Përdorni INTERNETIN në mënyrë të sigurtë!

ASNJËHERË MOS HAPNI MESAZHE NGA DËRGUES TË PANJOHUR!

Këto mesazhe mund të përmbajnë viruse ose dikush tenton që t'Ju merr të dhënat e Juaja!

www.sec.gov.mk

Përdorni INTERNETIN në mënyrë të sigurtë!

MBANI TË DHËNAT E JUAJA PERSONALE NË VENDNDODHJE TË SIGURTË !

On line mos i ndani informatat në vijim:

- Emrin dhe mbiemrin Tuaj
- Fotot e Juaja
- Numrin Tuaj të telefonit
- Adresën Tuaj
- NUAQ të Juaj
- Llogarinë Tuaj të transaksionit
- Fjalëkalimet e Juaja

Përse???

Ngase sulmuesit kibernetik mund të keqpërdorin të gjitha informatat!

www.sec.gov.mk

Mbrojtja më e mirë nga sulmet kibernetike!

Bërja e automatizuar e kopjeve kursen kohë dhe garanton se çdoherë do të keni versionet më të reja të dokumenteve të Juaja.

Ruajtja e këtillë lehtë instalohet dhe e njëjta është e pranueshme në raport me çmimin duke pasur parasysh mbrojtjen e të dhënave të rëndësishme që e ofrojnë.

Këtë informatë përdoreni si një kriter shtesë për përzgjedhje të mënyrës së ruajtjes së një kopje rezervë nga të dhënat e Juaja.

Ruajtja e të dhënave në re „cloud storage“ domethënë se ofruesi i shërbimeve i ruan të dhënat e Juaja në infrastrukturën e tij të qasshme përmes Internetit. Të dhënat e juaja në atë mënyrë janë fizikisht të ndara nga vendndodhja Juaj dhe sigurohet ruajtje e të njëjtave, si dhe shërbime interneti pa instaluar hardver të shtrenjë.

Përderisa nuk përdorni server të Juaj personal për e-postë, mesazhet e Juaja elektronike tashmë janë „cloud storage“. Kryesisht, kontaktet që janë të regjistruara në celularin Tuaj automatikisht regjistron në re, njësoj si edhe kopja nga komunikimi përmes aplikacioneve Viber, Messenger dhe WhatsApp.

Përfitim nga shërbimi i këtillë për ruajtje është niveli i lartë i qasjes që ofruesve të shërbimeve për ruajtjen e të dhënave në re ofron hapësirë falas, por të kufizuar për ruajtjen e të dhënave, me çfarë e njëjta me pagesë shtesë mund të zmadhohet.

Edhe pse kopja Ju është e regjistruar në një disk tjetër të jashtëm, kompjuter të posaçëm ose USB-pajisje, kufizoni qasjen deri te ato ashtu që: persona të tjerë të mos kenë qasje deri te ato kopje rezervë; nuk janë të ndërlidhura midis veti pajisjet në të cilat janë të regjistruara (fizikisht ose përmes rrjetit lokal kompjuterik) në pajisjen në të cilën gjenden të dhënat origjinale.

Përderisa këto pajisje në të cilat janë të regjistruara kopjet rezervë janë vazhdimisht të lidhura në rrjetin lokal kompjuterik, gjatë infektimit, i njëjti mund të transferohet edhe në pajisjen për ruajtje. Kjo domethënë se çdo kopje e tillë rezervë mund të jetë e infektuar, duke Ju lënë pa kopje rezervë nga e cila do të mund të ktheni të dhënat origjinale.

Me qëllim të sigurisë më të madhe, duhet që kopjet rezervë t'i ruani në një vendndodhje tjetër, ashtu që në rast të një fatkeqësie elementare ose vjedhjeje, nuk do e humbni kopjen rezervë. Andaj, ruajtja në re "cloud storage" janë mënyra më ekonomike dhe më efikase për t'u arritur ky qëllim.

Identifikoni të dhënat që janë të rëndësishme për punën Tuaj dhe pa të cilat nuk mund të funksiononi (fatura, fletë dorëzimi dhe dokumente të tjera me të dhëna financiare, personale dhe sensitive).

Çdoherë bëni kopje nga këto të dhëna në një pajisje të jashtme dhe të njëjtën e ruani në një vend të sigurtë larg pajisjeve në të cilat janë të regjistruara të dhënat dhe dokumentet origjinale.

Mbrojtje nga softver malicioz ose “malware”!

Antivirusi është i përfshirë falas në pajisjet e popullarizuara operative dhe i njëjti përdoret tek të gjithë kompjuterët, laptopët, tabletët dhe celularët e mençur. Ashtu, kompjuteri Juaj ose celulari tashmë kanë mbrojtje softverkike antivirus, mirëpo e njëjta zakonisht është falas dhe ofron mbrojtje minimale.
Andaj, mendoni me kujdes për furnizimin e mbrojtjes së licencuar komerciale antivirus, që do ta përmirëson sigurinë e pajisjeve që i përdorni.

Aplikacioni i dyshimtë është formë e mashtrimit me identitet e cila përfshin një mashtrues që ka aplikuar për llogari të re për shërbime ose produkte, dhe gjatë kësaj për të njëjtat përdor identitet falco.
Për instalimin e aplikacioneve nga Interneti në pajisjet duhet të përdoren ekskluzivisht aplikacione nga e-shitoret të cilat janë të miratuara nga prodhuesi i pajisjes operative (për celularët dhe tabletët këto janë Google Play Store ose Apple App Store).
Këto aplikacione kontrollohen nga ana e prodhuesit me qëllim që të sigurojnë nivel të caktuar të mbrojtjes.
Andaj duhet të përmbaheni nga instalimi i aplikacioneve nga palë të treta, nga burime të panjohura ose softverë piraterik, ngase të njëjtat nuk janë të kontrolluara dhe kryesisht përmbajnë viruse.

Softveri i të gjithë kompjuterëve, laptopëve, celularëve dhe tabletëve duhet çdoherë të jetë i përditësuar me versionet më të reja nga prodhuesit dhe furnizuesit e softverit dhe hardverit.
Zbatimi i përditësimit të pajisjes informatike është një nga punët më të rëndësishme që duhet të bëni për të përmirësuar sigurinë.

Muri mbrojtës “firewall” është pajisje rrjeti e sigurisë e cila e ndjek trafikun hyrës të rrjetit dhe vendos nëse do të lejojë ose do të bllokojë një trafik specifik në bazë të një pakoje të përkufizuar të procedurave të sigurisë. Muri mbrojtës është linja e parë e mbrojtjes në sigurinë e rrjetëzuar dhe krijon zonë të sigurtë midis rrjetit Tuaj kompjuterik dhe rrjeteve të jashtme siç është Interneti.
Të gjitha pajisjet operative përfshijnë mur falas të mbrojtjes, i cili është i lehtë për aktivizim dhe rekomandohet që i njëjti të jetë vazhdimisht i kyçur.

Pjisjet e këtilla për ruajtje kryesisht përdoren për transfer të të dhënave midis organizatave dhe njerëzve. Përderisa vetëm një përdorues i pakujdesshëm pa qëllim kyç një pajisje memorie, mund të bëjë dëm të madh.

KUJDES !!!

PHISHING SULM

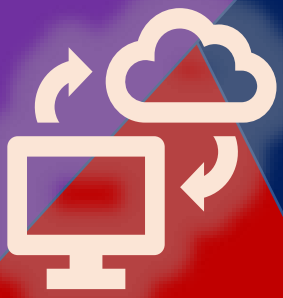
DALLONI DHE MBROHUNI NGA PHISHING SULMET !!!

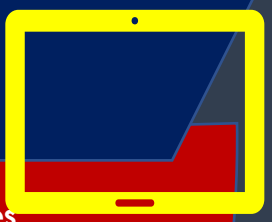
Hapa për ballafaqim me incidente kibernetike!

Rregullisht bëni kopje mbrojtëse të të dhënave të Juaja dhe ruani në një vend të sigurtë. Për vlerësim të rreziqeve, më tepër informata mund të gjeni duke shfletuar Internetin. Është e rekomandueshme që të keni Procedurë të juaj për menaxhim me IT sistemet të cilat Ju janë më se të nevojshme gjatë punës. Të tilla janë për shembull sistemet për e-postë dhe dhe faqja Juaj e internetit, kontabiliteti dhe puna arkivore. Parashikoni Plan për incidente, respektivisht mendoni se çfarë do ndodhte përderisa për një çast nuk keni qasje deri te këto sisteme ose të dhëna. Bëni një listë të sistemeve të cilat janë të renditura sipas përparësisë, e bazuar në kuptimin e asaj çfarë është e rëndësishme për të mos pasur ndërprerje të punës, e tëra me qëllim që të ndërmerrni mbrojtje përkatëse.

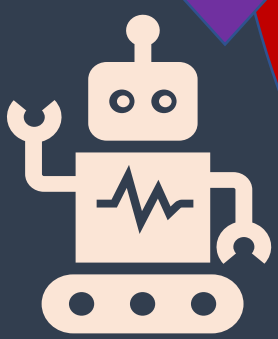
Incidentet kibernetike siç janë qasja e joautorizuar në IT sistemet dhe vjedhja ose shkatërrimi i të dhënave dhe mjeteve, konsiderohen vepra penale. Çdoherë ruani të gjitha informatat për incidentin i cili ka ndodhur, si lajmërime për qasje dhe skedarë të ndryshuar. Mos hezitoni të raportoni për incidentin i cili Ju ka ndodhur. Të dini se raportimi dhe ndarja e informatave me palë të tjera të interesit do të parandalojë përsëritjen e një incidenti të njëjtë të tillë. Denoncimin e incidentit deri te MKD-CIRT mund t'a bëni në faqen e internetit në vijim: https://mkd-cirt.mk/prijava-na-incident/

Pasi që do të ndodh një incident i caktuar kibernetik, me rëndësi është të bëni pasqyrë të asaj çfarë ka ndodhur dhe të mësoni nga gabimet e zbuluara. Ndërmerrni aktivitete me të cilat do ti tejkaloni mangësitë e zbuluara, e me atë do ta zvogëloni probabilitetin për rindodhi të një incidenti të ngjajshëm të këtillë dhe njëherit do ta zmadhoni sigurinë Tuaj.





Është e detyrueshme të kontrollohet aktiviteti i mbrojtjes antivirus, e nëse këtë nuk mund t'a bëni vetë, i drejtoheni një personi profesional i cili do të kryejë revizion të asaj se çfarë ka ndodhur. Për tejkalimin e problemeve të caktuara, udhëzime për të njëjtat mund të gjeni duke shfletuar Internetin. Zgjidhja e incidentit nënkupton riqasje në shërbimet, sistemet dhe qasjet të cilat kanë qenë të paqasshme. Varësisht nga lloji i incidentit mund të reagoni me pastrimin e pajisjeve të infektuara, ndryshim të fjalëkalimeve, kthimin e të dhënave nga "backup"-i, instalimin e mbindërtimeve dhe përditësimin e sistemeve dhe aplikacioneve operative.



Shenja të cilat bëjnë me dije për incidente kibernetike

Nëse kompjuterët punojnë të ngadalësuar, nëse fitoni mesazhe me shantazhim përmes e-postës, kur nuk mund të qaseni deri te llogaritë dhe të dhënat e juaja ose nëse njerëz të tjerë Ju njoftojnë se janë duke fituar mesazhe të çuditshme përmes e-postës të dërguara nga adresat e Juaja.

Përderisa dyshoni se ka ndodhur një incident kibernetik, hapi i rradhës është të zbuloni se çfarë saktësisht ka ndodhur. Në atë mund t'Ju ndihmojnë përgjigjet në pyetjet kush dhe kur ka paraqitur problem, cilat shërbime dhe sisteme janë të përfshira me problemin, cilat të dhëna janë fshirë ose të paqasshme (përderisa ka), kur për herë të parë keni kuptuar për problemin dhe cilat pjesë të punës janë të përfshira.

VINI RE SHENJAT !!!

PËRDORIMI I SIGURTË

Është probabilitet i madh, që pajisjet e Juaja (tabletët, kompjuterët personal ose telefonat) të vidhen ose të njëjtat t'i humbni. Pjesa më e madhe e pajisjeve përfshijnë vegla falas të bazuara në internet, të cilat në rast të humbjes mund t'i përdorni për ndjekjen e vendndodhjes së tyre, mbyllje dhe fshirje nga distanca e të dhënave. Këto vegla mund t'i përdorni për pajisjet e Juaja personale dhe zyrtare.

Përdorimi i një fjalëkalimi më të ndërlikuar kundrejt një më të thjeshtë që lehtë mund të qëllohet ose përsëri të nxirret nga profili Juaj në rrjetet sociale, mund të parandalohet që hakerët të qasen deri te pajisja dhe të dhënat e Juaja.

Mbindërtoni pajisjet e Juaja rregullisht dhe të njëjtat le të jenë çdoherë të vendosura në përditësim automatik. Prodhuesit e sistemeve operative siç janë Android ose iOS rregullisht publikojnë mbindërtime të sigurisë. Kur prodhuesi i pajisjes do të pushojë me mbështetje dhe lëshim të mbindërtimeve të reja të sigurisë për një lloj të caktuar të pajisjeve, në atë rast mendoni për zëvendësimin e tyre me të reja.

Aplikacionet të cilat i keni instaluar në pajisjet e Juaja, duhet rregullisht të jenë të përditësuara me "patches" nga prodhuesit e softverit. Kjo procedurë mundëson shtimin e funksioneve të reja dhe riparim të të gjitha cenueshmërive të sigurisë që më parë kanë qenë të zbuluara.

Përdorimi i Wi-Fi vendndodhjeve publike ose të hapura sikur ato në hotelet dhe restaurantet nuk rekomandohet, sepse nuk e dini kush e kontrollon hotspot-in. Përderisa lidheni në vendndodhje të këtilla, do të sillni veten në rrezik që t'i mundësoni qasje deri te të dhënat e Juaja një subjekti të padëshiruar të jashtëm. Andaj si masë të kujdesit përdorni rrjetin Tuaj celular 3G ose 4G, e cila tashmë ka inkorporuar masa të sigurisë. Çdoherë përdorni opsionin „tethering" (për pajisjet tjera të juaja, si laptopë, të ndajnë lidhjen Tuaj 3G/4G nga celulari), ose USB-pajisje për lidhje wireless "dongle" nga rrjeti Juaj celular.

QËNDRO I SIGURTË !!!

HAPA PËR PËRDORIM TË SAKTË TË FJALËKALIMEVE

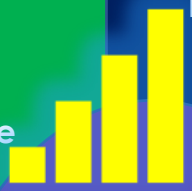
2FA kërkon dy metoda të ndryshme për të „dëshmuar“ identitetin Tuaj përpara se të mund të përdorni shërbim të caktuar, zakonisht fjalëkalim plus edhe një metodë. Kjo mund të jetë një kod i cili është i dërguar deri te telefoni Juaj i mençur (ose kod i cili është i gjeneruar nga tokeni për shërbime bankare) që duhet t'a futni krahas fjalëkalimit Tuaj, për rritje shtesë të sigurisë.

Praktikë e zakonshme është që fjalëkalimet të ndrrohen nëse dyshoni se janë të rrezikuara detajet për lajmërim gjatë përdorimit të një shërbimi të caktuar. I shkruani fjalëkalimet për llogaritë me rëndësi (siç janë e-posta dhe bankimi) dhe të njëjtat i ruani në vend të sigurtë (por jo në vetë pajisjet). Ato duhet të jenë mjaft të ndërlikuara, për shembull me përdorimin e frazës nga tre fjalë të rëndomta dhe gjatësi totale prej të paktën 8 karaktere, si dhe të përmbajnë karaktere nga grupet në vijim: shkronja të mëdha, shkronja të vogla, numra dhe shenja speciale.

"PASSWORD MANAGER" është program kompjuterik i cili u mundëson përdoruesve të ruajnë, gjenerojnë dhe menaxhojnë me fjalëkalimet e veta për aplikacione lokale ose shërbime rrjeti. "PASSWORD MANAGER" ndihmon në gjenerimin dhe kthimin e fjalëkalimeve të ndërlikuara, ruajtjen e fjalëkalimeve të tilla në bazë të shifruar të të dhënave ose përllogaritje e tyre me kërkesë paraprake.

Krahas fjalëkalimeve, mbrojtje shtesë mund të sigurojë përdorimi i PIN-it (Personal Identification Number), skanim i gishtit ose i fytyrës dhe enkriptim ose shifrim i të dhënave si mënyra për konfirmimin e autenticitetit.

Për çdo pajisje (kompjuter, telefon, tablet ose online shërbim), përdorni fjalëkalim për kufizim të qasjes deri te këto pajisje dhe shërbime përderisa të njëjtat përmbajnë të dhëna të ndjeshme. Krahas fjalëkalimeve, mbrojtje shtesë mund të sigurojë përdorimin e PIN-it (Personal Identification Number), skanim i gishtit ose i fytyrës dhe enkriptim ose shifrim i të dhënave si mënyra për konfirmimin e autenticitetit.



Praktika e përcaktuar gjatë krijimit të fjalëkalimit është që gjatësia e tij të përbëhet nga të paktën 8 karaktere, të përmbajë tre nga katër grupet e shenjave (shkronja të vogla, shkronja të mëdha, numra dhe shenja speciale)

Çdoherë ndrroni fjalëkalimet standarde të vendosura nga prodhuesit që vijnë me të gjitha pajisjet (telefonët e mençur, laptopët, drejtues të rrjetëzuar dhe lloje të tjera të pajisjes aktive kompjuterike dhe të rrjetit). Rregullisht bëni kontrollim të pajisjeve dhe aplikacioneve për atë nëse është bërë ndryshim i fjalëkalimeve standarde.

"PASSWORD MENAXHER " do të thotë aplikacione softuerike të instaluara në vend, qasje në shërbimet e rrjetit përmes portaleve të internetit dhe pajisjeve hardware në akcesin lokal, të cilat shërbejnë si çelës).