САЈБЕР АЗБУКА

А

Азбука основних сајбер препорука које могу помоћи да будемо сајбер свесни

Б

Бесплатан Wi-Fi је препоручен само за сурфовање нетом

В

Ваша лозинка је само ваша, баш као и ваша четкица за зубе

Г

Губитак података је на само један погрешан клик од нас

Д

Добра пракса је имати различите лозинке за сваки интернет налог

Ђ

Ђаци исто могу бити мете сајбер напада

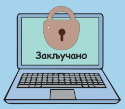
Е

Електронска трговина је безбедна ако се упознамо са могућим изазовима

Ж

Живот на мрежи такође може бити пун изазова

З



Закључавајте своје уређаје, кад год их не користите

И

Интернет је веома користан, само га треба пажљиво употребљавати

Ј

Једном објављен садржај на интернету остаје заувек на интернету

К

Креирање резервних копија је једна од основних превентивних мера

Л

Лозинка увек треба да буде комплексна

Љ

Људи су најслабија карика у ланцу сајбер одбране

М

Мултифакторска аутентификација је важна додатна мера заштите

Н

Национални ЦЕРТ је увек доступан свим корисницима

Њ

Њушкала постоје свуда, па и на интернету

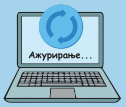
О

Онлајн трансакције само преко заштићене Wi-Fi конекције

П

Пријавите инцидент Националном ЦЕРТ-у

Р



Редовно ажурирање уређаја чини уређај отпорнијим на нападе

С

Сигурност је важна и на интернету

Т

Текстуалне поруке могу бити почетна тачка сајбер напада

Ћ

Ћаскање је безбедније када познајемо своје саговорнике

У

Уколико и на интернету нешто звучи сувише добро да би било истинито, вероватно није

Ф

Фишинг је најзаступљенији тип сајбер напада

Х

Хакерски напад се може догодити у било ком тренутку и било ком кориснику

Ц

Цена непажње корисника на интернету некада може бити веома висока

Ч

Чувајмо своју и поштујмо туђу приватност на интернету

Џ

Џак новца испод интернет дуге чувају једнорози

Ш

Што више препорука усвојимо, бићемо безбеднији на интернету

#BudimoSajberSvesni

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

А

Азбука основних сајбер препорука које вам могу помоћи да будете безбеднији док уживате или радите на интернету.

Национални ЦЕРТ Републике Србије представља кратке препоруке којима жели да приближи основне превентивне мере за заштиту од сајбер напада и на тај начин помогне свим корисницима да буду безбеднији док раде, уче или се забављају на интернету.

СРБ-ЦЕРТ

Б

Бесплатан бежични приступ интернету је препоручен само за сурфовање нетом

Бесплатан бежични приступ интернету (**Wi-Fi**) је често доступан корисницима на јавним местима попут кафеа, ресторана, хотела, аеродрома, возилима градског саобраћаја и сл. Како би били заштићени, препорука Националног ЦЕРТ-а је да корисници не приступају својим налозима, односно не уносе своје корисничко име и лозинку када бесплатно приступају интернету на јавним местима, нарочито не налозима за коришћење банкарских онлајн апликација, јер се креденцијали лако могу преузети. Овакав приступ интернету је пре свега намењен за сурфовање.

СРБ-ЦЕРТ

В

Ваша лозинка је само ваша, баш као и ваша четкица за зубе

Да ли је безбедно и хигијенски делити своју четкицу за зубе? Исти принцип би требало применити и за лозинке које корисници креирају за приступ налозима на интернету, јер лозинка представља основни вид заштите од злоупотребе налога. И када постоји велико поверење између корисника, злоупотребе се ипак догађају због чега је препорука Националног ЦЕРТ-а да лозинке ипак не треба делити са другим корисницима. Баш као и четкицу за зубе и лозинку треба периодично мењати.

СРБ-ЦЕРТ

Губитак података на рачунарима је на само један погрешан клик од корисника

Број сајбер напада се повећава из дана у дан. Напади на кориснике најчешће започињу слањем мејла који садржи инструкције да је неопходно кликнути на линк или отворити прилог који је у имејл поруци. Довољан је тај један погрешан клик да корисник остане без података или датотека попут фотографија, видео записа, научних радова, пословних података и сл. Важно је проверити ко је пошиљаоц имејл поруке и да ли је садржај поруке одговарајући. Уколико ипак постоји сумња у легитимитет поруке, препорука је контактирати пошиљаоца директно и проверити, како би спречили губитак важних података.

СРБ-ЦЕРТ

Добра пракса је имати различите лозинке за сваки интернет налог

Д

У намери да омогуће одговарајући степен безбедности, произвођачи брава креирају посебан кључ за свака улазна врата. У супротном, свако би могао да искористи јединствени кључ и уђе у наш посед. Сличан принцип је и на интернету. Уколико корисник има само једну лозинку и користи је за приступ свим својим налозима попут имејла, Инстаграма, Фејсбука, апликација за интернет или мобилно банкарство и сл., хакерима је посао изузетно олакшан. Управо из тог разлога препорука је креирати засебну лозинку за сваки интернет налог. За чување лозинки постоје апликације попут **Password Manager-a**. За приступ овој апликацији довољно је креирати једну комплексну лозинку.

СРБ-ЦЕРТ

Ђ

Ђаци исто могу бити мете сајбер напада

На интернету не постоји заштићена група корисника, постоји само разлика у типу сајбер напада. Када је реч о ђацима, најчешћи напади су усмерени на хаковање њихових налога на друштвенима мрежама, али то могу бити и напади попут вршњачког насиља где је основни циљ нападача да понизи, увреди или компромитује корисника. Препорука је да родитељи помогну најмађим корисницима док не савладају основне кораке заштите и на интернету.

Електронска трговина је безбедна ако се упознамо са могућим изазовима

Доба је дигитализације и велики број услуга прелази на интернет, па тако и услуге продаје. Пандемија вируса COVID 19 је само убрзала овај процес и самим тим омогућила корисницима да купују производе без одласка у продавницу. Већи број купаца на интернету је привукао и хакере који на различите начине злоупотребљавају поверење купаца које су стекле легитимне продавнице. Како би спречили могуће злоупотребе, корисници би требало да се увере да су на жељеној интернет страници тако што ће проверити назив и домен жељене продавнице у адресној линији интернет прегледача. Такође, треба проверити да ли продавница заиста нуди могућност онлајн плаћања или своје производе шаље корисницима искучиво поузећем.

СРБ-ЦЕРТ

Живот на мрежи такође може бити пун изазова

Различите врсте превара су могуће и редовно се дешавају у физичком свету. Исти је принцип и у свету интернета и зато би корисници требало да имају исти степен опреза као што је то случај у свакодневном животу, посебно имајући у виду да у интернет простору сваки корисник може постати жртва без визуелног или физичког контакта са нападачем, односно хакером.

СРБ-ЦЕРТ

Закључавајте своје уређаје, кад год их не користите

3

У намери да корисницима проближи свеопшти значај вишег степена заштите од злоупотреба на интернету, Национални ЦЕРТ саветује да се уређаји закључавају када се не користе. На тај начин се онемогућава приступ уређајима од стране других корисника који могу бити у улози нападача. Некада је довољно сасвим мало времена да се уређај компромитује и зато је важно да буде закључан кад год није у употреби, чак и када правите кратку паузу.

СРБ-ЦЕРТ

И

Интернет је веома користан, само га треба пажљиво употребљавати.

Бржи цивилизацијски развој је омогућен управо захваљујући развоју модерне технологије. Развој интернета омогућава корисницима инстант комуникацију, банкарске услуге, онлајн трговину, размену података, али и заказивање здравствених прегледа, упис детета у предшколску или школску установу, подношење захтева за израду личних докумената, избор туристичких дестинација, одржавање онлајн пословних састанака и сл.. Имајући у виду различите бенефите које интернет нуди, његово коришћење би требало посматрати управо из тог угла. Уколико се пажљиво употребљава, интернет може учинити живот знатно квалитетнијим, јер пружа могућност да се време организује у складу са приоритетима и потребама корисника.

СРБ-ЦЕРТ

Једном објављен садржај на интернету остаје заувек на интернету

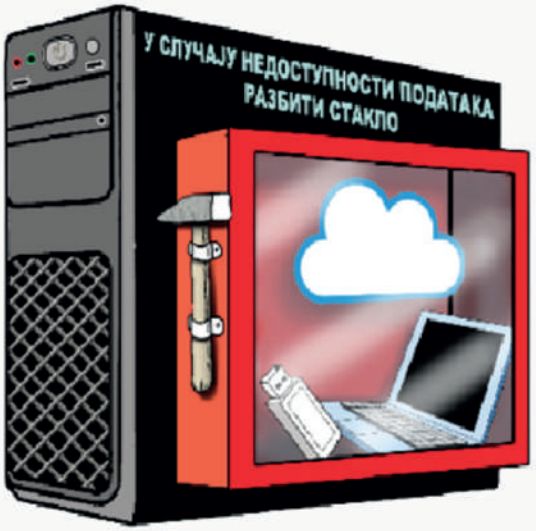
Ј

Могуће је да постоји мали број корисника који би отишао у теретану у свечаном оделу или скијашким чизмама. Неадекватна опрема може бити узрок повреда али и подсмеха, јер излази из оквира важећих културолошких или друштвених норми. Како би избегли могуће непријатности, Национални ЦЕРТ препоручује корисницима да примењују бонтон и на интернету и сходно томе направе одговарајућу селекцију садржаја пре његове објаве. Управо ће прави избор садржаја позитивно утицати на репутацију корисника, како на интернету тако и у физичком свету.

СРБ-ЦЕРТ

Креирање резервних копија је једна од основних превентивних мера

Креирање резервних копија свих важних датотека, познатији као Бекап (енг. *BackUp*), је процес који нам омогућава да се одбранимо од изнуђивачких хакерских напада под називом Рансомвер (енг. *Ransomware*). Овакав хакерски напад подразумева упад у уређај корисника и закључавање, односно енкриптовање, свих или најважнијих фајлова и датотека на уређају. Како би корисници били заштићенији од оваквих хакерских изнуда, креирање резервних копија је једна од основних превентивних мера коју могу применити да би се заштитили.



СРБ-ЦЕРТ

Л

Лозинка је основни вид заштите на интернету и зато би требало да буде комплексна

Како у физичком свету, тако и на интернету, постоје различити нивои заштите. Лозинка представља један од основних нивоа заштите интернет налога и као прва препрека би требало да буде што комплекснија како је хакери не би могли открити и злоупотребити на различите начине. Препорука Националног ЦЕРТ-а је да лозинка садржи најмање 9 карактера (алфанумеричких и специјалних карактера попут !?+$#“-:/ и сл). Уколико корисник креира једноставну лозинку, хакер може лако да је открије и преузме интернет налог или приступи банкарској апликацији корисника.

СРБ-ЦЕРТ

Љ

Људи постају жртве сајбер напада јер могу бити најслабија карика у ланцу одбране

Имајући у виду значај превентивног деловања у сајбер простору, компаније за развој софтверских и хардверских решења континуирано раде на унапређењу техничких аспеката одбране у жељи да заштите систем или уређај корисника од хакерских напада. Људи нису машине и грешка се може догодити сваком кориснику и зато је важно бити обазрив приликом коришћења интернета, јер хакери верују да је лакше преварити корисника него техничку заштиту система или уређаја.

СРБ-ЦЕРТ

Мултифакторска аутентификација додатно штити од злоупотребе налога и интернет банкарства

Мултифакторска аутентификација представља додатни вид заштите корисничких налога на интернету. Поступак подразумева коришћење најмање две, од могуће три методе аутентификације корисника. Приликом коришења мултифакторске аутентификације, корисник прво унесе своју лозинку, након тога користи други ниво заштите тако што нпр. унесе добијени СМС код, а као трећи ниво заштите може користити свој отисак прста.

СРБ-ЦЕРТ

Национални ЦЕРТ је увек доступан свим корисницима

Национални ЦЕРТ Републике Србије послује у оквиру Регулаторне агенције за електронске комуникације и поштанске услуге – РАТЕЛ. Од свог оснивања, 2017. године, активно учествује у домаћим и међународним активностима у области сајбер безбедности, у складу са својим надлежностима. У циљу унапређења пружања својих услуга, Национални ЦЕРТ Републике Србије је од 2018. године доступан свим корисницима током 365 дана у години, 24 часа дневно, путем интернет странице www.cert.rs или на дежурни број тел. 062/20-20-30.

СРБ-ЦЕРТ

Њушкала постоје свуда, па и на интернету

Њ

Објаве на интернету могу пружити доста информација о кориснику, како пријатељима корисника, тако и онима који то нису. Узмимо за пример објаву тренутне локације корисника, приликом постављања фотографија са годишњег одмора на друштвеним мрежама. Таква информација јасно указује да корисник није код куће и може бити злоупотребљена. Управо је то разлог због којег је препорука Националног ЦЕРТ-а да се садржај на интернету објављује уз додатни опрез од могућих злоупотреба, нарочито у случајевима који укључују личне податке попут матичног броја, броја платне картице и пратећег *PIN* заштитног кода, лозинке корисника и сл.

СРБ-ЦЕРТ

Онлајн трансакције

Уколико корисник приступа свом банкарском налогу путем апликације за електронско или мобилно банкарство, док је на јавно доступној тачки за приступ интернету, излаже себе ризику да постане жртва хакерског напада. Хакери су веома активни на јавно доступним и бесплатним ***Wi-Fi*** тачкама, које се често користе у ресторанима, кафеима, хотелима и сл. Како би се заштитили од оваквих напада, корисницима се препоручује употреба проверених и заштићених ***Wi-Fi*** тачака приликом коришћења онлајн финансијских трансакција, чиме би хакерима у значајној мери био онемогућен једноставан приступ и праћење уноса лозинке или других поверљивих података корисника.

СРБ-ЦЕРТ

Пријавите инцидент Националном ЦЕРТ-у

Пријава сајбер инцидента Националном ЦЕРТ-у омогућава квалитетније праћење тренутне ситуације у сајбер простору. Уколико сваки корисник пријави инцидент, тиме омогућава брзу и правовремену реакцију обавештавања осталих корисника о актуелном нападу, чиме се значајно умањује могућност ширења напада. Пријавом инцидента се омогућава и заштита критичне инфраструктуре Републике Србије, без чијег рада не би било могуће неометано функционисање државе и снабдевање свих грађана.

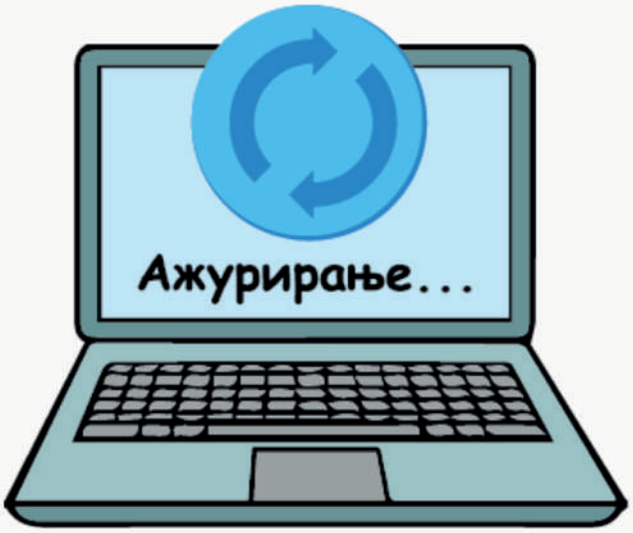
СРБ-ЦЕРТ

Пријави инцидент

Редовно ажурирање уређаја чини уређај отпорнијим на нападе

Р

Хакери редовно истражују постојеће рањивости оперативних система које корисници имају на својим уређајима. Крајњи циљ хакера је злоупотреба откривене рањивости, како би се омогућио неовлашћен приступ уређају корисника. Произвођачи софтверских и хардверских решења континуирано раде на развоју нових верзија својих оперативних система, које укључују одговарајуће закрпе за отклањање откривених рањивости. Редовним ажурирањем, онемогућава се злоупотреба рањивости уређаја, а самим тим и могућност хакерског напада на корисника.



СРБ-ЦЕРТ

Сигурност на интернету је могућа и највише зависи од тога како га користимо

Интернет омогућава свим корисницима велики број бенефита, али са собом носи и одређени ниво ризика уколико се не употребљава на адекватан начин. Остати сигуран на интернету је могуће уколико се свако од корисника понаша одговорно и примењује основне мере заштите од интернет напада.

СРБ-ЦЕРТ

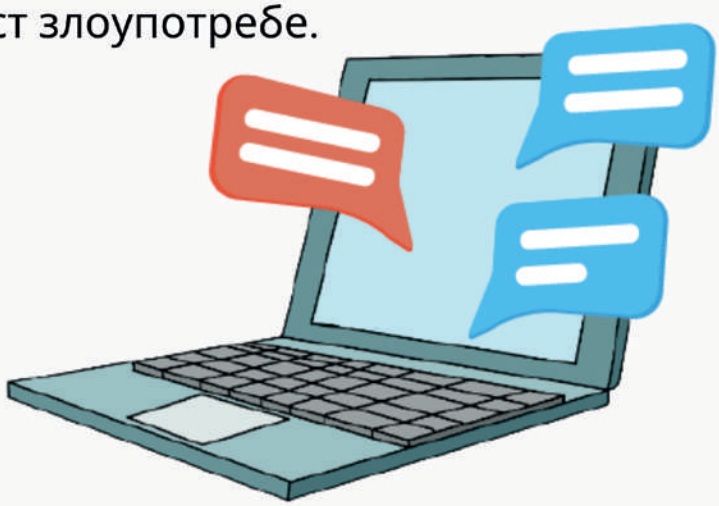
Текстуалне поруке могу бити почетна тачка сајбер напада

Током трајања пандемије вируса ***Covid19***, корисницима је било онемогућено да буду у директном контакту, већ је најчешћи вид комуникације био управо путем интернета. Такав вид комуникације је одговарао хакерима, јер је већи број корисника на интернету представљао и увећан број потенцијалних мета. Како би унапредили успешност својих напада, хакери су прешли и на слање малициозних линкова путем СМС порука на мобилне уређаје корисника. Треба бити опрезан приликом отварања СМС порука и проверити да ли је пошиљалац познат.

СРБ-ЦЕРТ

Ћаскање је безбедније када познајемо своје саговорнике

Од малих ногу нас уче да није пожељно разговарати са непознатим људима. Број непознатих корисника који су доступни на интернету је значајно већи него што је то случај у свакодневном животу. Са бројем корисника и сталним развојем апликација за комуницирање, увећава се и број могућих злоупотреба које се могу манифестовати на различите начине, понекад и са веома негативним последицама. Увек је безбедније када знамо ко се заиста налази са друге стране екрана, јер таква комуникација обезбеђује виши степен поверења и приватности и самим тим умањује могућност злоупотребе.



СРБ-ЦЕРТ

Уколико и на интернету нешто звучи сувише добро да би било истинито, вероватно није

У периодима годишњих одмора или празника, није ретка појава на интернету видети ''***First minute***'' или "***Last minute***'' понуде, које делују изузетно примамљиво. Атрактивне дестинације по веома ниској цени за одлазак на заслужени одмор корисника су удаљене само један клик од резервације. Све делује савршено, а и цена је повољнија од планираног буџета. Преостаје само да унесете податке о платној картици и резервација је завршена. Кад год се појави понуда која делује исувише добро да би била истинита, препорука је да се таква понуда детаљно провери пре уноса било каквих података корисника.

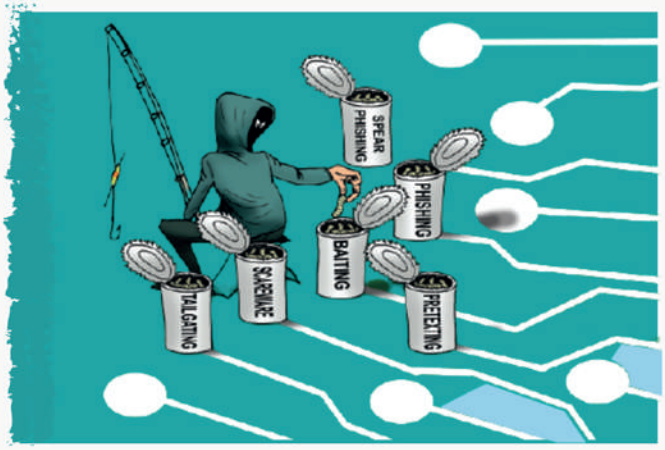
СРБ-ЦЕРТ

Ф

Фишинг је најзаступљенији тип сајбер напада

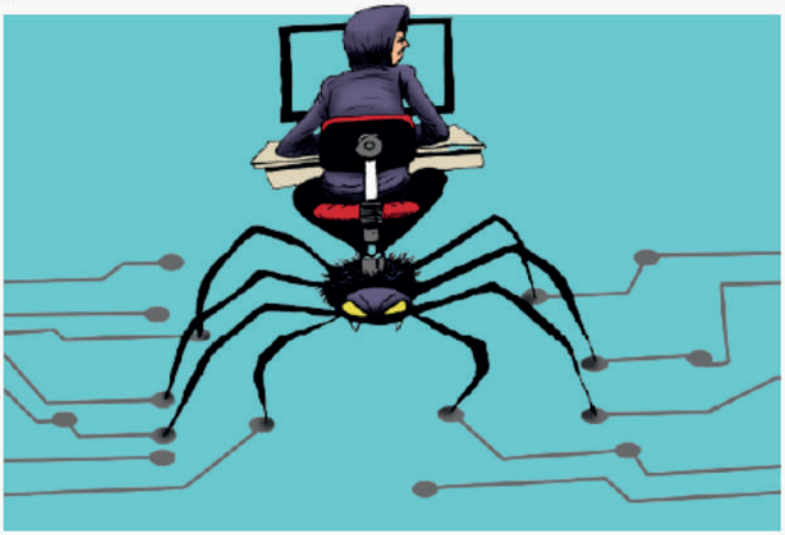
На основу постојећих статистичких анализа на светском нивоу, преко **90%** сајбер напада започиње фишинг имејл поруком. Фишинг имејл најчешће стиже корисницима са непознате имејл адресе. У тексту мејла се налазе инструкције које упућују корисника да кликне на прослеђени линк или отвори прилог. Приметна је и доза хитности поступања корисника у скоро свим имејл порукама, због чега је веома важно да корисници добро провере све имејл поруке које добијају од непознатих пошиљаоца. У случају да је пошиљалац познат, али инструкције у поруци не делују аутентично, препорука је ступити у директан контакт са пошиљаоцем и проверити веродостојност сумњиве имејл поруке.

СРБ-ЦЕРТ



Хакерски напад се може догодити у било ком тренутку и било ком кориснику

Светски статистички подаци указују да у току само једног дана више десетина хиљада интернет страница у свету буде хаковано. Дневно се блокира више хиљада малициозних апликација намењених мобилним уређајима. Хакерски напади се могу десити сваког тренутка, а жртве напада могу бити физичка лица, правна лица или компаније које су препознате као критична инфраструктура, попут сектора енергетике, финансија, здравства и сл. Применом превентивних мера корисник може значајно умањити могућност да постане жртва сајбер напада.



СРБ-ЦЕРТ

Ц

Цена непажње корисника на интернету некада може бити веома висока

Током неких сајбер напада је довољан само један погрешан клик, да се кориснику онемогући приступ фајловима и датотекама. За овакве или сличне грешке корисника, хакери траже одређену суму новца која може достићи и неколико милиона америчких долара или евра. Како хакерски напади најчешће започињу слањем фишинг мејлова, познавање основних мера превенције може бити веома значајно за одбрану корисника од хакерских напада.

СРБ-ЦЕРТ

Чувајмо своју и поштујмо туђу приватност на интернету

Ч

У реалном свету, али и у свету интернета, заштита приватности представља кључни елемент у обезбеђивању личне безбедности и људског достојанства. Непоштовањем своје или туђе приватности можемо довести себе или друге у опасност која се у неким случајевима може окарактерисати као минорна, али има и оних ситуација у којима је опасност на веома високом нивоу и може утицати чак и на нечији живот. У намери да интернет окружење учинимо безбеднијим за све, неопходно је да корисници чувају своју и поштују туђу приватност и на интернету.

СРБ-ЦЕРТ

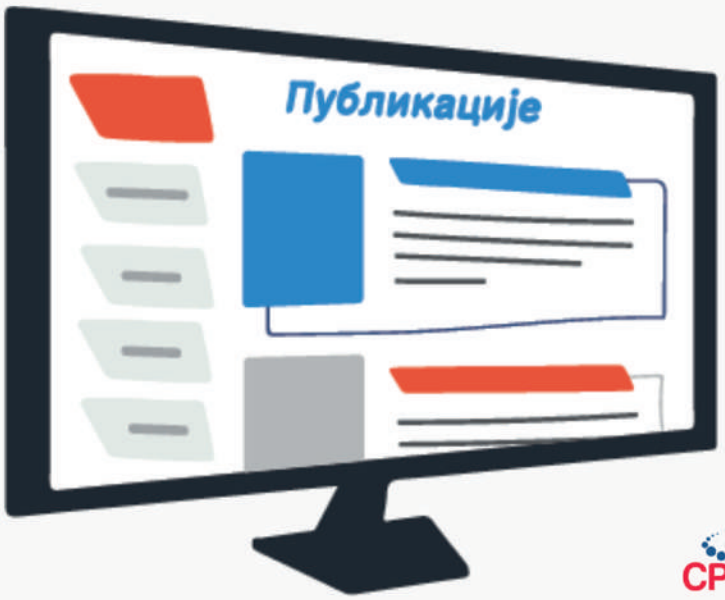
Џак новца испод интернет дуге чувају једнорози

Имајући у виду сталну људску потребу за проналажењем бољих услова за живот, на интернету се веома често могу наћи понуде различитих апликација које корисницима нуде могућност стицања велике финансијске добити са или без и мало уложреног труда. Порука често може имати призвук бајковитих тренутака који корисника упућују да преузме неку апликацију и пронађе пут до краја дуге где га очекује награда у виду великог џака са новцем. Будимо обазриви код оваквих и сличних порука, јер на крају интернет дуге корисник можда може видети само једнорога.

СРБ-ЦЕРТ

Што више препорука усвојимо, бићемо безбеднији на интернету

Безбедност на интернету се омогућава уз помоћ развоја различитих алата и вишеслојне заштите, на чему предано раде различите компаније. И поред имплементације свих расположивих безбедносних решења, главна мета хакерских напада је корисник. Усвајањем препорука корисници поступају превентивно и тиме штите себе и своје најближе од сајбер напада. Препоруке Националног ЦЕРТ-а су доступне свим корисницима на www.cert.rs/publikacije.



СРБ-ЦЕРТ