Користи го ИНТЕРНЕТ-от безбедно!

НИКОГАШ НЕ ОТВАРАЈТЕ ПОРАКИ ОД НЕПОЗНАТИ ИСПРАЌАЧИ !

Овие пораки може да содржат вируси или некој се обидува да Ви ги преземе Вашите податоци!

www.sec.gov.mk

Користи го ИНТЕРНЕТ-от безбедно!

ЧУВАЈТЕ ГИ ВАШИТЕ ЛИЧНИ ПОДАТОЦИ НА БЕЗБЕДНА ЛОКАЦИЈА !

On line не ги споделувајте следните информации:

- **Вашето име и презиме**
- **Вашите фотографии**
- **Вашиот телефонски број**
- **Вашата адреса**
- **Вашиот ЕМБГ**
- **Вашата трансакциска с-ка**
- **Вашите лозинки**

Зошто???

Затоа што сајбер напаѓачите може да ги злоупотребат сите информации!

www.sec.gov.mk

Најдобра заштита од сајбер-нападите !

Автоматизираното правење на резервни копии заштедува време и гарантира дека секогаш ќе ги имате најновите верзиии од вашите документи.

Ваквото складирање е лесно за инсталирање и истото е прифатливо во однос на цената со оглед на заштитата на важните податоци што ја нудат.

Оваа информација користете ја како дополнителен критериум за избор на начинот на складирање на резервната копија од Вашите податоци.

Иако, копијата Ви е запишана на друг екстерен диск, посебен компјутер или USB-уред, ограничете го пристапот до нив така што: други лица да немаат достапност до тие резервните копии; не се меѓусебно поврзани уредите на кои тие се запишани (физички или преку локална компјутерска мрежа) на уредот на кој се наоѓаат оригиналните податоци.

Доколку овие уреди на кои се запишани резервните копии се постојано поврзани на локалната компјутерска мрежа, при инфекција истата автоматски може да се пренесе и на уредот за складирање. Ова значи дека секоја таква резервна копија може да биде инфицирана, оставајќи Ве без резервна копија од која би можеле да ги повратите оригиналните податоци.

Заради поголема безбедност потребно е резервните копии да ги складирате на друга локација, така што во случај на елементарна непогода или кражба нема да ја изгубите резервната копија. Затоа складирањето во облак “cloud storage” се најекономичен и најефикасен начин за да се постигне оваа цел.

Складирање на податоци во облак „cloud storage “значи дека давателот на услуги ги чува Вашите податоци на негова инфраструктура достапна преку Интернет. Вашите податоци на тој начин се физички одделени од Вашата локација и се обезбедува складирање на истите, како и веб услуги без да инвестирате во скап хардвер.

Доколку не користите Ваш сопствен сервер за е-пошта, Вашите електронски пораки се веќе „cloud storage “. Најчесто контактите кои се запишани на Вашиот мобилен телефон автоматски се запишуваат во облак, исто како и копија од комуникацијата преку апликациите како Viber, Messenger и WhatsApp.

Придобивка од ваквата услуга за складирање е високото ниво на достапност што на даватели на услуги за складирање на податоци во облак нудат бесплатен, но ограничен простор за складирање податоци, пришто истиот со доплата може да се зголеми.

Идентификувајте ги податоците кои се важни за Вашето работење и без кои неможете да функционирате (фактури, испратници и други документи со финансиски, лични и чувствителни податоци).

Секогаш правете копија од овие податоци на надворешен уред и истиот чувајте го на безбедно место подалеку од уредите на кои се запишани оригиналните податоци и документи.

Заштита од малициозен софтвер или “malware”!

Антивирусот е вклучен бесплатно во популарните оперативни уреди и истиот се користи кај сите компјутери, лаптопи, таблети и смартфони. Па така, Вашиот компјутер или мобилен уред веќе имаат антивирусна софтверска заштита, но истата вообичаено е бесплатна и нуди минимална заштита. Затоа, внимателно размислете за набавка на лиценцирана комерцијална антивирусна заштита која ќе ја подобрат безбедноста на уредите кои ги користите.

Сомнителна апликација е форма на измама со идентитет која вклучува изманик кој аплицира за нова сметка за услуги или производи и притоа за истите користи лажен идентитет.
За инсталирање на апликации од Интернет на уредите треба да се користат исклучиво апликации од е-продавниците кои се одобрени од страна на производителот на оперативниот уред (за мобилните телефони и таблетите тоа се Google Play Store или Apple App Store).
Овие апликации се проверуваат од страна на производителот со цел да обезбедат одредено ниво на заштита.
Поради тоа треба да се воздржите од инсталирање на апликации од трети лица, од непознати извори или пиратски софтвери, бидејќи истите не се проверени и најчесто содржат вируси.

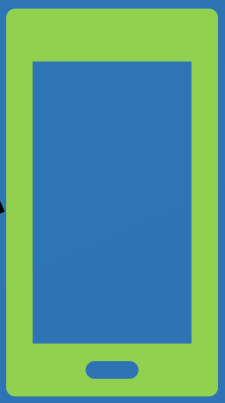
Софтверот на сите компјутери, лаптопи, мобилни телефони и таблети треба секогаш да бидат ажурирани со најновите верзии од производителите и добавувачите на софтвер и хардвер.
Примената на ажурирањето на информатичката опрема е една од најважните работи што треба да ја направите за да ја подобрите безбедноста.

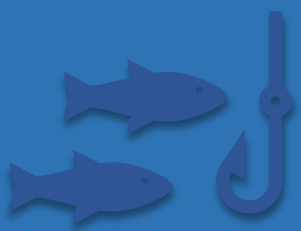
Заштитниот ѕид “firewall” е мрежен безбедносен уред што го следи влезниот и излезниот мрежен сообраќај и одлучува дали ќе дозволи или ќе блокира специфичен сообраќај врз основа на дефиниран пакет на безбедносни процедури.
Заштитиот ѕид е првата линија на одбрана во мрежната безбедност и создава сигурна зона помеѓу Вашата компјутерска мрежа и надворешните мрежи како што е Интернетот. Сите оперативни уреди вклучуваат бесплатен заштитен ѕид, кој е едноставен за активирање и препорачливо е истиот да биде постојано вклучен.

Ваквите уреди за складирање најчесто се користат за пренос на податоци помеѓу организации и луѓе. Доколку само еден невнимателен корисник ненамерно приклучи инфициран мемориски уред може да направи голема штета.

ВНИМАНИЕ !!!

ФИШИНГ НАПАД





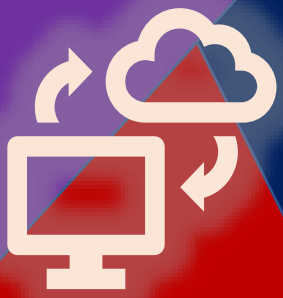
ПРЕПОЗНАЈТЕ ГИ И ЗАШТИТЕТЕ СЕ ОД ФИШИНГ НАПАДИТЕ !!!

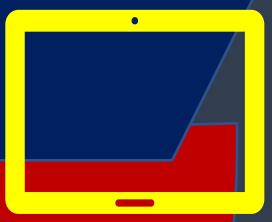
Чекори за справување со сајбер инциденти!

Редовно правете заштитна копија од Вашите податоци и чувајте ги на безбедно место. За проценка на ризиците, повеќе информации можете да најдете со пребарување на Интернет. Препорачливо е да имате своја Процедура за управување со ИТ системите кои Ви се најпотребни при работењето. Такви се на пример системите за е-пошта и Вашата веб- страница, сметководството и архивското работење. Предвидете План за инциденти, односно размислете што би се случило доколку одеднаш немате пристап до овие системи или податоци. Направете листа на системи кои се подредени според приоритет, базирана на разбирање на тоа што е важно за да нема прекин во работењето се со цел да преземете соодветна заштита.

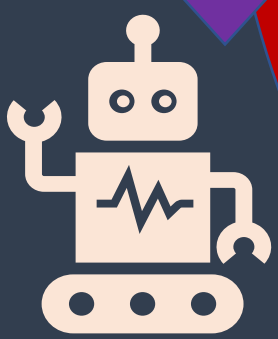
Сајбер-инцидентите како што се неовластениот пристап до ИТ системи и кражбата или уништувањето на податоци и средства, се сметаат за кривични дела. Секогаш чувајте ги сите информации за инцидентот кој се случил, како логови за пристап и променети датотеки. Не се двоумете да известите за инцидентот кој Ви се случил. Знајте дека известувањето и споделувањето на информации со други засегнати страни ќе спречи повторување на таков ист инцидент. Пријава на инцидент до MKD-CIRT можете да направите на следната интернет адреса: https://mkd-cirt.mk/prijava-na-incident/

Откако ќе се случи одреден сајбер инцидент, важно е да направите преглед на она што се случило и да научите од откриените грешки. Преземете активности со кои ќе ги надминете откриените недостатоци, а со тоа ќе ја намалите веројатноста за повторно случување на ваков сличен инцидент и воедно ќе ја зголемите Вашата безбедност.





Задолжително е да се провери активноста на антивирусната заштита, а доколку ова не можете да го направите сами, обратете се на стручно лице кој ќе направи ревизија на тоа што се случило. За надминување на одредени проблеми, упатства за истите можете да најдете со пребарување на Интернет. Решавање на инцидентот значи повторна достапност на услугите, системите и податоците кои биле недостапни. Во зависност од видот на инцидентот можете да реагирате со чистење на заразени уреди, промена на лозинки, враќање на податоци од “backup”, инсталација на надградби и ажурирање на оперативни системи и апликации.



Знаци кои укажуваат на сајбер-инциденти

Ако компјутерите работат бавно, ако добивате пораки по е-пошта со уцена, кога не можете да пристапите до своите сметки и податоци или ако други луѓе Ве известуваат дека добиваат чудни пораки по е-пошта испратени од Вашите адреси.

Доколку се сомневате дека се случил сајбер-инцидент, следен чекор е да откриете што точно се случило. Во тоа може да Ви помогнат одговорите на прашањата кој и кога пријавил проблем, кои услуги и системи се опфатени со проблемот, кои податоци се избришани или недостапни (доколку ги има), кога за прв пат сте дознале за проблемот и кои делови од работењето се опфатени.

ВНИМАВАЈТЕ НА ЗНАЦИ !!!

БЕЗБЕДНА УПОТРЕБА

Голема е веројатноста, Вашите уреди (таблетите, персоналните компјутери или телефоните) да бидат украдени или истите да ги загубите. Поголемиот дел од уредите вклучуваат бесплатни веб-базирани алатки, кои во случај на губење можете да ги користите за следење на нивната локација, далечинско заклучување и бришење на податоците. Овие алатки може да ги користите за Вашите лични и службени уреди.

Користењето на посложена лозинка наспроти едноставна што лесно може да се погоди или пак да се извлече од Вашиот профил на социјалните мрежи, може да ги спречи хакерите да пристапат до Вашиот уред и податоци.

Надградувајте ги Вашите уреди редовно и истите секогаш нека бидат поставени на автоматско ажурирање. Производителите на оперативните системи како Android или iOS редовно објавуваат безбедносни надградби. Кога производителот на уредот ќе престане со поддршка и издавање на нови безбедносни надградби за одреден тип на уреди, во тој случај размислете за нивна замена со нови.

Апликациите кои ги имате инсталирано на Вашите уреди, треба редовно да бидат ажурирани со “patches” од производителите на софтверот. Оваа постапка овозможува додавање на нови функции и поправка на сите безбедносни ранливости што претходно биле детектирани.

Користењето на јавни или отворени Wi-Fi локации како тие во хотелите и ресторaните не се препорачува, бидејќи не знаете кој го контролира хотспотот. Доколку се поврзете на вакви локации, се доведувате во ризик до Вашите податоци да му овозможите пристап на непожелен надворешен субјект. Затоа како мерка на претпазливост користете ја Вашата 3G или 4G мобилна мрежа, која веќе има вградено безбедносни мерки. Секогаш користете ја опцијата „tethering “(за вашите други уреди, како лаптопи, да ја споделуваат Вашата 3G/4G конекција од мобилниот телефон), или USB-уред за безжично поврзување “dongle” од Вашата мобилна мрежа.

БИДИ БЕЗБЕДЕН !!!

ЧЕКОРИ ЗА ПРАВИЛНО КОРИСТЕЊЕ НА ЛОЗИНКИ

2FA бара два различни методи за да го „докаже “Вашиот идентитет пред да можете да користите одредена услуга, обично лозинка плус уште еден метод. Ова може да биде код кој е испратен до Вашиот паметен телефон (или код што е генериран од токен за банкарски услуги) што мора да го внесете покрај Вашата лозинка, за дополнително зголемување на безбедноста.

“PASSWORD MANAGER” е компјутерска програма што им овозможува на корисниците да ги чуваат, генерираат и управуваат со своите лозинки за локални апликации или мрежни услуги. “PASSWORD MANAGER” помага во генерирање и враќање на комплексни лозинки, зачувување на такви лозинки во шифрирана база на податоци или нивно пресметување на претходно барање.

За секој уред (компјутер, телефон, таблет или онлајн услуга), користете лозинка за ограничување на пристапот до овие уреди и услуги доколку истите содржат чувствителни податоци. Покрај лозинките, дополнителна заштита може да обезбеди користењето на PIN (Personal Identification Number), скен од прст или на лице и енкриптирање или шифрирање на податоците како начини за потврдување на автентичноста.

Вообичаена пракса е лозинките да се менуваат доколку се сомневате дека се загрозени деталите за најава при користење на одредена услуга. Запишувајте ги лозинките за важните сметки (како што е е-пошта и банкарство) и истите чувајте ги безбедно (но не на самите уреди). Тие треба да се доволно сложени, на пример со користење на фраза од три случајни зборови и вкупна должина од најмалку 8 карактери, како и да содржат карактери од следните групи: големи букви, мали букви, броеви и специјални знаци.

Покрај лозинките, дополнителна заштита може да обезбеди користењето на PIN (Personal Identification Number), скен од прст или на лице и енкриптирање или шифрирање на податоците како начини за потврдување на автентичноста.

Утврдената пракса при креирање на лозинката е нејзината должина да се состои од најмалку 8 карактери, да содржи три од четирите групи на знаци (мали букви, големи букви, броеви и специјални знаци).

Секогаш менувајте ги стандардните лозинки поставени од производителите што доаѓаат со сите уреди (паметните телефони, лаптопите, мрежните насочувачи и други видови на активна компјутерска и мрежна опрема). Редовно правете проверка на уредите и апликациите за тоа дали е направена промена на стандардните лозинки.

“PASSWORD MANAGER” подразбира локално инсталирани софтверски апликации, пристап до мрежни услуги преку веб-портали и хардверски уреди на локален пристап, кои служат како клучеви.