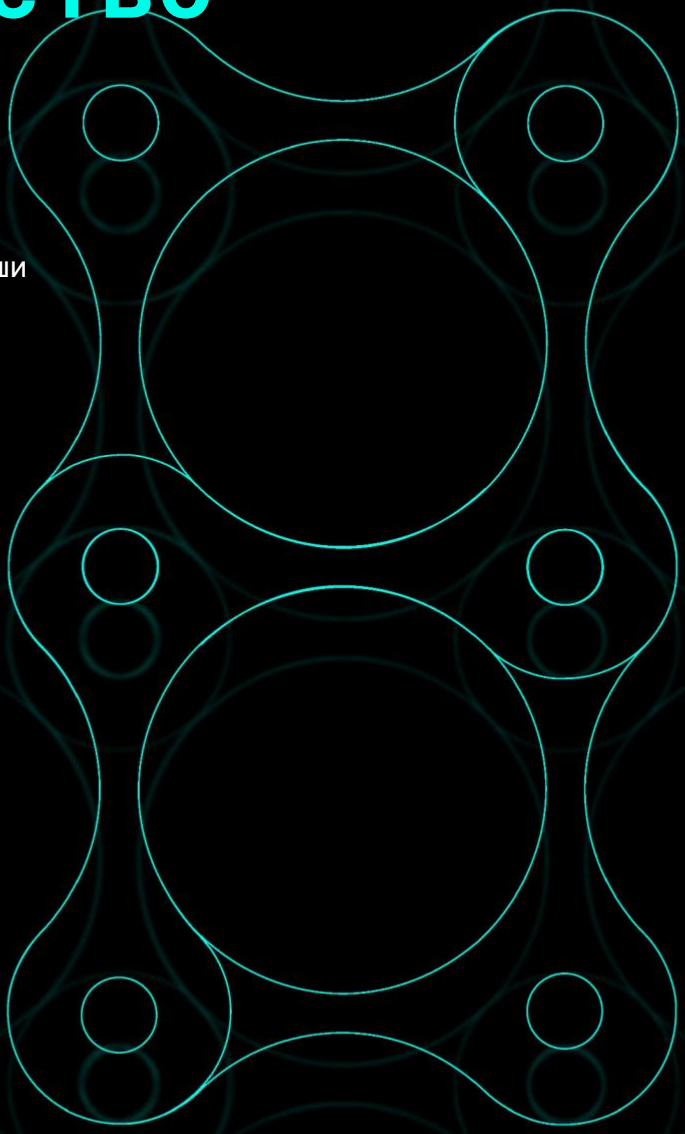
Прирачник за безбедност на информации за новинари и граѓанско општество

Од Арианит Доброши



INFOSEC for Balkans

Јули, 2019 г.

СОДРЖИНА

ВОВЕД

Овој прирачник е наменет за новинари и други работници од граѓанското општество во регионот на Југоисточна Европа, кои можеби во моментот се соочуваат со најсофистицирани безбедносни закани (infosec). Авторот смета дека е достоен компромис да се жртвува одредена строгост на безбедноста на информациите ако промовира поголемо усвојување на овие практики и алатки.

Овој прирачник е насочен кон луѓе со ниски безбедносни практики, како и на општата популација. Вака, ги утврдува основните практики за безбедност на информации што се соодветни за секого.

Секој дел од овој прирачник вклучува најмалку две нивоа на безбедност: многу основно ниво на безбедност што ги бараат сите да се практикуваат, и другиот дел, ризикот што треба да го има секој истражен новинар и службеник за безбедност. Сепак, некои новинари и службеници за безбедност во регионот се соочуваат со уште поголеми нивоа на закани и треба да бараат други подлабоки извори, од кои некои се наведени во вториот дел од овој прирачник.

Овој прирачник е напишан во јули 2019 година. Заканите за безбедноста на информациите и нивните мерки за ублажување постојано се развиваат, така што овој датум треба да се има предвид кога се однесува на тоа во иднина.

А) ЗА КОГО Е ОВОЈ ПРИРАЧНИК?

Овој прирачник е наменет за новинарите, особено оние кои работат во истражувачко новинарство и активисти на граѓанското општество, особено на оние кои се занимаваат со чувствителни теми поврзани со владеењето на правото. Така кажано, ова е добра алатка за користење од страна на секој што сака да го ажурира своето основно знаење за infosec, особено затоа што е достапен и на јазиците на регионот, на кои им недостасуваат ресурси во оваа област: албански, босански, македонски, црногорски и српски.

Техничкото ниво што е потребно за извршување на оваа работа е фундаментално и мора да биде достапно за сите. Некои од алатките бараат малку жртвување при употреба и вежбање по секојдневната практика.

Б) КАКО ДА ГО ПРОЧИТАТЕ ОВОЈ ПРИРАЧНИК?

Секој наслов на овој прирачник може да се прочита одделно, врз основа на вашите непосредни потреби за безбедност на информации. Сепак, се препорачува да ги покриете сите делови од овој прирачник, бидејќи тој е дизајниран како список на минимална работа што треба да ја вежбате за да се заштитите себе си и вашите ресурси. Може да се вратите на тоа кога имате повеќе време и да ги покриете сите. Првите поднаслови ги содржат основните работи што секој корисник на компјутер треба да ги практикува, иако според нашиот преглед тоа не е така. Вториот поднаслов треба да обезбеди безбедносно ажурирање за повеќето основни корисници.

Вториот дел од прирачникот вклучува создавање посилни, корисни лозинки за сите платформи. Во дел три ние го покриваме вашиот десктоп оперативен систем: работи што треба да се направат со вашиот оперативен систем Windows и малку помош при инсталирање на Linux Mint, што е стандарден и побезбеден систем, но лесен за употреба. Во четвртиот дел се обраќаме во безбедно пребарување, а во петтиот дел како да испраќаме безбедни пораки преку е-пошта. Во шестиот дел разгледуваме некои работи што треба да се направат за безбедноста на мобилниот систем, додека во седмиот дел се обраќаме на безбедноста во комуникацијата. Конечно, делот осум се однесува на споделувањето на податоците, додека деветтиот дел ни дава список на ресурси за читателите кои сакаат да направат повеќе.

В) ИДЕНТИФИКУВАЊЕ НА ВАШИТЕ БЕЗБЕДНОСНИ ПОТРЕБИ

Неовластениот пристап до вашите податоци може да резултира во негова употреба, откривање, упаднување, изменување, инспекција, снимање или уништување. Меѓутоа, бидејќи дигиталните закани се невидливи, сложени и честопати невидливи, може да се потценат или занемарат.

Постојат неколку начини да ги разгледате заканите со кои се соочувате и безбедноста на информациите што ги имате. Најосновната закана со која се соочуваат сите корисници се директните закани со кои се соочува секој граѓанин од регионот, иако во овој прирачник се насочени повеќе специјализирани закани.

Земјите во регионот ја спроведоа Директивата за задржување на податоци на ЕУ, со која се предвидува зачувување на метаподатоци (поврзани со податоци) за сите ракувани телекомуникации, вклучително и списоци на сите телефонски повици, IP адреси, текстуални пораки итн., испратени или примени за период од шест до дваесет и четири месеци, што може да се постигне со судска одлука. И покрај тоа што самата содржина на комуникацијата не штеди, напредокот од законскиот мандат до супервизија со мнозинство не е толку тежок и барањето за судски налог зависи од кршливоста на системите за владеење на правото во регионот. Дури и метаподатоците се екстремно откривачки бидејќи може да им овозможи на оние кои имаат можност да создаваат социјални графикони од вашиот живот и индиректно да ги идентификуваат содржините и ресурсите со кои се занимавате, дури и ретроспективно.

Во специјализирани закани, супервизијата користи специјализирани и софистицирани алатки против целта. Технологијата за ова стана поевтина, а пристапот до владите и приватните лица станува полесен. На пример, во 2015 година беше откриено дека владата на Северна Македонија прислушувала телефони на околу 20 000 луѓе. Исто така, постојат докази дека српската влада повторно го гласала Интернетот во одредени места каде може лесно да се добие. Ова беше пред неколку години и ситуацијата помина од лоша во полоша. Ако верувате дека се соочувате со овој вид закана, тогаш овој прирачник не е доволен за да се заштитите и треба да побарате посветена помош.

КРЕИРАЊЕ НА ПОБЕЗБЕДНИ ЛОЗИНКИ

Една безбедна лозинка е случајна, доста долга и комбинира список со големи букви, броеви и други знаци (на пр. Xkvv3.K3? Rrz). Сепак, можно е да имате безбедни лозинки користејќи комбинација на зборови, под услов да биде доволно долга, уникатна за услугата, случајни и да не се поврзани со вас. Комбинација на случајни зборови што лесно можете да ги запомните е доволно сигурна лозинка (на пр. WITHIN-WIRE-GRASS-pluto-save).

А) ДВОФАКТОРСКАТА АВТЕНТИКАЦИЈА

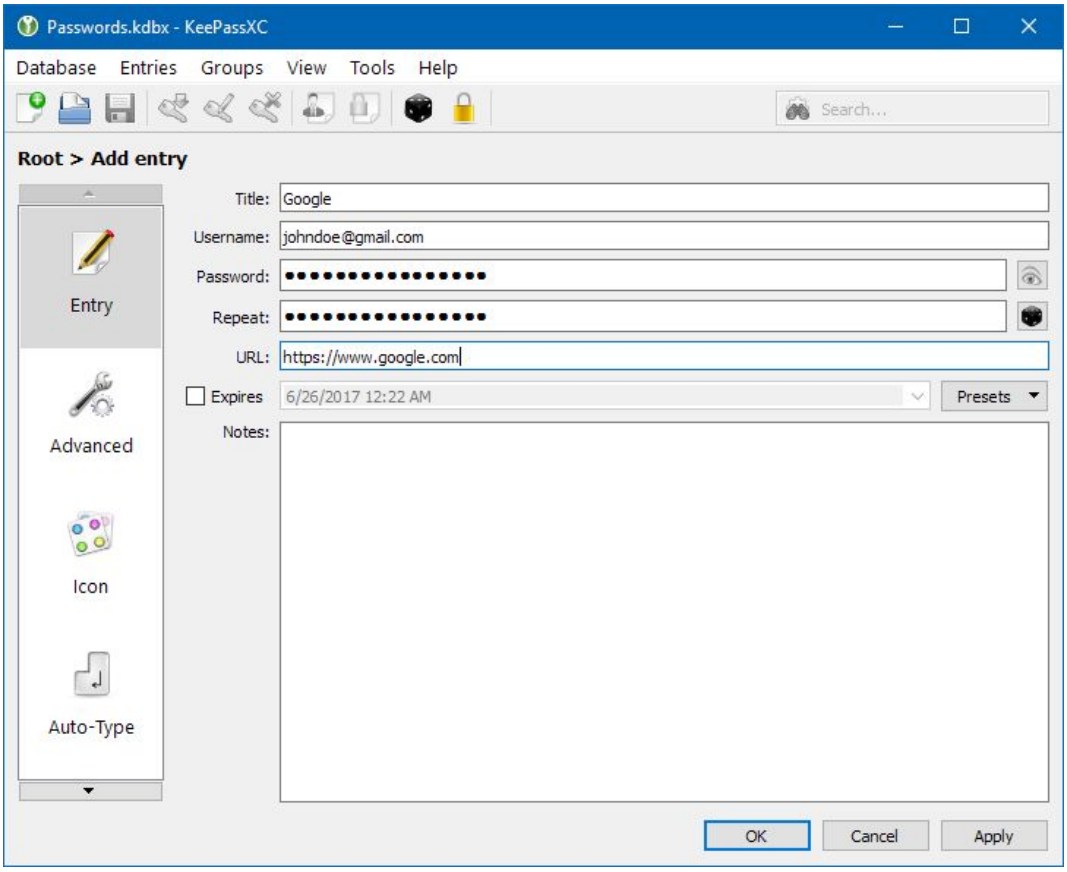
Кога и да е достапно, двофакторската автентикација обезбедува втора алатка на горниот дел од вообичаената лозинка за да ги обезбеди вашите сметки преку интернет. Двофакторската автентикација (2FA) може да се испрати на вашиот телефон преку телефонски повик, СМС, е-пошта или може да се генерира на вашиот Андроид телефон или со хардверски приклучок. Веќе можете да користите еден за вашите банкарски сметки. Вториот фактор додава дополнителен слој на заштита во случај вашата лозинка да биде загрозена. Овозможувањето автентикација на вториот фактор зависи од вашата програма и треба да погледнете под Settings > Password или слично за да го овозможите тоа. Сепак, сите услуги сè уште не го нудат тоа.

На пример, додека користите услуги на Google, можете да ја посетите https://myaccount.google.com/signinoptions, да се регистрирате со вашата сметка, да го активирате и да изберете алатка за да добиете привремена лозинка за втор пат, нормално по СМС. Забележете дека доколку го изгубите телефонскиот број, ќе бидете блокирани од вашата сметка. Затоа, мора да поставите барем една опција за резервна шанса, така што ќе можете да се регистрирате, дури и ако другите втори чекори не се достапни. Еднократните шифри за печатење може да бидат најлесниот начин да ви овозможат да се регистрирате ако го изгубите вашиот број или ако патувате.

Б) КОРИСТЕЊЕ НА СОФТВЕР ЗА КРЕИРАЊЕ И УПРАВУВАЊЕ СО ЛОЗИНКИ

Лозинките што ги користите мора да бидат единствени за секоја услуга што ја користите. Запомнувањето на безбедни лозинки брзо станува невозможно, се бара алатка за управување со нив. Можете да користите специјална програма за да го олесните креирањето и управувањето со безбедни лозинки. Добар отворен извор е KeePassXC (https://keepassxc.org) достапен за macOS Windows и Linux, менаџер за лозинка што ги чува корисничките имиња и лозинките во шифрирана база на податоци, заштитени со совршени лозинки. Исто така, доаѓа со PWGen, силен генератор на случајни лозинки.

Други популарни алтернативни софтверски програми се LastPass и 1Password. Тие ги чуваат шифрираните лозинки на интернет и некои карактеристики може да бидат достапни само под платената верзија, но тие обезбедуваат подобра употребливост и лозинките се чуваат на интернет. Да се биде затворен извор, невозможно е самостојно да се контролира безбедноста на овие два програми.



Слика од екранот на KeePassXC

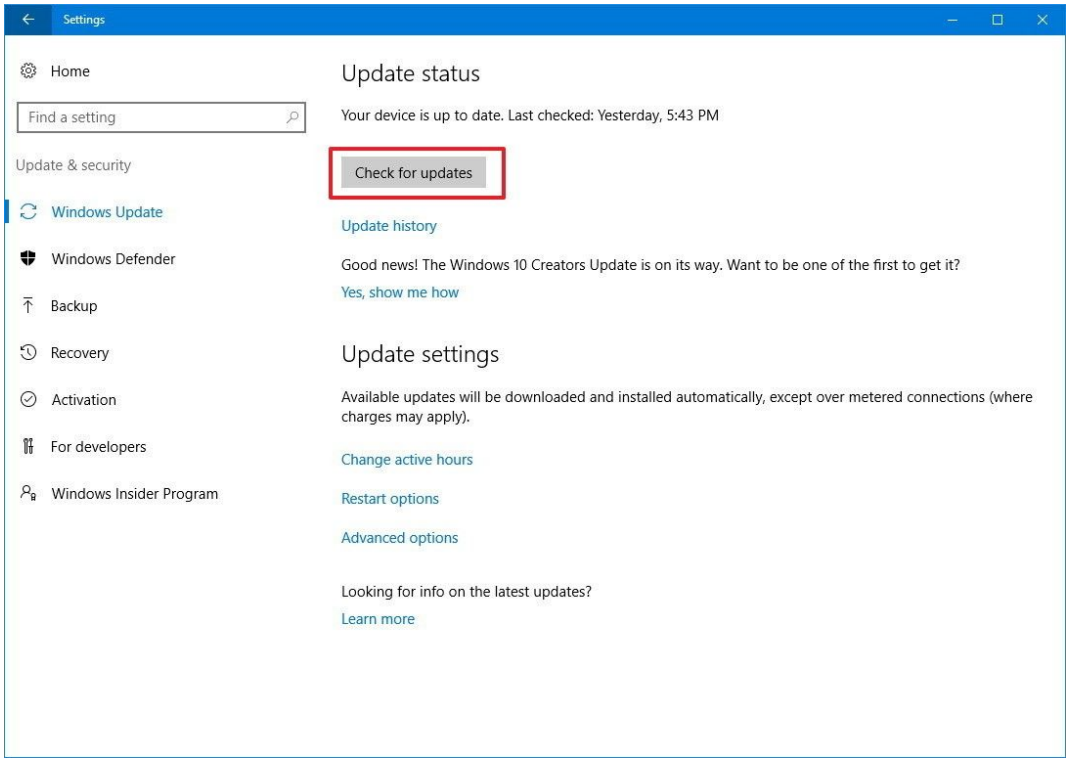
КОРИСТЕЊЕ НА ПОБЕЗБЕДЕН ОПЕРАТИВЕН СИСТЕМ

Оперативниот систем на вашиот десктоп е основа на вашата безбедна дневна пресметка. Во принцип, безбедноста на системот со ниска до висока е: Windows 7 или 10 кои се широко користени, но исто така и помалку безбедни, macOS кој е посигурен по дифолт, па не е адресиран овде, Linux Mint, вкус на системот Linux, адресиран овде, и Tails, исто така базиран на Linux, дизајнирани со сигурност на информации во умот, но со компромиси за употреба.

А) АЖУРИРАЊЕТО НА ВАШИОТ WINDOWS

Ажурирањето на Windows е од суштинско значење ако работите на машина поврзана со интернет. Многу пати, пиратските копии на Windows се забранети за ажурирање што ве изложуваат на сите видови на други штети и закани. Забележете дека Windows 7 ќе биде во функција на својот производител „Microsoft“ до крајот на 2019 година и затоа нема да се ажурира со збир на промени во безбедносниот софтвер по тој датум. Треба да се ажуриате на Windows 10 над оваа точка.

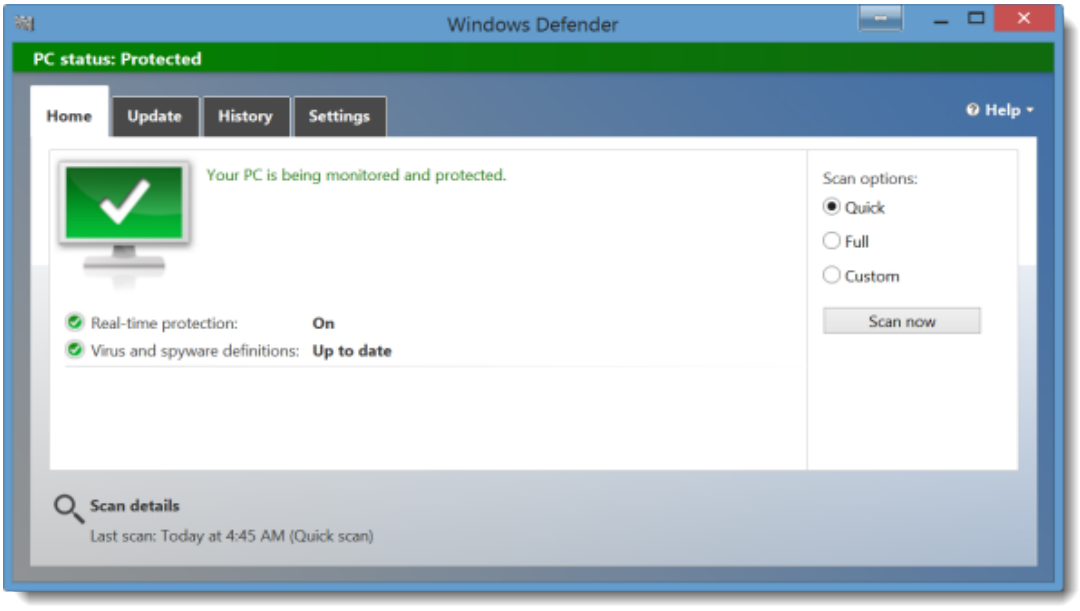
За да бидете сигурни дека вашиот Windows е ажуриран, треба да пребарувате за „Windows Update“ во лентата за пребарување на Windows, кликнете Check for Updates и проверете дали се гледа „No updates available“ на екранот. Забележете дека не сите ажурирања се безбедни ажурирања и затоа можете да ги игнорирате. Ако ажурирањето на Windows е невозможно да се изврши, тогаш треба да побарате помош за да се осигурате дека компјутерот е ажуриран.



Статусот на Windows Update

Покрај тоа, потребен ви е софтвер кој ве штити од вируси и штетници. Во повеќето случаи, вградениот Windows Defender е соодветен и не користи дополнителни ресурси на вашиот компјутер. За да ја стартувате, деинсталирајте ја другата антивирусна програма. Отидете во лентата за пребарување на Виндоус и напишете "Windows Defender". Осигурете се дека е можна заштита во реално време и ограничувањата на вирусот се ажурирани. Ако не, треба да ги освежите преку табулаторот Update.

Ако вашиот систем е застарен подолго време, извршете темелно скенирање на вашиот систем за да бидете сигурни дека е чист, што може да трае неколку часа. Ако не можете сами да ги решите можните наоди, треба да побарате помош.

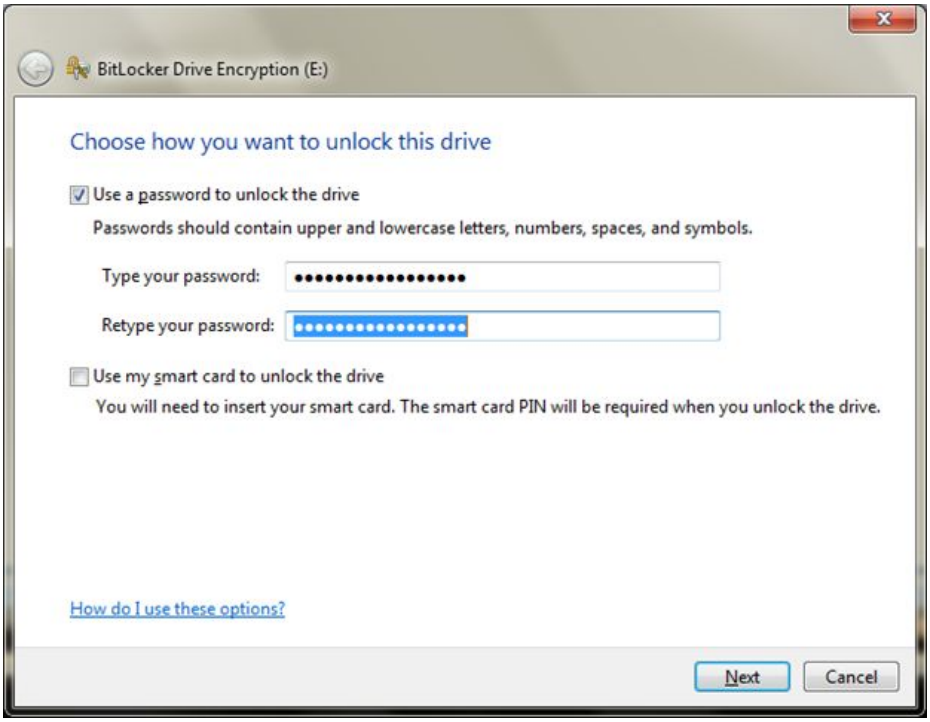


Windows Defender ажуриран

Б) КРИПТИРАЊЕ НА ДИСКОТ

Податоците на вашиот компјутерски диск лесно може да го прочитаа противникот кој има физички пристап до него, ако дискот не е криптиран. Повеќето верзии на Windows до Windows 7 Pro немаат стандардно инсталирано криптирање на дискот.

Целосно криптирање на дискот на BitLocker во системски простор бара компјутер со доверлив модул за платформа (TPM) вграден во вашиот компјутер. Овој чип ги генерира и чува клучевите за криптирање што ги користи BitLocker. Можете да го избегнете ова со употреба на Group Policy за да дозволите употреба на BitLocker без TPM иако ќе жртвите одредена безбедност.



згледот на Bitlocker

Може да криптирате несистемски погон или отстранлив диск без TPM, па затоа е подобро да ги имате вашите податоци на посебен погон (обично во просторот „D“).

Најлесен начин да го овозможите BitLocker во празно место е да отворите File Explorer и кликнете со маус два на просторот што го сакате, а потоа кликнете Turn on BitLocker. Ако не ја видите оваа опција во вашето мени за контекст, тогаш веројатно немате верзија на Pro или Enterprise на Windows, затоа ви треба друга алтернатива.

Предупредување: BitLocker ви обезбедува клуч за обновување што треба да го чувате безбедно чувајќи некаде безбедно надвор од постојниот компјутер или со внесување и зачувување физички. Во случај да го заборавите клучот или вашиот TPM модул е уништен, ова ќе ви овозможи повторно да ги користите вашите податоци.

Ако користите друг оперативен систем како што е Linux, опцијата за криптипање на дискот е обезбедена за време на инсталацијата. Погледнете го делот за инсталација на Linux Mint за да видите како да го активирате тоа.

За сите системи, добра самостојна алатка за слободен софтвер што ја почитуваат безбедносните професионалци е VeraCrypt (порано TrueCrypt) достапно овде https://www.veracrypt.fr.

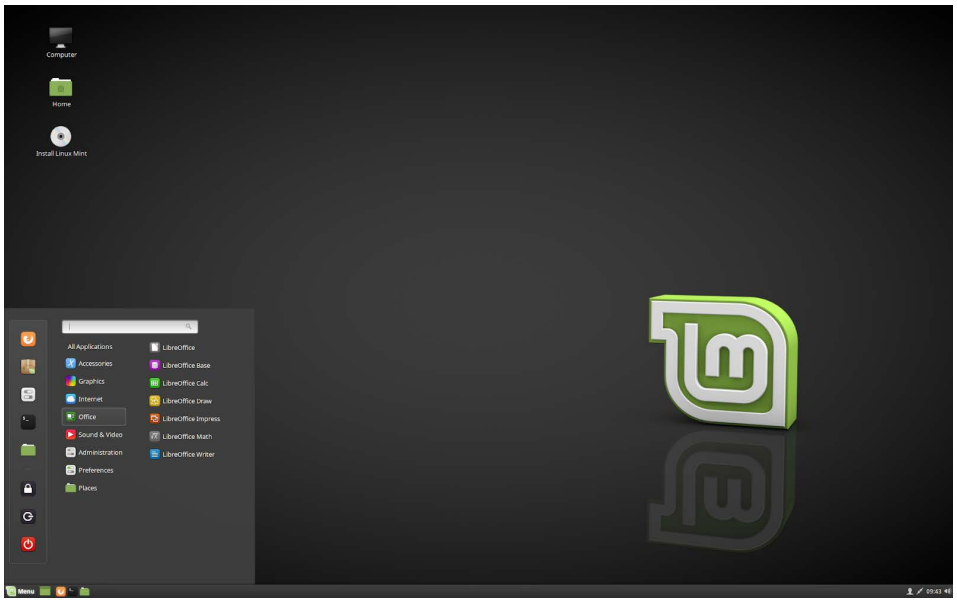
B) LINUX MINT: ПОБЕЗБЕДЕН ОПЕРАТИВЕН СИСТЕМ

Linux е слободен и оперативен систем со отворен извор. Тој е побезбеден од Windows бидејќи не се соочува со некои безбедносни проблеми на Windows, но ќе бара од вас да научите нов оперативен систем и понекогаш бара команди за пишување за да ги направите работите.

Постојат многу „вкусови“ или повторувања на Linux: Ubuntu, Fedora и Linux Mint се најпопуларните оние со општа намена и Tails се посветени на оние со поголеми безбедносни потреби. Треба да користите која било верзија што најчеста во вашата околина, така што можете да побарате помош ако заглавите. Ако ова не е остварлива опција, тогаш одете со Linux Mint, што ние го објаснуваме овде. Тој е покорисен за корисниците, има голема заедница за поддршка, е некомерцијален и има чувство за Windows кон оние што минуваат покрај тоа.

Бидејќи Linux има пристап до складиште на илјадници бесплатен софтвер со отворен извор, можеби ќе треба да научите нови апликации за да ги завршите работите, бидејќи некои производители на софтвер не објавуваат за Linux. Алтернативи од Windows до Linux се: LibreOffice за Microsoft Office, Gimp до Photoshop, Audacity for eiditing sound итн. Користете http://alternativeto.net за да најдете алтернативи на софтверот што го користите на Windows или Mac на Linux.

Следно, ќе ви покажеме како да инсталирате Linux Mint на вашиот компјутер.



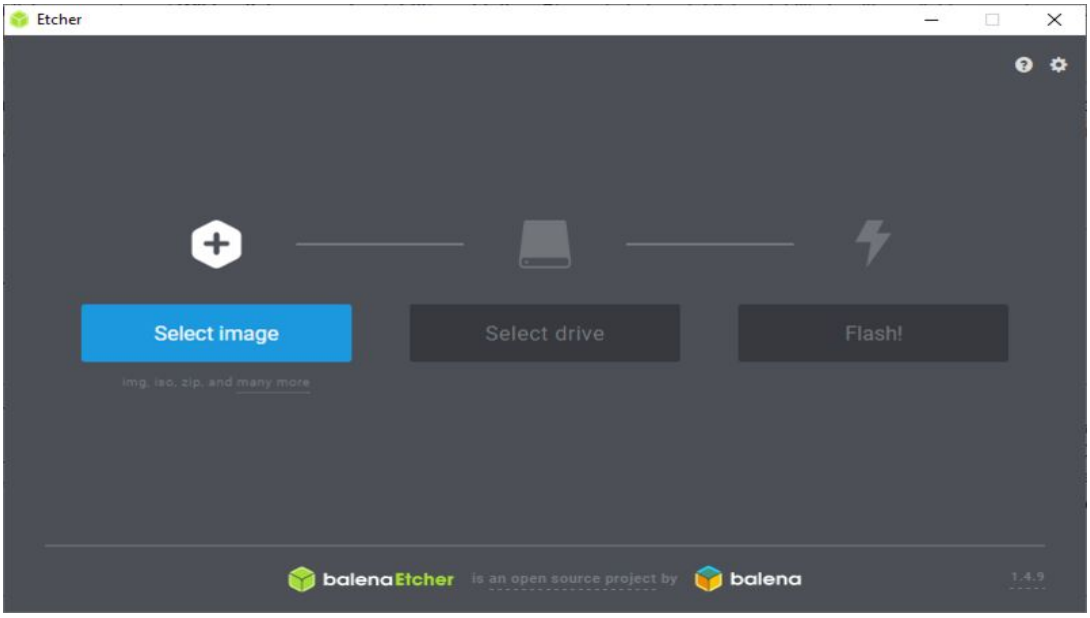
Linux Mint (Cinnamon) десктоп

ПОДГОТОВКА НА USB ИНСТАЛАЦИЈА

1. Зачувајте ги вашите податоци од вашиот Windows систем во надворешни медиуми. Најдобро е целосно да ја деинсталирате инсталацијата Windows иако Windows и Linux можат да работат рамо до рамо.
2. Преземете го Linux Mint Cinnamon ISO тука. Може да трае 30 минути или повеќе, во зависност од вашата врска: https://www.linuxmint.com/download.php.

ПРЕЗЕМЕТЕ ISO ОД USB СО ETCHER

1. Подгответе USB со најмалку 2 GB простор, каде што ќе ја нашишете ISO-датотеката.
2. На Windows или macOS, преземете го Etcher од тука https://etcher.io, инсталирајте го и започнете.
3. Во Etcher, кликнете **Select image** и изберете ја вашата датотека Linux Mint ISO.
4. Кликнете **Select drive** и изберете вашиот USB.
5. Кликнете **Flash!** Ова ќе го преземе ISO директно на USB.



Изгледот на Etcher

ИНСТАЛИРАЊЕ НА LINUX MINT

1. Вклучете го компјутерот преку USB

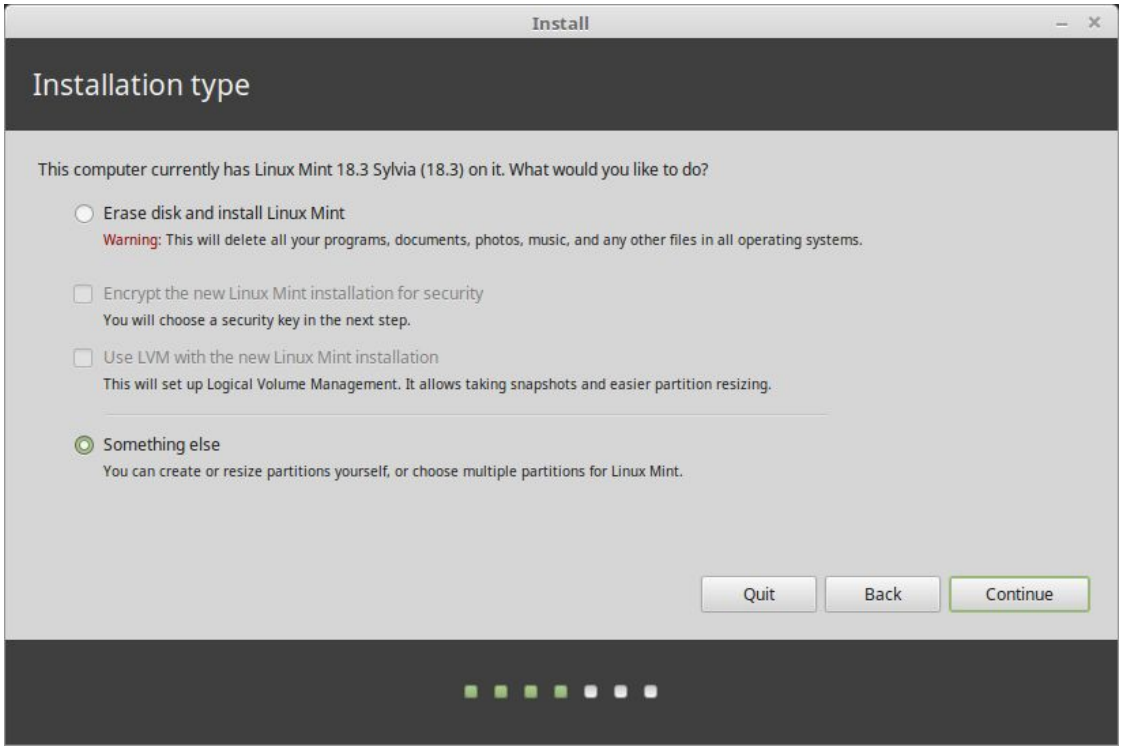
2. Кога ќе го вклучите вашиот компјутер користејќи USB, Linux Mint започнува сесија во живо. Автоматски се најавува и ви покажува работна површина со инсталерот на неа. Можете да го користите ова за да проверите како ви се допаѓа Linux Mint.

3. Директниот дел е сличен на нормалниот дел од Linux Mint, откако е трајно инсталиран на компјутерот, но побавен, бидејќи работи на USB. Промените што ги правите во живо не се постојани.

ИНСТАЛИРАЊЕ НА LINUX MINT НА КОМПЈУТЕР

1. За трајно инсталирање на Linux Mint на вашиот компјутер, кликнете двапати на десктоп **Install Linux Mint**
2. Изберете јазик.
3. Поврзете се на интернет.
4. Ако сте поврзани на интернет, притиснете го кутијата за да инсталирате мултимедијални шифри.
5. Ако Linux Mint е единствениот оперативен систем што сакате да го активирате на овој компјутер и сите податоци може да се изгубат на Hard Drive, изберете Erase disk и инсталирајте Linux Mint.
6. Ако друг оперативен систем е присутен на компјутерот, инсталаторот ви покажува опција да го инсталирате Linux Mint заедно. Ако ја изберете оваа опција, инсталерот автоматски го менува големината на постојниот оперативен систем, го поставува и инсталира заедно со него Linux Mint. Менито за подигање е поставено да избира помеѓу два оперативни системи секој пат кога ќе го стартувате вашиот компјутер.

Предупредување:



Криптирајте ја новата инсталација на Linux Mint за безбедност се однесува на целосно криптирање на дискот. Ако сте нови во Linux, наместо тоа користете криптирање на домашната директорија (можете да го изберете подоцна за време на инсталацијата).

7. Изберете ја временската зона.
8. Изберете го изгледот на тастатурата.
9. Внесете детали за корисникот. Вашето корисничко име е името на вашата сметка што се користи за локален пристап додека името на host (hostname) е името на вашиот компјутер.

10.За да ги заштитите вашите лични информации од луѓе кои имаат физички пристап до вашиот компјутер, кликнете го Encrypt my home folder.
11.Изберете силна лозинка.
12. Следете го slideshow-от додека Linux Mint се инсталиран на вашиот компјутер.
13. Откако ќе заврши инсталацијата, кликнете на Restart now.
14. Тогаш компјутерот ќе започне да се исклучува и ќе ве праша да го отстраните USB.
15. По рестартирањето, вашиот компјутер или треба да ви покаже мени за подигање или да го стартувате вашиот ново инсталиран систем Linux Mint Linux.

Г)TAILS: НАЈБЕЗБЕДЕН ОПЕРАТИВЕН СИСТЕМ

Tails има значење „The Live Amnesic Incognito System“. Тоа е оперативен систем со отворен извор, со основа Linux, кој ја штити приватноста и анонимноста на корисниците. Ниту една трага од употребата на вашиот компјутер не останува во системот откако ќе се исклучи, таа е насочена кон приватноста и безбедноста, анонимен пристап до интернет по дифолт, заобиколувајќи ја секоја цензура и доаѓа пред-инсталирано со безбедност овозможена со алатки со отворен извор. Овде не е опфатено во длабочина, но треба да го земете предвид ако мислите дека работите на многу чувствителни теми, особено на оние со кои се соочуваат државните актери со софистицирани разузнавачки агенции. Погледнете тука за повеќе https://tails.boum.org/.

ПОБЕЗБЕДНО ПРЕБАРУВАЊЕ НА ИНТЕРНЕТОТ

Пребарувањето на интернетот ве изложува на многу опасности. Овој дел ги опфаќа ризиците во комуникацијата помеѓу вашиот компјутер и серверот што е домаќин на веб-страницата што ја барате. Започнува со список на додатоци што секој корисник треба да ги користи. Потоа објаснува што е VPN и како да инсталирате. Конечно, за највисоко ниво на ризик, го објаснува Tor и Tor Browser за побезбедно пребарување.

А) ADD-ON ПАКЕТИ ЗА ВАШИОТ СЕГАШЕН ПРЕБАРУВАЧ

Треба да започнете со инсталирање на некои додатоци (add-ons) на вашиот сегашен пребарувач Firefox или Chromium (верзија на Chrome без услуги на Google).

Додатоци (Add-ons)

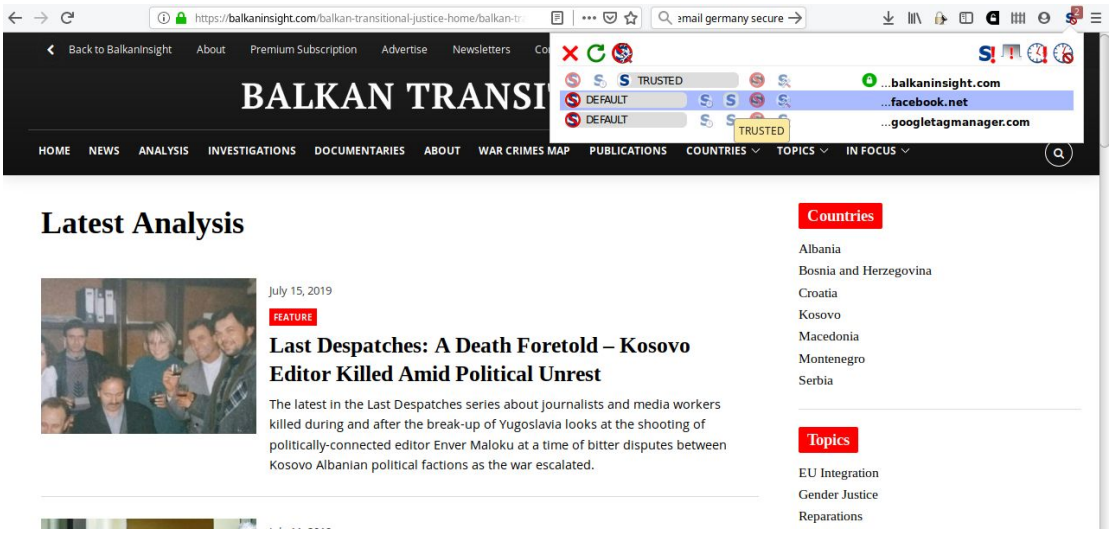
Најпопуларните пребарувачи сигурно ќе го направат вашиот идентитет, локација и активност. Сепак, постојат неколку екстензии кои ќе помогнат да се зголеми приватноста и безбедноста.

Се препорачуваат следниве екстензии достапни како Firefox и Chromium:

HTTPS Everywhere: Ја зајакнува криптирањето за сите врски помеѓу вашиот пребарувач и веб-серверот што го посетувате. Забележете дека некои веб-страници не нудат таква врска. Можете да го видите статусот на одредена врска со кликнување на иконите лево од лентата за адреса на вашиот пребарувач.
https://www.eff.org/https-everywhere

uBlock Origin: Ефикасен блокатор на реклами и трагач. Вообичаено е скриптите поставени на вашиот компјутер да ве идентификуваат и да го следат вашето однесување со создавање на вашиот профил за однесување преку Интернет. uBlock Origin ги блокира сите такви трагачи.
https://github.com/gorhill/uBlock#installation

Понапредни: NoScript Security Suite: Повеќето модерни веб-страници работат на JavaScript, јазик за скриптирање што може да се користи. NoScript дозволува JavaScript, Flash, Java и други извршни содржини да бидат насочени само од доверливи домени по ваш избор (на пр. страница на вашата банка), далечински отстранувајќи ги слабостите. Ако ви треба поголема заштита, NoScript дозволува овие скрипти да работат само на веб-страници на кои имате доверба. Така што е потребно извесно време да се изгради списокот на веб-страници на кои имате доверба со тоа што ќе дозволите легитимни и неопходни скрипти додека другите ќе бидат блокирани по дифолт.
https://noscript.net/getit



Поглед на додатокот NoScript со статус на JavaScript на страницата (код за блокирање од серверите на Facebook и Google)

Б) КОРИСТЕЊЕ НА VPN

VPN значи Virtual Private Network (виртуелна приватна мрежа). Тоа е форма на пренесување на сите ваши информации преку друг сервер што им се појавува на другите како да е од тој друг сервер. Оваа техника ја маскира вашата IP адреса што може да се искористи за да се идентификува вашата локација, а можеби и вие. Тунелот исто така ве штити од „злобните очи“ во ваша близина, како што е вашиот интернет провајдер или влада во вашата земја. VPN може да биде обезбедена од вашата компанија, на пример, дека вашите јавни WiFi конекции не можат да се прочитаат. VPN исто така ви овозможува да го заобиколите интернет-филтерот што е имплементиран во вашата надлежност.

Како и да е, дури и со VPN, вашиот сообраќај сè уште е подложен на наблудување и проследување од страна на самиот VPN, серверот за услуги на кој се поврзувате и од другите играчи откако VPN е јавно достапен.

Избирањето на добар оператор за VPN во пријателска надлежност со поволни закони е неопходно. Однесувањето на VPN зависи од довербата и угледот што тие го граделе како услуги и тие не се секогаш транспарентни без оглед на тоа што може да тврдат, или може одеднаш да се сменат. Повеќето VPN се плаќаат со кредитна картичка и можат да создадат профил на навика за прелистување кој ќе ве идентификува. Затоа, VPN-то се погодни само во некои сценарија за борба против заканите на вашата непосредна мрежа.

Две добри VPN услуги се FreedomeVPN со седиште во Финска и ProtonVPN со седиште во Швајцарија, но треба да направите свое истражување за да бидете сигурни дека добивате најдобра услуга. Сите тие чинат неколку евра месечно за користење, но FreedomeVPN нуди бесплатен основен слој, што ќе го демонстрираме овде.

Користење на апликацијата ProtonVPN Windows

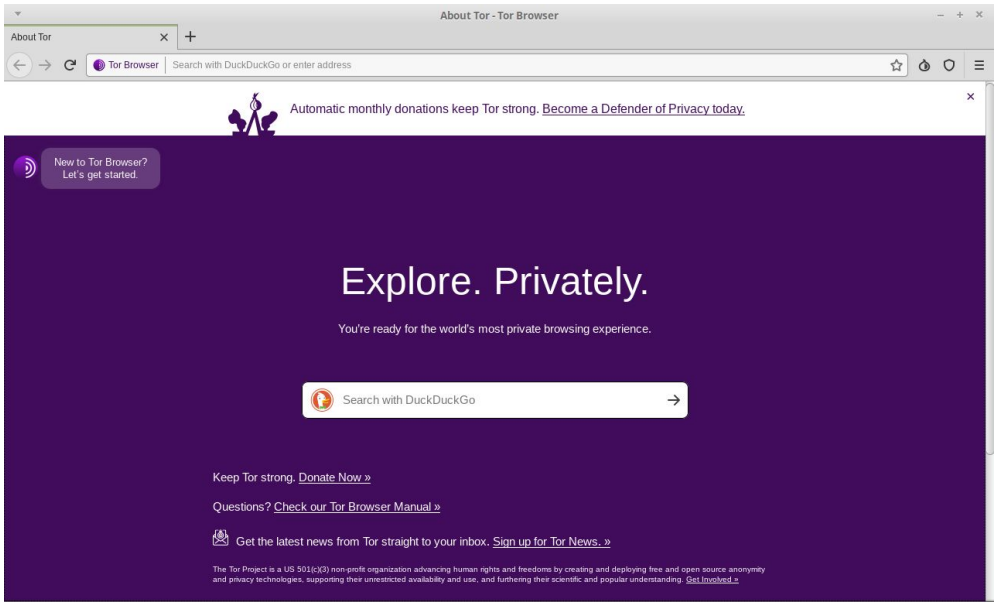
ProtonVPN и другите даватели на услуги ги објавуваат своите апликации главно за Windows, macOS, Android и iOS кои се скоро конфигурирани така што не ви требаат претходни конфигурации што се поинаку потребни. Подолу е упатството за тоа како да инсталирате и поврзете од Windows компјутер. Погледнете ја https://protonvpn.com/support/ за поголема помош на другите оперативни системи (macOS, Linux, Android и iOS).

1. Пребарувајте https://account.protonvpn.com/signup и пријавете се на ограниченият план. Ако имате сметка на ProtonMail, можете да ја користите.
2. За да преземете ProtonVPN, одете на https://protonvpn.com/download/ и кликнете **Download for Windows**.
3. Кога ќе заврши инсталацијата, пронајдете ја кратенката и кликнете двапати на неа за да започнете со апликацијата. Екранот за најавување ќе се појави таму каде што треба да ги внесете вашите податоци на ProtonVPN за да се најавите. Ставете ги податоци создадени во чекор 1.
4. Кога веќе сте најавени, ќе видите брза и лесна опција за навигација и врска.
5. Сега можете да го видите списокот на местото со сите што имаат список на VPN-сервери до кои можете да пристапите со кликнување на стрелката надолу. Изберете еден од нив и кликнете Quick Connect.

6. Забележете дека бесплатната сметка само ви овозможува да ги користите бесплатните сервери во Холандија, САД и Јапонија. Изберете ја онаа што е најблизу до вас за подобри резултати, веројатно Холандија или други ако сте жител на тие земји.
7. Си завршил.

B) ПОБЕЗБЕДЕН ПРЕБАРУВАЧ: TOR BROWSER

Пребарувањето на интернет е подложно на надзор на различни нивоа. Мрежата Tor Onion е создадена за да се заштити од интернет надзор и цензура. Tor Browser е безбеден пребарувач кој го насочува сообраќајот преку мрежата Onion и има други подобрувања за безбедност. Секоја сесија на пребарувачот Tor е единствена.



Отворање на екранот на Tor Browser

Користење на Tor Browser

1. Посетете ја официјалната веб-страница на Tor Browser за да го преземете пребарувачот Tor за вашата платформа https://www.torproject.org/download/ Подготвен е за Windows, macOS, Linux и Android. Проверете го побезбедениот дел за пребарување преку мобилен телефон подолу за да го користите истиот.
2. За Windows, преземете **.exe** file и почнете.
3. Кликнете на менито Start и стартувајте го Tor Browser.
4. Првиот пат кога ќе започнете да го користите Tor Browser, ќе го видите прозорецот Tor Network Settings. Ова ви нуди можност директно да се поврзете со мрежата Tor, која треба да работи во Југоисточна Европа, или да го конфигурирате пребарувачот Tor за вашата врска, во случај да користите (proxy) или Tor врските се блокирани од интернет-провајдерот на вашата земја.

Пребарувачот Tor им дава можност на корисниците самите да ги постават посакуваните нивоа на безбедност. Во пребарувачот Tor, кликнете на иконата за симболи (десно од лентата за адреса) и кликнете **„Advanced Security Options ..."** за да ги видите опциите. Оваа опција е стандардно поставена на **Standard**, со што се зголемува употребата. За да ги искористите највисоките нивоа на приватност и анонимност што може да ги понуди Tor, поставете ја лентата на најбезбедно ниво.

ПОБЕЗБЕДНО ИСПРАЌАЊЕ НА ПОРАКИ ПРЕКУ Е-ПОШТА

А) ПОБЕЗБЕДНИ УСЛУГИ ЗА ИСРПАЌАЊЕ НА ПОРАКИ ПРЕКУ Е-ПОШТА

За оние што сакаат да го сокријат нивниот идендитет или на други лица што комуницираат, треба да користат анонимни електронски сметки, својствени на кој било друг аспект на вашиот идентитет во интернет. Со други зборови тие не смеат да се врзаат со тебе на ниту еден начин. Сервиси како што се Gmail и Microsoft Live бараат еден број на телефон или адреса на алтернативна компанија, така што дава услуги да нема идеална проценка за аноним. ProtonMail, Tutanota и Posteo (бесплатно) ги дозволуваат корисниците да креираат сметка без ниту една ваква информација за идентификување.

Б) КРИПТИРАЊЕ НА Е-ПОШТА СО ВАШИОТ ПРЕБАРУВАЧ ПРЕКУ MAILVELOPE

Шифрирањето е-пошта користејќи го стандардот OpenPGP е вообичаена практика да се осигурате дека вашите e-mail пораки не се прочитани доколку се пресретнат додека се на пат или за време на паузи на серверите на давателот на услугата, како што е случајот со повеќето комерцијални даватели на услуги за е-пошта. Шифрирањето на е-поштата со OpenPGP сепак не е најзгодно за корисниците и доколку приватниот клуч за криптирање е украден, сите пораки до кои може да пристапува една страна можат да се прочитаат. Покрај тоа, ако приватниот клуч е изгубен, нема да можете да ги декодирате тие пораки. Исто така, шифрираната е-пошта не е совршена бидејќи адресата и линијата на субјектите (метаподатоците) може да се прочитаат ако се прислушуваат, затоа имајте го ова на ум кога го користите.

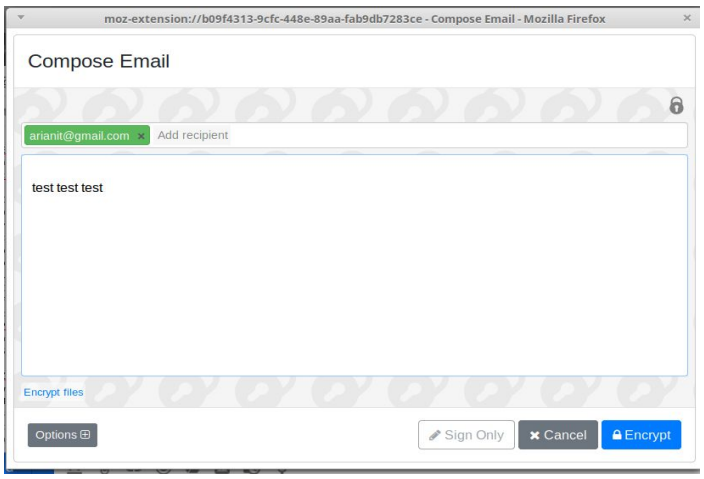
Mailvelope е бесплатен софтвер за криптирање крај до крај (end-to-end encryption), преку е-пошта во рамките на веб-пребарувач (Firefox или Chrome / Chromium) кој добро се интегрира во најпопуларните услуги за електронска трговија преку интернет. Може да се користи за криптирање и потпишување на е-пошта и додатоци при истовремено избегнување на домашен клиент за е-пошта (како Thunderbird) користејќи го стандардот OpenPGP. Покорисно е бидејќи не ве принудува да се префрлите на нов клиент за е-пошта.

Поставување на Mailvelope и клучот PGP

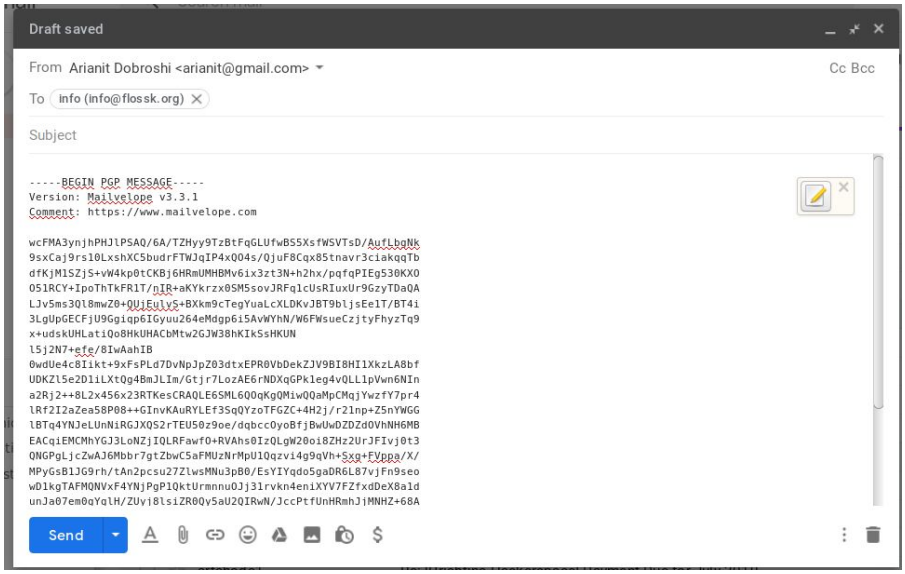
1. Одете во Firefox Add-ons и побарајте Mailvelope.
2. Во лентата со алатки, кликнете на иконата Mailvelope. Dashboard екранот ќе се отвори.
3. Стиснете Manage keys. Потоа Generate ако немате веќе постоечки клуч или Import ако сега имате едно.
4. Пополнете ги празните места користејќи го името поврзано со вашата сметка за е-пошта. Поставете сигурна лозинка што никогаш нема да ја заборавите, во спротивно го губите пристапот до клучот. Оставете ги другите поставки стандардно.
5. Стиснете Generate и чекајте малку. Вашиот клуч сега е генериран и подготвен за употреба. Ќе ви биде испратена порака за да можете да го испратите вашиот јавен клуч на серверот за да најдете други. Вашиот јавен клуч е она што другите го користат за да шифрираат пораки за вас. Вие го користите вашиот приватен клуч за да ги отворите тие.
6. Предупредување: Вашиот приватен клуч мора да се чува во тајност. Никогаш не го споделувајте со никого.

Испраќање на криптирани пораки преку е-пошта

1. За да шифрирате нечии е-пораки, прво мора да го внесете јавниот клуч на лицето во Mailvelope. Можете да го добиете директно на пр. преку е-пошта, пронајдете го на јавна веб-страница на некоја личност или на еден од главните сервери што ги содржат клучевите, како што се оние од Ubuntu или MIT.
2. Во Mailvelope, одете до **Key management**, ставете го текстот на јавниот клуч во полето или кликнете на **Search**. Пребарувајте по е-пошта или име и кликнете на клучниот код, кој треба да биде нешто како овој E7F3E1D6. Забележете, додека јавните сервери велат дека клучот му припаѓа на одредена личност, овој факт може да биде расипан, поради што можеби сакате да го потврдите клучниот код преку други средства со лицето што го поседува клучот.
3. Кликнете клучот за да го испратите. Сега сте подготвени да ги криптирате пораките и податоците на таа адреса.
4. Ако Mailvelope е активна, ќе добиете икона за да ја напишете вашата порака таму во полето за е-пошта (на пр. Gmail). Оваа порака ќе биде шифрирана со јавниот клуч на лицето што го испраќате, доколку прво сте го испратиле нивниот клуч.



Дел од текстот во Mailvelope



Изглед на криптирана порака во Gmail креирана со употреба на Mailvelope

БЕЗБЕДНОСТА НА МОБИЛНИОТ ОПЕРАТИВЕН СИСТЕМ

Повеќето од вашите пресметки сега се прават на мобилен телефон, вклучително и за чувствителна работа. Сепак, безбедноста на мобилната телефонија е во лоша форма со изложување на корисниците на многу слабости. Од застарени и неподдржани системи на Android до високо дозволени апликации, треба да размислите многу за користење на мобилни уреди за да направите чувствителна работа. Самиот Android и одредени апликации, дури и наводно безбедни оние како WhatsApp, ќе бараат од вас да ги ажурирате податоците за вашиот сервер, што е јасно зачувано и лесно може да се пристапи по судска наредба или од друга институција.

А) ОСНОВИТЕ: БЕЗБЕДНОСТА НА АПЛИКАЦИЈАТА ANDROID

Додека „Apple“ одобрува апликации за мобилни телефони пред да бидат објавени индивидуално на нејзината продавница за апликации, внимавајќи на оптоварувањето на приватноста што тие апликации им го наметнуваат на корисниците, истото не е случај со апликациите за Android од Google Play Store.

Ако користите Андроид, веројатно сте биле запрашани и ви е дадена апликација пристап до работи како што е вашата историја на повици, пораки, локација, камера, микрофон и друго. Пред верзијата 6.0, Андроид ги замолуваше корисниците да ги одобрат барањата за дозвола во пакет, предизвикувајќи сомнежи зошто на одредена апликација му е потребен пристап до микрофон, ако само се земе со слики.

Од верзијата 6.0 па натаму, Андроид им овозможува на корисниците да изберат кои дозволи ќе ги додели апликацијата. Треба да обрнете внимание на какви апликации инсталирате на вашиот телефон. Покрај тоа, ако не планирате да користите одредена карактеристика на апликација, на пр. фотографии обележани со вашата локација, тогаш не ги одобрувајте или дозволете ги на привремена основа само кога ви се потребни.

Да се проверат веќе одобрените дозволи:

1. Стиснете **Settings** кај вашиот уред.
2. Потоа стиснете **Apps and notifications**. Изберете која било апликација и притиснете на **Permissions** или **App permissions** за преглед на дозволите засновани на специфични дозволи.
3. Стиснете **On** или **Off**. Ако не сте сигурни, оневозможете го. Android ќе ве праша за дозвола кога е потребно и можете да донесете одлука врз основа на разумноста на барањето во таа ситуација.

Б) ОСНОВА: АЖУРИРАЊЕ НА ВАШИОТ ANDROID

Повеќето верзии на Android се застарени поради моделот на дистрибуција на софтвер што го користи Google (издавач на Android) со своите клиенти (производители на мобилни телефони). Честопати, Google ја губи контролата над ажурирање на својот софтвер, што сега е одговорност на производителот или компанијата што можеби нема да има поттик да го поддржува вашиот одреден уред преку ограничено време. Во принцип, уредите марката Google и најдобрите телефони на производителите имаат подолг период на поддршка. Уредите на Apple iOS исто така се поддржани подолго време. Ова е причината зошто секогаш да барате период на поддршка со ажурирања на софтверот пред да купите одреден модел.

Ажурирање на вашиот Android

Може да го видите бројот на верзијата со Android и ажурираното ниво на безбедност во **Settings**. Ќе добиете известувања кога ажурирањата ви се достапни, ако системот е се уште ажуриран. Можете исто така да проверите сами за ажурирања. Забележете дека овие упатства може да варираат во зависност од верзијата со Android. Проверете со веб-страницата на производителот на вашиот телефон ако имате потешкотии да ги следите.

Да видите која верзија на Android ја имате

1. Кликнете **Settings** до вашиот уред.
2. На крај, кликнете **System > Advanced > System update**. Ако не видите **Advanced**, кликнете **About phone.**
3. Видете вашата верзија на Android и безбедносното ниво на (patch) под соодветните наслови.

Добијте ги најновите ажурирања на Android достапни за вас

Кога ќе добиете известување за ажурирање, отворете го и притиснете го ажурирањето.

Ако сте го исчистиле известувањето или вашиот уред беше надвор од мрежата:

1. Отворете **Settings** кај вашиот уред.
2. На крај, стиснете **System > Advanced > System update**. Ако не видите **Advanced**, стиснете About phone.
3. Ќе го видите вашиот статус ажуриран. Следете го секој чекор на екранот.

БЕЗБЕДНОСТА ВО КОМУНИКАЦИЈА

А) ОСНОВИ: ИСПРАЌАЊЕ ПОРАКИ ПРЕКУ SIGNAL

Проверете ги овие безбедносни карактеристики додека го оценувате клиентот за итни пораки што го користите:

- дали пораките се кодираат за време на транзитот?
- се пораки кодирани до провајдерот ако постои такво нешто (т.е. не од учесниците)?
- дали се потврдени контактните идентитети?
- дали комуникацијата е безбедна ако се украдени клучевите?
- дали е софтверски код отворен за независен преглед?
- дали безбедносниот модел е правилно документиран?
- дали има независни ревизии на неодамнешните кодови?

Во овој поглед, WhatsApp е подобар од Viber, а Signal е подобар од WhatsApp.

Signal ги исполнува повеќето критериуми погоре и е приближен во однос на употребата со оние што веќе можете да ги користите, па затоа се препорачува. Signal е достапен бесплатно на Android, iOS и Desktop (Виндоус / Мек / Линукс), е со отворен извор и прегледуван од врсници, опфаќа текстови, повици и видео повици и датотеки, сите шифрирани и кога уредот е исклучен.

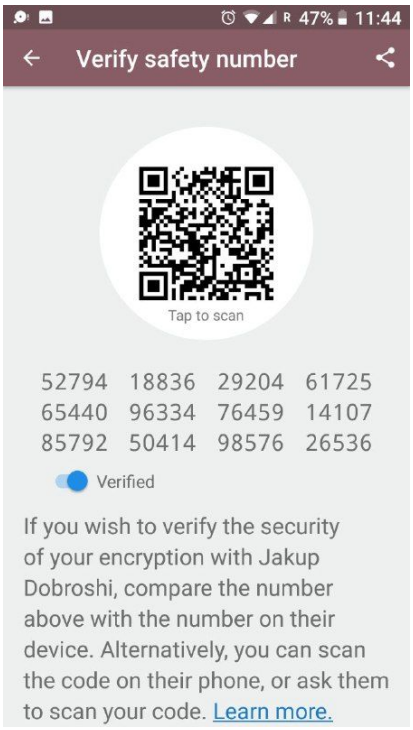
За да инсталирате Signal на вашиот Android / IOS:

1. Потврдете дека вашиот мобилен телефон работи со Android 4.4 / iOS 10.0 или понова верзија.
2. Барајте **Signal Private Messenger** во Google Play/App Store и инсталирајте го.
3. Следете го водичот во вашиот екран да завршите процесот на регистрација исто како другите апликации што го бараат вашиот телефонски број.

Верификација на вашите контакти

Во Signal, можете да го потврдите вашиот контакт за да осигурите дека сметката на која зборувате му припаѓа на лицето на кое тврди дека припаѓа и дека вашиот безбеден канал за комуникација не е оштетен.

1. Во Signal, и вие и вашиот контакт треба да отидете на екранот во кој нормално би разговарале со тој.
2. Притиснете ја иконата со три вертикални точки (горе десно), а потоа кликнете **settings > Verify safety number.**
3. Споредете ги дадените броеви или притиснете Тар за да го скенирате другиот уред со Signal за споредба. Можете исто така да го прочитате гласно или да го испратите на другата страна. Ако тие се исти, кликнете **Verified**.

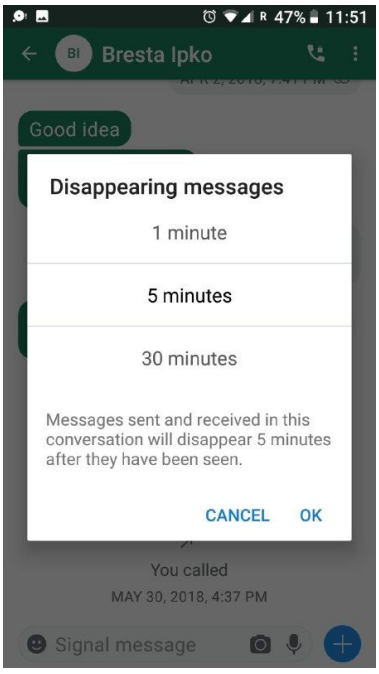


Изглед на екран за верификација во Signal

Автоматско бришење на пораки

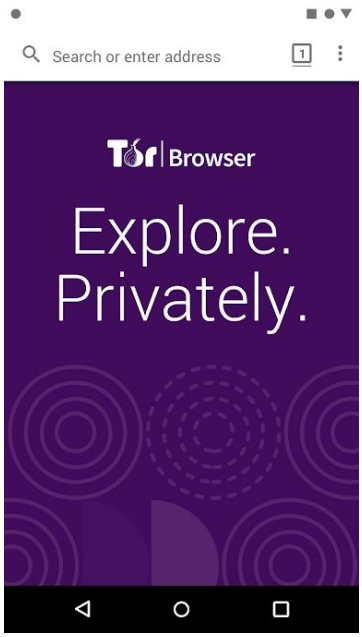
Можеби сакате пораките да бидат избришани по одреден период.

1. Во Signal, одете на екранот што обично разговарате со вашите контакти.
2. Притиснете ја иконата со три вертикални точки (горе десно), а потоа притиснете **Disappearing messages**.
3. На новиот екран, изберете го периодот. Ќе се појави порака во разговорот што го означува овој период.



Б) ПОБЕЗБЕДНО ПРЕБАРУВАЊЕ ПРЕКУ МОБИЛЕН ТЕЛЕФОН: TOR BROWSER

Tor Browser е исто така достапен за Android и iOS. Ако користите Android, можете да го преземете на Google Play Store со пребарување на Tor Browser за Android. Во Apple, пребарувајте Onion Browser.



Излгедот на Tor Browser во Android

СПОДЕЛУВАЊЕ НА ПОДАТОЦИ

Споделувањето на податоците што зазема многу простор е секојдневен предизвик. Два начина да се испраќаат податоци безбедно веќе се опфатени, преку шифрирана е-пошта преку OpenPGP и итни пораки, како што е Signal. За уште поголеми податоци, потребни се дополнителни решенија. Подолу се дадени уште два начина за тоа. Firefox Send е погоден за практични сценарија со низок ризик, додека OnionShare е доста безбеден, особено ако податоците прво се шифрираат.

А) БАЗА: FIREFOX SEND

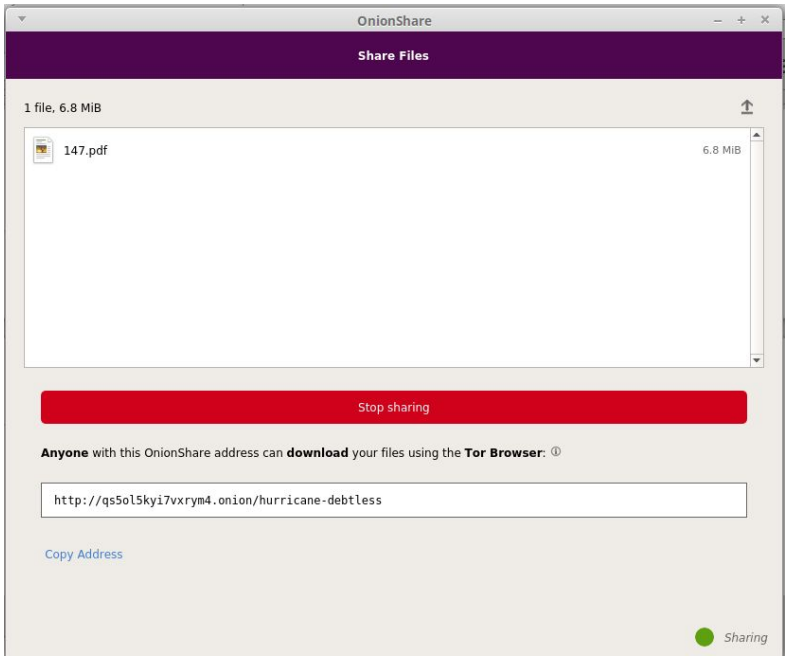
Firefox Send е најновото решение што е лесно за употреба. Можеби сакате прво да ја криптирате датотеката со употреба на опцијата Encrypt a File во Mailvelope (има ограничување од 50 MB) или со други средства пред да ја поставите датотеката. За да ја испратите, одете на http://send.firefox.com, изберете ја датотеката за да испратите и поставите опции. Забележете дека за поголемите датотеки е потребно повеќе време на серверот за да се најавите.

Б) ПОБЕЗБЕДНО СПОДЕЛУВАЊЕ: ONIONSHARE

OnionShare ви овозможува да споделувате податоци многу безбедно и анонимно со која било големина. Создава привремен скришум веб-сервер. Неспорна адреса е генерирана и вообичаено е примателот да се отвори во Tor Browser за да ги преземе податоците. И покрај тоа што е многу безбеден, недостаток на оваа алатка е тоа што ги правите (host) податоците на вашиот компјутер, така што треба да ги одржувате додека не се прифати од другите страни. Примачот исто така мора да го користи Tor Browser за да ги преземе податоците.

За да го користите:

1. Започнете со инсталирање на OnionShare за вашата платформа од тука https://onionshare.org
2. Откако ќе се инсталира, отворете OnionShare.
3. Додадете ја датотеката и кликнете на Start sharing. Нема ограничување колку големината на датотеката треба да биде. На крајот на процесот, OnionShare ќе ви даде адреса како оваа http://qs5ol5kyi7vxrym4.onion/hurricane-debtles кои мора да ги доставите до примателот преку безбеден канал. Забележете дека секој со адреса може да пристапува до датотеките под услов дека OnionShare сè уште да биде во функција.



Изгледот на OnionShare

КАДЕ ДА СЕ ОДИ ОД ОВДЕ?

Ако погледнете повнимателно со овој прирачник и сакате повеќе совети или се соочувате со закани на повисоко ниво, друг добар материјал за водство е бесплатно достапен преку Интернет, иако е претежно на англиски јазик, а некои делови се застарени.

Security in a Box - Дигитални безбедносни алатки и тактики
https://securityinabox.org/

Security in a Box е проект на Tactical Technology Collective и Front Line Defenders. Упатствата за тактики во оваа пакет-алатка ги опфаќаат основните принципи, вклучително и совети за тоа како посигурно да ги користите социјалните медиуми и мобилните телефони. Прирачниците за алатки обезбедуваат чекор-по-чекор инструкции за да ви помогнат да инсталирате, конфигурирате и користите некои основни софтверски и услуги за дигитална безбедност. The Community Toolkits (алатки за заедницата) се фокусираат на специфични групи на луѓе - понекогаш во одредени региони - кои се соочуваат со значителни закани за дигитална безбедност. Тие вклучуваат совети прилагодени на алатките и тактиките кои се релевантни за потребите на овие конкретни групи.

Surveillance Self-Defense: Безбедни совети за интернет, алатки и начини за комуникација
https://ssd.eff.org/

Тоа е список на упатства и планови за лекции од Electronic Frontier Foundation.

Безбедноста на информациите за новинарите, прирачник од Centre for Investigative Journalism
https://tcij.org/sites/default/files/u11/InfoSec for Journalists V1.3.pdf

Прирачник дизајниран за новинарите и медиумските организации за тоа како да ја практикуваат безбедноста на информациите во дигиталното време, додека ја заштитуваат нивната работа, ресурси и комуникации преку најразлични нивоа на ризик, вклучувајќи ги и највисоките нивоа на ризик.

Помошник за Дигитална безбедност за Новинари од Репортери без Граници
https://helpdesk.rsf.org/

Почнувајќи од јули 2019 година, RSF ќе обезбеди бесплатни видеа и консултации преку интернет за дигиталната безбедност во редовни основи. Овие семинари можат да се видат или во живо или во подоцнежно време. Семинарите ќе се фокусираат на тоа како да се заштитат сметките на социјалните медиуми од пиратеријата, како да се избегне цензурата со користење на VPN и кои апликации за размена на паметни телефони се најдобри за новинарска работа. Повеќе индивидуализирани услуги за поддршка ќе бидат обезбедени во иднина.

ЗА АВТОРОТ

Арианит Доброши е претседател на извршниот одбор на FLOSSK, невладина организација која промовира бесплатен софтвер со отворен извор во Косово. Тој обучува новинари и членови на граѓанското општество за алатки за приватност и лобира против законодавството за дигитален надзор во Косово. Може да стапите во контакт со него на: arianit.dobroshi@flossk.org.

Овој прирачник е објавен како дел од проектот Infosec за Балканот, финансиран од Радио Слободна Азија преку Фондот за Отворена технологија и имплементиран од Open Data Kosovo и FLOSSK.

Оригиналната верзија е напишана на англиски јазик. Исто така е достапен на албански, босански, македонски, црногорски и српски јазик.


OPEN
TECHNOLOGY
FUND


RFA
Radio Free Asia


ODK
OPEN DATA KOSOVO


Free Libre Open Source Software Kosova