу.

Schein (1992, p.17) дефинише сајбер културу као „образац заједничких основних претпоставки које је група научила док је решавала проблеме спољне адаптације и унутрашње интеграције, што је довољно добро функционисало да би се могло сматрати валидним и, као такве подучавати нове чланове као исправан начин схватања, мишљења и осећања о тим проблемима". Слично, *Schlienger* и *Teufel* (2002) упућују да би сајбер култура у оквиру организације требало да пружи подршку свим активностима на начин да информациона безбедност постане природни део свакодневног живота сваког запосленог.

Чињеница да информациона безбедност има културолошку димензију не треба да представља изненађење. Сајбер култури се прилази са два аспекта која су повезана, први, сајбер култура се сматра алатом за управљање и други, сајбер култура представља збир активности које осликавају понашање запослених. У том случају се сајбер култура посматра као збир образаца понашања запослених који може значајно допринети укупној вредности послодавца. Очигледан знак оваквог приступа заправо представља тенденција да се сајбер култура оцењује као добра или лоша. Овакав формални приступ овом појму указује на то колико култура у контексту информационе безбедности може бити корисна, па се може тестирати, мерити и унапређивати.

Ипак овакав приступ оставља нам и очигледно питање: Да ли то значи да се сајбер култура своди на акције? Да ли је сајбер култура само начин управљања пословањем? Ако је тако да ли је онда појам „култура" адекватан?

Друштвене науке појам културе посматрају као далеко сложенији и врло је редак формални приступ или опис. Стручњаци у овим областима приступају му кроз фокус на основне вредности, мишљења и ставове који обликују наше акције. Култура у овим областима није алат, већ критеријум за позиционирање у свету и обликовање схватања. Другим речима, поступци и обрасци понашања су изрази ставова и вредности.

Чини се да у схватању појма сајбер културе постоји сукоб међу научним дисциплинама, што заправо не би требало да чуди јер је реч о спајању две врло различите области. Научници који се баве информационом безбедношћу не баве се културом, док се они који се баве проучавањем културе не баве инфор-

мационом безбедношћу. Ипак, верујемо да је за обе области изузетно значајан свеобухватнији приступ који подразумева интегрисани рад и једних и других научника.

Сајбер култура као грана информационе безбедности

Информациона безбедност је пре свега једна динамична и иновативна област, и као таква тренутно изузетно актуелна. Иако и сама део опште безбедности, као изузетно инспиративна и широка област обухвата неколико грана које повезују различите научне области.

Управо је због чињенице да је утицај сајбер културе препознат као веома значајан, као и да ће од развоја ове области зависити и напредак савременог друштва, постоји тенденција за формирањем студијских програма.

Студијски програми из сајбер културе у земљама Запада постоје од 90-их година, када се јавила дефиниција три фазе сајбер културе. Популарна сајбер култура (*popular cyber culture*) потиче из журнализма и карактерише је описна природа, ограничени дуализам и коришћење интернета као граничне метафоре, студије сајбер културе (*cyber culture studies*) дају шири фокус на виртуелне заједнице и онлајн идентитете и позитивни утицај на студенте, као и студије критичне сајбер културе *(critical cyber culture studies)* као трећу фазу, која проширује идеју о сајбер култури и укључује четири области: онлајн интеракције, дигитални дискурс, приступ и онемогућавање интернета, као и интерфејс дизајн сајбер простора, и истражује однос и зависност између све четири области[3].

Свест и образовање, као компоненте сајбер културе, корисницима интернета могу пружити вештине неопходне за препознавање претњи, као и унапређење понашања уопште. Понашање корисника је предмет многих истраживања, као и овог нашег, у којима се врло често утврђује да је недостатак свести о сајбер ризицима и претњама оно што их чини лаком метом злоупотребе. Утврђено је да се корисници са више знања о информационој безбедности понашају другачије од корисника који немају развијену свест о значају информационе безбедности (*Al-shehri* 2012). Без обзира на чињеницу да ниво свести о значају информационе безбедности има позитиван утицај на понашање, постоји јаз између нивоа свести и одређеног понашања корисника (*Furnelletal.* 2008). Дакле, неопходан је рад на развоју сајбер културе и прихватљивих понашања корисника у новој реалности сајбер простора (*High-Level Experts Group (HLEG)* 2008, p.103).[4]

Такође, корисници су врло често представљени као најслабија карика, од чијег знања и вештина зависи безбедност организације у којој раде, али и нације уопште, међутим корисници су заправо у првој линији одбране у чије знање и вештине је потребно стално и стратешки улагати.

Постоји јасна тенденција државе за развојем свих грана информационе безбедности, посебно сајбер културе кроз подизање свести о њеном значају код грађана, као и друштву уопште. Као најважније компоненте сајбер културе препознати су подизање свести о значају информационе безбедности и образовање, те су као такви обухваћени Стратегијом развоја информационе безбедности.

3 Introducing Cyberculture, David Silver, 2000

4 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)

Метод истраживања

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 компаније или организације? Или врста делатности има значајан утицај?

За потребе овог истраживања коришћени су индикатори из норвешког модела који су врло детаљно испитани у пилот студији која је спроведена током 2015. године. 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 разумно поређење међу секторима, предузећима и групама популације.

Квантитативно истраживање спровела је агенција Smart+ Research[5], 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.

Питања из 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 образовања информационе 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 и сигурност сајбер простора?

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

На основу питања из истраживања развијен је сет индикатора, питања, која могу да обезбеде релевантне податке, адекватне за даљу анализу.

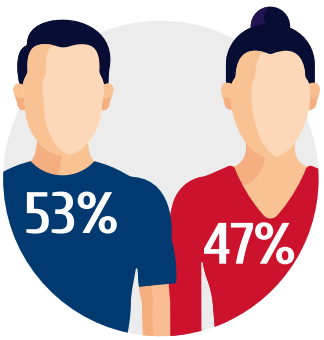
Демографска структура

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.

5 Агенција Smart+ Research

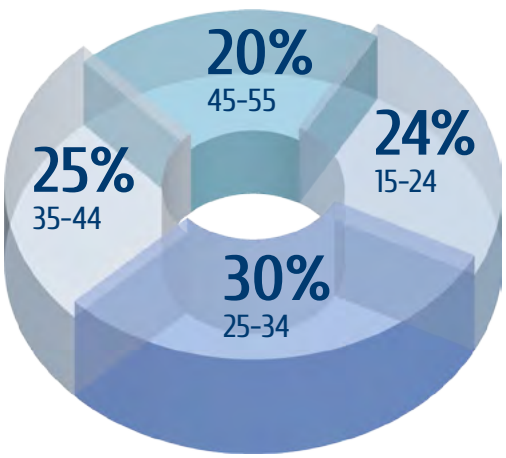
Репрезентативни узорак од 1250 испитаника гарантује минималну статистичку грешку од ±2.7% на интервалу поузданости од 95%, односно максималну статистичку грешку ±6.2% на интервалу поузданости од 95% за најмању јединицу узорка (најстарија старосна група – *45–54 година*).

Узорак

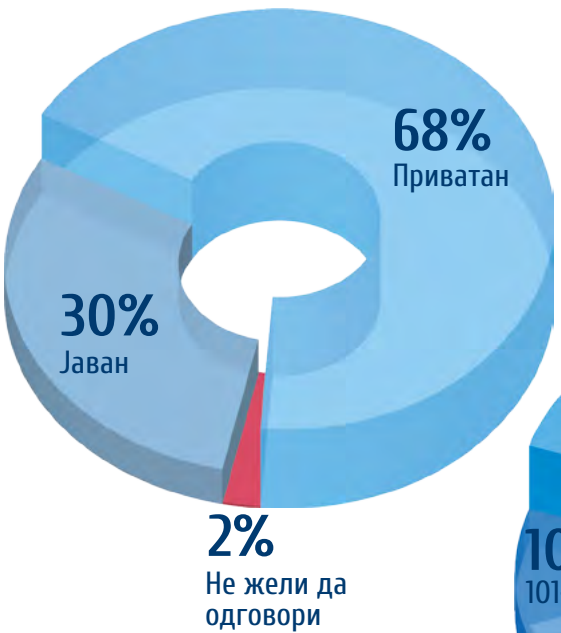


Величина места

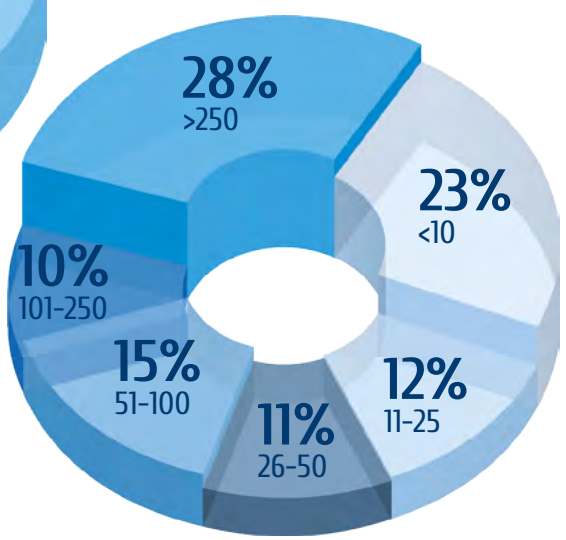
Узраст



Сектор запослења



Број запослених у фирми



Завршена средња школа (четворогодишња) 42

Завршен факултет/постдипломске студије 35

Завршена виша школа 12

Завршена средња школа (трогодишња) 6

Завршена основна школа 3

Не желим да одговорим 1

48 Ожењен/Удата

40 Самац

6 Разведен/а

1 Удовац/Удовица

6 Не желим да одговорим

Материјални статус домаћинства (самопроцена)

Национална сајбер култура у Србији

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 радимо ствари". 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 формално се преносе (у школи, на радном месту, у слободно време итд.) и неформално кроз интеракцију са пријатељима, родитељима, браћом и сестрама и другима. Као резултат тога, националне су културе 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 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.

Постоји неколико дефиниција сајбер културе, али још увек нема јединствене дефиниције, око које би се сложили сви стручњаци информационе безбедности. Међутим, постоји јединствени став о кључним препрекама за ову ситуацију: безбедност се односи на заштиту од претњи усмерених на одређене рањивости/слабости и у основи се односи на заштиту информационих добара. Сајбер култура обухвата понашање, претпоставке, уверења, вредности и знање које људи приликом употребе информационих средстава. Стога, сајбер култура се састоји од понашања и сета идеја и ставова.

До сада, већина студија о сајбер култури је усмерена на аспект понашања. Ово заправо значи да је фокус на проценту у ком запослени кликну на фишинг линк или да ли и зашто деле са другима своје лозинке. Последица овога је генерално мишљење да сајбер култура садржи елементе вредности и

ставова, а начин на који се обрађује тежи да ове елементе остави ван фокуса у корист понашања.

Начин на који се понашање посматра у контексту сајбер културе је да нам може указати на поступке људи, на оно што раде или што су радили. У сваком случају, врло мало може указати на оно шта ће урадити. Другим речима, фокус на понашању може створити слику безбедности из прошлости (ово је оно шта је рађено) али може врло мало указати на будуће понашање. Ипак, постоји тежња за развојем претпоставки понашања и у том смислу ради на благовремености мера заштите. Стога, уместо могућности да се сагледа шта су људи радили и како су се понашали, важније је кредибилно претпоставити шта ће људи у одређеној ситуацији највероватније урадити. Приступ сајбер култури примењен у овом истраживању не истиче понашање, већ се фокусира на ставове, вредности и мишљења која ће рећи нешто више о људима, шта би урадили или како би одговорили.

Овакав фокус нас је довео до неизбежног питања: Које кључне особине карактеришу ставове, вредности и мишљења у било којој сајбер култури? Који елементи чине основу сајбер културе?

У овом истраживању утврђене су кључне особине сајбер културе у Србији. Од становишта да се националној култури, овде сајбер култури, не може приступити само као понашању дошло се до становишта да је целисходније посматрати сајбер културу као сет вредности, мишљења и ставова о информационој безбедности. Информациона безбедност на националном нивоу се односи на широк спектар тема, почев од управљања и државне контроле над појединачним мишљењима о технолошким компетенцијама и преузимању ризика.

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 је појединачно понашање обликовано колективним нормама и понашањем.

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 у сајбер култури?

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 су истовремено и приморани 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.

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[6].

У студији *Kathryn Parsons, Agata Mc Cormac, 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".[7]

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.

6. Компетентност

Грађани су за скоро све услуге приморани 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.

6 Parsons, McCormac et al. (2010). *Human Factorsand Information Security:Individual, Culture andSecurity Environment*

7 Kreuter, M. W., &Strecher, V. (1995). *Changing inaccurateperceptions of health risk:Results from a randomisedtrial. Health Psychology*,14, 55–63

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.

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.

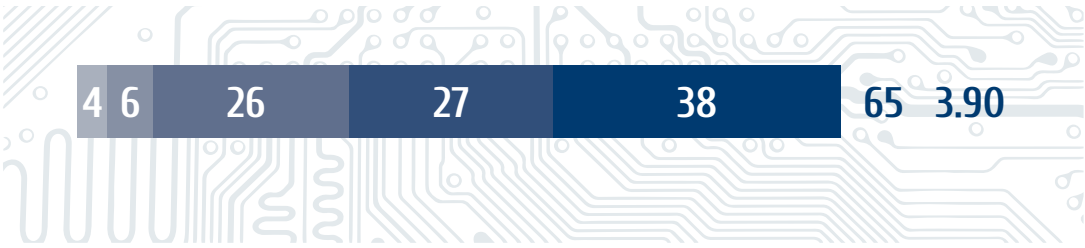
Дакле, мерење образаца понашања српске сајбер културе, подразумева две ствари: прво, желимо да створимо слику понашања грађана Србије у контексту информационе безбедности, и друго, желимо да видимо у којој мери се грађани придржавају „најбоље праксе".

Ови резултати говоре о томе како се грађани Србије позиционирају у односу на свет.

Колективизам - већина интернет популације Србије (66%) сматра да би требало да буде могуће остати анониман на интернету, док само 12% сматра да анонимност не би требало да буде могућа, а само 30% особа прихвата да њихове активности буду надгледане уколико би то допринело безбедности на интернету. Веза између личне активности и безбедности колектива се ретко увиђа, о чему говори чињеница да тек 10% сматра да интернет постаје безбеднији уколико је њихов рачунар/телефон безбедан.

„Требало би да буде могуће остати анониман на итнернету"

„Интернет неће бити безбеднији ако је мој рачунар/телефон безбедан"



Управљање и контрола - око 40% корисника интернета у Србији има негативан став о надгледању активности на интернету, односно није спремно да се одрекне своје анонимности зарад безбедности. Даље, мали број корисника сматра да му криминалистичке службе могу помоћи (31%) уколико би био жртва сајбер криминала, што је у складу са чињеницом да мање од 20% директно погођених то пријављује полицији.

„Прихватам да моје online активности буду надгледане ако ме то чини безбеднијим на интернету"

„Сајбер активисти имају значајну улогу у борби против сајбер криминала и сајбер ратова"

„Криминалистичке службе ће ми помоћи уколико будем жртва сајбер криминала"

„Сигуран сам да држава може да сачува безбедност мојих података"

Колико је ризична употреба е-Управе?

Колико је ризична употреба online банкарства?

Поверење - изразито мало, тек сваки четврти корисник интернета из Србије сматра да држава може да заштити безбедност његових података, што би могло да указује на ниско поверење у државне органе, посебно ако се узме у обзир претходно поменуто неослањање на криминалистичке службе.

Схватање ризика - сваки други корисник сматра да се излаже ризицима када је на интернету, а сваки пети се уздржава од коришћења онлајн услуга због претњи. На пример, особе које процењују коришћење мобилног и електронског банкарства ризичним ређе користе ове услуге (45% користи мобилно и 39% електронско банкарство) од оних који их не сматрају ризичним (64% односно 54%). Нешто више од половине (53%) интернет популације у Србији саопштава да је добро обавештено о онлајн претњама, док 15% сматра да то није случај.

Технолошки оптимизам и дигитализација - интернет популација Србије има доминантно позитиван став (78%) према употреби нових технологија.

„Излажем се ризицима када сам на интернету"

„Добро сам обавештен/а о online претњама"

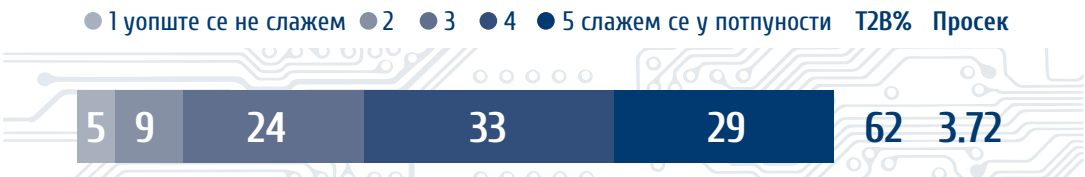
Интересовања - већина корисника (62%) је заинтересована за информационе технологије, што је у складу са позитивним ставом према употреби нових технологија. Интересовање за информациону безбедност је нешто мање, где се за њу интересује свака друга особа. Веза између интересовања и знања у домену информационих технологија је нешто већа него у домену информационе безбедности. Особе које се интересују за информациону безбедност се користе безбеднијим обрасцима понашања.

Технолошки оптимизам и дигитализација

„Ја сам за употребу нових технологија"

Интересовања

Колико вас занимају информационе технологије?



Колико вас занима информациона безбедност?

Компетентност – нешто више од половине корисника (58%) сматра да увек може да разликује безбедно од небезбедног на интернету. 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% признаје да то не зна.

Самопроцена знања из информационе технологије

Самопроцена знања из информационе безбедности

„Добро сам обавештен/а о online претњама"

„Знам шта је информациона безбедност"

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.

Нарушавање информационе безбедности

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 знања у односу на друге

Да ли разликујете шта је безбедно, а шта није безбедно радити online?

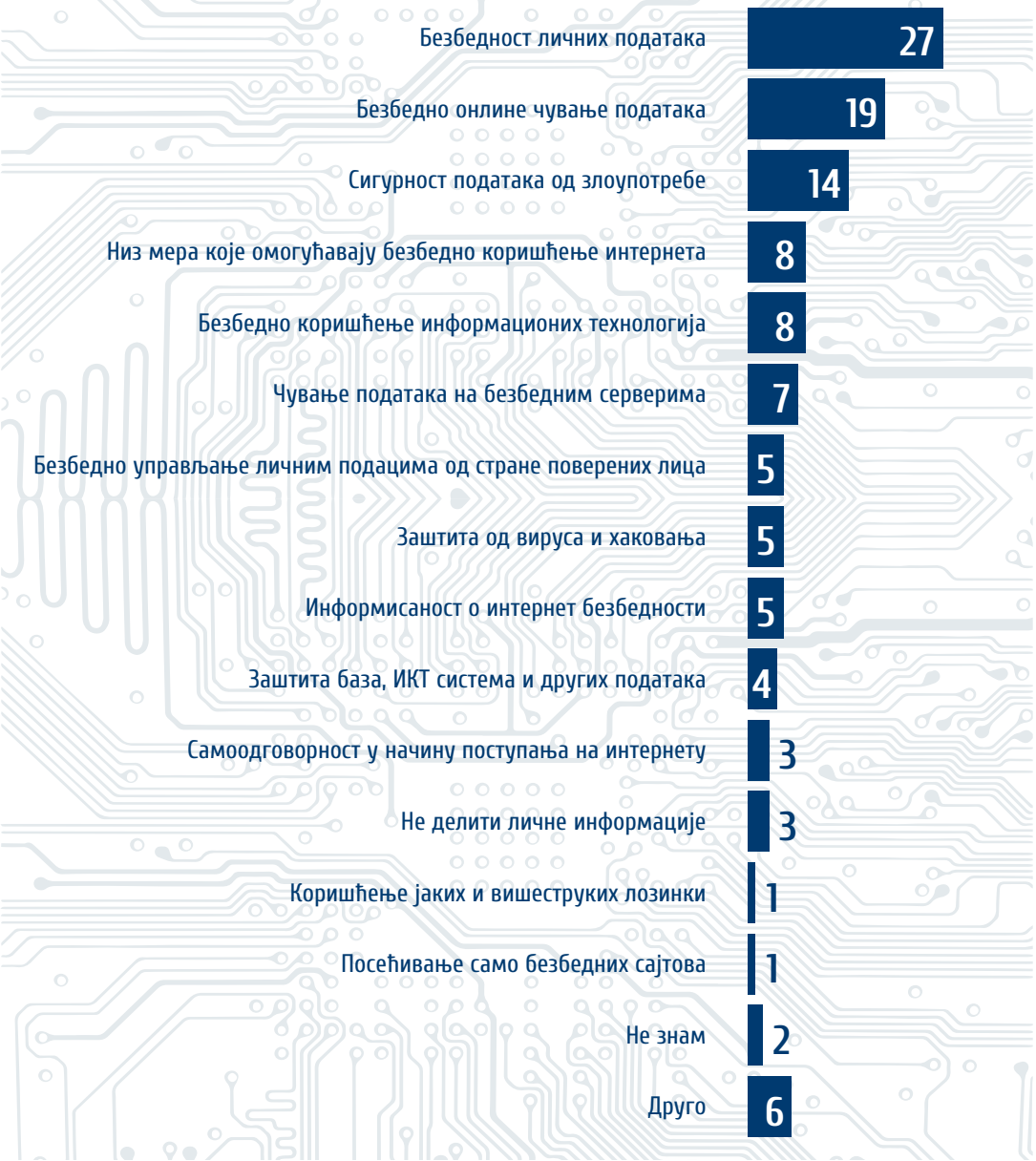
Српска интернет популација даје веће оцене процени свог интересовања него знања, како за информационе технологије тако и за безбедност, што може да индикује како потребу за едукативним програмима, тако и добру прогнозу њиховог успеха. У складу са тим је и жеља 60% циљне популације да учествује у некој врсти обуке о информационој безбедности. Већина (58%) сматра да зна о информационој безбедности исто колико и просечна особа, док 10% има утисак да заостаје за другима.

Чак 36% корисника у неким ситуацијама није сигурно шта је безбедно, а шта није безбедно на интернету, док 6% признаје да то никада не разликује.

Када дефинишу информациону безбедност својим речима, корисници најчешће дају одговоре који се тичу безбедности личних података и начина на који се они чувају онлајн.

Схватање информационе безбедности

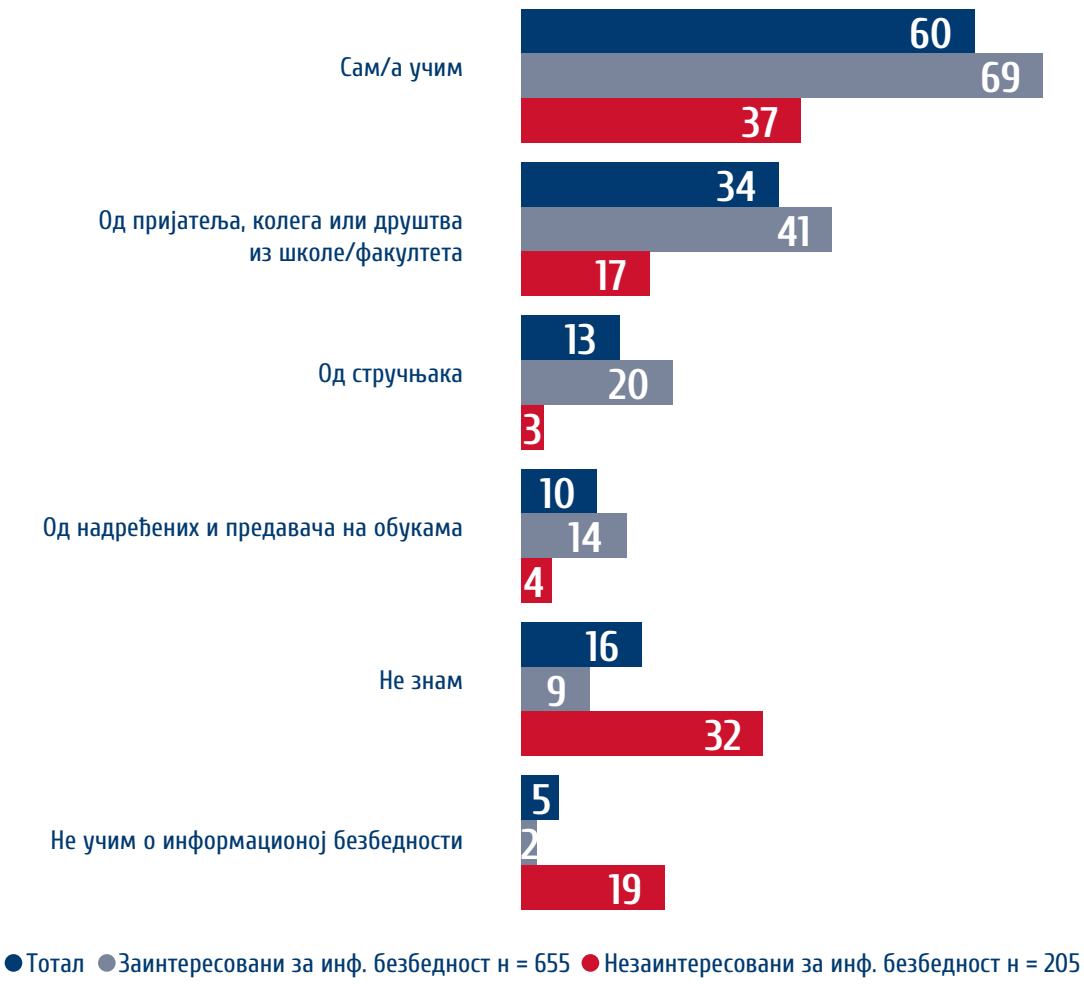
Шта је за вас информациона безбедност? Опишите овај појам у 2-3 реченице.



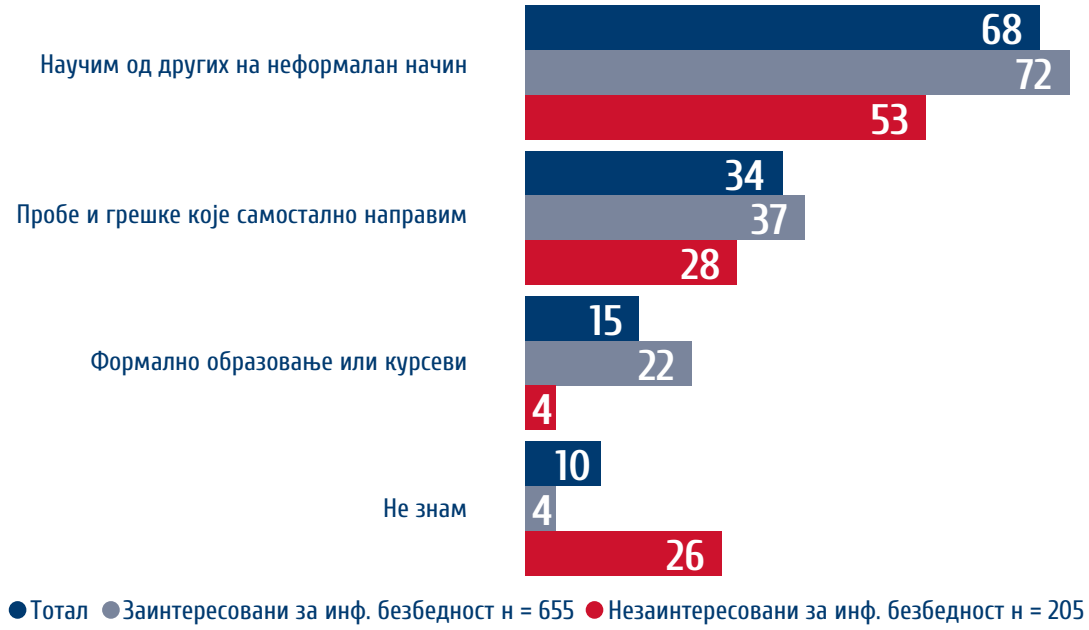
О информационој безбедности интернет корисници најчешће уче сами (60%), или од пријатеља, колега или друштва из школе/факултета (34%). Релативно мали проценат наводи да учи од стручњака (13%) или на обукама (10%). Сваки пети корисник наводи да не учи о информационој безбедности или да не зна од кога учи. Постоји битна разлика између заинтересованих и незаинтересованих за информациону безбедност – први су више склони да уче из било ког извора, док други далеко чешће не уче или не знају од кога уче.

Сличан образац се добија и када се посматра на који начин се нешто обично научи о информационој безбедности. Највећи број нешто научи од других, на неформалан начин (68%), упола мање то чини на основу сопствених проба/грешака, док најмање особа помиње формално образовање/курсеве. Чињеницу 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.

Од кога се учи



Како се обично научи



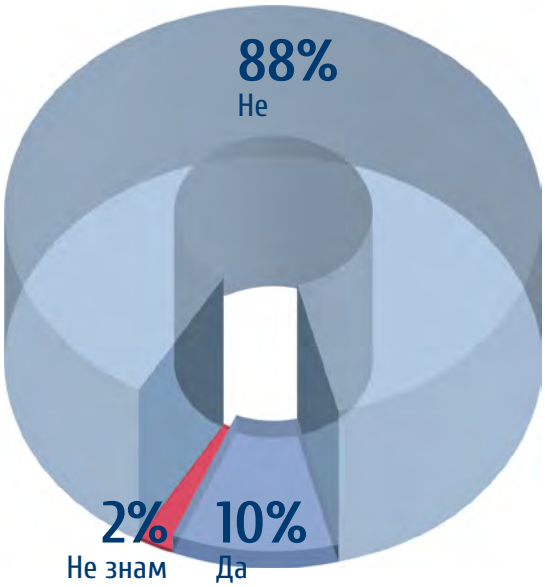
Сваки десети интернет корисник у Србији је похађао неку врсту обуке о информационој безбедности у претходне 2 године. Огромна већина ових корисника се окористила обуком, где 55% сматра да је допунила своје знање, а 38% да су њихове вештине значајно унапређене.

Запослене особе чешће су похађале обуку (11%) од незапослених (4%) без разлика у односу на то да ли раде у приватном или јавном сектору. Исто важи и за особе са примањима већим од просека (20%) у односу на оне са просечним (9%) или примањима мањим од просека (6%).

Већина српске интернет популације (57%) би желела да похађа неку обуку о информационој безбедности, док сваки четврти корисник изјављује да то не би желео.

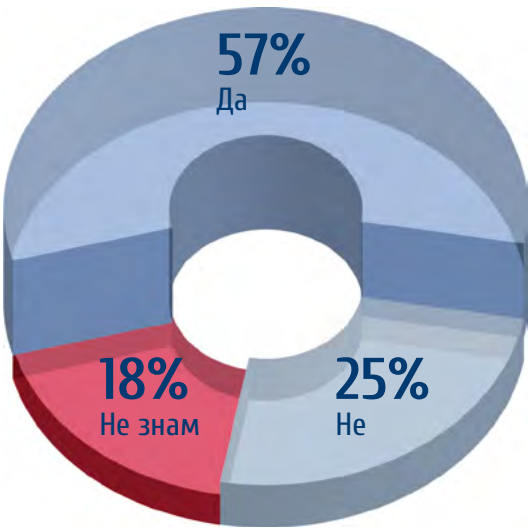
Млади (15-24) имају мању жељу за похађањем обуке од старијих узрасних група (42% има жељу, а 39% не). Запослени у јавном сектору су нешто заинтересованији за обуку (68%) у односу на запослене у приватном сектору (58%).

Похађање обуке



Сајбер вештине након обуке

Жеља за похађањем



Схватање ризика

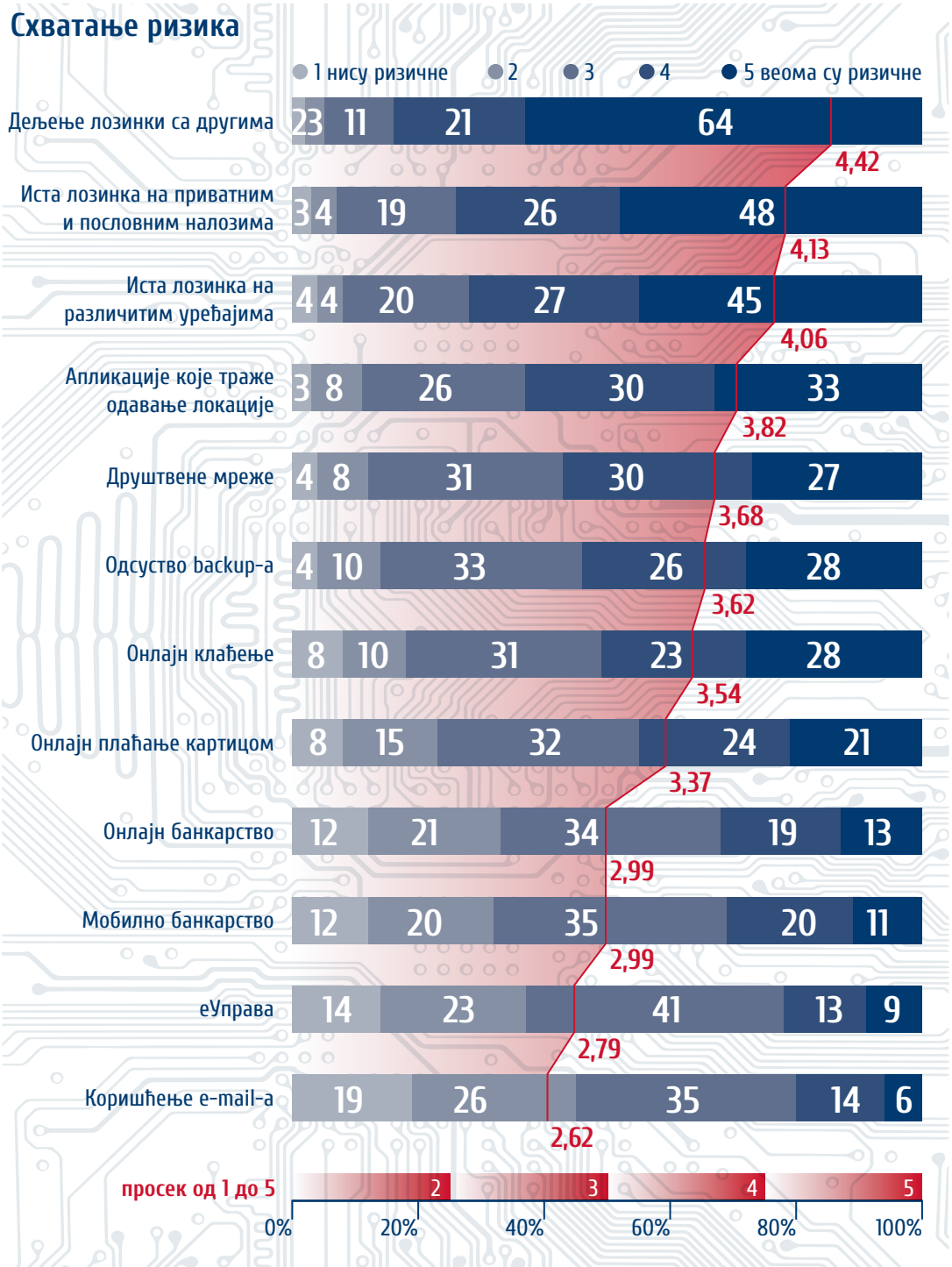
Схватање ризика заузима посебно место у нашем истраживању јер свако коришћење интернета подразумева и одређене дилеме о безбедности. Претње се могу манифестовати на много начина, а ми не успевамо да разумемо у потпуности сложени дигитални ланац догађаја који нас могу учинити рањивим. Да ли треба да отворимо 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.

Најризичнијим активностима процењују се оне које су везане за лоше руковање лозинкама као што су дељење лозинки са другима, поседовање исте лозинке на приватним и пословним налозима и на различитим уређајима.

Чак и у случају употребе имејла (који је процењен као најмање ризичан) свака пета особа сматра да је она повезана са значајним степеном ризика.



Особе које не разликују шта је безбедно радити онлајн, активности попут онлајн плаћања картицом, електронског и мобилног банкарства, коришћења еУправе и имејла сматрају знатно ризичнијим. Такође, склоне су да потцене ризик од одсуства резервних копија података (backup-а) у односу на остале две групе.

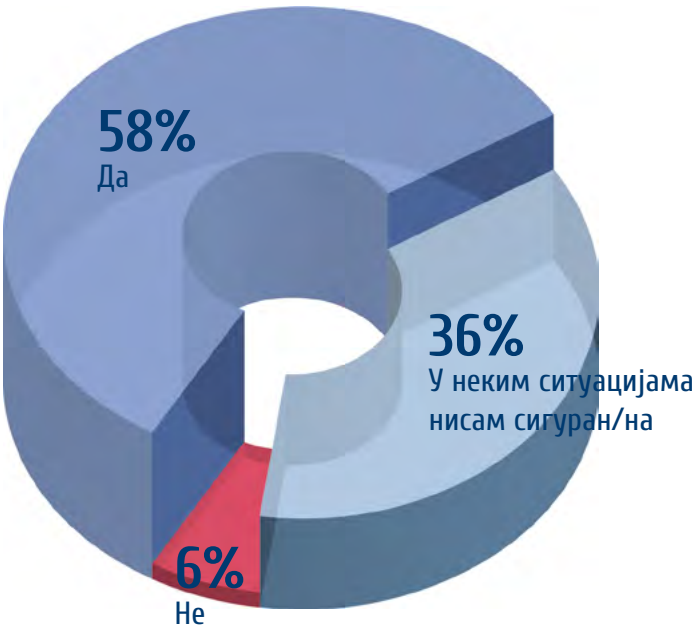
Особе које сматрају да разликују безбедно од небезбедног поступања процењују ризик на исти начин као и особе које у неким ситуацијама нису

сигурне, осим у случају електронског банкарства, плаћања картицом и употребе апликација које траже одавање локације, где несигурни ове активности сматрају за нијансу више ризичним.

Узрасне разлике у процени ризика су мале. Особе узраста 35-44 процењују дељење и коришћење исте лозинке на приватним и пословним налозима и на различитим уређајима као нешто ризичније од осталих узраста. Старији од 34 године виде одсуство резервних копија и интернет клађење као ризичније од млађих.

Корисници интернета у Србији који су прошли неку врсту обуке из информационе безбедности процењују дељење лозинке са другима, поседовање исте лозинке на приватним и пословним налозима и одсуство резервних копија као ризичније активности. Супротно томе, коришћење електронске поште, еУправе, мобилног и електронског банкарства виде као мање ризичне.

Да ли разликујете шта је безбедно, а шта није безбедно радити online

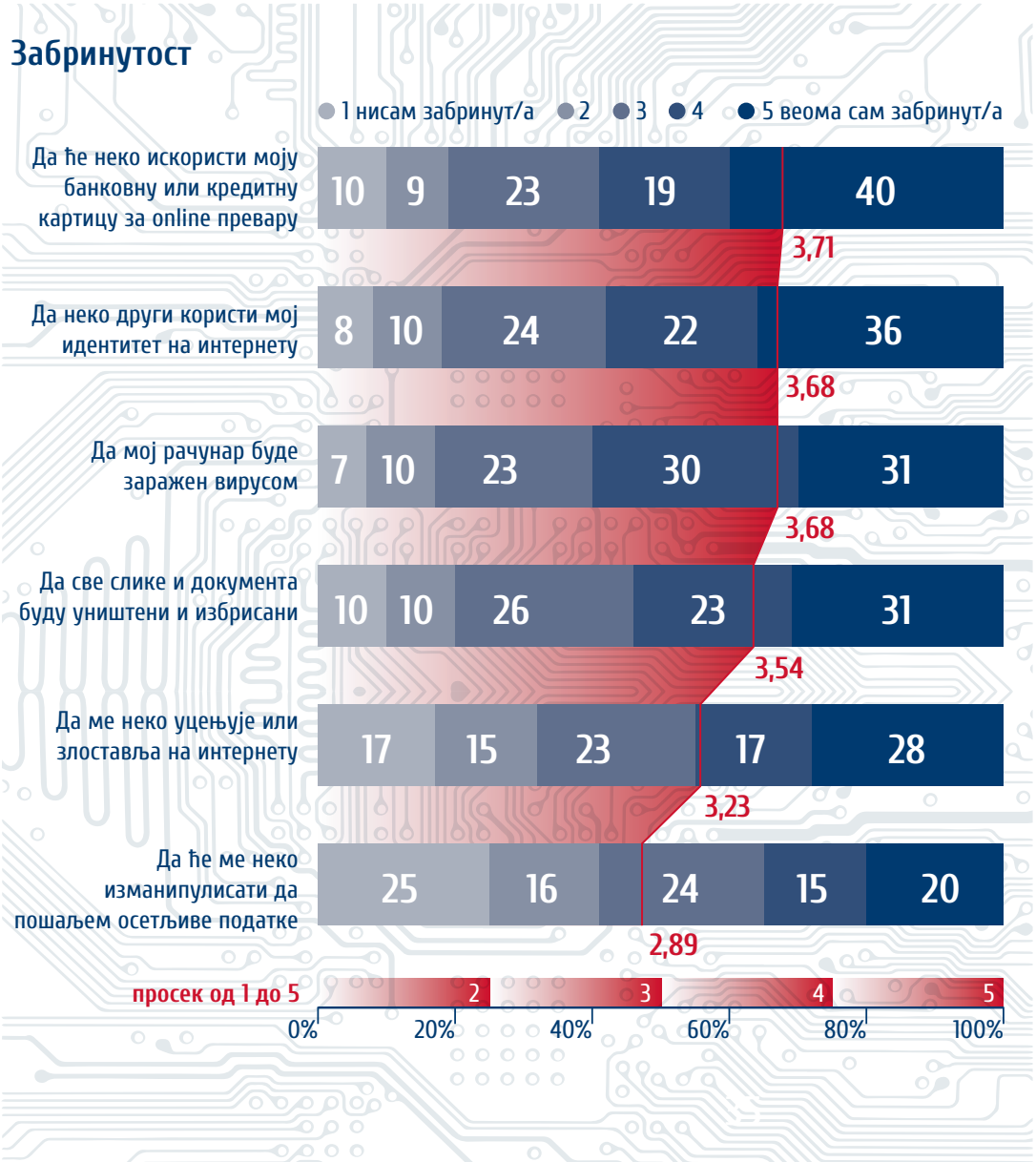


Висок проценат (око 60%) интернет популације у Србији је значајно забринут да ће неко други користити њихов идентитет на интернету, искористити њихову банковну картицу у онлајн превари, или да ће им рачунар бити заражен вирусом.

Већина је битно забринута и око тога да ће им сва документа и слике у рачунару бити обрисани (54%), а нешто мање њих стрепи од уцењивања/злостављања (45%) на интернету, или да ће бити изманипулисани да пошаљу осетљиве податке (35%).

Особе које у неким ситуацијама нису сигурне да могу да процене шта је безбедно су више забринуте за све претње осим уцењивања/злостављања и коришћења банковне картице за превару у односу на особе које сматрају да увек могу да процене безбедност.

Корисници који не могу да процене шта је безбедно су статистички значајно више забринути само по питању тога да им се може десити да их неко изманипулише да пошаљу осетљиве податке.



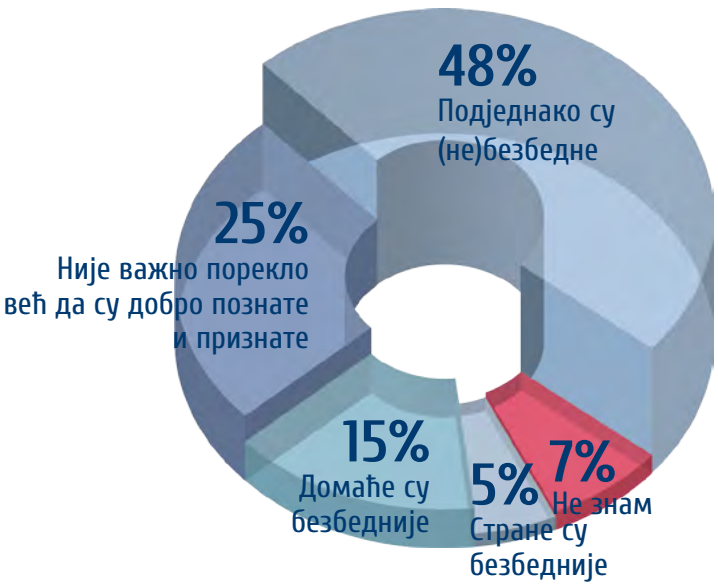
Доминантна већина (87%) српске онлајн популације фокус претње смешта у спољашњост, односно, сматрају да је већа претња од тога да ће их неко угрозити (нпр. хакерски напад), него да ће својим поступцима угрозити сопствену безбедност.

Отприлике сваки пети корисник интернета у Србији се уздржава од коришћења онлајн услуга због претњи. Већина (73%) не прави разлику између домаћих и страних онлајн продавница, док 15% домаће продавнице сматра безбеднијим.

Локус претње (шта је већа претња)

Уздржавање од online услуга због претњи

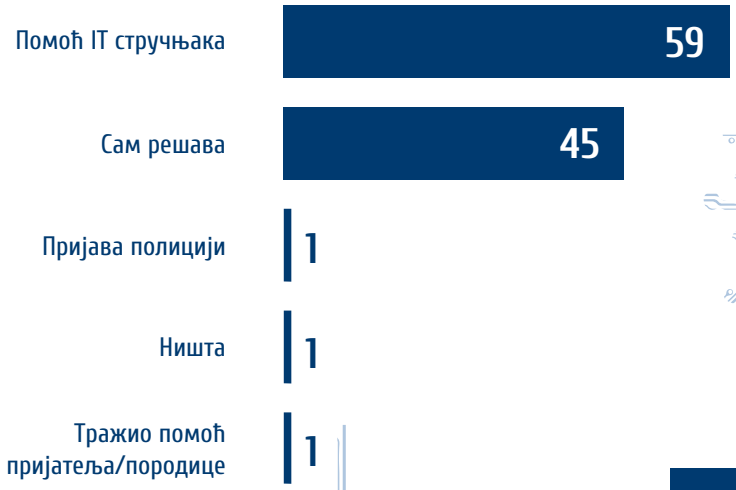
Домаће и стране online продавнице



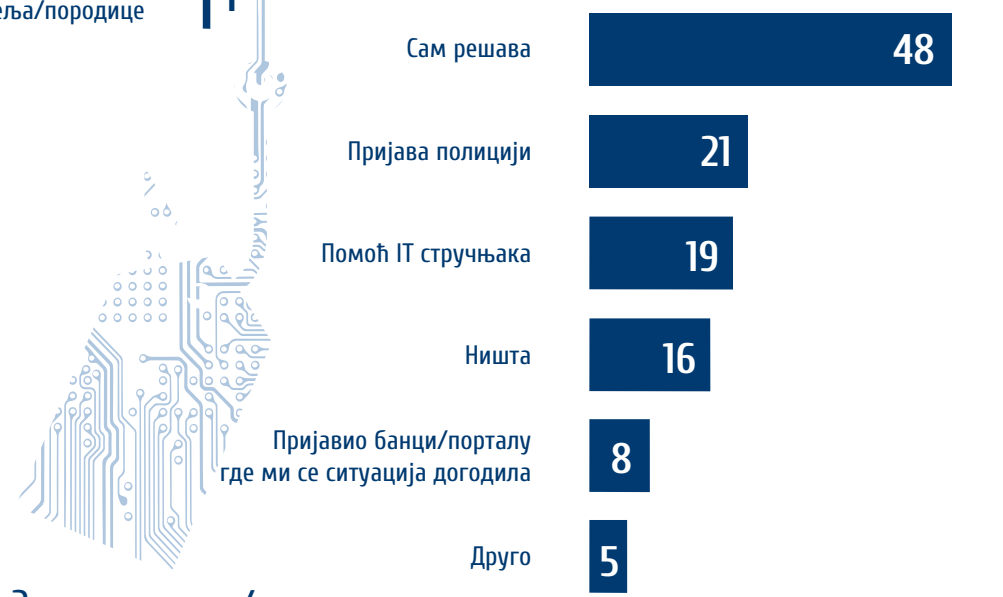
Више од половине интернет популације је имало искуство са вирусом на рачунару. Остале врсте нарушавања информационе безбедности су ређе, 9% је било жртва онлајн преваре, а нешто мање је злостављано, било уцењено или им је украден онлајн идентитет.

Упадљиво је да у свакој од ситуација нарушавања безбедности особа најчешће сама решава свој проблем, осим у случају зараженост компјутера вирусом, када ће пре потражити помоћ IT стручњака.

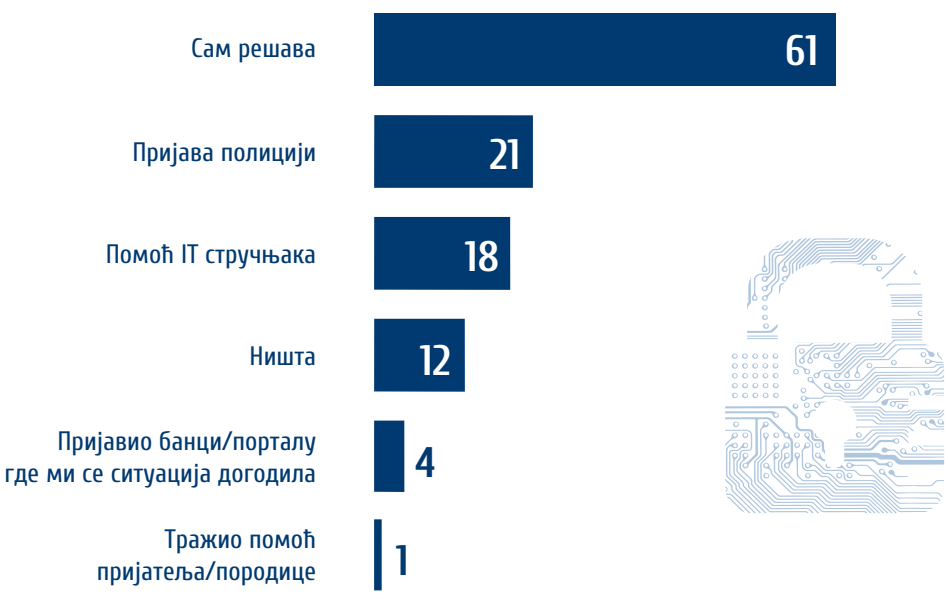
Вирус



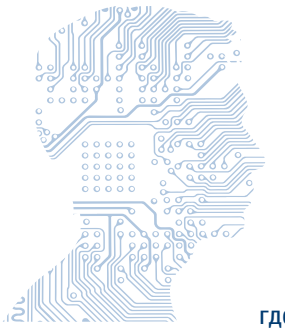
Online превара



Злостављање/уцењивање



Украден online идентитет

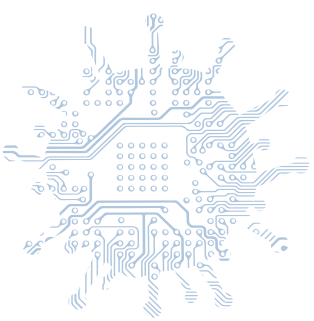


Приликом озбиљнијих нарушавања безбедности, као што су крађа идентитета, уцењивање/злостављање и онлајн преваре, тек око 1/5 корисника се одлучује да их пријави полицији.

Када размишљају о нарушавању безбедности хипотетички, већи број људи би се обратио за помоћ IT стручњацима, него што то заправо чине у реалним ситуацијама, односно, не очекују да ће се у конкретној ситуацији ослањати на себе.

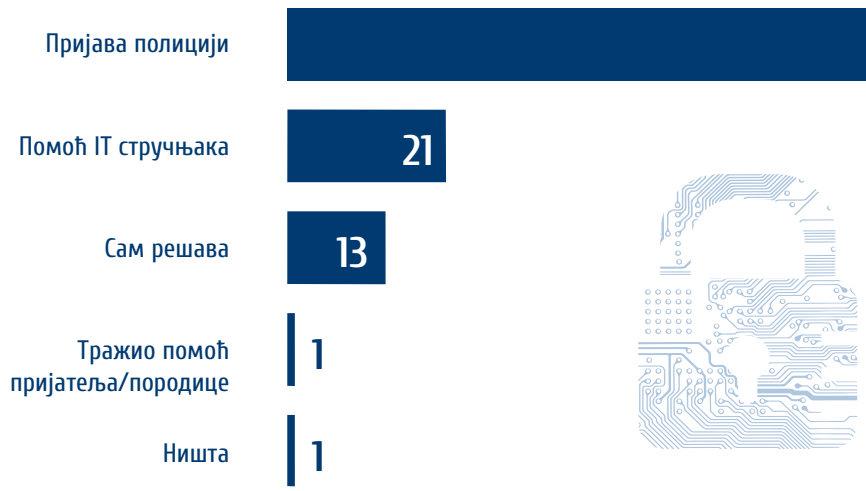
Посебно је упечатљива дискрепанца у броју особа које кажу да би пријавиле нарушавање безбедности полицији у хипотетичкој ситуацији у односу на реалну (у случају озбиљнијих нарушавања безбедности). Ово би могло да сугерише постојање баријера да се нарушавање безбедности пријави полицији.

Вирус



Online превара

Злостављање/уцењивање



Украден online идентитет

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 користите ISO/IEC 27001/27002, Закон о информационој безбедности или било који интерни оквир или политику 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 сигурне и 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 сигурне и безбедне навике?

Већина корисника интернета у Србији поседује антивирус програм на свом рачунару (81%). Иако највећи број оперативних система има интегрисан Firewall, само 31% корисника га користи што може да сугерише било да га држе искљученим било да нису свесни његовог присуства. Релативно мали број не користи ниједан безбедносни софтвер (5%), али се и категорија особа која не зна да ли има безбедносни софтвер (7%) може сматрати ризичном.

Ажурирање софтвера је најчешће аутоматизовано (60%), док око 1/4 корисника то чини ручно. Укупно 17% не ажурира/нема навике ажурирања/не зна да ли ажурира софтвер.

Чак један од пет корисника никада не прави резервне копије важних података. Ако се овде уброје и особе које не знају колико често праве резервне копије, долази се до тога да резервне копије не прави сваки трећи корисник. Мали број не би водио рачуна/не би знао шта да ради приликом продаје/бацања старог рачунара (8%).

Док огромна већина зна како да обрише посећену интернет страницу из историје, блокира непожељне поруке и мења опције о личним информацијама на друштвеним мрежама, мањи број (69%) зна како да пронађе информације о сигурности неке странице.

Учесталост backup-овања важних података

Понашање при продаји/бацању старог рачунара

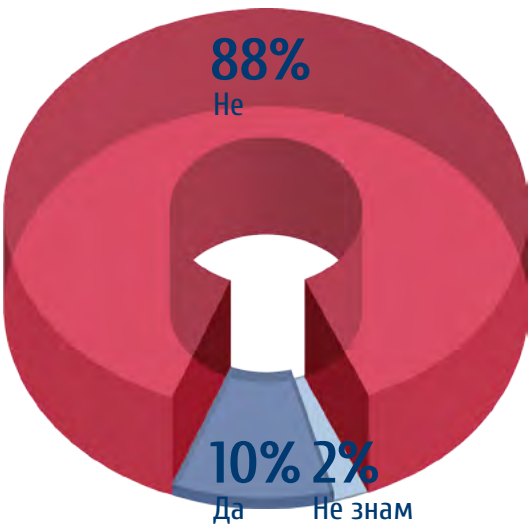
Вештине

Уопштено гледано, особе које су прошле кроз неку врсту обуке испољавају сигурније обрасце понашања. Резултате треба тумачити са опрезом јер циљ истраживања, па самим тим ни нацрт, није прилагођен испитивању ефеката обуке (нема претеста компетенција пре обуке, већ се само детектују разлике између група).

Приказани су само они обрасци понашања код којих постоји статистички значајна разлика између особа које су прошле кроз обуку о информационој безбедности у претходне 2 године и оних који нису.

Похађање обуке

Да ли сте похађали неку обуку о информационој безбедности у претходне 2 године?

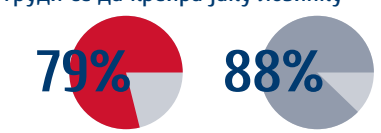


Користи антивирус програм

Користи firewall

Password manager

Труди се да креира јаку лозинку



Прави backup сваке недеље или чешће

Зна да нађе информације о сигурности странице

Никад не прави backup

Зна да блокира непожељне поруке на друштвеним мрежама

Закључци и препоруке за стратешко планирање

Истраживање сајбер културе пружило је свеобухватан приступ схватању информационе безбедности у Србији. Испитивање понашања, вредности, мишљења и ставова корисника интернета упућује на важне изазове и даје могућност сагледавања области информационе безбедности из угла грађана, који представља важан критеријум за обликовање схватања и позиционирање у односу на остале државе.

Готово цела онлајн популација у Србији користи паметни телефон-smartphone (94%), а посебно охрабрује доминантно позитиван став према употреби нових технологија (78%), као показатеља технолошког оптимизма и дигитализације. Већина корисника (62%) је заинтересована за информационе технологије, док је интересовање за информациону безбедност нешто мање (52%).

Приликом оцене знања, више од половине корисника (58%) сматра да може да разликује шта је безбедно од небезбедног на интернету. Међутим, своје знање из области информационе безбедности процењују као лошије у односу на знање из информационих технологија, па 58% корисника сматра да зна шта је информациона безбедност, док 13% корисника сматра да то не зна. Упркос томе, чак 31% корисника не зна да провери безбедност интернет странице, те се на ову вештину треба фокусирати у будућим едукацијама. Дакле, српска онлајн популација процењује своје интересовање о информационим технологијама и безбедности јачим него своје знање, што представља добру основу за развој едукативних програма.

Иако нацрт овог истраживања не допушта дефинитивне закључке о ефикасности едукативних програма о информационој безбедности, чињеница је да се код оних који су прошли кроз неку врсту обуке детектују битно бољи обрасци понашања везаних за безбедност на интернету. Приметно је да постоји и велика жеља за похађањем обука ове врсте коју је изразило чак 57% корисника, што је у озбиљном нескладу са 10% корисника који су похађали обуку у протеклих 2 године. Ексклузивност обука се огледа и у чињеници да је већа вероватноћа да ће прилику за похађање обуке имати запослени него незапослени, као и они са примањима изнад просека. С обзиром да је учење неформалним путем (породица, пријатељи) врло битан начин ширења информација о информационој безбедности, а да су формалне обуке релативно ретке, потребно је спречити потенцијално ширење лажних информација. Један од начина је успостављање поуздане базе знања, тј. обучених појединаца из различитих друштвених категорија, који ће своје компетенције настављати да шире неформалним путем. Потенцијално решење је имплементација обука у образовни систем.

Утврђена је повезаност између интересовања о информационој безбедности, (начина) учења, конкретних знања и безбедних облика понашања. Директна импликација је да информативни материјал, односно садржај обука треба да буде изражен на занимљив начин, који побуђује интересовање, а не дат у хладним техничким терминима и страним изразима.

- 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.

Резултати истраживања показују да је присутна битна дискрепанца између начина на који корисници интернета у Србији сматрају да би реаговали у ситуацијама нарушавања информационе безбедности и начина на који стварно реагују у таквим ситуацијама. Корисници интернета у хипотетичким ситуацијама као што су крађа идентитета, уцењивање/злостављање и онлајн преваре решење најпре виде у подношењу пријаве полицији 31%, док се у реалним ситуацијама то релативно ретко чини, мање од 20% случајева.

Сваки четврти корисник (25%) сматра да држава може да заштити безбедност његових података што може указивати на недовољно поверење у институције, на шта указује и низак проценат корисника који траже заштиту криминалистичких служби.

- Решење може бити информисање о начину на који надлежне институције могу да помогну, о примерима решених случајева, веће пропраћености делатности служби за вискотехнолошки криминал у медијима и наглашавање значаја пријаве кривичног дела како неко други не би страдао на исти начин. На овај начин би се утицало на ширење свести да свако може бити жртва сајбер криминала и охрабрило заједничко деловање грађана и државе у борби против сајбер криминала и превенцији од сајбер напада. Са тим у вези је и неувиђање сопствене одговорности за безбедност колектива, односно дачинећи безбедним себе, сопствени рачунар, паметни телефон чинимо безбедним и друге.

Схаватање ризика процењено је испитивањем различитих фактора, а као најризичнија активност процењује се лоше управљање лозинкама. Чак 64% корисника сматра да дељење лозинке са другима није ризично, а само 2% да је веома ризично. Такође, 48% корисника сматра да коришћење исте лозинке на приватним и пословним налозима није ризично, а 45% да коришћење исте лозинке на различитим уређајима није ризично.

Процена ризика еУправе је релативно ниска у односу на остале онлајн активности, али и даље постоји известан број особа које је сматрају високо ризичном (21%), или умерено ризичном (41%), што би их могло обесхрабрити да користе ове услуге. Утврђено је да особе које су прошле кроз неку врсту обуке о информационој безбедности процењују употребу е-Управе, али и употребе електронске поште и банкарства, као мање ризичне, чему вероватно доприносе како реалистичнија перцепција претње тако и доживљај компетентности да се са различитим претњама избори.

Чак 87% корисника истиче да је већа претња да ће неко други угрозити њихову безбедност, док само 13% сматра да ће нешто што сами чине угрозити њихову онлајн безбедност, што указује да корисници немају довољно сазнања о безбедносним ризицима и да нису свесни својих поступака.

Један од 5 корисника (22%) не креира резервне копије података, али ако њима додамо 11% корисника који не знају да ли праве резервне копије података долазимо до податка да сваки трећи корисник не креира резервне копије података (33%).

Већина корисника (81%) користи анти-вирус, док 31% користи Firewall, из чега се може проценити да вероватно велики број није свестан да је Firewall углавном интегрисан у оперативни систем. Задовољавајући је податак да 5% корисника не користи ни један безбедносни софтвер, али ако овом податку придружимо и кориснике који су одговорили са не знам добијамо податак да 12% корисника не користи безбедносни софтвер.

- Креирање и спровођење едукативних програма који би се фокусирали на јачање вештина креирања копија резервних података, коришћења анти-вирусних софтвера, начина креирања јаких лозинки и коришћење апликација за управљање лозинкама може значајно утицати на унапређење знања и понашања корисника.

Имајући у виду да чак 18% стално запослених не зна да ли крши интерна правила информационе безбедности свог послодавца, иако знају да правила постоје, поставља се питање о томе да ли су правила формулисана на разумљив начин? Даље, 13% њих свесно крши ова правила. Овим истраживањем није испитивана природа кршења ових правила – могуће је и да су она за запослене на неки начин спутавајућа, што би поново довело у питање сам садржај ових правила.

- 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.

Полазећи од резултата 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 Roislien, 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 Solmsand J. van Vuuren, Proceedings of the Ninth International Symposiumon Human Aspects of Information Security & Assurance (HAISA 2015)

www.cert.rs