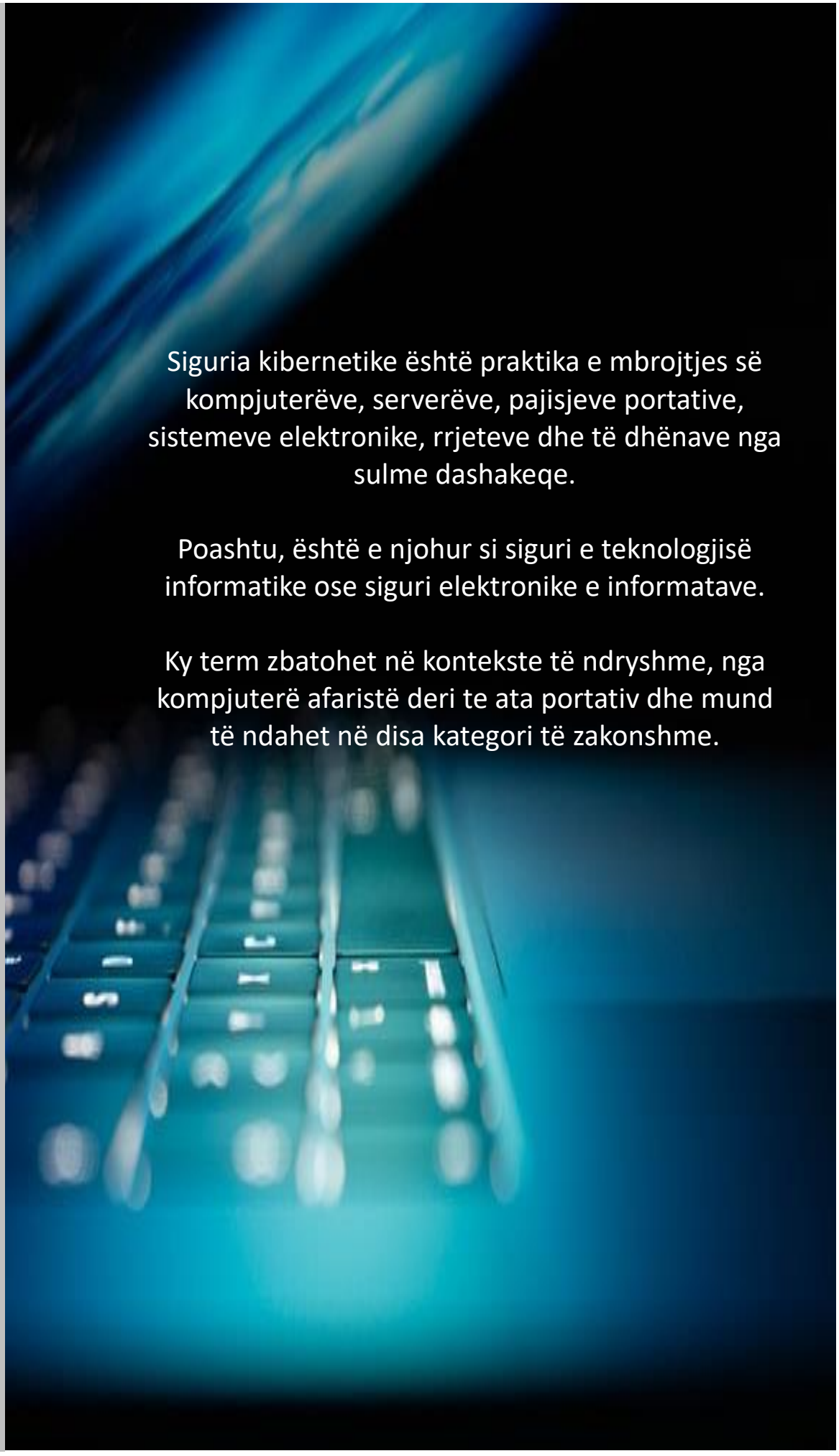
EDUKOHU PËR SIGURI KIBERNETIKEзаштитете ги

Mbroni on-line llogaritë e Juaja

Komisioni I letrave me vlerë i
Republikës së Maqedonisë së Veriut

Tetor 2021

ÇFARË ËSHTË SIGURIA KIBERNETIKE



Siguria kibernetike është praktika e mbrojtjes së kompjuterëve, serverëve, pajisjeve portative, sistemeve elektronike, rrjeteve dhe të dhënave nga sulme dashakeqe.

Poashtu, është e njohur si siguri e teknologjisë informatike ose siguri elektronike e informatave.

Ky term zbatohet në kontekste të ndryshme, nga kompjuterë afaristë deri te ata portativ dhe mund të ndahet në disa kategori të zakonshme.

ÇFARË ËSHTË SIGURIA KIBERNETIKE

Siguria e rrjetit është praktikë e sigurimit të rrjetit kompjuterik nga ndërhyrës, pa dallim nëse janë sulmues të shënjesuar ose softver malicioz oportunist.

Siguria e aplikacionit përqëndrohet në ruajtjen e softverit dhe pajisjeve pa kërcënime. Aplikacioni i kompromituar mund të sigurojë qasje deri te të dhënat të cilat janë të dizajnuara për t'i mbrojtur.

Siguria e infomatave i mbron integritetin dhe privatësinë e të dhënave edhe në procesin e ruajtjes dhe të tranzitit.

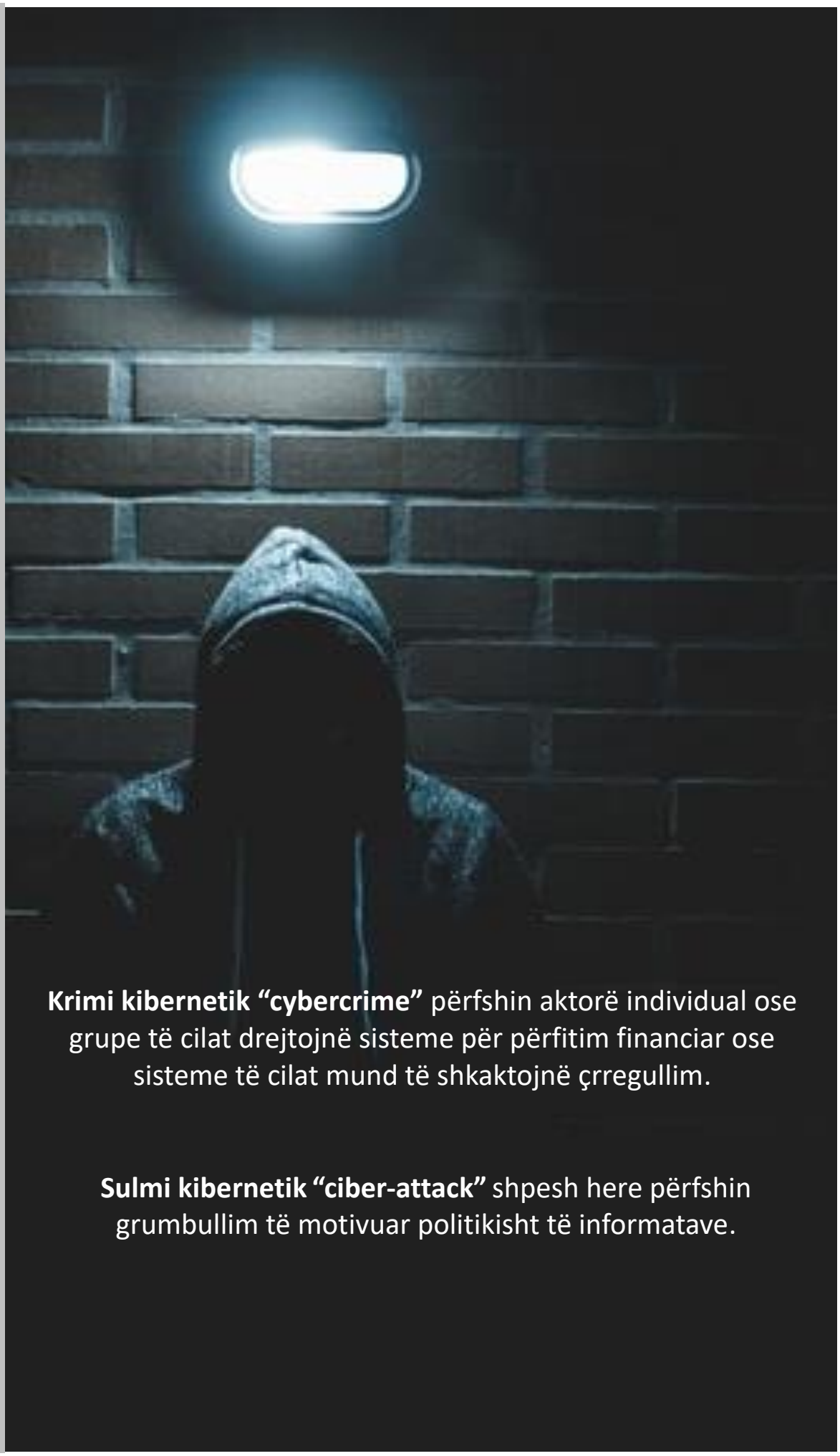
Siguria operative i përfshin proceset dhe vendimet për menaxhim dhe mbrojtje të qasjes deri te të dhënat. Këtu nënkuptohen lejet që i kanë përdoruesit gjatë qasjes deri te rrjeti dhe procedurat që përcaktojnë se si dhe ku mund të mbahen ose ndahen të dhënat.

ÇFARË ËSHTË SIGURIA KIBERNETIKE

Menaxhimi me situatë të paparashikueshme dhe vazhdimësi në punën si dhe politikat për ripërtrirje gjatë situatave të paparashikueshme diktojnë se si institucioni do ti kthejë operacionet dhe informatat në të njëjtin kapacitet të punës, si para situatës së ngjarë të paparashikueshme.

Edukimi për përdorues përfundimtar i referohet faktorit më të paparashikueshëm për siguri kibernetike: **NJERIU**. Gjithësecili që nuk i ndjek udhëzimet e procedurave të sigurisë mundet rastësisht të transferojë virus në një sistem të sigurisë. Informimi paraprak i përdoruesve që të fshijnë shtojca të dyshimta për e-postë, të shmangin kyçje në USB-pajisje të joidentifikuara dhe praktika të tjera shumë të rëndësishme gjatë menaxhimit me teknologjinë informatike janë me rëndësi jetike për sigurinë e çdo institucioni.

LLOJET E KËRCËNIMEVE KIBERNETIKE



Krimi kibernetik “cybercrime” përfshin aktorë individual ose grupe të cilat drejtojnë sisteme për përfitim financiar ose sisteme të cilat mund të shkaktojnë çrregullim.

Sulmi kibernetik “ciber-attack” shpesh here përfshin grumbullim të motivuar politikisht të informatave.

SUGJERIME PËR MBROJTJE NGA KËRCËNIME KIBERNETIKE

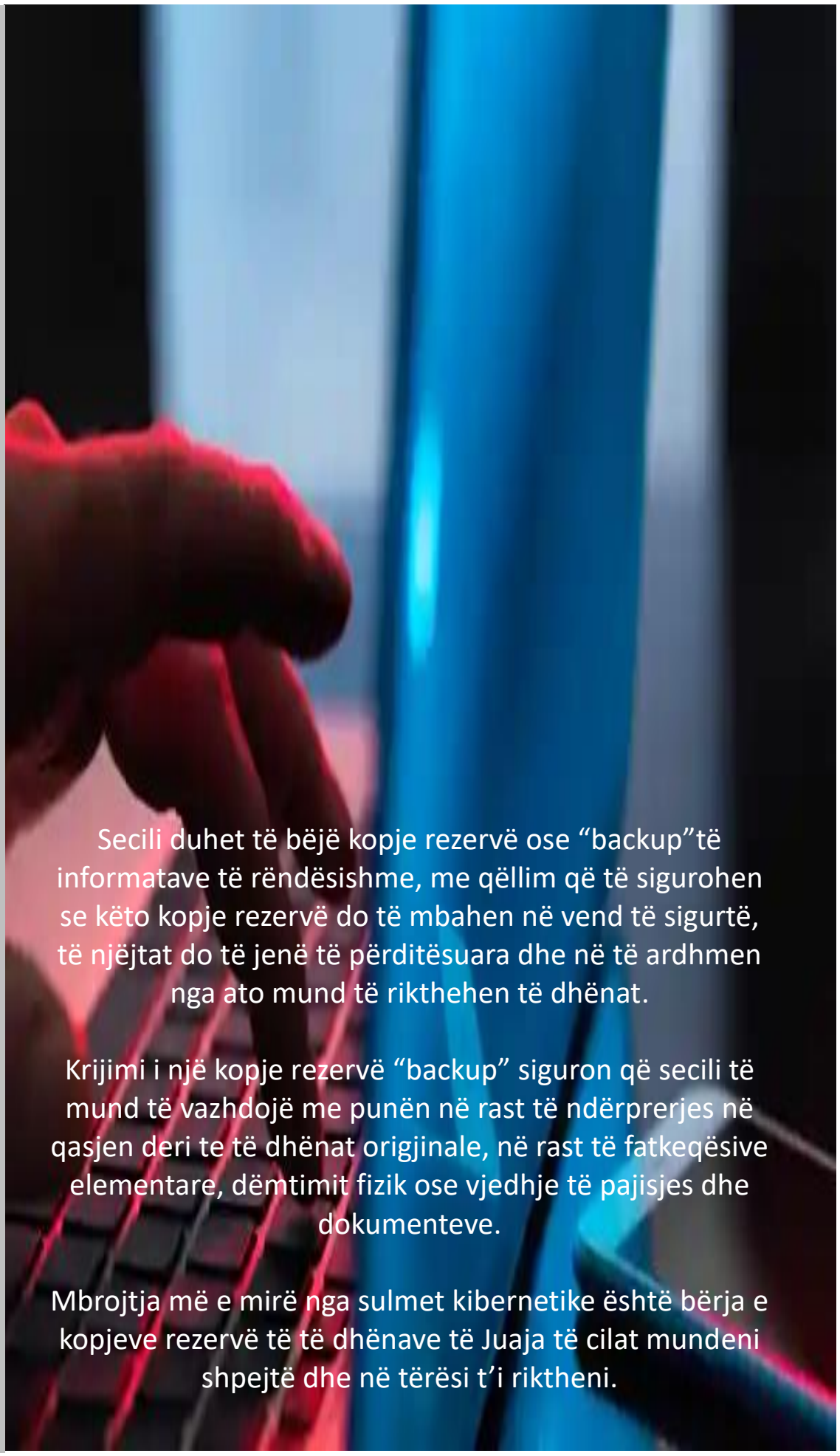
Komisioni i letrave me vlerë i
Republikës së Maqedonisë së Veriut

Tetor 2021

KËRCËNIME KIBERNETIKE

Kërcënimet kibernetike bëhen më të sofistikuara dhe Ju nuk mund të ndiqni çdo hap që e bëjnë, mirëpo përpiquni që të mos keni asnjë ndërveprim me diçka që është dashakeqëse.

ÇDOHERË BËNI KOPJE OSE “ BACKUP” TË TË DHËNAVE TË JUAJA



Secili duhet të bëjë kopje rezervë ose “backup”të informatave të rëndësishme, me qëllim që të sigurohen se këto kopje rezervë do të mbahen në vend të sigurtë, të njëjtat do të jenë të përditësuara dhe në të ardhmen nga ato mund të rikthehen të dhënat.

Krijimi i një kopje rezervë “backup” siguron që secili të mund të vazhdojë me punën në rast të ndërprerjes në qasjen deri te të dhënat origjinale, në rast të fatkeqësive elementare, dëmtimit fizik ose vjedhje të pajisjes dhe dokumenteve.

Mbrojtja më e mirë nga sulmet kibernetike është bërja e kopjeve rezervë të të dhënave të Juaja të cilat mundeni shpejtë dhe në tërësi t’i riktheni.

ÇDOHERË BËNI KOPJE OSE “ BACKUP” TË TË DHËNAVE TË JUAJA

HAPI 1: BËNI SELEKTIM TË TË DHËNAVE PËR TË CILAT DUHET TË BËNI “BACKUP”

HAPI 2: MBANI KOPJEN REZERVË “BACKUP”-in MË LARG ORIGJINALIT

HAPI 3: RUAJTJA E TË DHËNAVE NË RE DHE/OSE “CLOUD STORAGE”

HAPI 4: BËRJA E KOPJES REZERVË OSE “BACKUP” I TË DHËNAVE LE TË JETË AKTIVITET I JUAJ I PËRDITSHËM OSE “CLOUD STORAGE”

MBROHUNI NGA SOFTVERI MALICIOZ OSE “ MALWARE

Softveri malicioz “**malware**” është softver të cilin e ka krijuar një haker kibernetik për të çrregulluar ose dëmtuar kompjuterin përmes fshirjes së të dhënave të rëndësishme, keqpërdorimin e pajisjeve të Juaja dhe shantazhim me mbylljen ose shifrimin e dokumenteve, paraqitje të viruseve dhe programeve që vetëreplikohen dhe e infektojnë softverin legjitim.

HAPI 1: PËRDORNI SOFTVER ANTIVIRUS PËR MBROJTJEN E PAJISJEVE

HAPI 2: AKTIVIZONI MUR MBROJTJEJE OSE “FIREWALL”

HAPI 3: KENI KUJDES NË APLIKACIONE TË DYSHIMTA

HAPI 4: MIRËMBANI PAJISJEN INFORMATIKE

HAPI 5: KONTROLLONI DISQET, USB-pajisjet DHE KARTELAT MEMORIKE

PHISHING SULM

Komisioni I letrave me vlerë i
Republikës së Maqedonisë së Veriut

Tetor 2021

KENI KUJDES NGA PHISHING SULM

Phishing sulm është sulm nga inxheneringu social i cili shpesh përdoret për vjedhje të të dhënave të përdoruesve, përfshirë edhe ingerencat për lajmërim dhe numrat e kartelave kreditore. Kjo ndodh kur sulmuesi, i maskuar si një subjekt i besueshëm e përgënjeshtron viktimën që të hap e-postën, instant mesazhin ose mesazhin tekstual. Më pas, pranuesi është i mashtruar për të klikuar në lidhjen dashakeqe, që mund të sjell deri te instalimi i një softveri malicioz, ngrirje e sistemit si pjesë e sulmit ose zbulim i informatave të ndjeshme.

PËR DALLIMIN E PHISHING SULMEVE

Disa sulmues do të tentojnë që të krijojnë mesazhe të cilat në shikim të parë janë shumë të ngjajshme me mesazhet zyrtare me kyçjen në logot dhe grafikat e ngjajshme me të Juajat ose të institucioneve me të cilat bashkëpunoni, andaj me kujdes dhe në hollësi shqyrtoni mesazhin për të dalluar shenjat nga falsifikimi.

Përderisa në titullin e mesazhit Ju drejtohen me adresën Tuaj për e-postë ose shkruan „i nderuar“, „kolegë“ ose përdoret një term i ngjajshëm gjenerik, kjo mund të jetë shenjë se dërguesi nuk Ju njeh dhe mesazhi mund të jetë i dërguar për phishing-mashtrim.

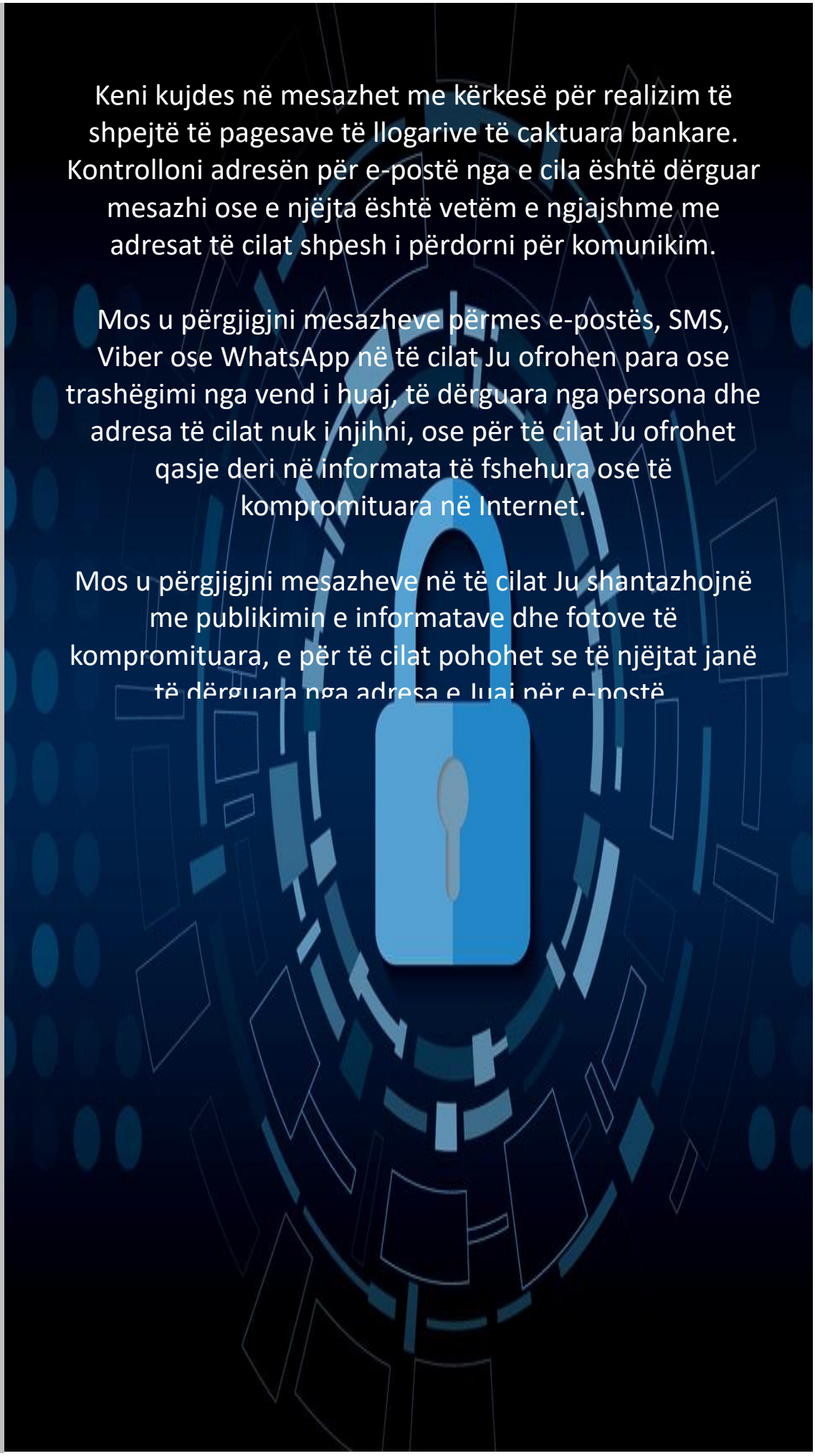
Të dyshoni në mesazhet në tekstin e të cilave nga Ju kërkohet që të veproni shpejtë ose hollësi nga tipi „dërgoni mesazh brenda 24 orë“ ose „Jeni fitues i ..., klikoni menjëherë këtu“.

SHENJA PËR DALLIMIN E PHISHING SULMEVE

Keni kujdes në mesazhet me kërkesë për realizim të shpejtë të pagesave të llogarive të caktuara bankare. Kontrolloni adresën për e-postë nga e cila është dërguar mesazhi ose e njëjta është vetëm e ngjajshme me adresat të cilat shpesh i përdorni për komunikim.

Mos u përgjigjni mesazheve përmes e-postës, SMS, Viber ose WhatsApp në të cilat Ju ofrohen para ose trashëgimi nga vend i huaj, të dërguara nga persona dhe adresa të cilat nuk i njihni, ose për të cilat Ju ofrohet qasje deri në informata të fshehura ose të kompromituara në Internet.

Mos u përgjigjni mesazheve në të cilat Ju shantazhojnë me publikimin e informatave dhe fotove të kompromituara, e për të cilat pohohet se të njëjtat janë të dërguara nga adresa e Juaj për e-postë



KRIJIMI DHE MENAXHIMI ME FJALËKALIME QASJA DHE PËRDORIMI I SAKTË I PAJISJEVE

Komisioni i letrave me vlerë i
Republikës së Maqedonisë së Veriut

Tetor 2021

HAPA PËR PËRDORIM TË SAKTË TË FJALËKALIMEVE

Përdorimi i fjalëkalimeve është me rëndësi të madhe si mbrojtje primare. Me përdorimin e fjalëkalimeve sigurohet niveli më i ultë i mbrojtjes së qasjes deri te të dhënat e juaja, parandalohet qasja e joautorizuar dhe përdorimi i të njëjtave. Pajisjet (laptopë, tableta dhe telefona të mençur) mund të përmbajnë të dhënat e Juaja personale si dhe të dhëna të tjera të rëndësishme për Ju, si dhe hollësirat për on-line llogaritë në të cilat qaseni.

HAPI 1: VENDOSNI FJALËKALIM PËR QASJE DERI TE TË DHËNAT

HAPI 2: ÇDOHERË PËRDORNI FJALËKALIM TË FUQISHËM

HAPI 3: MENAXHIM ME FJALËKALIME “PASSWORD MANAGER”

HAPI 4: KONFIRMIM I AUTETINCITETIT ME DY FAKTORË “2FA-two factor authentications”

HAPI 5: PËRDORIM I MË TEPËR FJALËKALIMEVE

HAPI 6: NDRYSHIM I SHPESHTË I FJALËKALIMEVE

REKOMANDIME PËR PËRDORIM TË SIGURTË TË PAJISJEVE TË MENÇURA

Celularët dhe tabletët shpesh përdoren për përdorime dhe operacione nga më të ndryshmet, andaj për atë qëllim vijojnë hapa dhe rekomandime për përdorimin e tyre të sigurtë:

HAPI 1: QASJE E SIGURTË DERI TE PAJISJET

HAPI 2: PAJISJET E HUMBURA OSE TË VJEDHURA MUND T'I NDIQNI, MBYLLNI OSE T'I FSHINI

HAPI 3: MBINDËRTIM I RREGULLT DHE NË KOHË I PAJISJEVE HAPI

4: PËRDITËSIM I RREGULLT DHE NË KOHË I APLIKACIONEVE

HAPI 5: MOS U LIDHNI NË WI-FI VENDNDODHJE TË PANJOHURA

INCIDENTE TË NDRYSHME KIBERNETIKE

Incident kibernetik është qasje e joautorizuar ose tentim për qasje në sistemet IT të një institucioni. Këtu bëjnë pjesë sulmet malicioze të cilat kanë për qëllim vjedhjen e të dhënave, shantazhime ose keqpërdorimin e të dhënave të Juaja dhe të sistemeve IT ose shkaktim dëmi. Shembuj për incidente kibernetike janë mohimi i një shërbimi, sulm me të cilin pamundësohet qasja në shërbimet e Juaja dhe ndërpritet puna e Juaj normale rrjedhore. Arsye për incidente mund të jenë edhe dëmtime fizike, fatkeqësi natyrore ose vjedhje.

HAPI 1: ÇDOHERË TË JENI TË PËRGATITUR PËR INCIDENTE KIBERNETIKE

HAPI 2: IDENTIFIKIMI I NJË INCIDENTI TË RËNDOMTË KIBERNETIK

HAPI 3: NDËRPRERJE DHE ZGJIDHJE E INCIDENTIT KIBERNETIK

HAPI 4: NJOFTIM PËR INCIDENTIN KIBERNETIK DHE NDARJE E INFORMATAVE

HAPI 5: MËSONI NGA INCIDENTI KIBERNETIK