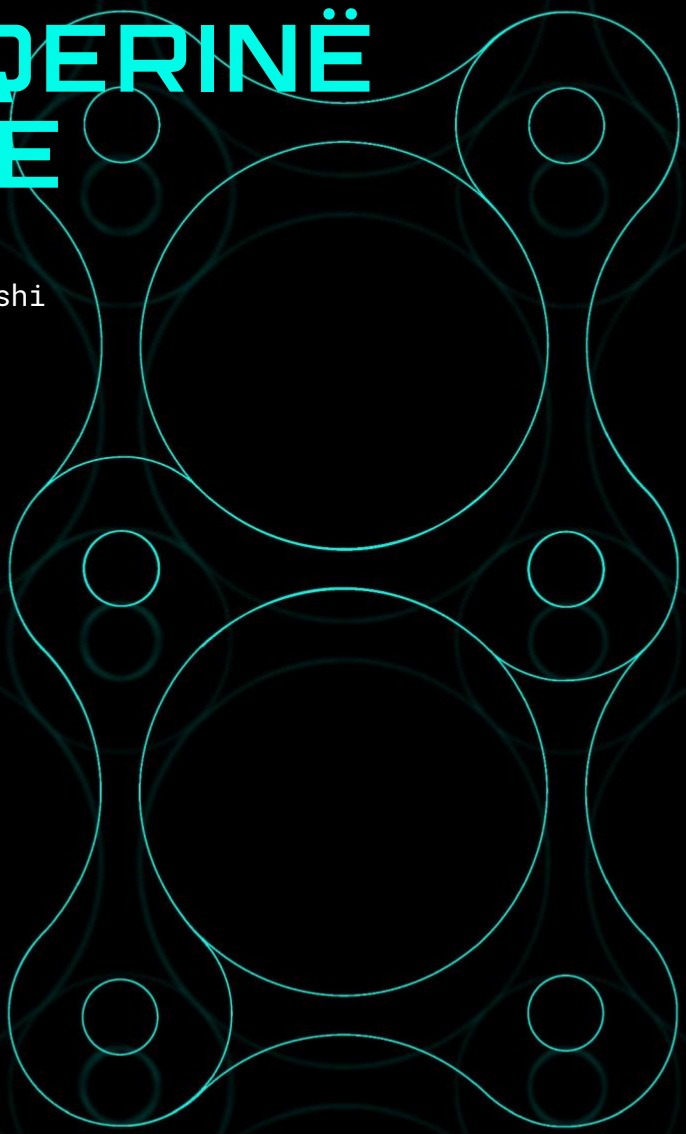
MANUAL I SIGURISË SË INFORMACIONIT PËR GAZETARËT DHE SHOQERINË CIVILE

Nga Arianit Dobroshi



INFOSEC for Balkans

Jul 2019

TABELA E PËRMBAJTJES

HYRJE

Ky manual ka për qëllim gazetarët dhe punonjësit e tjerë të shoqërisë civile të rajonit të Evropës Juglindore të cilët aktualisht mund të mos përballen me kërcënimet më të sofistikuara të sigurisë (infosec). Autori beson se është një kompromis i denjë për të sakrifikuar disa rreptësi të sigurisë së informacionit, nëse kjo promovon miratim më të lartë të këtyre praktikave dhe mjeteve.
Ky manual synon audiencën me praktika të ulëta të sigurisë, si dhe popullsinë e përgjithshme. Si i tillë, ai përcakton praktikat themelore të sigurisë së informacionit të përshtatshme për të gjithë.
Çdo seksion i këtij manuali përfshin të paktën dy nivele të sigurisë: nivelin shumë themelor të kërkuar për llogaritjen e sigurt e cila duhet të praktikohet nga të gjithë, dhe një seksion rreziku më të lartë për të cilin duhet të synojë çdo gazetar hetues dhe oficer sigurie që bën punë të ndjeshme në rajon. Sidoqoftë, disa gazetarë dhe oficerë të sigurisë në rajon përballen me nivele edhe më të larta kërcënimi dhe duhet të kërkojnë burime të tjera më të thella, disa prej të cilave janë renditur në pjesën e fundit të këtij manuali.
Ky manual është shkruar në korrik 2019. Kërcënimet për sigurinë e informacionit dhe masat e tyre zbutëse vazhdimisht po evoluojnë, kështu që kjo datë duhet të mbahet në mend kur i referoheni asaj në të ardhmen.

A)PËR KË ËSHTË KY MANUAL?

Ky manual ka për qëllim gazetarët, veçanërisht ata që punojnë në gazetarinë hulumtuese dhe aktivistët e shoqërisë civile, veçanërisht ata që merren me tema të ndjeshme në lidhje me sundimin e ligjit. Thënë kështu, është një mjet i mirë për t'u përdorur nga kushdo që dëshiron të përditësojë njohuritë e tyre themelore për infosec, veçanërisht pasi që është i disponueshëm edhe në gjuhët e rajonit, të cilave u mungojnë burimet në këtë fushë: shqip, boshnjakisht, maqedonisht, malazezisht dhe serbisht.

Niveli teknik i kërkuar për të zbatuar këtë punë është themelor dhe duhet të jetë i arritshëm nga të gjithë. Disa nga mjetet kërkojnë një sakrificë në përdorimin dhe praktikimin nga praktika e zakonshme.

B) SI TA LEXOJMË KËTË MANUAL?

Çdo titull i këtij manuali mund të lexohet veçmas bazuar në nevojat tuaja të menjëhershme të sigurisë së informacionit. Sidoqoftë, rekomandohet të mbuloni të gjitha pjesët e këtij manuali pasi është hartuar si një listë e punës minimale që duhet të praktikoni për të mbrojtur veten dhe burimet tuaja. Ju mund të ktheheni tek ajo kur të keni më shumë kohë dhe t'i mbuloni të gjitha ato. Nëntitujt e parë përmbajnë bazat themelore që çdo përdorues i kompjuterit duhet të praktikojë, megjithëse në vrojtimin tonë nuk është kështu. Nëntitulli i dytë duhet të sigurojë një përditësim të sigurisë për shumicën e përdoruesve bazik.

Pjesa e dytë e manualit përfshin krijimin e fjalëkalimeve më të fortë, të dobishëm për të gjitha platformat. Në pjesën e tretë ne mbulojmë sistemin tuaj të funksionimit të desktopit: gjëra që duhet të bëni me sistemin tuaj operativ Windows dhe pak ndihmë në instalimin e Linux Mint, i cili është një sistem më i sigurt i parazgjedhur, por i lehtë për t'u përdorur. Në pjesën e katërt ne adresojmë në shfletim të sigurt dhe në pjesën e pestë dërgimi i porosive me e-mail në mënyrë të sigurt. Në pjesën e gjashtë shikojmë disa gjëra për të bërë për sigurinë e sistemit celular ndërsa në pjesën e shtatë ne adresojmë sigurinë e komunikimit. Më në fund, pjesa e tetë adreson shpërndarjen e të dhënave, ndërsa pjesa e nëntë na jep një listë të burimeve për lexuesit që duan të bëjnë më shumë.

C)IDENTIFIKIMI I NEVOJAVE TUAJA TË SIGURISË

Qasja e paautorizuar në të dhënat tuaja mund të sjellë përdorimin, zbulimin, prishjen, modifikimin, inspektimin, regjistrimin ose shkatërrimin e saj. Sidoqoftë, për shkak se kërcënimet digjitale janë të padukshme, komplekse dhe shpesh të pazbulueshme, ato mund të nënvlerësohen ose anashkalohen.
Ka disa mënyra për të parë kërcënimet me të cilat përballeni dhe sigurinë e informacionit që keni. Kërcënimi më themelor me të cilin përballen të gjithë përdoruesit janë kërcënimet e drejtpërdrejta me të cilat has çdo qytetar i rajonit, megjithëse kërcënimet më të specializuara janë në shënjestër të këtij manuali.

Vendet e rajonit kanë zbatuar Direktivën e BE-së për ruajtjen e të dhënave, e cila detyron mbajtjen e metadatave (të dhëna në lidhje me të dhënat) për të gjitha telekomunikimet e trajtuara, përfshirë listat e të gjitha telefonatave, adresave IP, mesazheve tekstuale etj, të dërguara ose të marra për një periudhë midis gjashtë deri në njëzet e katër muaj, të cilat mund të arrihen me një vendim gjykate. Ndërsa përmbajtja e komunikimit në vetvete nuk është e kursyer, përparimi nga mandati ligjor në mbikëqyrje me shumicë nuk është aq i vështirë dhe kërkesa për urdhër gjyqësor varet nga brishtësia e sistemeve të sundimit të ligjit në rajon. Edhe metadata është jashtëzakonisht zbuluese pasi mund të lejojë që ata që disponojnë të krijojnë grafikët shoqërorë të jetës tuaj dhe indirekt të identifikojnë përmbajtjen dhe burimet me të cilat merreni, madje edhe në mënyrë retrospektive.
Me kërcënime të specializuara, pala që kryen mbikëqyrje përdor mjete të specializuara dhe të sofistikuara kundër objektivit. Teknologjia për këtë është bërë më e lirë, dhe qasja në të nga qeveritë dhe palët private po bëhet më e lehtë. Për shembull, u zbulua në vitin 2015 që qeveria e Maqedonisë së Veriut kishte përgjuar telefonat e rreth 20.000 njerëzve. Ekzistojnë gjithashtu prova që qeveria serbe po rivotonte internetin në pika të caktuara, ku mund të merrej lehtë. Kjo ishte vite më parë dhe situata ka shkuar të përkeqësohet. Nëse besoni se përballeni me këtë lloj kërcënimi, atëherë ky manual nuk është i mjaftueshëm për të mbrojtur veten dhe ju duhet të kërkoni ndihmë të përkushtuar.

2. KRIJIMI I FJALËKALIMEVE TË SIGURT

Një fjalëkalim i sigurt është i rastësishëm, mjaft i gjatë dhe kombinon një listë të sipërme dhe të poshtme shkronja rasti, numra dhe karaktere të tjera (psh. xkvv3.K3? rrz). Sidoqoftë, është e mundur të keni fjalëkalime të sigurta duke përdorur kombinimin e fjalëve me kusht që të jetë mjaft e gjatë, unike për shërbimin, e rastësishme dhe jo e lidhur me ju. Një kombinim i fjalëve të rastit që lehtë mund t'i mbani mend është një fjalëkalim i sigurt sa duhet (p.sh. WITHIN-WIRE-GRASS-pluto-save).

A)VËRTETIMI I DY FAKTORËVE

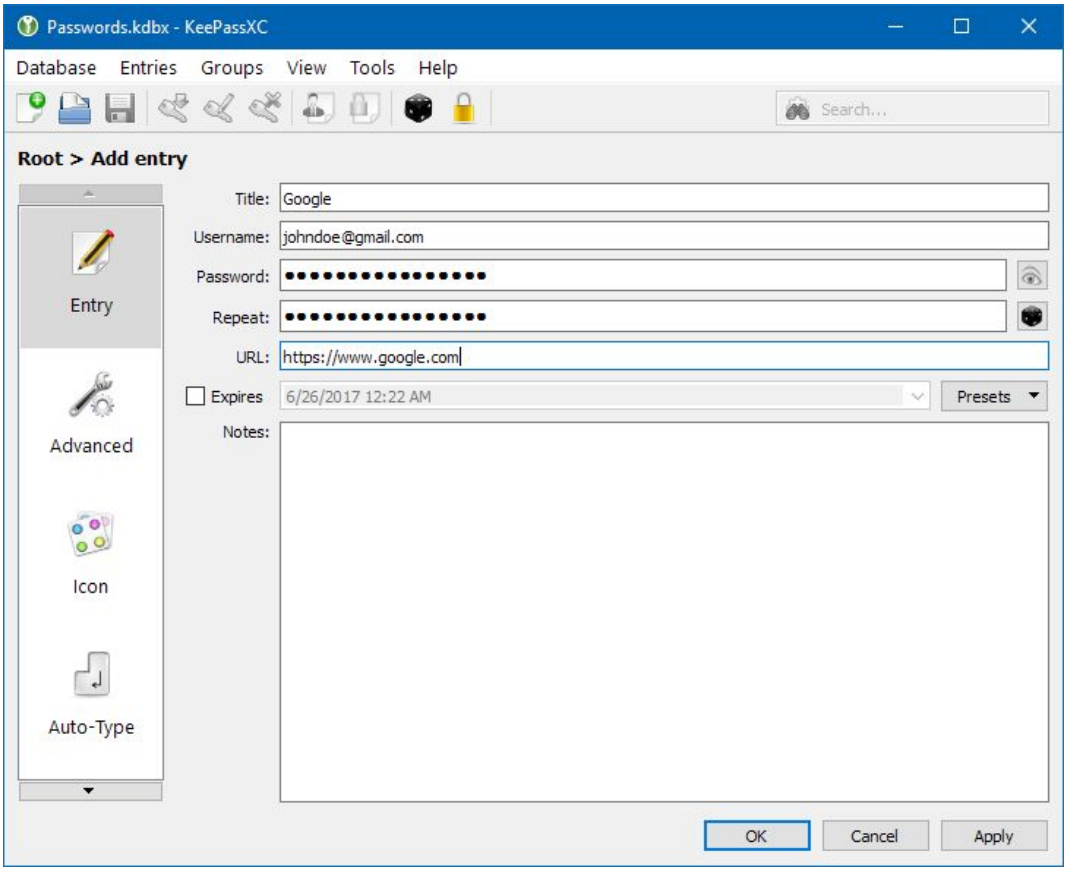
Kurdo që të jetë në dispozicion, vërtetimi i dy faktorëve siguron një mjet të dytë në krye të fjalëkalimit tuaj të zakonshëm për të siguruar llogaritë tuaja në internet. Faktori i dytë i vërtetimit (2FA) mund të dërgohet në telefonin tuaj përmes një telefonate, SMS, email ose mund të gjenerohet në telefonin tuaj Android ose nga një xhiton harduerik. Ju tashmë mund të përdorni një për llogaritë tuaja bankare. Faktori i dytë shton një shtresë shtesë mbrojtjeje në rast se fjalëkalimi juaj rrezikohet. Mundësimi i vërtetimit të faktorit të dytë varet nga programi juaj dhe duhet të shikoni nën Cilësimet > Fjalëkalimi ose të ngjashëm për ta aktivizuar atë. Sidoqoftë, jo të gjitha shërbimet e ofrojnë atë ende.

Për shembull, ndërsa përdorni Shërbimet e Google-s, mund të vizitoni https://myaccount.google.com/signinoptions, të regjistroheni me llogarinë tuaj, ta aktivizoni atë dhe të zgjidhni një mjet për të marrë një fjalëkalim të përkohshëm për herë të dytë, normalisht një SMS. Vini re se nëse humbni numrin tuaj të telefonit, do të jeni të bllokuar nga llogaria juaj. Prandaj, duhet të vendosni të paktën një mundësi rezervë, në mënyrë që të regjistroheni edhe nëse hapat e tjerë të dytë nuk janë të disponueshëm. Kodet e printimit një herë mund të jenë mënyra më e lehtë për t'ju lejuar të regjistroheni nëse humbni numrin tuaj ose nëse udhëtoni.

B) SHFLETUES MË I SIGURT: TOR BROWSER

Fjalëkalimet që përdorni duhet të jenë unike për çdo shërbim që përdorni. Kujtimi i fjalëkalimeve të sigurta shpejt bëhet e pamundur, duke kërkuar një mjet për t'i menaxhuar ato. Për të lehtësuar krijimin e fjalëkalimeve të sigurta, si dhe menaxhimin e tyre, mund të përdorni një program të dedikuar. Një burim i mirë i hapur është KeePassXC (https://keepassxc.org) i disponueshëm për macOS Windows dhe Linux, një menaxher i fjalëkalimeve që ruan emrat e përdoruesve dhe fjalëkalimet në një bazë të dhënash të koduar, të mbrojtur nga një fjalëkalim të përkryer. Ajo gjithashtu vjen me PWGen, një gjenerues i fortë i fjalëkalimeve të rastësishme.

Programe të tjera alternative janë LastPass dhe 1Password. Ato ruajnë fjalëkalimet e koduara në internet dhe disa karakteristika mund të jenë të disponueshme vetëm nën versionin e paguar, por ato sigurojnë përdorueshmëri më të mirë dhe fjalëkalimet ruhen në internet. Duke qenë burim i mbyllur, është e pamundur të kontrollohet në mënyrë të pavarur siguria e këtyre dy mjeteve.



Pamja e ekranit KeePassXC

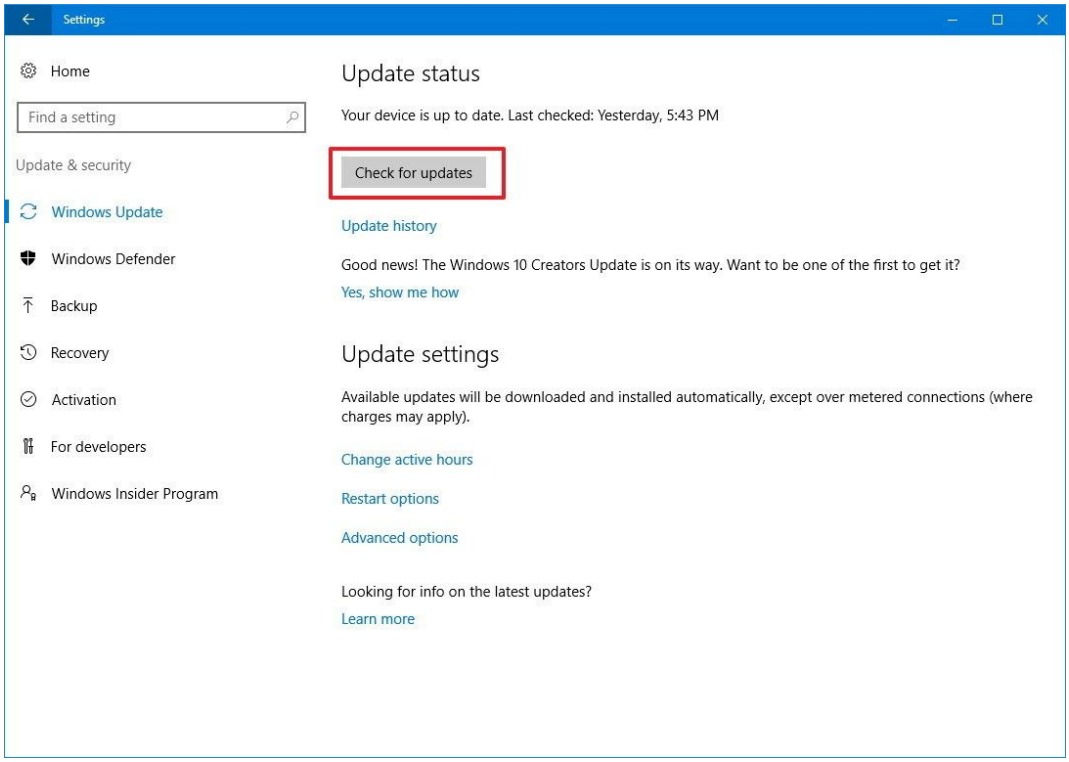
PËRDORIMI I NJË SISTEMI OPERATIV MË TË SIGURT

Sistemi operativ i desktopit është baza e llogaritjes suaj të sigurt të përditshëm. Në përgjithësi, siguria e një sistemi të renditur nga e ulët në të lartë është: Windows 7 ose 10 të cilat përdoren më gjerësisht por edhe më pak të sigurta, macOS e cila është më e sigurt si parazgjedhje kështu që nuk adresohet këtu, Linux Mint, një shije sistemi Linux që adresohet këtu, dhe Tails, gjithashtu i bazuar në Linux, i dizajnuar me sigurinë e informacionit në mendje por me kompromise të përdorimit.

A) MBAJTJA E WINDOWSIT TË PËRDITËSUAR

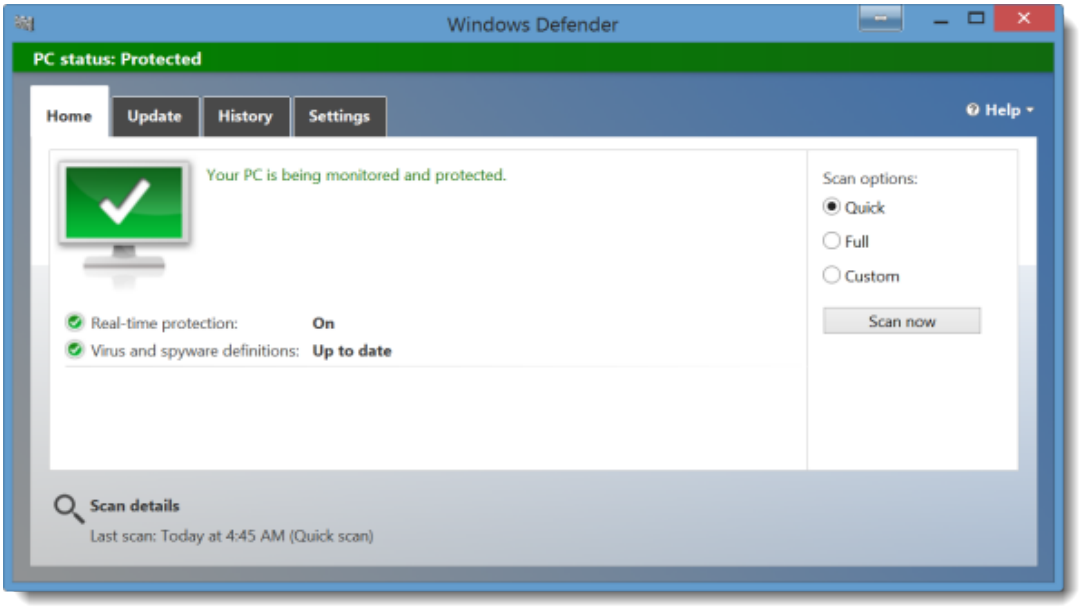
Mbajtja e Windows-it të përditësuar është thelbësore nëse punoni në një makinë të lidhur me internet. Shumë herë, kopjet e piratuara të Windows janë të ndaluar nga përditësimi që ju ekspozon ndaj të gjitha llojeve të dëmtimeve dhe kërcënimeve të tjera. Vini re se Windows 7 do të dalë jashtë funksioni nga prodhuesi i saj Microsoft deri në fund të vitit 2019 dhe për këtë arsye nuk do të përditësohet me grup ndryshimesh në një program kompjuterik të sigurisë pas kësaj date. Ju duhet të përditësoheni në Windows 10 përtej kësaj pike.

Për të siguruar që Windows juaj është përditësuar, duhet të kërkoni për “Windows Update” në shiritin e kërkimit të Windows, klikoni Kontrollo përditësime dhe të siguroheni që në ekran shfaqet “Asnjë përditësim nuk është në dispozicion”. Vini re se jo të gjitha përditësimet janë përditësime të sigurisë dhe prandaj mund t’i injoroni ato. Nëse një përditësim i Windows-it është i pamundur të ekzekutohet, atëherë duhet të kërkoni ndihmë për të siguruar që kompjuteri juaj të jetë i përditësuar.



Statusi i Windows Update

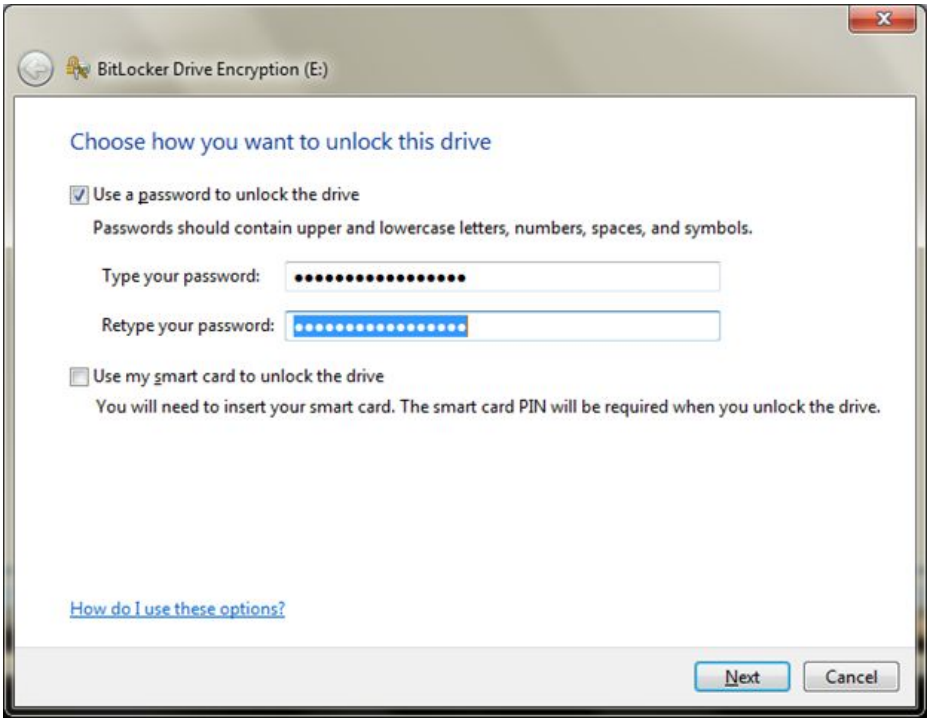
Përveç kësaj, keni nevojë për një softuer që ju mbron nga viruset dhe dëmtuesit. Në shumicën e rasteve, ndërtuar në Windows Defender është adekuat dhe nuk përdor burime shtesë në kompjuterin tuaj. Për ta ekzekutuar, çinstaloni programin tjetër antivirus. Shkoni në shiritin e kërkimit të Windows dhe shtypni "Windows Defender". Sigurohuni që mbrojtja në kohë reale të jetë e mundur dhe përkufizimet e virusit të jenë të përditësuara. Nëse jo, duhet t'i rifreskoni ato përmes skedës Update.
Nëse sistemi juaj ka qenë i vjetruar për një kohë të gjatë, kryeni një skenim të plotë të sistemit tuaj për të siguruar që ai është i pastër, i cili mund të zgjasë disa orë. Nëse nuk mund të zgjidhni vetë gjetjet e mundshme, duhet të kërkoni ndihmë



Windows Defender i përditësuar

B) KRIPTIMI I DISKUT

Të dhënat në diskun e kompjuterit tuaj mund të lexohen lehtësisht nga një kundërshtar që ka qasje fizike në të nëse disku nuk është i koduar. Shumica e versioneve të Windows deri në Windows 7 Pro nuk kanë instaluar kriptim të diskut si parazgjedhje.
Kriptimi i plotë i diskut në BitLocker në një hapësirë të sistemit kërkon një kompjuter me një Modul të besueshëm të platformës (TPM) të ndërtuar në PC-në tuaj. Ky çip gjeneron dhe ruan çelësat e kriptimit që përdor BitLocker. Ju mund ta shmangni këtë duke përdorur Politikën e Grupit për të lejuar përdorimin e BitLocker pa TPM edhe pse do të sakrifikoni disa siguri.



Dukja e BitLocker

Ju mund të kriptoni një njësi josistemore ose një disk të heqshëm pa TPM, kështu që është e pëlqyeshme që të dhënat tuaja t'i keni në një disk të veçantë (zakonisht në hapësirën 'D').

Mënyra më e lehtë për të aktivizuar BitLocker në një hapësirë është të hapni File Explorer dhe të klikoni me të djathtën e miut në hapësirën që dëshironi, pastaj klikoni Turn on BitLocker. Nëse nuk e shihni këtë mundësi në menynë tuaj të kontekstit, atëherë ka mundësi mos keni një edicion Pro ose Enterprise të Windows, kështu që keni nevojë për një alternative tjetër.

Paralajmërim: BitLocker ju siguron një çelës kthimi të cilin duhet ta mbani të sigurt duke e ruajtur atë diku të sigurt jashtë kompjuterit ekzistues ose duke e shtypur atë dhe duke e ruajtur atë fizikisht. Në rast se harroni tastin tuaj ose moduli juaj TPM është shkatërruar, kjo do t'ju lejojë të përdorni përsëri dokumentet tuaja.

Nëse disku juaj i sistemit është i koduar me një fjalëkalim dhe ju keni një TPM, nuk do të vini re asgjë. Nëse keni kriptuar një disk josistemor ose disk të heqshëm, Windows ju bën thirrje të zhbllokoni hapësirën kur të keni qasje të parë. Shtypni fjalëkalimin tuaj për të zhbllokuar nëse e përdorni gjatë çdo rifillimi.
Nëse përdorni një sistem tjetër operativ siç është Linux, opsioni i kriptimit të diskut ofrohet gjatë instalimit. Shihni pjesën e instalimit Linux Mint për të parë se si ta aktivizoni këtë.
Për të gjitha sistemet, një mjet i mirë i pavarur me burim të hapur të respektuar nga profesionistë të sigurisë është VeraCrypt (dikur TrueCrypt) i arritshëm këtu https://www.veracrypt.fr .

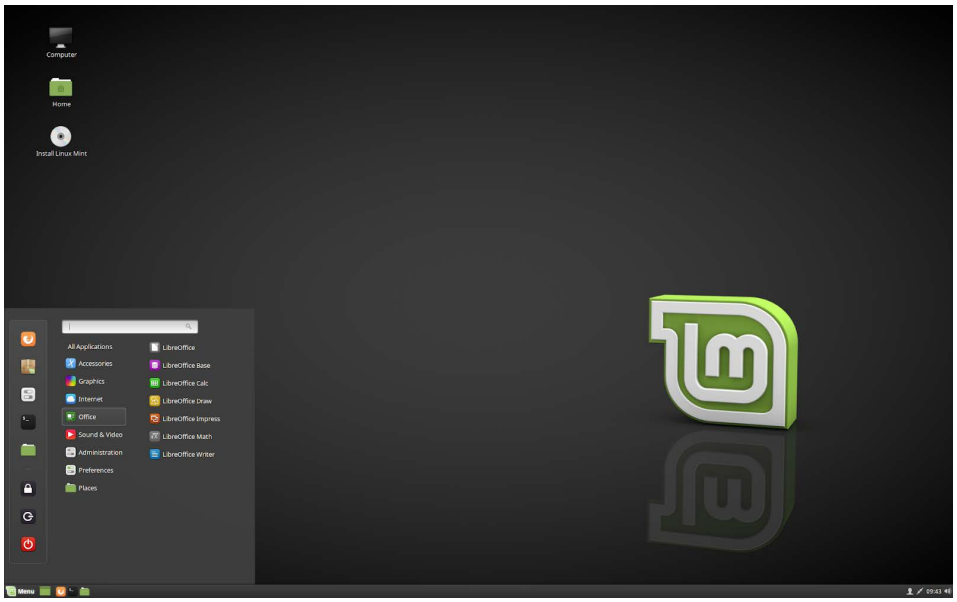
C) LINUX MINT: SISTEM OPERATIV MË I SIGURT

Linux është sistemi operativ falas dhe me burim të hapur. shtë më e sigurt se Windows pasi nuk përballet me disa nga çështjet e sigurisë së Windows, por do t'ju kërkojë të mësoni një sistem të ri operativ dhe ndonjëherë kërkon shtypjen e komandave për të kryer gjërat.

Ka shumë "shije" ose përsëritje të Linux: Ubuntu, Fedora dhe Linux Mint janë ato më të njohura për qëllime të përgjithshme, dhe Tails u janë kushtuar atyre me nevoja më të larta sigurie. Ju duhet të përdorni cilindo version që është më i zakonshëm në rrethinën tuaj, kështu që mund të kërkoni ndihmë nëse ngecni. Nëse kjo nuk është një mundësi e mundshme, atëherë shkoni me Linux Mint, të cilën ne i shpjegojmë këtu. shtë më miqësor për përdoruesit, ka një komunitet të madh mbështetës, është jokomercial dhe ka një ndjenjë Windows për ata që kalojnë prej tij.

Ndërsa Linux ka qasje në një depo të mijëra programeve me burim falas dhe të hapur, mund të të duhet të mësosh aplikacione të reja për t'i bërë gjërat, pasi disa prodhues të softuerëve nuk i prodhues për Linux. Alternativa prej Windows në Linux janë: LibreOffice për Microsoft Office, Gimp to Photoshop, Audacity for editing sound etj. Përdorni http://alternativeto.net për të gjetur alternativa për programin që përdorni në Windows ose Mac në Linux.

Më tej ne do të tregojmë se si të instaloni Linux Mint në kompjuterin tuaj.



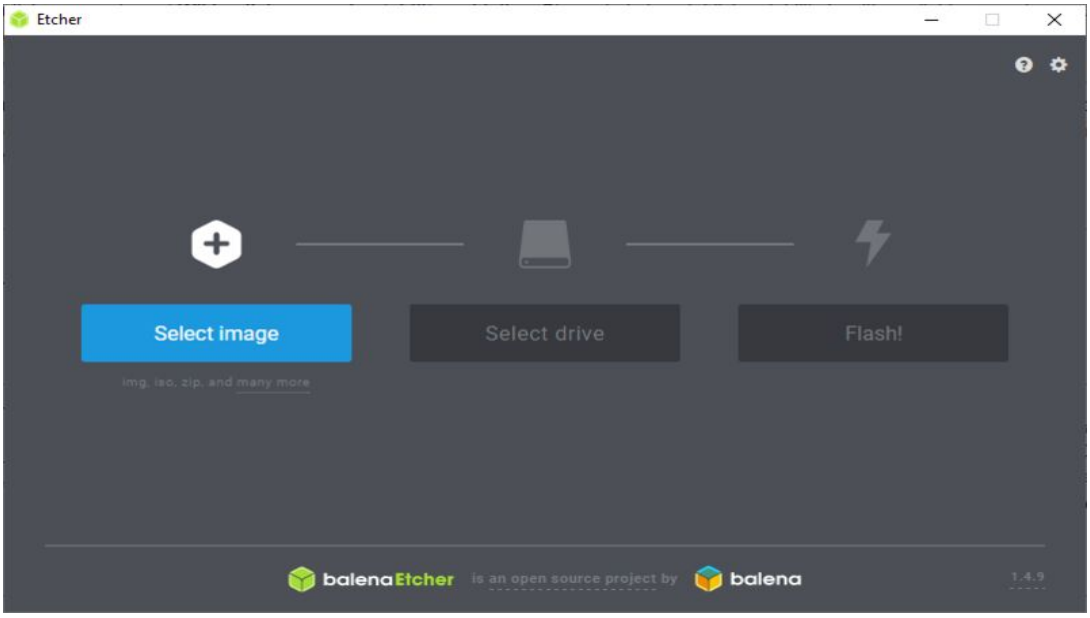
Linux Mint (Cinnamon) desktop

PERGATITJA E INSTALIMIT ME USB

1. Ruani të dhënat tuaja nga sistemi juaj Windows në media të jashtme. shtë më mirë të fshini plotësisht instalimin e Windows megjithëse Windows dhe Linux mund të funksionojnë krah për krah.
2. Shkarkoni këtu Linux Mint Cinnamon ISO. Mund të zgjasë 30 minuta ose më shumë në varësi të lidhjes tuaj https://www.linuxmint.com/download.php.

SHKARKOJE ISO PREJ USB ME ETCHER

1. Përgatitni një USB me të paktën 2 GB hapësirë, ku do të shkruani skedarin ISO.
2. Në Windows apo macOS, shkarkoni Etcher prej këtu https://etcher.io, instaloje dhe filloni.
3. Në Etcher klikoni ***Select image*** dhe zgjedhni skedarin tuaj Linux Mint ISO file.
4. Klikoni ***Select drive*** dhe zgjedhni USB tuaj.
5. Klikoni ***Flash!*** Kjo do ta shkarkojë ISO drejt në USB.



Dukja e Etcher

INSTALIMI I LINUX MINT

1. Kyçni kompjuterin tuaj me anë të USB.

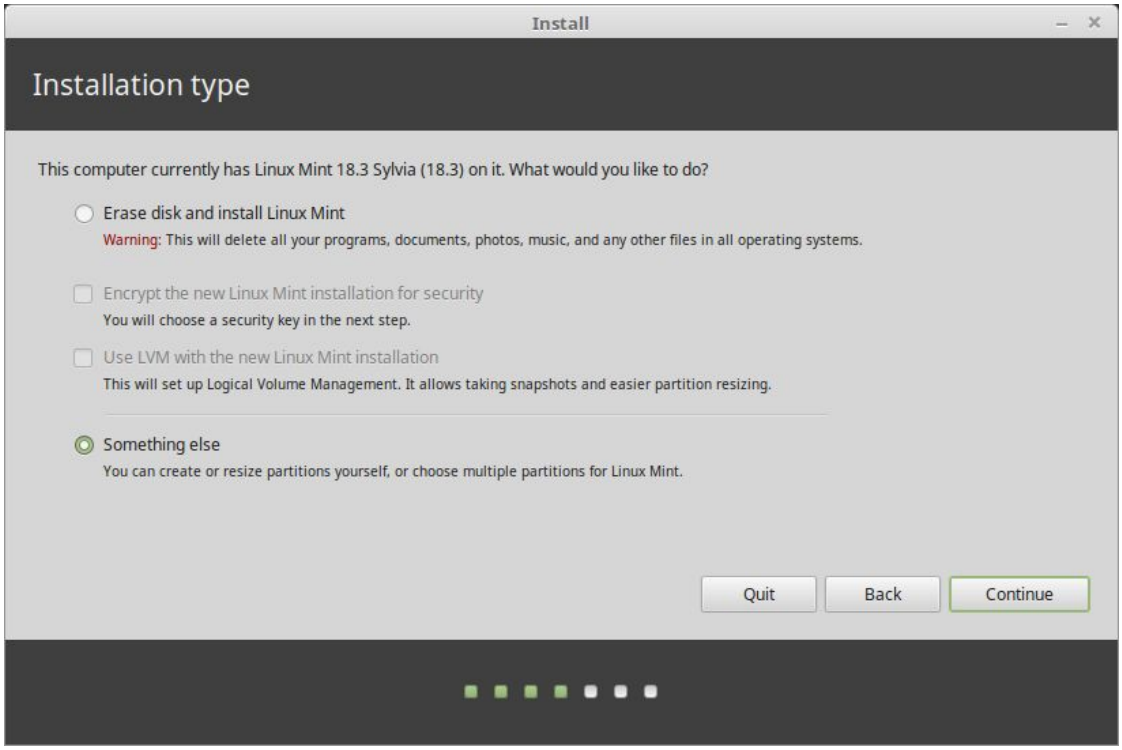
2. Kur të kyçni kompjuterin me anë të USB flash, Linux Mint fillon një sesion të drejtpërdrejtë. Ju futet automatikisht dhe ju tregon një desktop me instaluesin në të. Ju mund ta përdorni këtë për të provuar se si ju pëlqen Linux Mint.

3. Sesioni i drejtpërdrejtë është i ngjashëm me një sesion normal të Linux Mint pasi të instalohet përgjithmonë në kompjuter, por më i ngadalshëm pasi që funksionon nga USB. Ndryshimet që ju bëni në sesionin e drejtpërdrejtë nuk janë të përhershme.

INSTALIMI I LINUX MINT NË KOMPJUTER

1. Për të instaluar përgjithmonë Linux Mint në kompjuterin tënd, në desktop kliko dy herë ***Install Linux Mint***
2. Zgjidhni gjuhën tënde.
3. Lidhuni me internet.
4. Nëse lidheni me internet, shtypni kutinë për të instaluar kodet multimedia.
5. Zgjidhni mënyrën e instalimit.
6. Nëse Linux Mint është i vetmi sistem operativ që dëshironi të veproni me të në këtë kopmjuter dhe të gjitha të dhënat mund të humbasin në ***Hard Drive***, zgjedh ***Erase disk*** dhe instaloni Linux Mint.

PARALAJMËRIM



Kriptimi i instalimit të ri Linux Mint për sigurinë i referohet kriptimit të plotë të diskut. Nëse jeni i ri në Linux përdorni drejtorinë e shtëpisë (mund ta zgjidhni atë më vonë gjatë instalimit).

7. Nëse një sistem tjetër operativ është i pranishëm në kompjuter, instaluesi ju tregon një mundësi për të instaluar Linux Mint së bashku. Nëse zgjidhni këtë mundësi, instaluesi automatikisht ndryshon madhësinë e sistemit tuaj operativ ekzistues, bën vend dhe instalon Linux Mint përkrah tij. shtë vendosur një menu boot për të zgjedhur midis dy sistemeve të funksionimit sa herë që ndizni kompjuterin tuaj.
8. Zgjidhni zonën kohore.
9. Zgjidhni paraqitjen e tastierës tuaj.
10. Vendosni detalet e përdoruesit. Emri juaj i përdoruesit është emri i llogarisë tuaj që përdoret për të hyrë në vend, ndërsa emri i hostit (hostname) është emri i kompjuterit tuaj.
11. Për të mbrojtur të dhënat tuaja personale kundër njerëzve që kanë qasje fizike në kompjuterin tuaj, shtypni Encrypt my home folder.
12. Zgjidhni fjalëkalim të vështirë.
13. Ndiqni slideshow-in përderisa Linux Mint është duke u instaluar në kompjuterin tuaj.
14. Pasi të jetë përfunduar instalimi, klikoni Restart Now.
15. Pastaj kompjuteri do të fillojë të fiket dhe t'ju kërkojë të hiqni USB. Pas rindezjes, kompjuteri juaj duhet t'ju tregojë një menu boot ose të fillojë sistemin tuaj të ri të instaluar Linux Mint Linux.

D)TAILS: NJË SISTEM OPERATIV EDHE MË I SIGURT

Tails ka kuptimin “The Live Amnesic Incognito System”. shtë një sistem operativ me burim të hapur, me bazë Linux, që mbron intimitetin dhe anonimitetin e përdoruesit. Asnjë gjurmë e përdorimit të kompjuterit tuaj nuk lihet në sistem pasi të jetë mbyllur, ai është i drejtuar ndaj intimitetit dhe sigurisë, duke hyrë në internet në mënyrë anonime në mënyrë të paracaktuar, duke anashkaluar çdo censurë, dhe vjen si i parainstaluar me siguri të aktivizuar me mjete me burim të hapur. Ajo nuk është adresuar në thellësi këtu, por duhet ta konsideroni nëse mendoni se po punoni në tema shumë të ndjeshme, veçanërisht me ato që përballen aktorët shtetërorë me agjenci të sofistikuara të inteligjencës. Shih këtu për më shumë **https://tails.boum.org/.**

SHFLETIMI I INTERNETIT NË MËNYRË MË TË SIGURT

Shfletimi i internetit ju ekspozon ndaj rreziqeve të shumta. Kjo pjesë adreson rreziqet në komunikimin midis kompjuterit tuaj dhe serverit që pret faqen e internetit që po kërkoni. Fillon me një listë të shtesave (add-on) që çdo përdorues duhet ta përdorë. Pastaj shpjegon se çfarë është VPN dhe si të instalohet një. Së fundmi, për nivelin më të lartë të rrezikut, shpjegon Tor-in dhe shfletuesin Tor për shfletim më të sigurt.

A) PAKETAT ADD-ON PËR SHFLETUESIN TËND TË TANISHËM

Ju duhet të filloni duke instaluar disa shtesa (add-ons) në shfletuesin tuaj aktual Firefox ose Chromium (një version i Chrome pa shërbimet e Google).

Shtesat (Add-ons)

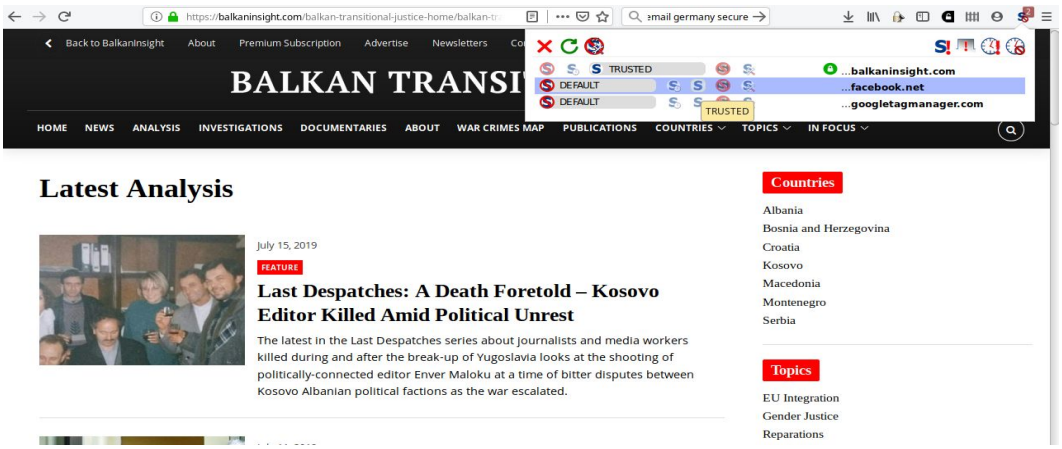
Shumica e shfletuesve të njohur janë të sigurtë që e bëjnë identitetin, vendndodhjen dhe aktivitetin tuaj në dispozicion. Sidoqoftë, ka disa zgjerime që do të ndihmojnë në rritjen e intimitetit dhe sigurisë.

Zgjerimet e mëposhtme në dispozicion si Firefox dhe Chromium rekomandohen:

HTTPS Everywhere: Forcon kriptimin për të gjitha lidhjet midis shfletuesit tuaj të internetit dhe serverit të internetit që po vizitoni. Vini re se disa faqe në internet nuk ofrojnë një lidhje të tillë. Ju mund të shihni statusin e një lidhjeje të veçantë duke klikuar në ikonat në të majtë të shiritit të adresave të shfletuesit tuaj. https://www.eff.org/https-everywhere

uBlock Origin: Një bllokues efikas i reklamave dhe gjurmuesve. shtë e zakonshme për skriptet e vendosura në kompjuterin tuaj për t'ju identifikuar dhe për të ndjekur sjelljen tuaj duke krijuar profilin tuaj të sjelljes në internet. uBlock Origin bllokon të gjithë gjurmuesit e tillë.
https://github.com/gorhill/uBlock#installation

Më të përparuar: NoScript Security Suite: Shumica e ueb-faqeve moderne funksionojnë në JavaScript, një gjuhë skriptimi e cila mund të shfrytëzohet. NoScript lejon JavaScript, Flash, Java dhe ërmbajtje të tjera të ekzekutueshme të drejtohen vetëm nga fushat e besuara të zgjedhjes suaj (p.sh. faqja juaj e bankave), duke lehtësuar dobësitë e shfrytëzueshme nga distanca. Nëse keni nevojë për më shumë mbrojtje, NoScript lejon që këto shkrime të ekzekutohen vetëm në faqet në të cilat keni besim. Thënë kështu, duhet ca kohë për të ndërtuar listën e vendeve që ju besoni duke lejuar skriptet legjitime dhe të nevojshme ndërsa ato të tjera bllokohen si parazgjedhje. https://noscript.net/getit



Pamja e shtesës NoScript me statusin e JavaScript në faqe (bllokimi i kodit nga Facebook dhe serverët Google)

B) PËRDORIMI I VPN

VPN ka kuptimin e Virtual Private Network (Rrjeti Virtual Privat). shtë një formë e kalimit të të gjithë informacioneve tuaja përmes një serveri tjetër që u shfaqet të tjerëve sikur të jetë nga ai server tjetër. Kjo teknikë maskon IP-në tuaj e cila mund të përdoret për të identifikuar vendndodhjen tuaj dhe ndoshta edhe juve. Tuneli gjithashtu ju mbron nga 'sytë e këqij' në afërsinë tuaj, siç është ISP-ja juaj ose qeveria në vendin tuaj. VPN mund të ofrohet nga kompania juaj duke siguruar për shembull që lidhjet tuaja publike WiFi nuk mund të lexohen. VPN gjithashtu lejon të anashkaloni çdo filtër të internetit të implementuar në juridiksionin tuaj.

Sidoqoftë, edhe me VPN trafiku juaj është akoma i ndjeshëm ndaj monitorimit dhe përcjelljes nga vetë VPN, serveri i shërbimit me të cilin lidheni dhe nga lojtarët e tjerë pasi të dalë VPN në internet publik.

Përzgjedhja e një ofruesi të mirë VPN në një juridiksion miqësor me ligje të favorshme është thelbësore. Sjellja e VPN varet nga besimi dhe reputacioni që ata kanë ndërtuar si shërbime dhe këto nuk janë gjithmonë transparente pavarësisht nga ato që mund të pretendojnë, ose papritmas mund të ndryshojnë. Shumica e VPN paguhen me kartë krediti dhe ato mund të ndërtojnë një profil të zakonit tuaj të shfletimit i cili do t'ju identifikojë. Prandaj, VPN janë të përshtatshme vetëm në disa skenarë për të luftuar kërcënimet në rrjetin tuaj të menjëhershëm.

Dy shërbime të mira VPN janë FreedomeVPN me qendër në Finlandë dhe ProtonVPN me qendër në Zvicër, por ju duhet të bëni vetë hulumtimin tuaj për të siguruar që po merrni shërbimin më të mirë. Të gjithë ata kushtojnë disa euro në muaj për t'u përdorur, por FreedomeVPN ofron një shtresë themelore falas, të cilën do t'i demonstrojmë këtu.

Përdorimi i aplikacionit ProtonVPN Windows

ProtonVPN dhe ofruesit e tjerë të shërbimeve publikojnë aplikacionet e tyre kryesisht për Windows, macOS, Android dhe iOS të cilat janë konfiguruar gati prandaj nuk ju nevojitet ndonjë paraprakisht konfigurim i kërkuar ndryshe. Më poshtë është udhëzimi se si të instaloni dhe lidheni nga një PC Windows. Shikoni https://protonvpn.com/support/ për më shumë ndihmë në sistemet e tjera të funksionimit (macOS, Linux, Android dhe iOS).

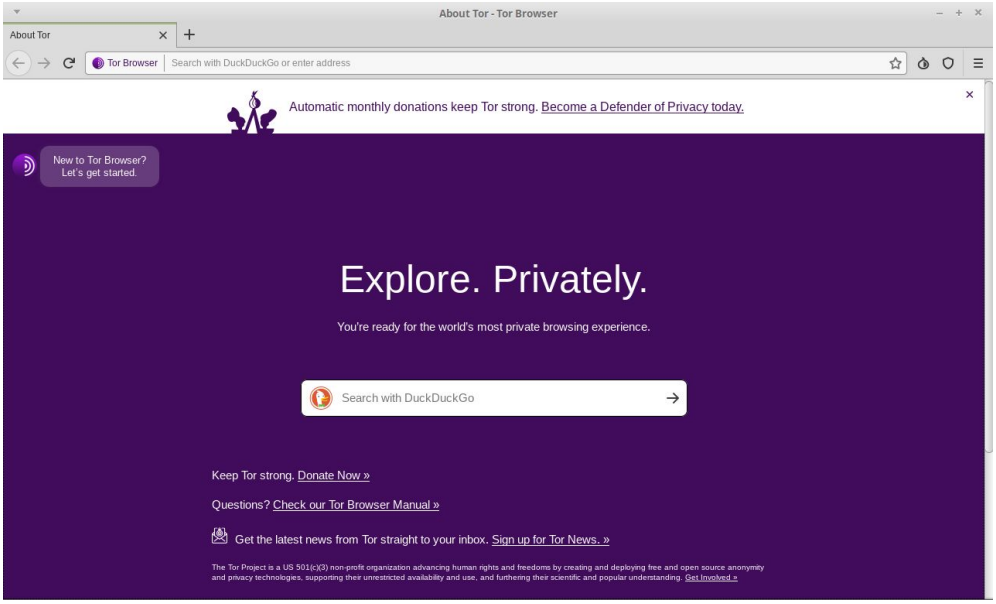
1. Shkoni në https://account.protonvpn.com/signup dhe regjistrohuni për planin e kufizuar. Nëse keni një llogari ProtonMail, mund ta përdorni atë.
2. Për ta shkarkuar ProtonVPN, shkoni te https://protonvpn.com/download/ dhe klikoni **Download for Windows.**
3. Kur të përfundojë instalimi, gjeni shkurtoren dhe klikoni dy herë mbi të për të filluar aplikacionin. Ekrani i hyrjes do të shfaqet aty ku duhet të futni letrat kredenciale të ProtonVPN për t'u identifikuar. Vendosni letrat kredenciale të krijuara në hapin 1.
4. Kur të identifikoheni, do të shihni opsionet për navigim dhe lidhje të shpejtë dhe të lehtë.
5. Tani mund ta shihni listën e vendit me secilin që ka një listë të serverëve VPN që mund të përdorni duke klikuar shigjetën poshtë. Zgjedhni njërin prejt tyre dhe kliko Quick Connect.

Ekrani i lidhjes ProtonVPN

6. Vini re se llogaria falas ju lejon të përdorni vetëm serverët falas në Holandë, SHBA dhe Japoni. Zgjedhni atë më të afërt për ju për një performancë më të mirë, me gjasë Holandën, ose ato të tjera nëse jeni rezident të atyre shteteve.
7. Mbarove.

C) SHFLETUES MË I SIGURT: TOR BROWSER

Shfletimi në internet i nënshtrohet mbikëqyrjes në nivele të ndryshme. Rrjeti Tor Onion është krijuar për të mbrojtur kundër gjurmimit, mbikëqyrjes dhe censurimit në internet. Tor Browser është shfletuesi i sigurt që drejton trafikun e tij përmes rrjetit Onion dhe ka përmirësime të tjera të sigurisë. Çdo seancë e shfletuesit Tor është unik.



Hapja e ekranit të Tor Browser

Përdorimi i Tor Browser

1. Shkoni në faqen zyrtare të Tor Browser për të shkarkuar Browser Tor për platformën tuaj https://www.torproject.org/download/ shtë i gatshëm për Windows, macOS, Linux dhe Android. Shikoni pjesën e shfletimit më të sigurt celular më poshtë për ta përdorur atë në celular.
2. Për Windows, shkarko **.exe file** dhe fillo.
3. Klikoni në menynë Start dhe filloni Tor Browser.
4. Herën e parë kur filloni të përdorni Shfletuesin Tor, do të shihni dritaren Tor Network Settings. Kjo ju ofron mundësinë që të lidheni direkt me rrjetin Tor i cili duhet të funksionojë në Evropën Juglindore, ose të konfiguroni shfletuesin Tor për lidhjen tuaj në rast se ju përdorni një proxy ose lidhjet Tor janë bllokuar nga ISP / i vendit tuaj.

Shfletuesi Tor u jep përdoruesve një mundësi për të përcaktuar nivelin e dëshiruar të sigurisë. Në shfletuesin Tor, klikoni në ikonën e simbolit (në të djathtë të shiritit të adresës) dhe klikoni "Advanced Security Options ..." për të parë opsionet. Ky opsion është vendosur në Standard si parazgjedhje, gjë që rrit përdorimin. Për të përfituar nga niveli më i lartë i intimitetit dhe anonimitetit që mund të ofrojë Tor, vendosni shiritin në nivelin më të sigurt ose më të sigurt.

DËRGIMI MË I SIGURT I POROSIVE ME E-MAIL

A) SHFLETUES MË I SIGURT: TOR BROWSER

Për ata që dëshirojnë të fshehin identitetin e vërtetë të tyre ose të tjerëve me të cilët po komunikojnë, duhet të përdoren llogari anonime elektronike, të pandara me ndonjë aspekt tjetër të identitetit tuaj në internet. Me fjalë të tjera, ato nuk duhet të lidhen me ju në asnjë mënyrë. Shërbime si Gmail dhe Microsoft Live kërkojnë një telefon ose adresë alternative elektronike, kështu që këta ofrues nuk janë idealë për llogari anonime. ProtonMail, Tutanota dhe Posteo (me pagesë) lejojnë përdoruesit të krijojnë llogari pa një informacion të tillë identifikues.

B)KRIPTIMI I POROSIVE ME E-MAIL NË SHFLETUES ME MAILVELOPE

Kriptimi i postës elektronike duke përdorur standardin OpenPGP është një praktikë e zakonshme për të siguruar që mesazhet tuaja të postës elektronike të mos lexohen nëse përgjohen gjatë rrugës ose gjatë pushimit në serverët e ofruesit të shërbimit, siç është rasti me shumicën e ofruesve të shërbimit tregtar të postës elektronike. Kriptimi i postës elektronike me OpenPGP megjithatë nuk është më i përshtatshmi për përdoruesit dhe nëse është i vjedhur çelësi privat i kriptimit, të gjitha mesazhet që një palë i ka qasje mund të lexohen. Për më tepër, nëse çelësi privat është i humbur, nuk do të mund të deshifroni ato mesazhe. Gjithashtu, email-i i koduar nuk është i përsosur pasi linja e adresuar dhe e temës (metadata) mund të lexohet nëse përgjohet, kështu e keni parasysh këtë kur e përdorni.

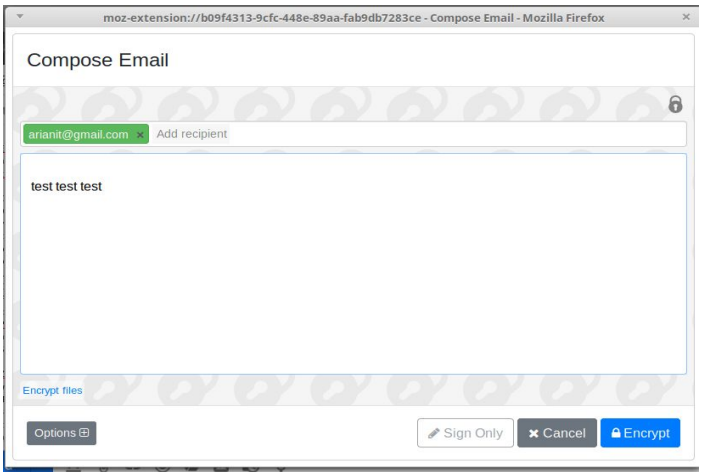
Mailvelope është një softuer falas për kriptimin nga fundi në fund **(end-to-end encryption)** të përmbajtjes së postës elektronike brenda një shfletuesi të internetit (Firefox ose Chrome / Chromium) që integron mirë me shërbimet më të njohura tregtare elektronike në internet. Mund të përdoret për të kriptuar dhe nënshkruar mesazhe elektronike dhe bashkëngjitjet duke shmangur një klient amtare me email (si Thunderbird) duke përdorur standardin OpenPGP. shtë më e dobishme pasi nuk ju detyron të kaloni në një klient të ri me email.

Vendosja e Mailvelope dhe çelësi juaj PGP

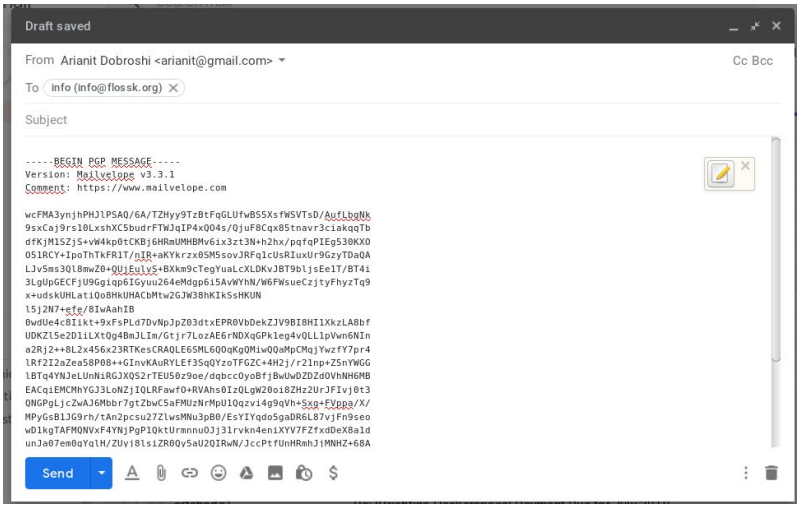
1. Shkoni te Firefox Add-ons dhe kërkoni për *Mailvelope*.
2. Në shiritin e veglave, klikoni në ikonën Mailvelope. *Dashboard* ekrani do të hapet.
3. Klikoni **Manage keys**. Pastaj **Generate** nëse nuk keni një çelës ekzistues ose **Import** nëse tashmë leni një.
4. Vendosni fushat duke përdorur emrin e lidhur me llogarinë tuaj të postës elektronike. Vendosni një fjalëkalim të sigurt që nuk do të harroni, përndryshe ju humbni qasjen në çelës. Lini cilësimet e tjera të paracaktuar.
5. Kliko **Generate** dhe prisni pak. Çelësi juaj tani është gjeneruar dhe gati për t'u përdorur. Do t'ju dërgohet një mesazh për të qenë në gjendje të ngarkoni çelësin tuaj publik në server për të gjetur të tjerët. Çelësi juaj publik është ajo që të tjerët përdorin për të koduar mesazhe për ju. Ju përdorni çelësin tuaj privat për t'i hapur ato.
6. **Paralajmërim:** Çelësi juaj privat duhet të mbahet sekret. Asnjëherë mos e ndani me askënd.

Dërgimi i porosive të kriptuara me e-mail

1. Për të kriptuar email-at e dikujt, së pari duhet të importoni çelësin publik të personit në Mailvelope. Ju mund ta merrni atë direkt p.sh. përmes emailit, gjeni atë në faqen e internetit publike të një personi ose në një nga serverët kryesorë që pret çelësat e dhënë siç janë ato nga Ubuntu ose MIT.
2. Në Mailvelope, shkoni tek ***Key management***, bëjeni paste tekstin të çelësit publik në kuti ose klikoni ***Search***. Kërkoni me email ose emër dhe klikoni në kodin e çelësit, i cili duhet të jetë diçka si kjo *E7F3E1D6*. Vini re, ndërsa në serverat publik thuhet se çelësi i përket një personi të caktuar, ky fakt mund të jetë i prishur, kjo është arsyeja pse ju mund të dëshironi të konfirmoni kodin kyç përmes disa mjeteve të tjera me personin që zotëron çelësin.
3. Klikoni çelësin për ta dërguar atë. Tani jeni gati për të kriptuar mesazhe dhe të dhëna në atë adresë.
4. Nëse Mailvelope është aktiv, në kutinë e mesazheve të shërbimit tuaj të postës elektronike (p.sh. Gmail) do të pranoni një ikonë për të shkruar mesazhin tuaj atje. Ky mesazh do të kodohet me çelësin publik të personit që po i dërgoni, me kusht që të keni dërguar së pari çelësin e tyre.



Hapësira e tesktit në Mailvelope



Dukja e një mesazhi të kriptuar në Gmail e krijuar duke përdorur Mailvelope

SIGURIA NË SISTEMIN OPERATIV TË CELULARËVE

Shumica e llogaritjeve tuaja tani bëhen në celular, përfshirë edhe për punë të ndjeshme. Megjithatë, siguria e lëvizshme është në gjendje të keqe duke i ekspozuar përdoruesit ndaj shumë dobësive. Nga sistemet Android të vjetruara dhe të pambështetura deri tek aplikacionet që kërkojnë leje shumë, ju duhet të mendoni shumë nëse përdorni pajisje mobile për të bërë punë të ndjeshme. Vetë Android dhe aplikacione të caktuara, madje gjoja ato të sigurta si WhatsApp, do t'ju kërkojnë të përditësoni të dhënat tuaja në server, të cilat ruhen në mënyrë të qartë dhe mund të jenë lehtësisht të arritshme me urdhër gjykate ose ndonjë institucioni tjetër.

BAZAT: SIGURIA E APLIKACIONIT ANDROID

Ndërsa Apple aprovon aplikacione celulare përpara se ato të publikohen në App Store-in e saj individualisht, duke bërë kujdes të duhur për ngarkesën e intimitetit që u imponojnë atyre aplikacioneve për përdoruesit, nuk ndodh e njëjta gjë me aplikacionet Android nga Google Play Store.

Nëse përdorni Android, me siguri ju është kërkuar dhe iu është dhënë aplikacioneve qasje në gjëra të tilla si historinë e thirrjeve tuaja, mesazheve, vendndodhjes, kamerës, mikrofonit dhe më shumë. Para versionit 6.0, Android u kërkoi përdoruesve të aprovojnë kërkesat për leje në një paketë, duke ngritur dyshimet pse një aplikacioni të caktuar ka nevojë për qasje në mikrofon nëse merret vetëm me foto. Nga versioni 6.0 e tutje, Android lejon përdoruesit të zgjedhin lejet që do t'i japin aplikacionit. Ju duhet t'i kushtoni vëmendje asaj se çfarë aplikacionesh instaloni në telefonin tuaj. Për më tepër, nëse nuk planifikoni të përdorni një veçori të caktuar të aplikacionit, p.sh. fotot e etiketuara me vendndodhjen tuaj, atëherë mos i aprovoni ato leje ose i aprovoni ato në baza të përkohshme vetëm kur ju duhen.

Për të kontrolluar lejet e dhëna tashmë:

1. Hapni **Settings** te pajisja juaj.
2. Shtypni **Apps** and **notifications**. Zgjedh çfarëdo aplikacioni, dhe shtyp **Permissions ose App permissions** për të rishikuar lejet bazuar në lejen specifike.
3. Shtyp **On** apo **Off**. Nëse nuk jeni i sigurt, çaktivizoni atë. Android do t'ju kërkojë leje kur të ketë nevojë dhe ju mund të merrni vendimin bazuar në arsyeshmërinë e kërkesës në atë situatë.

BAZAT: MBAJTJA E ANDROIDIT TUAJ TE PERDITESUAR

Shumica e version eve Android janë të vjetruara për shkak të modelit të shpërndarjes së softuerëve që Google (prodhuesi i Android) përdor me klientët e tij (prodhuesit e telefonit celular). Shpeshherë, Google humbet kontrollin mbi përditësimin e softuerit të tij, i cili tani është në përgjegjësi të prodhuesit ose kompanisë që nuk mund të ketë një nxitje për të mbështetur pajisjen tuaj të veçantë përtej një kohe të kufizuar. Në përgjithësi, pajisjet e markës Google dhe telefonat më të mirë të prodhuesve kanë periudha më të gjatë mbështetjeje. Pajisjet Apple iOS gjithashtu mbështeten për një kohë më të gjatë. Kjo është arsyeja pse gjithmonë duhet të kërkoni një periudhë mbështetjeje me përditësimet e softuerit përpara se të blini një model të caktuar.

Përditësimi i Androidit tuaj

Ju mund të shihni numrin e versionit Android dhe nivelin e përditësuar të sigurisë në Settings. Do të merrni njoftime kur përditësimet janë të disponueshme për ju nëse sistemi është akoma i përditësuar. Ju gjithashtu mund të kontrolloni vetë përditësimet. Vini re se këto udhëzime mund të ndryshojnë në varësi të versionit Android. Këshillohuni me faqen e internetit të prodhuesit të telefonit tuaj nëse keni vështirësi t'i ndjekni ato.You can see your device's Android version number and security update level in your Settings.

Për të parë se cilin version të Androidit e keni ju

1. Hapni Settings te pajisja juaj.
2. Në fund, shtypni System > Advanced > System update. Nëse nuk shihni Advanced, shtyp About phone.
3. Shihni versionin tuaj Android dhe nivelin e sigurisë së patch-it nën titujt përkatës

Merrni përditësimet më të fundit të Android-it që janë në dispozicion për ju

Kur të merrni një njoftim për përditësim, hapeni atë dhe shtypni përditësimin.
Nëse e keni pastruar njoftimin ose pajisja juaj ka qenë jashtë linje:

1. Hapni Settings te pajisja juaj.
2. Në fund, shtypni System > Advanced > System update. Nëse nuk shihni Advanced, shtypni About phone.
3. Do të shihni statusin tuaj të përditësuar. Ndiqni çdo hap në ekran.

SIGURIA NË KOMUNIKIM

A)BAZAT: DËRGIMI I POROSIVE ME SIGNAL OSNOVE: RAZMENA PORUKA SA SIGNALOM

Shikoni këto karakteristika të sigurisë, ndërsa vlerësoni klientin e mesazheve të menjëhershme që përdorni:

- a janë të koduara mesazhet gjatë kalimit?
- janë mesazhe të koduara tek ofruesi nëse ekziston një (d.m.th., jo nga pjesëmarrësit)?
- a vërtetohen identitetet e kontakteve?
- a është komunikimi i sigurt nëse çelësat janë vjedhur?
- a është kodi i softuerit i hapur për rishikim të pavarur?
- a është dokumentuar si duhet modeli i sigurisë?
- a ka pasur auditime të pavarura të kodeve të fundit?

Në këtë aspekt, WhatsApp është më i mirë se Viber, dhe Signal është më i mirë se WhatsApp.

Signal-i plotëson pjesën më të madhe të kritereve të mësipërme dhe është mjaft afër nga pikëpamja e shfrytëzimit për ato që ju mund të përdorni tashmë, prandaj është e rekomanduar. Signal-i është në dispozicion falas në Android, iOS dhe Desktop (Windows / Mac / Linux), është me burim të hapur dhe është rishikuar nga kolegët, mbulon tekstet, thirrjet dhe video-thirrjet dhe skedarët, të gjitha të kriptuara dhe gjatë pushimit të pajisjes.

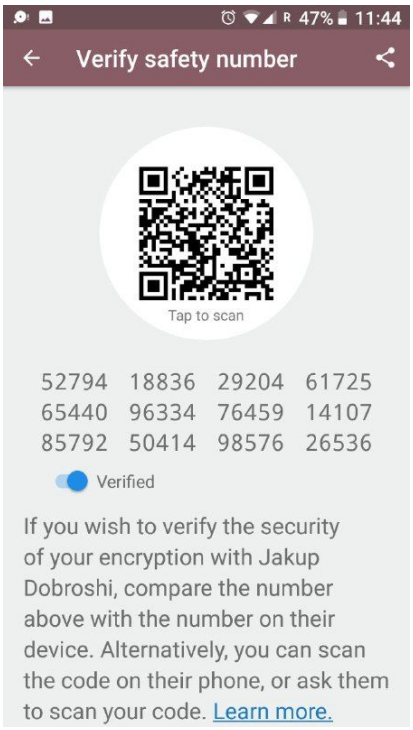
Për të instaluar Signal-in në Androidin-in/IOS-in tuaj,

1. 1. Konfirmoni se celulari juaj është i version it Android 4.4/ iOS 10.0 ose më të fundit.
2. 2. Kërkoni ***Signal Private Messenger*** në Google Play/App Store dhe instalojeni.
3. 3. Ndiqni udhëzimet në ekran për të përfunduar procesin e regjistrimit të ngjashëm me aplikacionet e tjerë që kërkojnë nga ju që të regjistroni numrin tuaj të telefonit.

Verifikimi i kontakteve tuaja

Në Signal, ju jeni në gjendje të verifikoni kontaktin tuaj për të siguruar që llogaria me të cilën po bisedoni i takon vërtetë personit për të cilin pretendon se i përket, dhe se kanali juaj i sigurt i komunikimit nuk ka qenë i dëmtuar.

1. Në Signal, si ju, ashtu edhe kontakti juaj duhet të shkoni në ekranin në të cilin normalisht do të bisedonit me kontaktin tuaj.
2. Shtypni ikonën me tri pika vertikale (lart djathtas), pastaj klikoni ***Conversation settings > Verify*** safety number.
3. Krahasoni numrat e dhënë ose shtypni ***Tap*** për të skanuar pajisjen tjetër me Signal-in për tu krahasuar. Ju gjithashtu mund ta lexoni atë me zë të lartë ose ta dërgoni atë në palën tjetër. Nëse ato janë të njëjta, klikoni ***Verified***.

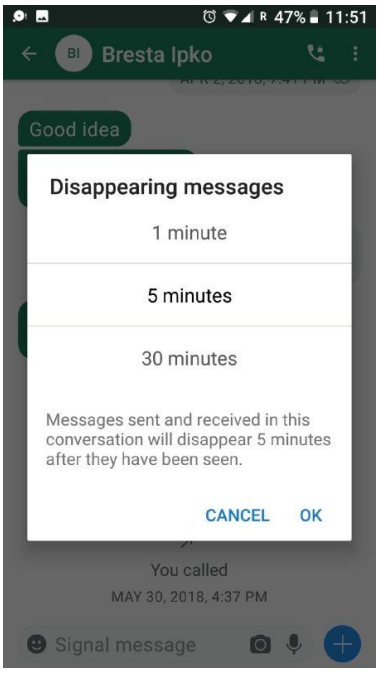


Dukja e ekranit për verifikim në Signal

Fshirja automatike e mesazheve

Ju mund të dëshironi që mesazhet të fshihen pas një periudhe të caktuar.

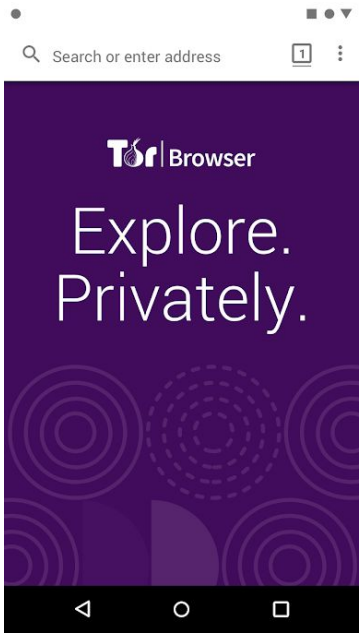
1. Në Signal, shko te ekrani që ju normalisht bisedoni me kontaktet tuaja.
2. Shtypni ikonën me tre pika vertikale (lart djathtas), pastaj shtypni ***Disappearing messages.***
3. Në ekranin e ri, zgjedh periudhën. Një mesazh do të shfaqet në bisedë që tregon këtë periudhë.



Fshirja e mesazheve në Signal, vendosja e fshirjes automatike në 5 minuta

SHFLETIMI MË I SIGURT PËRMES CELULARIT: TOR BROWSER

Tor Browser është gjithashtu i disponueshëm për Android dhe iOS. Nëse përdorni Android, mund ta shkarkoni në Google Play Store duke kërkuar *Tor Browser for Android*. Në Apple, App Store kërko për *Onion Browser*.



Dukja e Tor Browser në Android

SHPËRNDARJA E TË DHËNAVE

Shpërndarja e të dhënave që zënë hapësirë të madhe është një sfidë e përditshme. Dy mënyra për të dërguar të dhëna në mënyrë të sigurt tashmë janë mbuluar, përmes emailit të koduar të OpenPGP dhe përmes mesazheve të menjëhershme siç është Signal. Për të dhëna edhe më të mëdha, zgjidhje të tjera janë të nevojshme. Më poshtë janë dy mënyra të tjera për ta bërë atë. Firefox Send është i përshtatshëm për skenarë me rrezik të ulët dhe praktik ndërsa OnionShare është mjaft i sigurt, veçanërisht nëse të dhënat janë të koduara në fillim.

A) BAZA: FIREFOX SEND

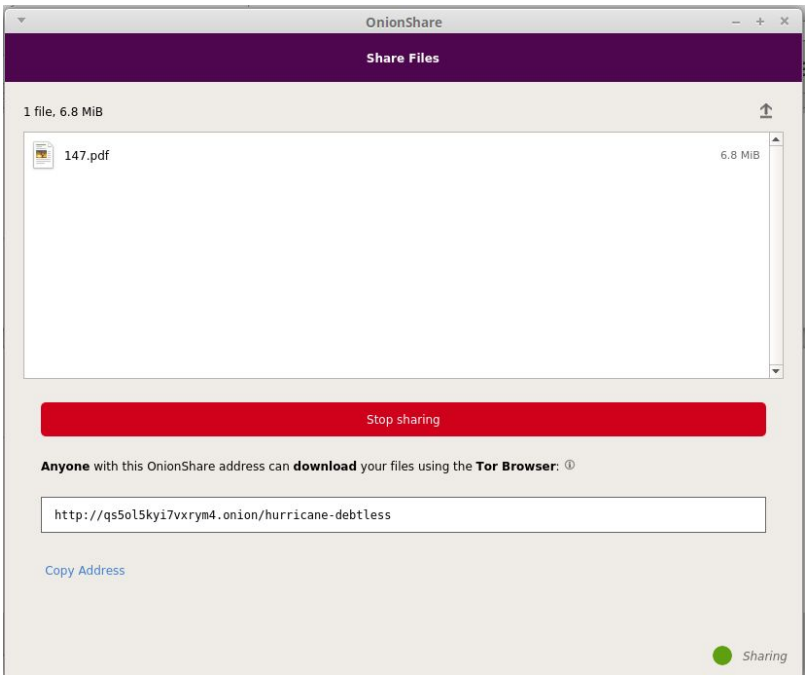
Firefox Send është një zgjidhja më e fundit që është e lehtë për t'u përdorur. Ju mund të dëshironi të kriptoni skedarin së pari duke përdorur opsionin Encrypt a File në Mailvelope (ka një kufizim prej 50 MB) ose përmes mjeteve të tjera përpara se të ngarkoni skedarin. Për ta dërguar atë, shkoni në http://send.firefox.com, zgjidhni skedarin për të ngarkuar dhe vendosni opsionet. Vini re se skedarët më të mëdhenj kërkojnë dhe më shumë kohë në server që të regjistroheni.

B) SHPËRNDARJA MË E SIGURT: ONIONSHARE

OnionShare ju lejon të shpërndani dokumente shumë të sigurt dhe në mënyrë anonime të çfarëdo madhësie. Krijon një server të përkohshëm vjedhurazi të internetit. Një adresë e pakontestueshme gjenerohet dhe është e përbashkët që marrësi të hapet në Shfletuesin Tor për të shkarkuar skedarët. Ndërsa është shumë i sigurt, dobësi e këtij mjeti është që ju bëni host skedarët në kompjuterin tuaj, prandaj ju duhet të vazhdoni mbani atë derisa të pranohet nga palët e tjera. Marrësi gjithashtu duhet të përdorni Shfletuesin Tor për të marrë dokumentet.

Për ta përdorur atë:

1. Filloni duke instaluar OnionShare për platformën tuaj nga këtu https://onionshare.org
2. Pasi të instalohet, hapni OnionShare.
3. Shtoni dokumentin dhe klikoni ***Start sharing.*** Nuk ka asnjë kufizim se sa madhësi duhet të ketë dokumenti. Në fund të procesit, OnionShare do t'ju japë një adresë të tillë si kjo http://qs5ol5kyi7vxrym4.onion/hurricane-debtles të cilën duhet t'ia dorëzoni marrësit përmes një kanali të sigurt. Vini re se çdokush me adresë mund të ketë qasje në dokumentet me kusht që OnionShare të jetë akoma në veprim.



Dukja e OnionShare

KU TË SHKOJMË PREJ KËTU?

Nëse e keni vështruar më shumë këtë manual dhe dëshironi më shumë këshilla ose ballafaqoheni me kërcënime të nivelit më të lartë, materiali tjetër i mirë i udhëzimit është i qasshëm lirisht në internet, megjithëse është kryesisht në gjuhën angleze dhe në disa pjesë është e vjetruar.

Security in a Box - Mjete dhe taktika digjitale të sigurisë

https://securityinabox.org/

Security in a Box është një projekt i Tactical Technology Collective dhe Front Line Defenders. Udhëzuesit e Taktikave në këtë pako mjetesh mbulojnë parimet themelore, duke përfshirë këshilla se si të përdorim mediat sociale dhe telefonat mobil më sigurt. Manualët e mjeteve ofrojnë udhëzime hap pas hapi për t'ju ndihmuar të instaloni, konfiguroni dhe përdorni disa softuer dhe shërbime thelbësore të sigurisë digjitale. Veglat e Komunitetit (The Community Toolkits) përqendrohen në grupe specifike të njerëzve - ndonjëherë në rajone specifike - të cilët përballen me kërcënime të rëndësishme digjitale të sigurisë. Ato përfshijnë këshilla të përshtatura për mjetet dhe taktikat që janë të rëndësishme për nevojat e këtyre grupeve të veçanta.

Surveillance Self-Defense: Këshilla, mjetet dhe mënyrat e komunikimeve më të sigurta në internet
https://ssd.eff.org/

shtë një listë e udhëzuesve dhe planeve mësimore nga Electronic Frontier Foundation.

•Siguria e informacionit për gazetarët, një manual nga Centre for Investigative Journalism
https://tcij.org/sites/default/files/u11/InfoSec for Journalists V1.3.pdf

Një manual i krijuar për të udhëzuar gazetarët dhe organizatat e medieve se si të praktikojnë sigurinë e informacionit në epokën digjitale, duke mbrojtur punën e tyre, burimet dhe komunikimet në një shumëllojshmëri të niveleve të rrezikut, përfshirë nivelet më të larta të rrezikut.

Ndihmës i Sigurisë Digjitale për Gazetarët nga Reporterët pa Kufij
https://helpdesk.rsf.org/

Duke filluar nga korriku 2019 RSF do të ofrojë video falas online dhe konsultime online mbi sigurinë digjitale në baza të rregullta. Këto seminare mund të shihen ose live ose në një kohë të vonë. Seminaret do të përqendrohen në mënyrën e mbrojtjes së llogarive të medieve sociale nga piratimi, si të mënjanohen censurimet duke përdorur një VPN dhe cilat aplikacione për mesazhe në telefona të mençur janë më të mirat për punën gazetareske. Më shumë shërbim mbështetës të individualizuar do të ofrohet në të ardhmen.

RRETH AUTORIT

Arianit Dobroshi është President i Bordit Ekzekutiv në FLOSSK, një organizatë joqeveritare që promovon softuer falas dhe me burim të hapur në Kosovë. Ai ka trajnuar gazetarët dhe anëtarët e shoqërisë civile për mjetet e intimitetit dhe ka lobuar kundër legjislacionit të mbikëqyrjes digjitale në Kosovë. Mund të kontaktoni në arianit.dobroshi@flossk.org.

Ky Manual është botuar si pjesë e projektit InfoSec për Ballkanin i financuar nga Radio Azia e Lirë përmes Fondit të Teknologjisë së Hapur dhe implementuar nga Open Data Kosovo dhe FLOSSK.

Versioni origjinal u shkrua në anglisht. Ai është gjithashtu në dispozicion edhe në gjuhën shqipe, boshnjake, maqedonase, malazeze dhe serbe.


OPEN
TECHNOLOGY
FUND


RFA
Radio Free Asia


ODK
OPEN DATA KOSOVO


Free Libre Open Source Software Kosova