ЕДУЦИРАЈ СЕ ЗА САЈБЕР БЕЗБЕДНОСТ

Заштитете ги Вашите on-line сметки

Комисија за хартии од вредност на
Република Северна Македонија

Октомври 2021

ШТО Е САЈБЕР БЕЗБЕДНОСТ

Сајбер безбедност е практика на одбрана на компјутери, сервери, мобилни уреди, електронски системи, мрежи и податоци од злонамерни напади.

Исто така е познато како безбедност на информатичката технологија или електронска безбедност на информациите.

Овој термин се применува во различни контексти, од деловни до мобилни компјутери и може да се подели во неколку вообичаени категории.

КАТЕГОРИИ НА САЈБЕР БЕЗБЕДНОСТ

Безбедноста на мрежата е практика на обезбедување на компјутерска мрежа од натрапници, без разлика дали се насочени напаѓачи или опортунистички малициозен софтвер.

Безбедноста на апликацијата се фокусира на чување на софтвер и уреди без закани. Компромитираната апликација може да обезбеди пристап до податоците кои се дизајнирани да ги заштити.

Безбедноста на информациите ги штити интегритетот и приватноста на податоците и во процесот на складирање и на транзит.

Оперативната безбедност ги вклучува процесите и одлуките за управување и заштита на пристапот до податоци. Тука се подразбираат дозволите што ги имаат корисниците при пристап до мрежа и процедурите што одредуваат како и каде може да се чуваат или споделуваат податоците.

КАТЕГОРИИ НА САЈБЕР БЕЗБЕДНОСТ

Управувањето со непредвидливи ситуации и континуитет во работењето **како и политиките за обновување при непредвидени ситуации** диктираат како институцијата ќе ги врати операциите и информациите во истиот работен капацитет, како пред настанатата непредвидена ситуација.

Едукацијата за крајни корисници се однесува на најнепредвидливиот фактор за сајбер безбедност: **ЧОВЕКОТ**. Секој оној кој не ги следи насоките на безбедносните процедури може случајно да пренесе вирус во еден безбеден систем. Однапред информираноста на корисниците да бришат сомнителни прилози за е-пошта, да избегнуваат приклучување на неидентификувани USB-уреди и многу други значајнипрактики при управување со информатичката технологија се од витално значење за безбедноста на секоја институција.

ВИДОВИ НА САЈБЕР ЗАКАНИ

Сајбер криминалот “cybercrime” вклучува поединечни актери или групи кои насочуваат системи за финансиска корист или системи кои можат да предизвикаат нарушување.

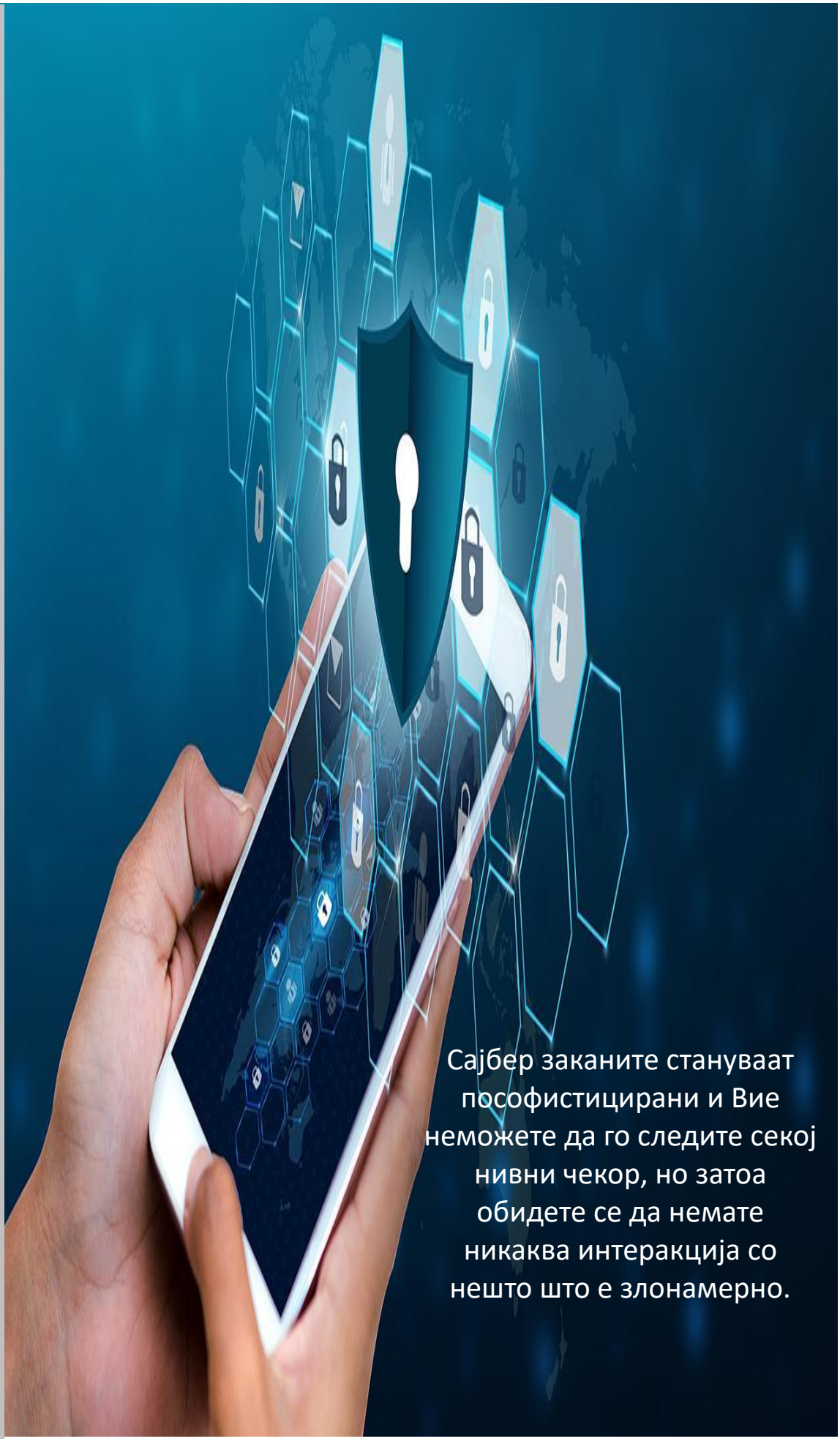
Сајбер нападот “ciber-attack” често пати вклучува политички мотивирано собирање на информации.

УКАЖУВАЊА ЗА ЗАШТИТА ОД САЈБЕР ЗАКАНИ

Комисија за хартии од вредност на
Република Северна Македонија

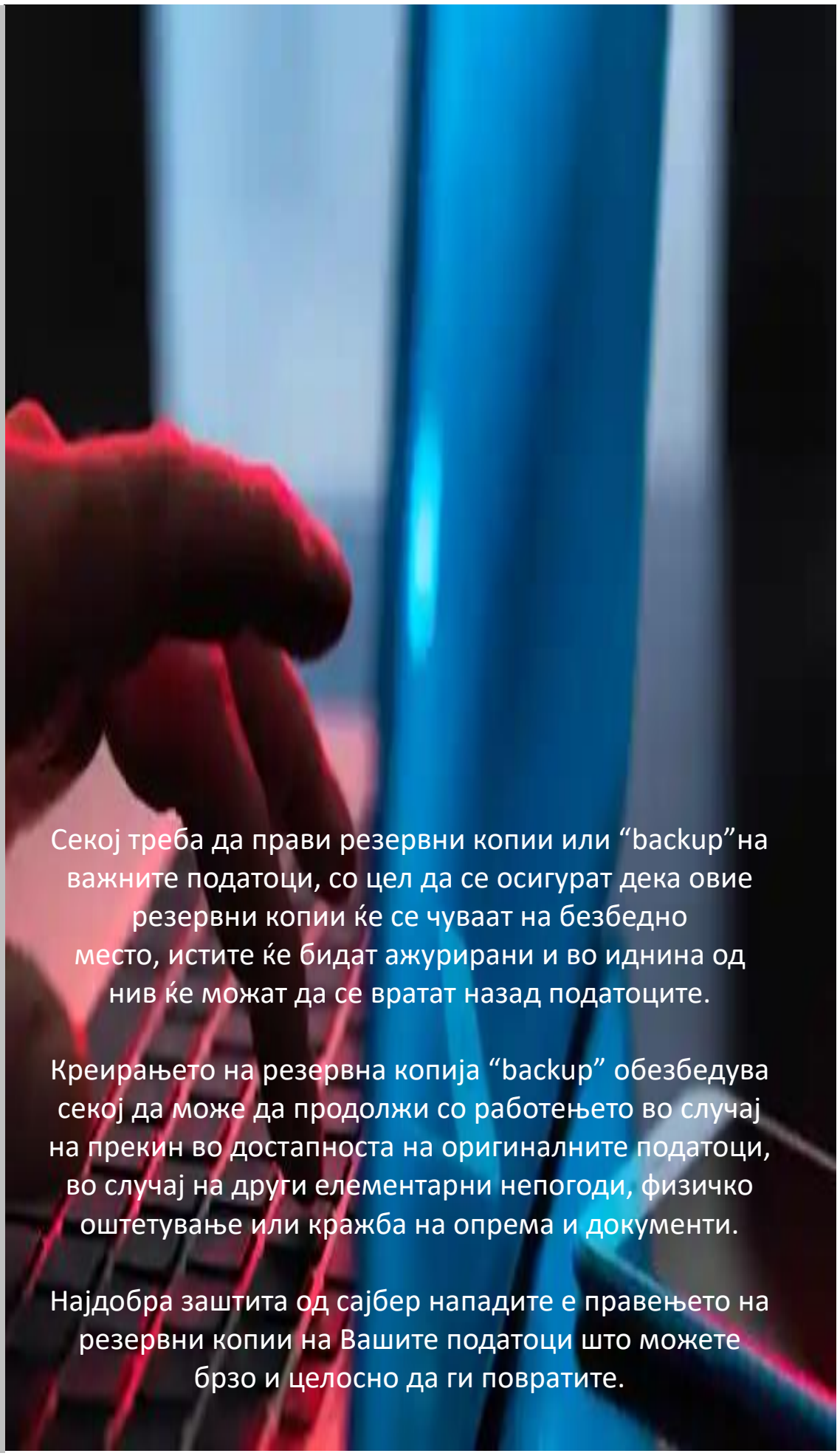
Октомври 2021

САЈБЕР ЗАКАНИ



Сајбер заканите стануваат пософистицирани и Вие неможете да го следите секој нивни чекор, но затоа обидете се да немате никаква интеракција со нешто што е злонамерно.

СЕКОГАШ ПРАВЕТЕ КОПИЈА ИЛИ “ BACKUP” НА ВАШИТЕ ПОДАТОЦИ



Секој треба да прави резервни копии или “backup”на важните податоци, со цел да се осигурат дека овие резервни копии ќе се чуваат на безбедно место, истите ќе бидат ажурирани и во иднина од нив ќе можат да се вратат назад податоците.

Креирањето на резервна копија “backup” обезбедува секој да може да продолжи со работењето во случај на прекин во достапноста на оригиналните податоци, во случај на други елементарни непогоди, физичко оштетување или кражба на опрема и документи.

Најдобра заштита од сајбер нападите е правењето на резервни копии на Вашите податоци што можете брзо и целосно да ги повратите.

СЕКОГАШ ПРАВЕТЕ КОПИЈА ИЛИ “ BACKUP” НА ВАШИТЕ ПОДАТОЦИ

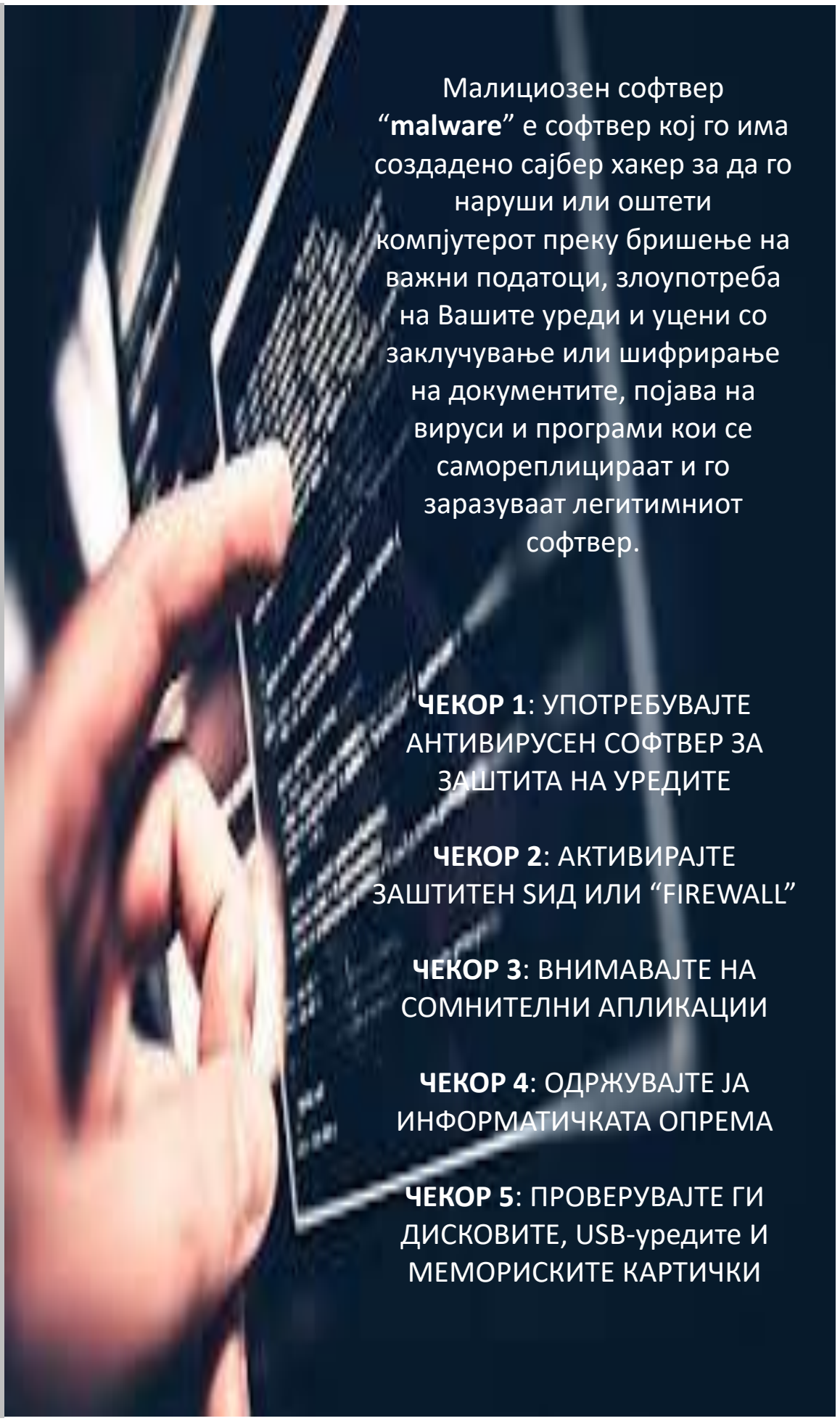
ЧЕКОР 1: НАПРАВЕТЕ СЕЛЕКЦИЈА НА ПОДАТОЦИ ЗА КОИ ТРЕБА ДА НАПРАВИТЕ “BACKUP”

ЧЕКОР 2: ЧУВАЈТЕ ЈА РЕЗЕРВНАТА КОПИЈА “BACKUP”-от ПОДАЛЕКУ ОД ОРИГИНАЛОТ

ЧЕКОР 3: СКЛАДИРАЊЕ НА ПОДАТОЦИ ВО ОБЛАК И/ИЛИ “CLOUD STORAGE”

ЧЕКОР 4: ПРАВЕЊЕТО РЕЗЕРВНА КОПИЈА ИЛИ “BACKUP” НА ПОДАТОЦИТЕ НЕКА БИДЕ ВАШАТА СЕКОЈДНЕВНА АКТИВНОСТ ИЛИ “CLOUD STORAGE”

ЗАШТИТЕТЕ СЕ ОД МАЛИЦИОЗЕН СОФТВЕР ИЛИ “ MALWARE”



Малициозен софтвер “**malware**” е софтвер кој го има создадено сајбер хакер за да го наруши или оштети компјутерот преку бришење на важни податоци, злоупотреба на Вашите уреди и уцени со заклучување или шифрирање на документите, појава на вируси и програми кои се самореплицираат и го заразуваат легитимниот софтвер.

ЧЕКОР 1: УПОТРЕБУВАЈТЕ АНТИВИРУСЕН СОФТВЕР ЗА ЗАШТИТА НА УРЕДИТЕ

ЧЕКОР 2: АКТИВИРАЈТЕ ЗАШТИТЕН SИД ИЛИ “FIREWALL”

ЧЕКОР 3: ВНИМАВАЈТЕ НА СОМНИТЕЛНИ АПЛИКАЦИИ

ЧЕКОР 4: ОДРЖУВАЈТЕ ЈА ИНФОРМАТИЧКАТА ОПРЕМА

ЧЕКОР 5: ПРОВЕРУВАЈТЕ ГИ ДИСКОВИТЕ, USB-уредите И МЕМОРИСКИТЕ КАРТИЧКИ

ФИШИНГ НАПАД

Комисија за хартии од вредност на
Република Северна Македонија

Октомври 2021

ВНИМАВАЈТЕ НА ФИШИНГ НАПАД

Фишинг напад е напад од социјален инженеринг кој често се користи за кражба на кориснички податоци, вклучувајќи ги ингеренциите за најава и броевите на кредитните картички.Тоа се случува кога напаѓачот маскирајќи се како доверлив субјект ја залажува жртвата да отвори е-пошта, инстант порака или текстуална порака. Потоа, примателот е измамен да кликне на злонамерната врска, што може да доведе до инсталација на малициозен софтвер, замрзнување на системот како дел од напад или откривање на чувствителни информации.

ЗНАЦИ ЗА ПРЕПОЗНАВАЊЕ НА ФИШИНГ НАПАДИ

Некои напаѓачи ќе се обидат да создадат пораки кои на прв поглед се многу слични на официјалните пораки со вклучување на логоа и графики слични на Вашите или на институциите со кои соработувате, па затоа внимателно и детално разгледајте ја пораката за да ги воочите знаците од фалсификување.

Доколку во насловот од пораката Ви се обраќаат со Вашата адреса за е-пошта или пишува „почитуван “, „колега “или се користи сличен генерички термин, тоа може да биде знак дека испраќачот не Ве познава и пораката можеби е испратена за фишинг-измама.

Бидете сомнителни на пораките во чиј текст од Вас се бара брзо да дејствувате или детали од типот **„испратете порака во рок од 24 часа “или „Добитници сте на ..., веднаш кликнете тука “**.

ЗНАЦИ ЗА ПРЕПОЗНАВАЊЕ НА ФИШИНГ НАПАДИ

Внимавајте на пораки со барање за брза реализација на плаќања на одредени банкарски сметки. Проверете ја адресата за е-пошта од која пораката е испратена или истата е само слична на адреси кои често ги користите за комуникација.

Не одговарајте на пораки по е-пошта, SMS, Viber или WhatsApp во кои Ви се нудат пари или наследство од странство испратени од лица и адреси кои не ги познавате, или за кои Ви се нуди пристап до скриени или компромитирачки информации на Интернет.

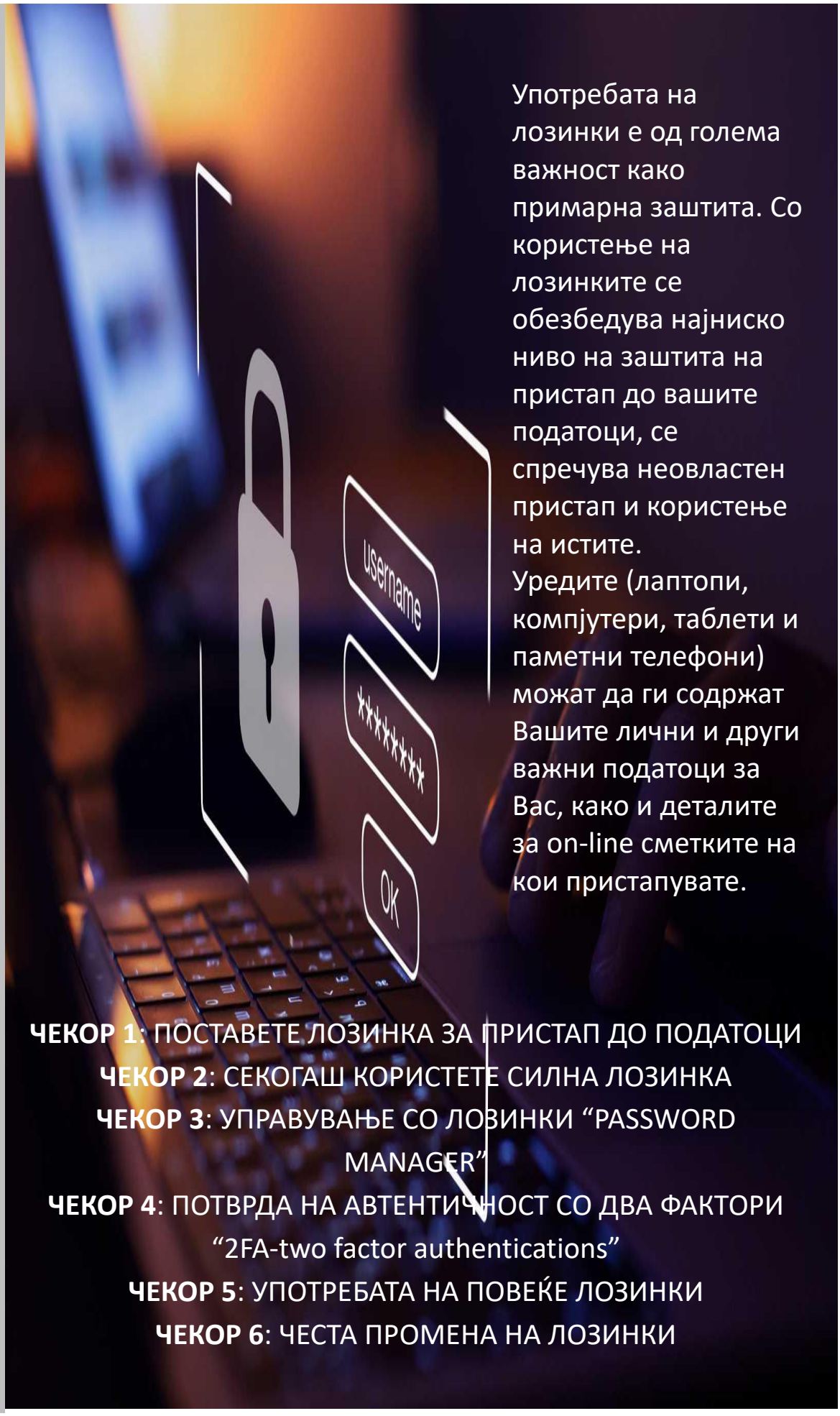
Не одговарајте на пораки во кои Ве уценуваат со објава на компромитирачки информации и слики, а за кои се тврди дека истите се испратени од Вашата адреса за е-пошта.

КРЕИРАЊЕ И УПРАВУВАЊЕ СО ЛОЗИНКИ ПРИСТАП И ПРАВИЛНО КОРИСТЕЊЕ НА УРЕДИ

Комисија за хартии од вредност на
Република Северна Македонија

Октомври 2021

ЧЕКОРИ ЗА ПРАВИЛНО КОРИСТЕЊЕ НА ЛОЗИНКИТЕ



Употребата на лозинки е од голема важност како примарна заштита. Со користење на лозинките се обезбедува најниско ниво на заштита на пристап до вашите податоци, се спречува неовластен пристап и користење на истите.
Уредите (лаптопи, компјутери, таблети и паметни телефони) можат да ги содржат Вашите лични и други важни податоци за Вас, како и деталите за on-line сметките на кои пристапувате.

ЧЕКОР 1: ПОСТАВЕТЕ ЛОЗИНКА ЗА ПРИСТАП ДО ПОДАТОЦИ

ЧЕКОР 2: СЕКОГАШ КОРИСТЕТЕ СИЛНА ЛОЗИНКА

ЧЕКОР 3: УПРАВУВАЊЕ СО ЛОЗИНКИ “PASSWORD MANAGER”

ЧЕКОР 4: ПОТВРДА НА АВТЕНТИЧНОСТ СО ДВА ФАКТОРИ “2FA-two factor authentications”

ЧЕКОР 5: УПОТРЕБАТА НА ПОВЕЌЕ ЛОЗИНКИ

ЧЕКОР 6: ЧЕСТА ПРОМЕНА НА ЛОЗИНКИ

ПРЕПОРАКИ ЗА БЕЗБЕДНА УПОТРЕБА НА ПАМЕТНИ УРЕДИ

Мобилните телефони и таблети често се користат за најразлични потреби и операции, па за таа цел следуваат чекори и препораки за нивно безбедно користење:

ЧЕКОР 1: БЕЗБЕДЕН ПРИСТАП ДО УРЕДИТЕ

ЧЕКОР 2: ИЗГУБЕНИТЕ ИЛИ УКРАДЕНИТЕ УРЕДИ МОЖЕ ДА ГИ СЛЕДИТЕ, ЗАКЛУЧИТЕ ИЛИ ИЗБРИШЕТЕ

ЧЕКОР 3: РЕДОВНО И НАВРЕМЕНО НАДГРАДУВАЊЕ НА УРЕДИТЕ

ЧЕКОР 4: РЕДОВНО И НАВРЕМЕНО АЖУРИРАЊЕ НА АПЛИКАЦИИ

ЧЕКОР 5: НЕ СЕ ПОВРЗУВАЈТЕ НА НЕПОЗНАТИ WI-FI ЛОКАЦИИ

РАЗНИ САЈБЕР ИНЦИДЕНТИ

Сајбер-инцидент е неовластен пристап или обид за пристап до ИТ системите на една институција. Тука спаѓаат малициозните напади кои имаат за цел кражба на податоци, уцени или злоупотреба на вашите податоци и ИТ системи или предизвикување на штета. Примери за сајбер-инциденти се негирање на услуга, напад со кој се оневозможува достапноста на Вашите услуги и се прекинува Вашето тековно нормално работење. Причини за инциденти може да бидат и физички оштетувања, природни непогоди или кражба.

ЧЕКОР 1: СЕКОГАШ БИДЕТЕ ПОДГОТВЕНИ ЗА САЈБЕР ИНЦИДЕНТИ

ЧЕКОР 2: ИДЕНТИФИКАЦИЈА НА СЛУЧЕН САЈБЕР ИНЦИДЕНТ

ЧЕКОР 3: ПРЕКИН И РЕШАВАЊЕ НА САЈБЕР ИНЦИДЕНТОТ

ЧЕКОР 4: ИЗВЕСТУВАЊЕ ЗА САЈБЕР ИНЦИДЕНТ И СПОДЕЛУВАЊЕ НА ИНФОРМАЦИИ

ЧЕКОР 5: НАУЧЕТЕ ОД САЈБЕР ИНЦИДЕНТОТ