Udhëzues për Kërcënimet Kibernetike:

Identifikimi dhe lufta kundër rreziqeve për përdoruesit dhe qytetarët në sektorin publik dhe privat

Aleksandar Bratiç

Tetor 2022

DCAF Geneva Centre for Security Sector Governance

Rreth DCAF

DCAF – Qendra e Gjenevës për qeverisjen e sektorit të sigurisë i është përkushtuar përmirësimit të sigurisë së shteteve dhe njerëzve të tyre brenda kornizës së qeverisjes demokratike, sundimit të ligjit, respektimit të të drejtave të njeriut dhe barazisë gjinore. Që nga themelimi i tij në vitin 2000, DCAF ka kontribuar në krijimin e paqes dhe zhvillimit më të qëndrueshëm duke ndihmuar shtetet partnere dhe aktorët ndërkombëtarë që mbështesin këto shtete, për të përmirësuar qeverisjen e sektorit të tyre të sigurisë përmes reformave gjithëpërfshirëse dhe pjesëmarrëse. DCAF krijon produkte inovative të njohurive, promovon norma dhe praktika të mira, ofron këshilla ligjore dhe politikash dhe mbështet ndërtimin e kapaciteteve të palëve të interesuara në sektorin e sigurisë shtetërore dhe joshtetërore.

DCAF - Qendra e Gjenevës për qeverisjen e sektorit të sigurisë
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Gjenevë, Zvicër
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Design & layout: DTP studio

Ky publikim është hartuar në kuadër të projektit "Qeverisja e mirë në sigurinë kibernetike në Ballkanin Perëndimor" DCAF – Qendra e Gjenevës për Qeverisjen e Sektorit të Sigurisë, mbështetur nga Zyra për Punët e Jashtme, Komonuelthin dhe Zhvillimin e Britanisë së Madhe.

DCAF Geneva Centre for Security Sector Governance

Përmbajtje

Përmbledhje ekzekutive

Bota varet nga sistemet dhe teknologjitë digjitale në gati të gjitha aspektet e jetës së përditshme, në tregti, financa, komunikime, etj.

Në këtë botë digjitale, të dhënat tona personale luajnë një rol qendror. Prandaj, është e rëndësishme të kuptohet se të dhënat personale janë shumë më të vlefshme dhe shumë më të prekshme se kurrë më parë.

Nuk është e pazakontë të dëgjosh për thyerje të të dhënave dhe kërcënime kibernetike që prekin miliona përdorues, dhe për kompanitë dhe institucionet që luftojnë aktivisht për të mbrojtur të dhënat e tyre kundër praterisë dhe krimit kibernetik. Të gjithë ne luajmë një rol në sigurimin e hapësirave kibernetike. Siguria kibernetike është pra një domosdoshmëri jo vetëm për sistemet e mëdha në organizata, por për të gjithë ne, në kompjuterët tanë personalë, telefonat celularë dhe tabletat.

Kërcënimi kibernetik (ose kërcënimi i sigurisë kibernetike) është një veprim keqdashës që synon të vjedhë ose të dëmtojë të dhënat, ose të shkatërroj sistemet personale ose madje edhe një organizatë të tërë.

Ky udhëzues do të paraqes kërcënime të ndryshme kibernetike, të cilat përfshijnë një gamë të gjerë të llojeve të ndryshme të sulmeve. Më të zakonshmet janë:

- Sulmet e inxhinierisë sociale
- Sulmet phishing
- Shkarkime në kalim (Drive-By Downloads)
- Sulmet MITM
- Sulm USB drop
- Malware

Përvetësimi i kërcënimeve të ndryshme kibernetike do t'ju ndihmojë të mbroni veten, të dhënat tuaja personale dhe sistemet tuaja.

Sulme të zakonshme kibernetike

Sulme të inxhinierisë sociale

Në një sulm të inxhinierisë sociale, viktima mashtrohet dhe manipulohet nga një sulmues për të hequr dorë nga të dhënat personale ose qasja në kompjuterin e tij/saj. Ky lloj sulmi mbështetet në ndërveprimin njerëzor dhe zakonisht përfshin manipulimin e përdoruesve në mënyrë që ata të shkelin procedurat e sigurisë dhe praktikat më të mira për të fituar qasje të paautorizuar në sisteme ose të ndajnë informacione të ndjeshme.

Kriminelët kibernetikë e paraqesin veten si individë të besuar për të kryer sulme të inxhinierisë sociale. Sulmi pastaj ekzekutohet duke mashtruar përdoruesit për të klikuar lidhjet keqdashëse ose duke fituar fizikisht qasje në një kompjuter.

Mashtrime online

Ekzistojnë metodologji të ndryshme të cilat lehtësojnë mashtrimet online, që përfshijnë mashtrimet nga kriminelët kibernetikë. Shumë prej tyre iniciohen përmes emaileve phishing, mesazheve të dërguara në mediat sociale ose mesazhe SMS në telefonat celularë, telefonatave të rreme për mbështetje teknologjike dhe të tjera. Qëllimi i këtyre mashtrimeve mund të shkojë nga vjedhja e kartës së kreditit, në kapjen e kredencialeve të identifikimit dhe fjalëkalimit të përdoruesit, deri në vjedhjen e identitetit.[1]

Mashtrimet në internet kanë sukses sepse ato përmbajnë elementë realistë të mjaftueshëm për t'i bërë ato të duken të besueshme, veçanërisht kur viktima nuk bën kujdes. Kriminelët kibernetikë që shpikin mashtrime të tilla mësojnë të përfitojnë nga teknologjia e re dhe janë viktimat ato që paguajnë koston. Për të shmangur të bëheni viktimë e mashtrimeve në internet, si përdorues duhet të jeni shumë të kujdesshëm në lidhje me shpërndarjen e të dhënave personale, dhe gjithmonë:

- Të shmangni klikimin në dritaret pop-up ose lidhjet ose bashkëngjitjet në tekstet ose emailet. Tekstet dhe emailet e dyshimta duhet të fshihen menjëherë.
- Të dini me kë po komunikoni.
- Të ndërpritni menjëherë çdo telefonatë që kërkon të dhëna personale ose detaje të kartës së kreditit përmes telefonit.

Sulme phishing

Shumica e të gjitha sulmeve kibernetike fillojnë me një email phishing. Phishing është një lloj sulmi i inxhinierisë sociale në të cilin kriminelët kibernetikë mashtrojnë viktimat për të dorëzuar informacion të ndjeshëm ose për të instaluar malware.

Edhe pse masat teknike të sigurisë vazhdojnë të përmirësohen, phishing mbetet një nga mënyrat më të lira dhe më të lehta për kriminelët kibernetikë për të fituar qasje në informacion të ndjeshëm dhe personal. Përdoruesit thjesht duhet të klikojnë në një link dhe siguria e tyre mund të rrezikohet në atë masë që ata mund të bëhen viktima të vjedhjes së identitetit. Përdoruesit gjithashtu mund të kompromentojnë informacionin e tyre personal, kredencialet e hyrjes (emrat e përdoruesve dhe fjalëkalimet) dhe informacionin financiar (numrat e kartës së kreditit) nëse klikojnë linkun.

1 Online Scams, Avoiding Internet Scams, Norton, https://us.norton.com/internetsecurity-online-scams.html#

Si funksionon phishing-u

Shumica e fushatave phishing përdorin një nga dy metodat themelore:

1. **Bashkëngjitje keqdashëse** në emaile, të cilat zakonisht kanë përshkrim alarmuese si 'FATURA'. Kur hapen, këto shtojca instalojnë malware në pajisjen e përdoruesit.
2. **Lidhje me faqe keqdashëse të internetit** që shpesh janë klone të faqeve të ligjshme. Lundrimi në uebfaqe mund të shkaktojë shkarkimin e malware, ose faqja e hyrjes në uebfaqe mund të përmbajë skedare që vjedhin kredencialet.[2]

Llojet e sulmeve të phishing

Spear Phishing

Spear phishing është një sulm keqdashës i email-it që synon një organizatë apo individ të caktuar, duke ndjekur qasje të paautorizuar në informacione të ndjeshme.[3] Tentativat spear phishing nuk ka të ngjarë të ekzekutohen nga sulmues të rastit, por nga kriminelë kibernetik në kërkim të përfitimeve financiare ose informacioneve të tjera të vlefshme.

Në një sulm spear phishing, një email dërgohet nga një burim i besueshëm por çon në një faqe interneti të rreme me malware. Këto emaile përdorin mjete të ndryshme për të tërhequr vëmendjen e përdoruesve.

Spear phishing është shumë më efektive se sulmet e tjera phishing, por kërkon që kriminelët kibernetik të shpenzojnë kohë dhe burime duke ndërmarrë kërkime para sulmit, pasi ata do të jenë më të suksesshëm në qoftë se njohin objektivin e tyre para se të nisin sulmin.

Whale Phishing / Whaling

Whale Phishing është e ngjashme me spear phishing, me disa dallime të dukshme. Ndërsa spear phishing zakonisht synon anëtarët e një grupi, whale phishing është i fokusuar në një individ specifik - zakonisht 'peshku më i madh' në një organizatë të synuar ose një individ me pasuri ose fuqi të konsiderueshme.

Vishing

Vishing, ose "voice phishing", përfshin manipulimin e njerëzve përmes telefonit. Sulmuesit joshin një objektiv që të zbulojë një informacion të ndjeshëm në një tentativë për të përdorur këto të dhëna për përfitimin e tyre, zakonisht për të përfituar financiarisht.

Smishing

Termi smishing i referohet sms phishing, dhe përfshin një mesazh tekst në vend të një email-i. Objektivat në përgjithësi marrin një mesazh me tekst mashtrues që i detyron ata të japin informacion personal ose financiar për kriminelët kibernetikë që pretendojnë të jenë një agjenci qeveritare, bankë ose kompani të tjera të ligjshme.

Sulmuesit që përdorin smishing shpesh kërkojnë informacione personale ose bankare të llogarisë, të tilla si kredencialet e llogarisë, numrat e kartës së kreditit dhe numrat e identifikimit. Pastaj, ata e përdorin këtë informacion për të kryer sulme të ndryshme, duke përfshirë mashtrimet financiare, dhuratat ose mbështetjen e klientëve.

2 What is phishing? Everything you need to know, IT Governance UK

3 What is Phishing?, gfidigital.com

Shkarkime në kalim (drive-by downloads)

Në një sulm të shkarkimit në kalim, shkarkimet e skripteve keqdashëse përfundojnë në një kompjuter ose pajisje tjetër pa dijeninë e përdoruesit, duke e ekspozuar përdoruesin ndaj kërcënimeve kibernetike të ndryshme. Kjo mund të ndodhë në çdo pajisje që drejton çdo sistem operativ dhe zakonisht ndodh kur një përdorues shfleton një faqe interneti të kompromet uar.

Sulmet njeriu në mes (man in the middle MITM)

Një sulm MITM ndodh kur një kriminel kibernetik futet fshehurazi midis pajisjeve, ose midis një pajisjeje dhe një rrjeti wi-fi të pasigurt, për të kapur komunikimet që pastaj mund të lexohen dhe/ose modifikohen. Në një rast të tillë, përdoruesi mund t'ia kalojë pa dashje kredencialet ose informacione të tjera një krimineli kibernetik.

Sulm USB drop

Në një sulm USB Drop, një pajisje USB që përmban kod keqdashës është e lidhur në një kompjuter.

Zakonisht, kërcënimi kibernetik nga ky lloj sulmi është malware ose virus. Infeksioni nëpërmjet një USB mund të jetë si i qëllimshëm, ashtu edhe i paqëllimshëm, në varësi të malware-it në fjalë.

Do ishte mirë që organizatat të mos i besonin teknologjisë USB të vjetruar, dhe të përdornin fuqinë e rrjeteve digjitale të siguruara duke përdorur ruajtjen në cloud.

Malware

Malware është një term i përgjithshëm që përdoret për të përcaktuar çdo skedar ose program që ka për qëllim të dëmtojë ose të shkatërrojë një kompjuter. Kjo përfshin:

- **Softuer Botnet** i projektuar për të infektuar një numër të madh të pajisjeve të lidhura në internet. Disa botnet përbëjnë shumë pajisje, ku secila përdor një sasi relativisht të vogël të fuqisë përpunuese. Kjo mund ta bëjë të vështirë zbulimin e këtij lloji malware, madje edhe gjatë ndodhjes së botnet-it.
- **Sulmet Ransomware**, kriptojnë informacionin e përdoruesit dhe kërkojnë pagesë në këmbim të çelësit të dekriptimit, për të marrë informacionin. Megjithatë, pagimi i shpërblesës nuk garanton rikthimin e të dhënave të koduara.
- **Spyware** përdoret për të ndjekur në mënyrë të paligjshme aktivitetin kompjuterik të një përdoruesi dhe për të korrur të dhënat personale.
- **Trojan-ët** që shfaqen si softuer legjitim por kryejnë aktivitet keqdashës kur ekzekutohen.
- **Viruset dhe krimbat**, të cilat janë kod keqdashës të instaluar pa dijeninë e përdoruesit. Viruset mund të përsëriten dhe të përhapen në kompjuterë të tjerë duke u bashkangjitur në skedarë të tjerë kompjuterikë.

Krimbat gjithashtu shumëfishohen vet, por nuk kanë nevojë të bashkëngjiten në një program tjetër për ta bërë këtë. [4]

4 Types of Cyber Threat in 2019, IT Governance USA

Si të qëndroni të sigurt në internet

Trajtojnë me kujdes të dhënat personale dhe identitetin tuaj digjital

Si individë, ne identifikojmë dhe kategorizojmë veten në shumë mënyra, duke përdorur emrin, adresën, moshën, profesionin dhe të tjera. Identiteti ynë përfaqësohet gjithashtu në shumë forma, nga patentat e shoferit, kartat e sigurimit social, certifikatat e lindjes, distinktivët e punës dhe shkollës.

Duke marrë parasysh të gjitha këto forma të ndryshme të identitetit në përdorim në rutinën tonë të përditshme, si në internet ashtu edhe jashtë tij, është e pashmangshme që shumica e të dhënave tona private të ekzistojnë në hapësirat kibernetike dhe hapësira të tjera, dhe ka shumë të ngjarë të përdoren pa pëlqimin tonë. Ne thjesht nuk e kemi idenë se sa nga këto të dhëna ruhen në vende në të cilat asnjëherë nuk jemi futur, dhe mund të aksesohen dhe shfrytëzohen nga njerëz që nuk i njohim.

Është e qartë se gjëra të tilla si fjalëkalimet, të dhënat bankare dhe të dhënat personale nuk duhet të jepen kurrë, por edhe informacioni rreth rrethit të ngushtë ose emri i kafshës shtëpiake mund të përdoret nga kriminelët kibernetikë për të cenuar sigurinë tuaj. Këto fakte të personalizuara mund t'i ndihmojnë ata t'u përgjigjen pyetjeve të sigurisë që kanë për qëllim të mbrojnë llogaritë e juaja ose të ofrojnë sugjerime që do t'i çojnë deri te fjalëkalimi/et e juaja. Gjithmonë duhet të supozoni se hakerat janë vazhdimisht në kërkim të mënyrave për të shfrytëzuar të dhënat tuaja personale.

Vjedhja e identitetit dhe shkeljet e të dhënave paraqesin kërcënime të mëdha për disa arsye, por ndoshta kryesisht sepse ato kompromentojnë ndjesinë e vetvetes, pasi identiteti është themelor për mënyrën se si ndërveprojmë në botë. Kështu, për të rifituar kontrollin e të dhënave tuaja personale:

Mos përdorni të dhënat personale në emrat e përdoruesve ose fjalëkalimet që lidhen me llogaritë online

Mos i jepni të dhënat personale për të fituar zbritje në dyqanet online

Mos jepni informacione private të panevojshme në mediat sociale

Gjithmonë verifikoni se si të dhënat tuaja personale do të përdoren dhe sigurohen në aplikacione

Gjithmonë verifikoni nëse një faqe interneti është e sigurt (https ndaj http) para se të jepni të dhëna personale

Jini të kujdesshëm ndaj çdo shërbimi të ofruar falas, për të cilin mund të "paguani" pa dijeni me të dhënat tuaja

Përdorni fjalëkalime të ndërlikuara

Gjithmonë përdorni fjalëkalime të ndërlikuara që nuk përmbajnë: kombinime të numrave të lehta për t'u qëlluar (si 12345, 111111, 123321, etj.), emra të njohur, ose vargje shkronjash të formuara nga një vijë horizontale ose vertikale në një tastierë QWERTY (si asdfghjkl, qazwsx, 2wsx, etj.).

Çuditërisht, fjalëkalimi më i përgjithshëm –"password" – mbetet shumë i përhapur! Nëse e përdorni këtë si fjalëkalim, ndryshojeni TANI.

Ja disa sugjerime për të krijuar një fjalëkalim të sigurt:

- Përdorni të paktën 15 karaktere ose më shumë nëse është e mundur
- Përzieni shkronjat (shkronja të vogla dhe të mëdha), numrat dhe simbolet

- Asnjëherë mos përdorni sekuenca të numrave ose shkronjave (si “qwerty”)
- Shmangni zëvendësimet, si në “Ra!nb0w5”, ku shkronjat në një fjalë të zakonshme thjesht zëvendësohen nga numra dhe simbole me pamje të ngjashme

Përdorni fjalëkalime të ndryshme për llogari të ndryshme. Në këtë mënyrë, edhe nëse një llogari cenohet, të tjerat nuk janë në rrezik.

Mbajtja mend e fjalëkalimeve, veçanërisht llojin e fjalëkalimeve komplekse të rekomanduara këtu, mund të jetë një sfidë. Sidoqoftë, kjo mund të zgjidhet duke përdorur një menaxher fjalëkalimesh. Këshillohet të përdoren vetëm menaxherë fjalëkalimesh me reputacion si LastPass ose 1Password.[5]

Kontrollo dy herë lidhjet para se të klikosh

Sigurohu që të dish dhe t’u besosh lidhjeve para se të klikosh mbi to në emaile ose të vizitosh faqet e internetit.

Një nga mënyra për të verifikuar sigurinë e një lidhjeje është të vendosni miun mbi të, pa klikuar;. Kjo do të tregojë një pamje paraprake të lidhjes së plotë në shiritin e statusit të një shfletuesi uebi, duke i mundësuar përdoruesit të verifikojë që lidhja përputhet me informacionin në email dhe shkon në faqen e identifikuar. Gjithashtu është mirë të verifikoni lidhjen e saktë duke e kërkuar atë në mënyrë të pavarur, bazuar në informacionin në email.

Nëse një email përfshin udhëzime regjistrimi, gjithmonë duhet të shfletoni faqen zyrtare në fjalë dhe, në vend që të klikoni lidhjen e regjistrimit të dhënë në email. Kjo vlen edhe për linqet e dërguara nga miqtë në aplikacionet e rrjetit social.

Nëse një email ose uebfaqe kërkon që ju të hyni në bankën tuaj ose në llogari të tjera të ndjeshme, gjithmonë rekomandohet të telefononi dhe të verifikoni kërkesën me atë institucion.

Gjithmonë mendohuni dy herë para se të klikoni mbi shkarkimet. Disa kriminelë kibernetikë synojnë të infektojnë pajisjet me malware duke mashtruar përdoruesit për të shkarkuar aplikacione të kompromet uara dhe softuerë të tjerë. Para shkarkimit, kujdesuni që uebfaqja ose aplikacioni i lidhur me lidhjen e shkarkimit të jetë i ligjshëm dhe shmangni shkarkimin e çdo gjëje që duket e dyshimtë.

Përdorni rrjete wi-fi të sigurta

Përveç rasteve kur është thjesht e pashmangshme, mos përdorni kurrë rrjete wi-fi të pasigurta ose të hapura, të cilave u mungon mbrojtja me fjalëkalim. Nëse nuk mund ta shmangni këtë, mos hyni në asnjë llogari ose aplikacion në internet ndërsa jeni të lidhur dhe mos ndani kurrë asnjë informacion personal ose financiar në internet.

Kriminelët kibernetikë shpesh vendosin hotspote të rreme wi-fi për të mashtruar përdoruesit që nuk dyshojnë. Sapo dikush hyn në këto rrjete në telefonin e tij, një kriminel kibernetik mund të shohë pothuajse gjithçka që bën. Për të siguruar që lidhja wi-fi që përdorni në publik nuk është një hotspot i krijuar për këto qëllime të dobishme, zakonisht është më e lehtë t’i kërkohet një punonjësi të ndonjë biznesi ose kompanie emri i rrjetit të tyre wi-fi.

5 Catherine McNally, How to Stay Safe Online: Internet Safety Tips and Resources, reviews.org

Gjithashtu, pajisjet nuk duhet të vendosen për t'u lidhur automatikisht me rrjetet wi-fi, përveçse në punë ose në shtëpi. Rregulloni pajisjen që gjithmonë të pyes para se të lidheni, në mënyrë që të jeni në dijeni se kur dhe në cilat rrjete lidhen.

Përdorni një VPN

Një VPN, ose rrjet virtual privat, ofron një lidhje të sigurt për pajisjet tuaja me internetin, duke parandaluar aktorët e keqdashës që të ndjekin aktivitetin tuaj ose qasjen në informacionin tuaj. Një VPN mund të jetë një mënyrë e mirë për të siguruar një lidhje wi-fi në shtëpi, dhe jashtë në publik kur përdorni wi-fi të pasigurt.

E vetmja pengesë në rastin e VPN-ve është se ato mund të ngadalësojnë shpejtësinë e internetit. Kjo është për shkak se VPN drejton të dhënat përmes një serveri tjetër.

Ndërsa më shumë njerëz punojnë nga shtëpia, një mënyrë për të qëndruar të mbrojtur është të përdorni një VPN (dhe ta përditësoni rregullisht).

Faqet e që janë të paraprira nga https://

Shkronja "s" në https:// qëndron për "secure" dhe tregon se çdo e dhënë e futur në një uebfaqe e paraprirë nga ky prefiks do të kodohet. Prandaj, kur hyni në ndonjë uebfaqe, gjithmonë duhet të kontrolloni që adresa (në shiritin e adresës së shfletuesit të internetit) fillon me https:// dhe jo http://. Mund të shihni gjithashtu një simbol të bllokimit ngjitur me adresën e uebit, që tregon se uebfaqja është e sigurt.

Kur bëni blerje online dhe siguroni të dhëna personale si llogaria bankare ose informacioni i kartës së kreditit, gjithmonë kontrolloni dy herë që faqja e internetit në të cilën keni lundruar të jetë e sigurt.

Çaktivizo Bluetooth

Komunikimet me Bluetooth mund të kompromentohen dhe madje të manipulohen pa dijeninë e përdoruesit. Kjo nuk do të thotë se nuk duhet të përdorni kurrë Bluetooth për të çiftuar pajisjet, por është më mirë ta fikni kur nuk është në përdorim aktiv.

Instaloni antivirus dhe antimalware

Thjesht nuk është e këshillueshme të lundroni në ueb pa ndonjë mbrojtje nga viruset dhe malware. Edhe softueri antivirus falas dhe me kosto të ulët mund të jetë efektiv nëse zgjidhni me kujdes dhe mençuri. Një shpenzim i vogël mund të vlejë shumë për të garantuar më mirë shmangjen e problemit me malware ose ransomware.

Nëse tashmë përdorni antivirus ose softuer antimalware, sigurohuni që ai të jetë vazhdimisht i përditësuar!

Softuerët antivirus dhe antimalware që rekomandohet gjerësisht janë:

- Microsoft Defender (vjen i parainstaluar me sistemin operativ Windows OS dhe vetëm duhet të aktivizohet dhe përditësohet)
- Norton AntiVirus Plus
- Bitdefender
- AVG

- Malwarebytes
- AVAST
- SpyBot search and destroy

Ruani të dhënat e juaja

Kompjuterët dhe pajisjet e tjera i ruajnë të gjitha të dhënat tona të rëndësishme, por nëse këto pajisje kompromethohen, dëmtohen, humbasin ose vidhen, këto të dhëna të rëndësishme mund të humbasin. Pavarësisht nëse kjo humbje është për shkak të dështimit të harduerit, vjedhjes, katastrofës natyrore ose infektimit nga malware, rikuperimi i të dhënave mund të jetë i shtrenjtë ose i pamundur.

Kështu, një kopje rezervë – **dhe një kopje dixhitale e informacionit tuaj më të rëndësishëm** – është me rëndësi thelbësore. Kur bëni backup të të dhënave, kopjet e skedarëve tuaj (fotografi, dokumente, video, etj.) ruhen në një pajisje të jashtme ose shërbim cloud online. Kjo do të thotë se mund t'i rikthesh skedarët nëse diçka shkon keq. Rekomandojmë të regjistroheni rregullisht.[6]

Ka disa mënyra për të bërë backup të dhënat. Ja pikat e forta dhe të dobëta të secilit:

- **Bëni backup në një disk të jashtëm**: Kjo mund të bëhet duke përdorur cilsimet e ndërtuara për backup në shumicën e kompjuterëve, ose duke lidhur periodikisht diskun me kompjuterin dhe duke përdorur mjetin për backup ose duke e lënë atë të lidhur për backup automatik në një orar të caktuar.
  Pro: I lirë dhe i shpejtë
  Kundër: Disqet e jashtëm mund të humbasin ose të vidhen, dhe mund të prishen me kalimin e kohës
- **Backup në kompjuterin tuaj**: Në varësi të pajisjes dhe sistemit operativ, ekzistojnë mënyra të ndryshme për të bërë kopje rezervë të të dhënave në një kompjuter. Për shembull, iCloud është në dispozicion për përdoruesit e pajisjeve iOS; Time Machine për përdoruesit të Mac; dhe mjete të ndryshme në versione të ndryshme të Windows (8.1, 10, dhe 11, etj.) për përdoruesit e PC-ve.
  Pro: I lirë dhe i shpejtë
  Kundër: Kopja rezervë mund të humbasë ose të vidhet
- **Backup në cloud**: Bakup mund të ruhen në "cloud" në shërbime si Dropbox , Google Drive, Microsoft OneDrive, ose të ngjashme. Kjo ju lejon të sinkronizoni automatikisht kopjet rezervë me pajisjet e tjera, dhe do të thotë se nëse kompjuteri juaj nuk funksionon ose është vjedhur, ju do të keni gjithsesi kopje të të gjithë skedarëve të kopjuar në internet.
  Pro: E lehtë, e shpejtë, në shumë raste falas, dhe mbrojtja më e mirë kundër të gjitha llojeve të humbjes së të dhënave
  Kundër: Shumica e shërbimeve cloud ofrojnë vetëm disa gigabajt hapësirë ruajtjeje falas, dhe shumica e njerëzve do të duhet të paguajnë për hapësirë shtesë në mënyrë që të ruajnë të gjithë skedarët e tyre[7]

Vlen të merret parasysh se ku ruani të dhënat më të rëndësishme duhet dhe të siguroheni që kopjet e shumëfishta të ruhen në çdo kohë. Në rastin ideal, ato kopje duhet të ekzistojnë në më shumë vende.

6 Back Up and Restore - Microsoft Windows, Cyber.gov.au

7 Best ways to back up your computer, Nerds in a Flash

Konkluzion

Ndërsa peizazhi i kërcënimit kibernetik bëhet më kompleks dhe kriminelët kibernetikë përfitojnë nga teknologjitë dhe tendencat në zhvillim, duke përfshirë mediat sociale, vendet e punës në distancë dhe varësinë tonë nga telefonat smart, është më thelbësore se kurrë që përdoruesit të kuptojnë se si të qëndrojnë të sigurt në hapësirat kibernetike. Qasja më e mirë është zbatimi i rekomandimeve në këtë udhëzues, të cilat përshkruajnë sjellje të zgjuara dhe rekomandojnë mjete të ndryshme. Përfundimisht, qëndrimi i sigurt në internet kërkon një ekuilibër të përgatitjes, parandalimit dhe ndërgjegjësimit. Ju mund të shmangni të bëheni viktimë, ose të paktën të shmangni rezultatet më të këqija nga ngjarjet e sigurisë kibernetike, nëse përgatiteni për humbjen e të dhënave duke ruajtur skedarët, të parandaloni prishjen e të dhënave duke instaluar mjete të përshtatshme dhe të njiheni vazhdimisht me llojet e sulmeve të favorizuara nga kriminelët kibernetikë.

Referenca

Online Scams, Avoiding Internet Scams, Norton

What is phishing? Everything you need to know, IT Governance UK

What is Phishing?, gfidigital.com

Types of Cyber Threat in 2019, IT Governance USA

What Is Cyberbullying, StopBullying.gov

Catherine McNally, How to Stay Safe Online: Internet Safety Tips and Resources, reviews.org

Back Up and Restore - Microsoft Windows, Cyber.gov.au

Best ways to back up your computer, Nerds in a Flash

Shtojcë: lista kontrolluese e praktikave të mira

SULME TË ZAKONSHME KIBERNETIKE	
INXHINIERI SOCIALE	- In social engineering attacks, a target is misled and manipulated by an attacker into relinquishing personal data or access to their computer(s). These attacks rely on human interaction and usually involve the manipulation of a user so that they violate security procedures and best practices to gain unauthorized access to systems or share sensitive information.
SULME PHISHING	- Phishing is a type of social engineering attack in which cybercriminals trick victims into handing over sensitive information or installing malware. These attacks can take different forms: • Spear Phishing – a malicious email targets a specific organization or individual, pursuing unauthorized access to sensitive information. • Whale Phishing/Whaling – an attack focused on a specific individual, usually the "biggest fish" at the target organization or an individual with noteworthy wealth or power. • Vishing – an attempt to obtain a victim's personal data and use it to gain financially by manipulating a target over the phone. • Smishing – a misleading SMS message meant to compel the recipient to provide personal or financial information (account credentials, credit card numbers, etc.), sent by cybercriminals pretending to be a government agency, bank, or other legitimate company.
SHKARKIME NË KALIM (DRIVE-BY DOWNLOADS)	- In a drive-by download attack, a user unintentionally and unknowingly downloads malicious script on to a computer or other device by navigating to or browsing compromised websites, exposing the user to various cyberthreats.
SULMET NJERIU NË MES (MAN IN THE MIDDLE MITM)	- MITM attacks occur when a cybercriminal secretly inserts themselves between devices, or between a device and an insecure wi-fi network, to intercept communications that may then be read and/or modified. This can lead to a user unintentionally passing credentials or other information to the cybercriminal.
SULM USB DROP	- In a USB drop attack, a USB device containing malicious code is plugged into a computer.
MALWARE	- **Botnet software**: infects large numbers of devices connected to the internet. - **Ransomware attack**: encrypts user information, then requires payment in return for the decryption key needed to retrieve it. - **Spyware**: a form of malware used to illicitly monitor a user's computer activity and harvest personal information. - **Trojan**: a type of malware that hides as legitimate software but performs malicious activity when executed. - **Viruses and worms**: malicious code installed without a user's knowledge. Viruses can replicate and spread to other computers by attaching themselves to other computer files. Worms are also self-replicating, but do not need to attach themselves to another program to do this.

SI TË QËNDRONI TË SIGURT NË INTERNET	
KURRË MOS E NDANI INFORMACIONIN PERSONAL	- **Kurrë mos ndani, online ose personalisht:** • fjalëkalime • detajet bankare • të dhëna personale - **Për të rimarrë kontrollin e të dhënave tuaja personale:** • Mos përdorni të dhënat personale në emrat e përdoruesve ose fjalëkalimet që lidhen me llogaritë online • Mos i jepni të dhënat personale për të fituar zbritje në dyqanet online • Mos jepni informacione private të panevojshme në mediat sociale • Gjithmonë verifikoni se si të dhënat tuaja personale do të përdoren dhe sigurohen në aplikacione • Gjithmonë verifikoni nëse një faqe interneti është e sigurt (https ndaj http) para se të jepni të dhëna personale • Jini të kujdesshëm ndaj çdo shërbimi të ofruar falas, për të cilin mund të “paguani” pa dijeni me të dhënat tuaja
KRIJONI DHE PËRDORNI FJALËKALIME KOMPLEKSE	- **Gjithmonë përdorni fjalëkalime komplekse që:** • janë të paktën 15 karaktere të gjatë (më të gjatë, nëse është e mundur); • përzieni shkronjat (si me shkronjë të vogël ashtu edhe me shkronjë të madhe), numrat dhe simbolet • asnjëherë mos përdorni sekuenca të numrave ose shkronjave (si “qwerty”) • Shmangni zëvendësimet, si në- “Ra!nb0w5”,- ku shkronjat në një fjalë të zakonshme thjesht zëvendësohen nga numra dhe simbole me pamje të ngjashme - **Përdorni fjalëkalime të ndryshme për llogari të ndryshme.** - **Përdorimin një menaxher fjalëkalimesh**
KONTROLLONI DY HERË LIDHJET PARA SE TË KLIKOSH	- **Kur lexoni email ose vizitoni faqet e internetit, përdoruesit gjithmonë duhet të dinë dhe t’u besojnë lidhjeve para se të klikojnë mbi to. Për të shmangur klikimin në lidhjet keqdashëse**: • Vendosni miun mbi lidhjet për të parë një paraqitje të lidhjes dhe për të verifikuar që ajo përputhet me informacionin në email ose tregon faqen e internetit e duhur. • Nëse një email përfshin një lidhje regjistrimi, është më e sigurt të mos klikoni lidhjen e dhënë në email por të shkoni në faqen zyrtare të organizatës/kompanisë përkatëse dhe të hyni aty. • Nëse një email ose uebfaqe kërkon që një përdorues të hyjë në llogari bankare ose llogari të tjera, telefononi gjithmonë për të verifikuar kërkesën. • Para se të shkarkoni nga ndonjë faqe interneti, sigurohuni që të kontrolloni legjitimitetin e faqes dhe gjithmonë shmangni shkarkimin e çdo gjëje që duket e dyshimtë për ndonjë arsye.
PËRDOR RRJETE WI-FI TË SIGURTA	- Përveç rasteve kur është thjesht e pashmangshme, kurrë mos përdorni rrjete wi-fi të pasigurta ose të zhbllokuara, të cilave u mungon mbrojtja me fjalëkalim. - Kur përdorni një rrjet të hapur wi-fi, shmangni hyrjen në çdo llogari në internet ose futjen e ndonjë informacioni personal ose financiar në aplikacione - Rregulloni pajisjet në mënyrë që ato të mos lidhen automatikisht me rrjetet wi-fi
PËRDORNI NJË VPN	- Një rrjet virtual privat, ose VPN ofron një lidhje të sigurt për pajisjet tuaja me internetin, duke parandaluar që aktorë këqdashës të ndjekin aktivitetin tuaj ose qasjen në informacionin tuaj. - Ka shumë ofrues VPN, dhe një VPN duhet të shkarkohet, instalohet dhe të lidhet me një server.
PËRDORNI UEBFAQE TË SIGURTA (HTTPS)	- Kur regjistroheni online, URL-ja në adresin e shfletuesit duhet të fillojë me https://, njo http:// (“s” qëndron për “secure” (e sigurt)). - Mund të shfaqet gjithashtu një simbol i bllokimit pranë adresave të sigurta të faqes së internetit.
FIKNI BLUETOOTH-in	- Nëse ndonjëherë lidheni me pajisje përmes Bluetooth, sigurohuni që ta fikni atë kur nuk është në përdorim aktiv, për të shmangur kompromet imin ose madje manipulimin.
PËRDORNI ANTIVIRUS DHE ANTIMALWARE	- Edhe antivirusi falas dhe me kosto të ulët dhe softueri antimalware mund të ndihmojnë në mbrojtjen e përdoruesve nga malware ose ransomware. Sigurohuni që të mbani të përditësuar softuerin antivirus dhe antimalware!
BACKUP I TË DHËNAVE	- Kur të dhënat bëhen backup, kopjet e skedarëve (p.sh., fotografi, dokumente, video, etj.) ruhen në një pajisje të jashtme ose në një shërbim cloud online. - Kjo kopje dixhitale e të dhënave mund të ndihmojë në rivendosjen e një sistemi nëse kompromet ohet, kështu që është e rëndësishme që backup të bëhet rregullisht.

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva