



Основе информационе безбедности



Препоруке за заштиту корисничких налога, уређаја и података

Овај водич садржи кључне смернице за безбедно коришћење интернета, са циљем унапређења информационе безбедности, едукације и заштите корисника у онлајн окружењу.

САДРЖАЈ

	ЗАШТИТА	03
	ПРЕПОРУКЕ ЗА ОНЛАЈН КУПОВИНУ	06
	САВЕТИ ЗА ЛОЗИНКЕ	07
	ФИШИНГ ПРЕВАРЕ	08





ЗАШТИТА ФАЈЛОВИ И УРЕЂАЈИ



Ажурирање софтвера

Застарели софтвер повећава ризик од компромитовања уређаја. Ради смањења ризика, подесите аутоматска ажурирања софтвера и редовно проверавајте да ли су оперативни систем и сви програми ажурирани. На тај начин обезбеђујете да уређаји имају најновије безбедносне закрпе и остају заштићени од познатих рањивости. Ажурирања инсталирајте што је пре могуће након објављивања, нарочито када отклањају критичне безбедносне рањивости. Преузмите и инсталирајте мобилне апликације искључиво из званичних продавница (*Google Play*, *App Store* и *Microsoft Store*), уз проверу произвођача, броја преузимања и корисничких оцена.



Заштитите датотеке

Направите резервне копије важних датотека на екстерном диску или у облаку (*cloud*). Користите антивирусни софтвер за заштиту датотека и уређаја.



Користите двофакторску аутентификацију (2FA)

Никада не одобравајте 2FA захтев за, који нисте сами покренули. Поред уноса лозинке, потребно је потврдити свој идентитет додатним фактором:

- 1 апликација за аутентификацију
- 2 хардверски безбедносни кључ
- 3 биометријска потврда, или
- 4 једнократни верификациони код



Користите лозинке

За сваки уређај или кориснички налог поставите јединствену и комплексну лозинку. Не користите исту лозинку за више корисничких налога, јер компромитовање једног може угрозити и остале.



Шифровање уређаја

Шифрујте уређаје и друге медије који садрже осетљиве податке. Енкрипција штити податке од неовлашћеног приступа, посебно у случају губитка или крађе уређаја. При преносу података преко мреже, користите протоколе и сервисе који обезбеђују шифровану комуникацију.



ЗАШТИТА

БЕЖИЧНА МРЕЖА**Заштита рутера**

Промените подразумевану административну лозинку рутера. Користите комплексну лозинку за Wi-Fi мрежу. Редовно проверавајте да ли постоји нова верзија *firmware*-а за рутер. Искључите удаљени приступ администрацији рутера, јер може представљати чест вектор напада.

**Коришћење WPA3 или WPA2**

Уколико рутер подржава безбедносни протокол WPA3 (или бар WPA2), препоручује се његово коришћење ради заштите података од неовлашћеног приступа и/или злоупотребе. Важно је не користити старе протоколе WEP или WPA.

**Подесите заштитни зид**

Заштитни зид (*firewall*) је безбедносни систем (уређај или софтвер) који служи као баријера између поуздане интерне мреже и мање поузданих спољних мрежа, попут интернета. Заштитни зид надгледа и контролише долазни и одлазни мрежни саобраћај на основу унапред дефинисаних безбедносних правила.

Већина савремених оперативних система има уграђен заштитни зид који треба оставити укљученим.

**Немојте користити застареле уређаје**

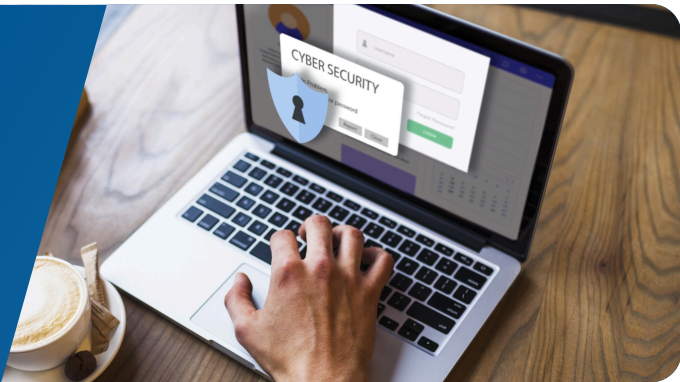
Уређаје које више не користите због застарелости, искључите са мреже. Њихова безбедност може бити угрожена због застарелих функционалности. Ови уређаји су рањиви и могу бити искоришћени од стране нападача за улазак у мрежу. Ресетујте уређаје на фабричка подешавања, пре него што их одложите или продате.

Посебно обратите пажњу на *IoT* уређаје, који представљају један од најчешћих улазних вектора напада. То су камере, *DVR*, паметни *TV* уређаји и остали.



ЗАШТИТА

ИДЕНТИТЕТ И ПРИВАТНОСТ



Заштитите свој онлајн идентитет

Када отварате нови кориснички налог, инсталирате апликацију или набављате нови уређај, подесите безбедносне опције за дељење информација. Редовно проверавајте и ажурирајте подешавања, да се уверите да нису промењена без вашег знања.



Пажљиво делите информације

Будите обазриви пре објављивања било ког податка на друштвеним мрежама. Размислите шта објава открива, ко је може видети и како може утицати на вас и остале особе. Злоупотреба често почиње од информација које се деле на друштвеним мрежама. Ограничите видљивост личних података само особама којима верујете. Нападаци ове информације могу користити за социјални инжењеринг, крађу идентитета или покушаје откривања лозинки.



Опрезно користите бесплатне Wi-Fi мреже

Јавне Wi-Fi мреже могу представљати безбедносни ризик јер корисник нема контролу над њиховом конфигурацијом и заштитом. Искључите аутоматско повезивање на јавне мреже. Ако користите бесплатне јавне Wi-Fi мреже, избегавајте пријављивање на корисничке налоге електронске поште и не обављајте финансијске трансакције путем апликација за електронско банкарство. Уколико сте у могућности, користите мобилну приступну тачку (*hotspot*), или другу поуздану мрежу како бисте остварили поузданију и шифровану везу.



Закључавање екрана

Користите PIN, лозинку или биометријску заштиту за закључавање мобилног телефона, рачунара, таблета и осталих уређаја.



QR код преваре

Честа је злоупотреба QR кодова у фишинг нападима, позната као *quishing*. Важно да пре скенирања QR кода проверите његов извор. Скенирање може водити на лажну интернет страницу или да покрене преузимање злонамерног садржаја. Опрезно са QR кодовима постављеним на јавним местима, огласима или налепницама, јер могу бити замењени злонамерним кодовима.



ПРЕПОРУКЕ ЗА ОНЛАЈН КУПОВИНУ



Заштитите податке и новац приликом онлајн куповине:



Користите безбедан начин плаћања

За плаћања користите виртуелну картицу која није директно повезана са текућим рачуном. Ограничите расположиви износ само на суму потребну за конкретну куповину. Проверите да ли адреса интернет странице почиње са **https://** и да ли је приказана иконица катанца.



Редовно проверавајте своје изводе

Проверавајте банкарске изводе и стање на рачуну. Активирајте обавештења (електронска или SMS порука) као додатни сервис банке у којој имате рачун. На тај начин, након сваке трансакције извршене платном картицом, добијате информацију којом се потврђује трансакција.



Проверите продавца пре куповине

Пре сваке онлајн куповине проверите поузданост продавца и погледајте рецензије других корисника. Уверите се да су наведени контакт подаци и физичка адреса продавца тачни и проверљиви. Будите посебно опрезни са продавницама које нуде нереално ниске цене, јер то може бити индикатор потенцијалне преваре. Проверите старост домена продавца. Недавно регистровани домени могу бити индикатор потенцијалне преваре и разлог за додатну проверу.



Не делите личне податке

PIN број и CVV/CVC код платне картице, једнократни кодови које добијате на телефон путем СМС поруке или апликације, као и подаци за приступ корисничком налогу, намењени су искључиво вама и служе само за потврду идентитета и ауторизацију трансакција. Ове податке никада не треба делити са другим лицима, без обзира на то да ли се особа представља као запослени у банци, продавац или као техничка подршка. Банка не позива клијенте телефоном и не тражи личне или безбедносне податке.



САВЕТИ ЗА ЛОЗИНКЕ



Постоји више начина за креирање јединствене и комплексне лозинке. У наставку текста дати су основни савети:



Користите комплексне и јединствене лозинке или приступне фразе. Препоручује се да лозинка садржи најмање 12 карактера и комбинацију малих и великих слова, бројева и специјалних знакова. Не треба користити уобичајене речи, личне податке, фразе или појмове из приватног живота. На овај начин умањујете ризик од неовлашћеног приступа и додатно унапређујете безбедност својих корисничких налога.



Не користите исту лозинку за различите корисничке налоге. Не препоручује се чување лозинки у интернет прегледачима, посебно када је реч о налозима за електронску пошту и приступ банкарским рачунима. За безбедно креирање и чување лозинки, препоручује се коришћење поузданих апликација као што су менаџери лозинки. Ако је тешко запамтити лозинку, немојте је записивати у изворном облику, већ користите подсетник (*hint*) који упућује на праву лозинку.



Ако апликација приликом креирања корисничког налога захтева унос сигурносних питања, саветује се избор оних на која само ви знате одговор. Питања служе за случај поновног постављања лозинке. Не користите питања чији се одговори могу пронаћи на интернету. Ако постоји могућност избора, предност треба дати двофакторској аутентификацији, уместо сигурносних питања.



Лозинку је неопходно одмах променити уколико постоји сумња да је кориснички налог компромитован, након потврђеног безбедносног инцидента, у случају откривања или цурења лозинке, као и када је иста лозинка коришћена на више различитих сервиса. Ради додатне заштите корисничког налога, препоручује се редовна измена лозинке, најмање једном у три месеца.



ФИШИНГ ПРЕВАРЕ



Фишинг (*phishing*) је врста преваре чији је циљ прикупљање и злоупотреба личних и финансијских података, као што су лозинке за друштвене мреже и електронску пошту, бројеви платних картица, бројеви банкарских рачуна, CVV/CVC кодови платних картица, PIN бројеви. Нападаци шаљу поруке путем електронске поште, SMS порука, апликација за размену порука (*Viber, WhatsApp*), друштвених мрежа. У порукама се од корисника траже лични и финансијски подаци, које нападачи касније користе за отварање нових или приступ постојећим корисничким налозима. Уобичајени облици фишинг напада укључују:



Обавештења о наводним сумњивим активностима или покушајима пријављивања на кориснички налог.



Поруке у којима се наводи да имате право на повраћај новца од државе или се нуде купони за бесплатне производе.



Обавештења да постоји проблем са корисничким налогом или платном картицом уз захтев да унесете личне и финансијске податке. Циљ оваквих порука је преузимање поверљивих личних података и података о платној картици.



Слање лажних електронских или SMS порука грађанима, које изгледају као званична преписка државних органа. У порукама се наводи да је против примаоца покренута истрага или да постоји неизмирена обавеза.



Захтев да приступите линку и потврдите личне податке или извршите уплату. Линк најчешће води на лажну интернет страницу која изгледа као легитимна, са циљем преузимања личних података, адресе електронске поште и лозинке, или покретања злонамерног софтвера.



Слање лажних фактура или докумената у прилогу електронске поште или SMS поруке. Документ послат од непознатог пошиљача не треба отварати.



ВАЖНО! Будите обазриви приликом пријема позива, SMS или електронских порука од непознатих пошиљача који траже потврду личних података. Не приступајте линковима, не преузимајте прилоге из сумњивих електронских порука. За интернет плаћања користите посебну картицу и ограничите износ на суму потребну за конкретну куповину. Применом вештачке интелигенције, фишинг поруке могу бити уверљиве и персонализоване, јер нападач користи јавно доступне информације са друштвених мрежа. Треба бити опрезан и када порука изгледа познато или је лично прилагођена.



Основе информационе безбедности

www.cert.rs