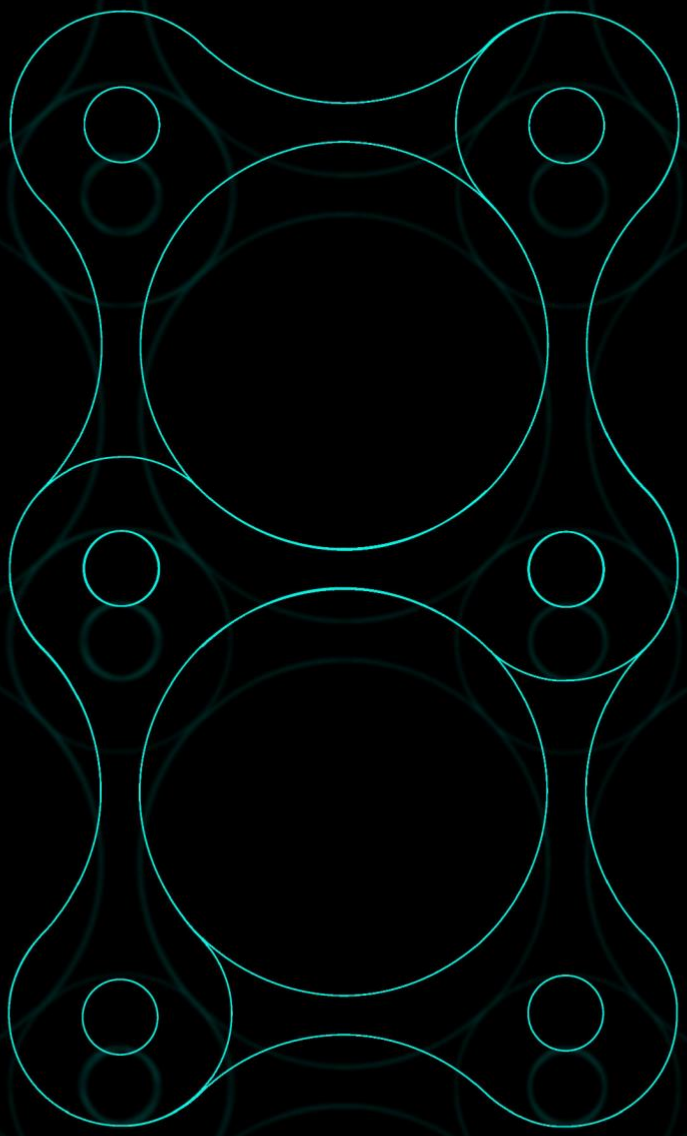
PRIRUČNIK ZA SIGURNOST INFORMACIJA ZA NOVINARE I CIVILNO DRUŠTVO

Arianit Dobroshi



INFOSEC
for Balkans

Jul 2019

PREGLED SADRŽAJA

UVOD

Ovaj priručnik ima na umu novinare i druge radnike civilnog društva u regionu Jugoistočne Evrope koji se trenutno možda ne suočavaju sa najsofisticiranijim informacionim bezbjednosnim prijetnjama (infosec). Autor smatra da je dostojan kompromis žrtvovati određenu rigoroznost informacione sigurnosti, ako to promoviše veće usvajanje ovih praksi i alata.

Ovaj priručnik cilja publiku sa malim stepenom zaštite kao i opštu populaciju. Kao takav, postavlja osnovne prakse bezbednosti informacija pogodne za sve.

Svaki odjeljak ovog priručnika obuhvaća najmanje dva nivoa sigurnosti: osnovni nivo potreban za sigurno računanje koji bi trebalo da praktikuje svako, i odjeljak s većim rizikom kojem bi trebali da teže svi istraživački novinari i organizacije civilnog društva koji rade na osjetljivim poslovima u regionu. Ipak, neki aktivisti I organizacijama civilnog društva u regionu suočavaju se sa još većim stepenom prijetnje i trebalo bi da potraže druge dublje resurse, od kojih su neki navedeni u posljednjem dijelu ovog priručnika.

Ovaj priručnik je napisan u julu 2019. Prijetnje sigurnosti informacija i njihove mjere ublažavanja stalno se razvijaju, tako da ovaj datum treba imati na umu kada se na njega ubuduće pozivate.

A) ZA KOGA JE OVAJ PRIRUČNIK

Ovaj priručnik je namijenjen novinarima, posebno onima koji rade u istraživačkom novinarstvu, i aktivistima civilnog društva, posebno onima koji se bave osetljivim temama u vezi sa vladavinom zakona. Rečeno je da je to dobro sredstvo koje mogu koristiti svi koji bi željeli nadograditi svoje osnovno znanje o sigurnosti informacija, pogotovo jer je ono dostupno i na jezicima regiona, koji nemaju resurse u ovoj oblasti: albanskom, bosanskom, makedonskom, crnogorskom i srpskom .

Tehnički nivo potreban za sprovođenje ovog rada je osnovni i svako ga treba dostići. Neki od alata zahtijevaju određenu žrtvu upotrebljivosti i praktičnosti iz uobičajene prakse.

B) KAKO ČITATI OVAJ PRIRUČNIK

Svaki naslov ovog priručnika može se pročitati zasebno, na osnovu vaših neposrednih potreba za informacionom sigurnošću. Bez obzira na to, preporučuje se da obuhvatite sve odjeljke ovog priručnika jer je on koncipiran kao spisak najmanjeg obima koji biste trebali da praktikujete da biste zaštitili sebe i svoje izvore. Možete mu se vratiti kada imate više vremena i sve to pokrijete. Prvi podnaslovi pokrivaju same osnove koje bi svaki korisnik računara već trebalo da vježba, mada u našem zapažanju to još nije slučaj. Drugi podbroj trebalo bi da osigura nadogradnju sigurnosti za većinu osnovnih korisnika.

Odjeljak 2 ovog priručnika pokriva stvaranje jačih lozinki, korisnih za sve platforme. U dijelu 3 pokrivamo vaš operativni sistem za radnu površinu: stvari koje biste trebali da radite sa Windows operativnim sistemom i neke pomoći prilikom instaliranja Linuk Mint-a, koji je po difoltu sigurniji sistem, ali i jednostavan za upotrebu. U odjeljku 4 bezbjedno se obraćamo pregledavanju, a u dijelu 5 sigurno upravljanje e-poštom. U odjeljku 6 pogledamo neke stvari koje se moraju uraditi za bezbjednost mobilnog sistema, dok se u dijelu 7 bavimo bezbjednošću komunikacije. Na kraju, u dijelu 8 se govori o dijeljenju datoteka, dok se u dijelu 9 nalazi lista resursa za čitaoce koji žele više.

C) IDENTIFICIRANJE SIGURNOSNIH POTREBA

Neovlašteni pristup vašim podacima može podrazumijevati njegovu upotrebu, otkrivanje, ometanje, izmjenu, inspekciju, snimanje ili uništenje. Međutim, pošto su digitalne prijetnje nevidljive, složene i često neodredive, one se mogu podcijeniti ili previdjeti.

Postoji nekoliko načina na koje možete sagledati prijetnje s kojima se susrećete i potrebe za informacijskom sigurnošću. Najosnovnija prijetnja s kojom se suočava cijela populacija jesu prijetnje mreža s kojima se susreće svaki građanin regije, mada se ciljana publika u ovom priručniku može suočiti sa više specijaliziranih ciljanih prijetnji.

Zemlje regije primijenile su EU direktivu o zadržavanju podataka koja nalaže posjedovanje metapodataka (podataka o podacima) o svim obrađenim telekomunikacijama, uključujući liste svih telefonskih poziva, IP adrese, tekstualnih poruka itd. Poslanih ili primljenih u razdoblju između šest do dvadeset četiri mjeseca, kojima se može pristupiti sudskim nalogom. Iako sami komunikacijski sadržaji nisu spremljeni, napredovanje od zakonskog mandata do veleprodajnog nadzora nije tako teško, a zahtjev za sudskim nalogom ovisi o krhkosti sistema vladavine zakona u regiji.

Čak su i metapodaci vrlo otkrivajući jer bi mogli omogućiti onima koji ih posjeduju da grade društvene grafikone svog života i neizravno identificiraju sadržaj i izvore s kojima sarađujete, čak i retrospektivno. Uz specijalizirane prijetnje, stranka koja provodi nadzor koristi specijalizirane i sofisticirane alate protiv cilja. Tehnologija za to sve je jeftinija, a pristup vladama i privatnim strankama postaje lakši. Na primjer, otkriveno je 2015. godine da je vlada sjeverne Makedonije prisluškivala telefone oko 20.000 ljudi.

Postoje i dokazi da je srpska vlada preusmeravala internet na određene tačke, gde je mogao lako da se prisluškuje. To je bilo prije nekoliko godina i situacija se vjerojatno pogoršala. Ako vjerujete da se suočavate sa takvom vrstom prijetnje, ovaj priručnik nije dovoljan da biste se zaštitili i trebali biste potražiti posvećenu pomoć.

STVARANJE JAČIH LOZINKI

Sigurna lozinka je slučajna, dovoljno dugačka i kombinira popis malih i malih slova, brojeva i drugih znakova (npr. Xkvv3.K3? Rrz). Bez obzira na to, moguće je imati sigurne lozinke koristeći kombinaciju riječi pod uvjetom da je dovoljno dugačka, jedinstvena za uslugu, slučajna i nije povezana s vama. Kombinacija nasumičnih riječi kojih se lako možete sjetiti je dovoljno sigurna lozinka (npr. WITHIN-WIRE-GRASS-pluto-save).

A) DVA FAKTORA AUTENTIFIKACIJE

Kad god je dostupno, dvofaktorska provjera identiteta pruža drugo sredstvo uz vašu uobičajenu lozinku za zaštitu web naloga. Drugi faktor autentifikacije (2FA) može vam se poslati na telefon putem poziva, SMS-a, e-pošte ili biti generisan na vašem Android telefonu ili hardverskim žetonom. Možda ga već koristite za svoje bankovne račune. Drugi faktor dodaje dodatni sloj zaštite u slučaju da je ugrožena vaša lozinka.

Omogućavanje provjere autentičnosti drugog faktora ovisi o vašem softveru i potražite ga u Settings>Password (Postavke> Lozinka) ili slično da biste ga omogućili. Međutim, još ga ne nude sve usluge. Na primjer, dok koristite Google usluge, možete posjetiti **https://myaccount.google.com/signinoptions** , prijaviti se sa svojim računom, omogućiti ga postoji i odabrati sredstvo za primanje svoje druge privremene lozinke, obično SMS-om. Imajte na umu da ćete izgubiti svoj nalog ako izgubite svoj telefonski broj.

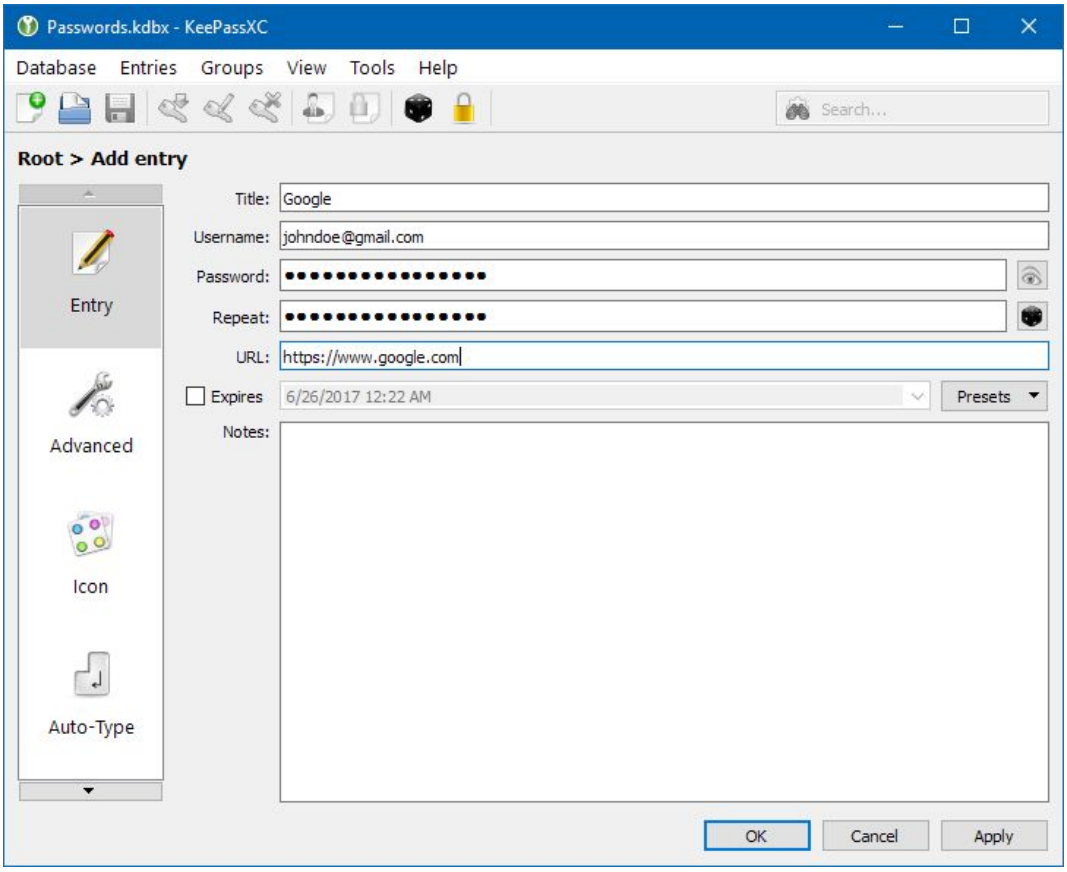
Stoga biste trebali postaviti i najmanje jednu sigurnosnu kopiju tako da se možete prijaviti čak i ako vaši drugi koraci nisu dostupni. Jednokratne lozinke za ispis mogu vam biti najlakši način da se prijavite ako izgubite svoj broj ili putujete.

B) KORIŠTENJE SOFTVERA ZA KREIRANJE I UPRAVLJANJE LOZINKAMA

Lozinke koje koristite trebaju biti jedinstvene za svaku uslugu koju koristite. Memoriranje sigurnih lozinki ubrzo postaje nemoguće, pa je potreban alat za upravljanje njima. Da biste olakšali stvaranje sigurnih lozinki i upravljanje njima, možete koristiti namjenski softver.

Dobar open source je KeePassXC (**https://keepassxc.org**)dostupan za Windows macOS i Linux, upravitelj lozinki koji pohranjuje korisnička imena i lozinke u lokalnu šifriranu bazu podataka, zaštićenu glavnom lozinkom. Takođe dolazi sa PWG-enom, snažnim generatorom slučajnih lozinki.

Ostali alternativni komercijalni softveri su **LastPass** i **1Password.** Oni pohranjuju šifrirane lozinke na mreži, a neke funkcije mogu biti dostupne samo pod plaćenom verzijom, ali pružaju bolju upotrebljivost, a lozinke se pohranjuju na mreži. Budući da je zatvoreni izvor, nemoguće je neovisno revizirati sigurnost ova dva alata.



Pregled ekrana KeePassKSC

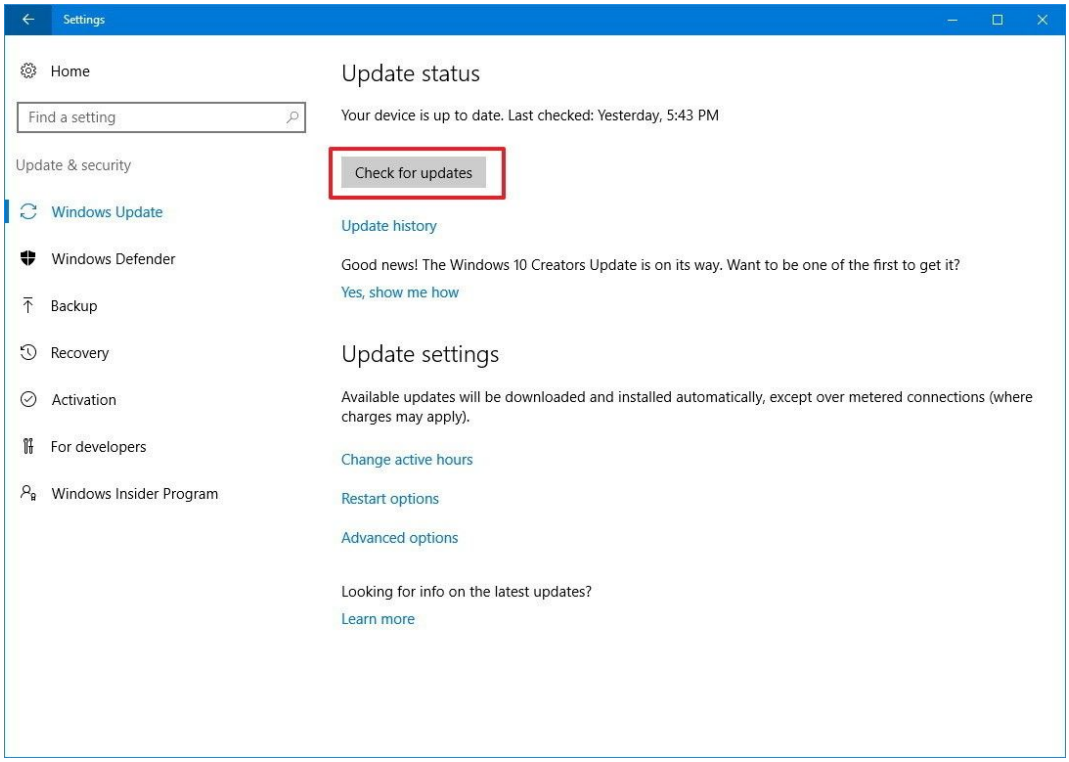
KORIŠTENJE SIGURNIJEG OPERATIVNOG SISTEMA

Operativni sistem za desktop je osnova vašeg svakodnevnog sigurnog korištenja računala. Općenito, sigurnost sustava rangiranog od niskog do visokog iznosi: Windows 7 ili 10 koji su najčešće korišteni, ali i najmanje zaštićeni, macOS koji je prema zadanim postavkama sigurniji pa se ovdje ne obrađuje, Linux Mint, ovdje opisan Linux sustavski ukus i Tails, također Linux zasnovan, dizajniran s obzirom na informacijsku sigurnost, ali s kompromisima upotrebljivosti.

A) AŽURIRANJE SISTEMA WINDOWS

Ažuriranje Windows-a je kritično ako radite na računaru povezanom s internetom. Previše puta, piratske Windows kopije spriječene su da primaju ažuriranja koja vas izlažu svim vrstama zlonamjernog softvera i drugim prijetnjama. Imajte na umu da bi Windows 7 izdavač Microsoft trebao povući do kraja 2019. godine te ga nakon tog datuma neće ažurirati sigurnosnim zakrpama. Trebali biste nadograditi na Windows 10 nakon te točke.

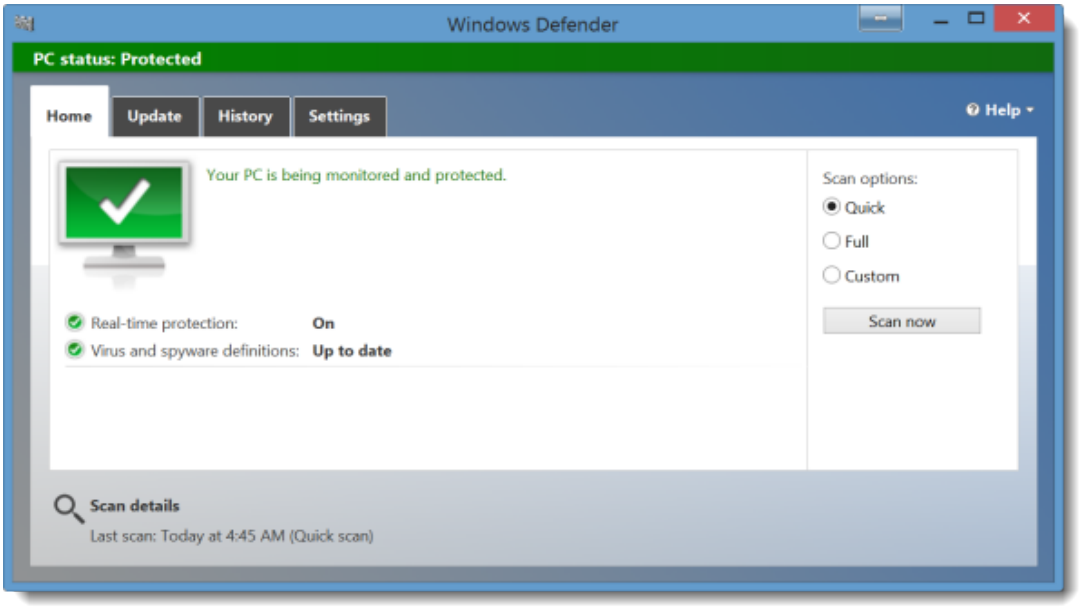
Da biste osigurali da je vaš Windows ažuriran, trebali biste potražiti „Windows Update“ na traci za pretragu Windows-a, kliknite Provjeri ažuriranja i osigurajte da ćete dobiti ekran poput onog na kome piše „Nema ažuriranja.“ Primjetite da nisu sve nadogradnje sigurnosna ažuriranja i zato ih možete zanemariti. Ako je ažuriranje operativnog sistema Windows nemoguće pokrenuti, potražite pomoć kako biste bili sigurni da je vaše računalo ažurirano.



Status ažuriranja Windows-a

Pored toga, potreban vam je softver koji vas štiti od virusa i zlonamjernog softvera. U većini slučajeva ugrađeni program Windows Defender je odgovarajući i ne koristi dodatne resurse na računaru. Da biste ga pokrenuli, deinstalirajte drugi antivirusni softver. Idite na traku za pretragu Windows-a i upišite "Windows Defender". Provjerite je li uključena zaštita u stvarnom vremenu i suvremene definicije virusa. Ako ne, trebali biste ih ažurirati na kartici Ažuriranje.

Ako je vaš sistem duže vreme zastario, pokrenite cjelokupno skeniranje sistema kako biste se uvjerili da je čist, a to može potrajati nekoliko sati. Ako ne možete sami riješiti bilo koji potencijalni nalaz, potražite pomoć.

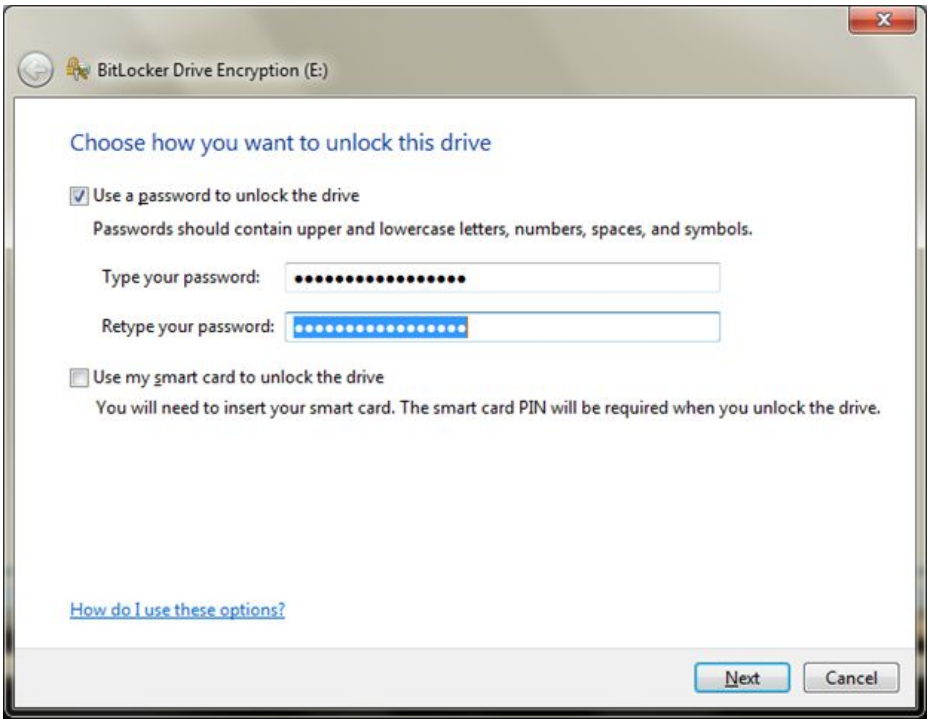


Ažurirani Windows Defender

B) ŠIFRIRANJE DISKA

Podatke na vašem računarskom disku lako može da pročita protivnik koji ima fizički pristup njemu ako disk nije šifriran. Većina verzija operativnog sistema Windows do Windows 7 Pro podrazumevano nije instalirana enkripcija diska. Windows 7 Ultimate i Windows 10 Pro i Enterprise standardno dolaze s softverom Bit Locker.

Za šifriranje punog diska BitLockera na sistemskom pogonu potreban je računar sa pouzdanim platformskim modulom (TPM) ugrađenim u vaš PC. Ovaj čip generira i čuva ključeve za šifriranje koje BitLocker koristi. Ovo možete izbjeći korištenjem grupnih politika kako biste omogućili korištenje BitLocker-a bez TPM-a, iako ćete žrtvovati određenu sigurnost.



BitLocker ekran

Možete šifrirati disk bez sistema ili izmjenjivi uređaj bez TPM-a, tako da je pametno imati svoje podatke na zasebnom pogonu (obično pogon 'D'). Najlakši način za omogućavanje BitLocker-a za pogon je otvaranje File Explorer-a i desnim klikom na disk, a zatim kliknite na Uključi BitLocker. Ako u kontekstnom meniju ne vidite ovu opciju, vjerovatno nemate Pro ili Enterprise izdanje Windows-a pa vam je potrebna druga alternativa.

Upozorenje: BitLocker vam pruža ključ za oporavak koji biste trebali čuvati bilo da ga pohranite negdje na sigurno izvan postojećeg računala ili da ga ispisujete i fizički spremite. U slučaju da zaboravite svoj ključ ili je vaš TPM modul uništen, to će vam omogućiti ponovno pristup datotekama.

Ako je vaš sistemski kod šifriran lozinkom i imate TPM, nećete ništa primijetiti. Ako ste šifrirali nesistemski ili izmjenjivi pogon, Windows će od vas tražiti da otključate pogon kad prvi put pristupite njemu. Upišite svoju lozinku za otključavanje ako se koristi tokom svakog ponovnog pokretanja.

Ako koristite neki drugi operativni sistem, kao što je Linux, nudi se mogućnost enkripcije diska tokom instalacije. Pogledajte odjeljak za instalaciju Linux Mint-a da biste vidjeli kako to omogućiti.

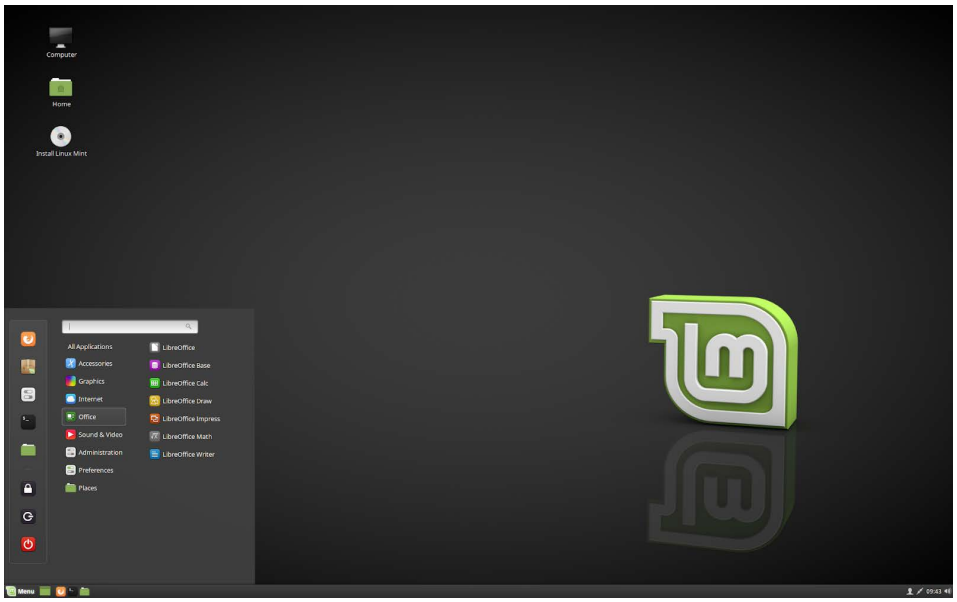
Za sve sisteme dobar neovisni alat otvorenog koda koji poštuju sigurnosni profesionalci je VeraCrypt (ranije TrueCrypt) dostupan ovdje **https://www.veracrypt.fr.**

C) LINUX MINT: SIGURNIJI OPERATIVNI SISTEM

Linux je besplatni i otvoreni izvorni operativni sistem. Sigurniji je od Windows-a jer se ne suočava sa nekim sigurnosnim problemima Windows-a, ali će vam trebati da naučite novi operativni sistem i ponekad zahtijeva da unosite komande da biste to učinili. Postoje mnogi „okusi“ ili iteracije Linuxa: popularniji su Ubuntu, Fedora i Linux Mint, a Tails su posvećeni onima sa većim sigurnosnim potrebama. Trebali biste koristiti onu verziju koja je najčešća u vašem okruženju, tako da možete potražiti pomoć ako se zaglavite.

Ako to nije izvediva opcija, tada krenite sa Linux Mintom, što ovdje objašnjavamo. Najprikladnija je za korisnike, ima veliku podršku zajednice, nekomercijalna je i ima Windows osjećaj za one koji se prebacuju s nje. Dok Linux ima pristup skladištu od hiljade besplatnog i otvorenog koda softvera, možda ćete morati naučiti nove aplikacije da biste to učinili, jer neki izdavači softvera ne objavljuju za Linux.

Alternativa za Windows u Linuxu su: LibreOffice za Microsoft Office, Gimp za Photoshop, Audacity za uređivanje zvuka itd. Upotrijebite **http://alternativeto.net** za pronalaženje alternativa softveru koji koristite u Windows ili Mac na Linuxu.**http://alternativeto.net** Zatim ćemo pokazati kako instalirati Linux Mint na računar.



Linux Mint (Cinnamon) desktop

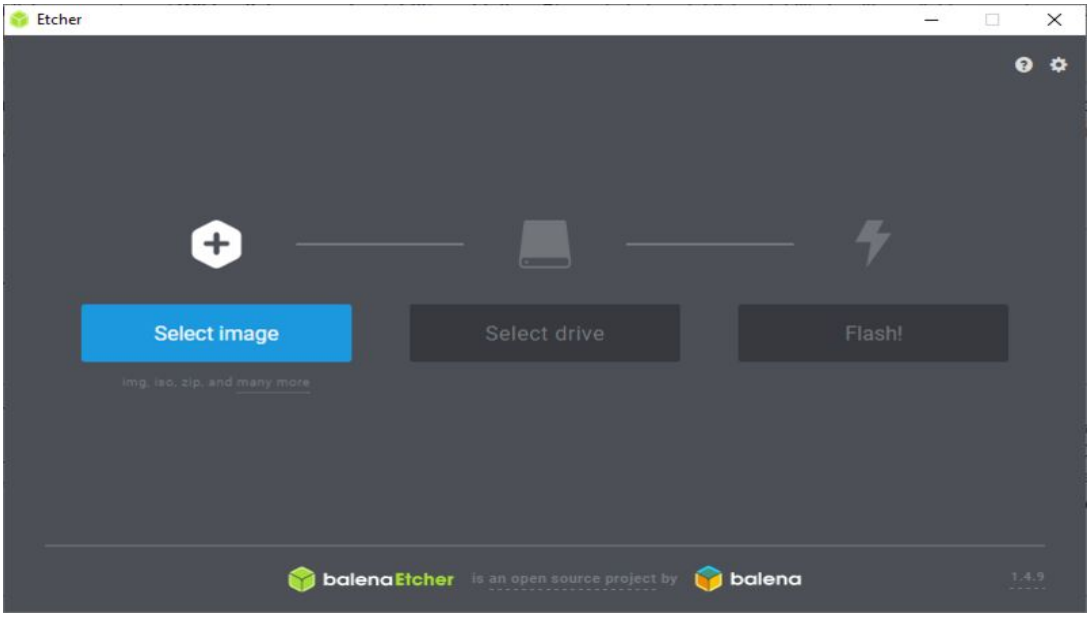
PRIPREMA INSTALACIJSKI USB

1. Napravite sigurnosnu kopiju podataka iz svog Windows sistema na vanjske medije. Najbolje je obrisati Windows instalaciju u potpunosti iako Windows i Linux mogu raditi jedan pored drugog.

2. Ovdje preuzmite Linux Mint Cinnamon ISO h**ttps://www.linuxmint.com/download.php.** Može biti potrebno oko 30 minuta, ovisno o vašoj internet vezi.

ZAPISIVANJE ISO NA USB FLEŠ UREĐAJU SA ETCHER-OM

1. Pripremite prazan USB fleš uređaj s najmanje 2 GB prostora za pohranu u koji ćete upisati ISO datoteku.
2. U Windows-u ili macOS-u preuzmite Etcher odavde **https://etcher.io,** instalirajte ga i pokrenite.
3. Na Etcher-u kliknite na Select image i odaberite svoju Linux Mint ISO datoteku.
4. Kliknite Select drive i odaberite USB fleš uređaj.
5. Kliknite Flash! Ovo će zapisati ISO na USB fleš uređaju.



Etcher ekran

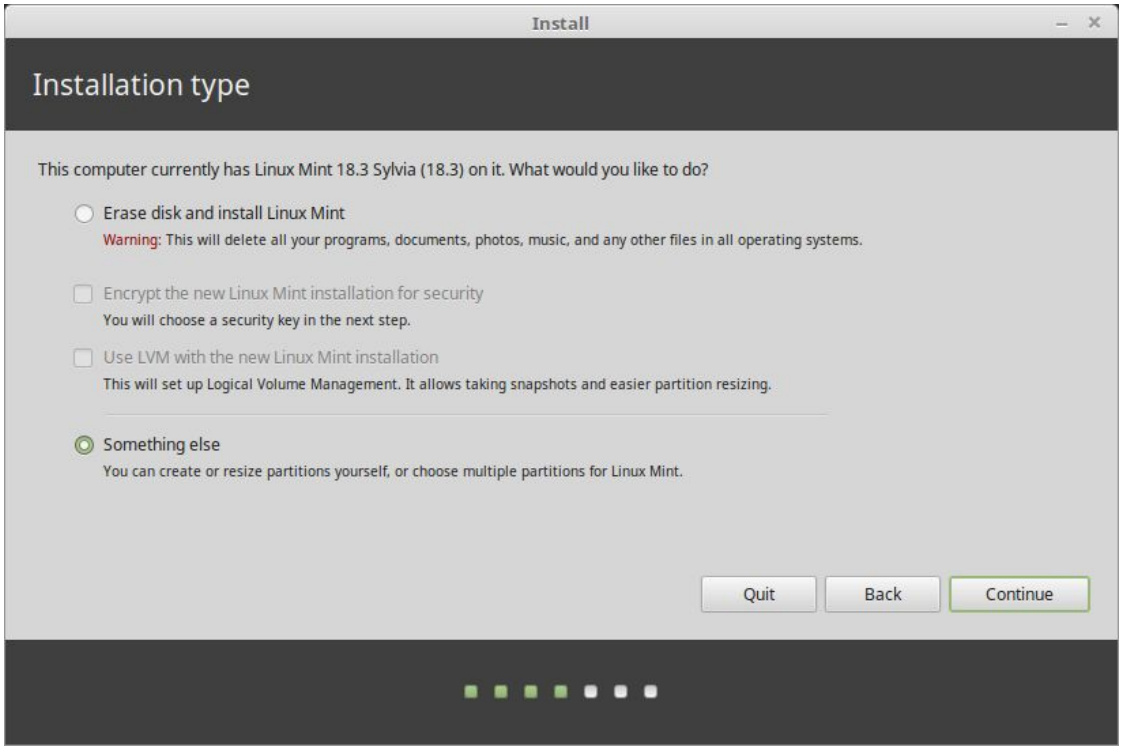
INSTALACIJA LINUX MINT-A

1. Uključite računar sa USB pogona.
2. Kada pokrenete računar s USB fleš pogona, Linux Mint započinje sesiju uživo. Automatski se prijavljuje u sistem i prikazuje vam radnu površinu s instalacijskim programom na njemu. Ovo možete koristiti za testiranje kako vam se sviđa Linux Mint.
3. Sesija uživo je slična uobičajenoj sesiji Linux Mint nakon što se trajno instalira na računar, ali sporije jer se pokreće s USB pogona. Promjene koje unesete u sesiju uživo nisu trajne.

INSTALIRANJE LINUX MINT-A NA RAČUNARU

1. Da biste trajno instalirali Linux Mint na svoj računar, na radnoj površini dvaput kliknite **Instaliraj Linux Mint**
2. Odaberite svoj jezik.
3. Povežite se s Internetom.
4. Ako ste povezani na Internet, potvrdite okvir da biste instalirali multimedijske kodeke.
5. Odaberite vrstu instalacije.
6. Ako je Linux Mint jedini operativni sistem koji želite pokrenuti na ovom računalu i svi podaci se mogu izgubiti na tvrdom disku, odaberite **Obriši disk** i instalirajte Linux Mint

UPOZORENJE



Šifriranje nove Linux Mint instalacije radi sigurnosti odnosi se na potpunu enkripciju diska. Ako ste novi u Linuxu, umjesto toga koristite šifriranje kućnog direktorija (možete ga odabrati kasnije

7. Ako je na računaru prisutan drugi operativni sistem, instalacijski program vam nudi mogućnost instaliranja Linux Mint-a uz njega. Ako odaberete ovu opciju, instalacijski program automatski promijeni veličinu vašeg postojećeg operativnog sistema, napravi mjesta i instalira Linux Mint pored njega. Izbornik za pokretanje postavljen je za izbor između dva operativna sistema svaki put kada pokrenete računalo.
8. Odaberite vremensku zonu.
9. Odaberite raspored tipkovnice.
10. Unesite svoje korisničke podatke. Vaše korisničko ime je vaše ime računa koje se koristi za lokalnu prijavu, dok je ime računara ime vašeg računara.
11.Da biste zaštitili svoje lične podatke od ljudi koji imaju fizički pristup vašem računalu, označite Šifriraj moju kućnu mapu.
12. Odaberite jaku lozinku.
13. Pratite prezentaciju dok je na vaš računar instaliran Linux Mint.
14. Kada je instalacija završena, kliknite Restart Now (Ponovo pokreni).
15. Tada će se računar početi isključivati i tražiti da uklonite USB. Nakon ponovnog pokretanja, računar bi vam trebao pokazati meni za pokretanje ili pokrenuti vaš novi instalirani operativni sistem Linux Mint.

D) REPOVI: JOŠ SIGURNIJI OPERATIVNI SISTEM

Tails označava 'Amnesic Incognito Live System'. Radi se o otvorenom izvoru, Linux operativnom sistemu koji štiti privatnost i anonimnost korisnika. Nakon isključivanja sistem ne ostavlja trag upotrebe vašeg računara, on je orijentisan na privatnost i sigurnost, podrazumevano pristupa anonimno internetu, čime se zaobilazi svaka cenzura, i dolazi unapred instaliran alatima otvorenog koda koji omogućavaju bezbednost.

Ovdje nije obrađeno detaljno, ali trebali biste ga uzeti u obzir ako smatrate da radite na vrlo osjetljivim temama, posebno onim koji se suočavaju s državnim akterima sa sofisticiranim obavještajnim agencijama. Pogledajte ovdje više **https://tails.boum.org/.**

SIGURNIJE PREGLEDAVANJE INTERNETA

Pretraživanje interneta izlaže vas brojnim rizicima. U ovom se odjeljku rješavaju rizici u komunikaciji između vašeg računala i poslužitelja koji gostuje web stranicu koju pregledavate. Započinje s popisom dodataka koji bi svaki korisnik trebao koristiti. Zatim objašnjava šta je VPN i kako ga instalirati. I na kraju, za najviši nivo rizika objašnjava Tor i Tor pretraživač za sigurnije pregledavanje.

A) DODATNI PAKETI ZA VAŠ TRENUTAČNI PRETRAŽIVAČ

Prvo biste trebali instalirati nekoliko dodataka ili proširenja na vaš trenutačni pretraživač Firefox ili Chromium (verzija Chromea bez Googleovih usluga).

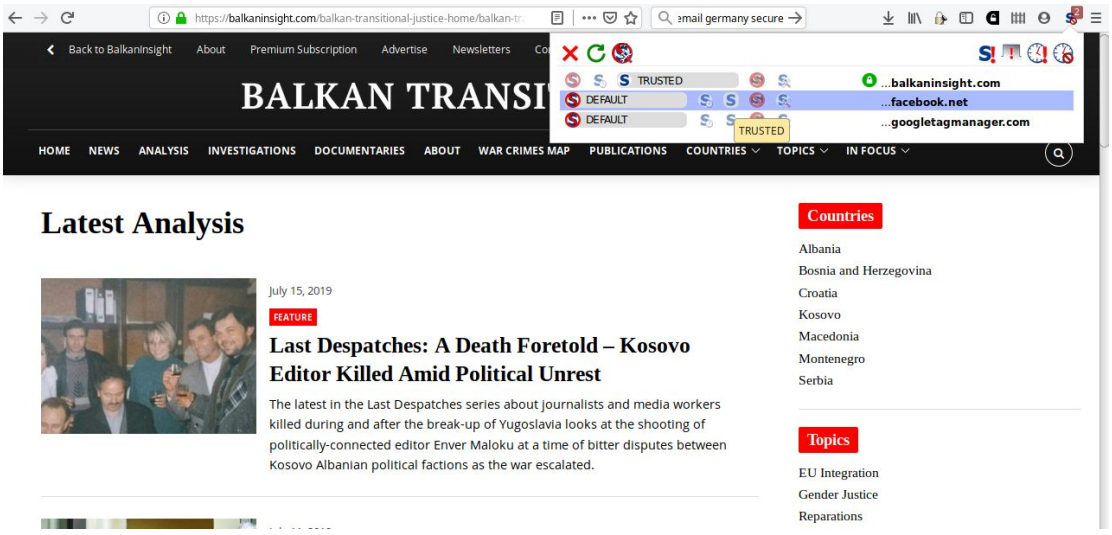
Dodaci

Većina najpopularnijih pretraživača sigurno omogućava vaš identitet, lokaciju i aktivnost. Međutim, postoje neka proširenja koja će pomoći povećanju privatnosti i sigurnosti. Sljedeća proširenja koja su dostupna i za Firefox i Chromium preporučuju se:

HTTPS Everywhere: forsira šifriranje za sve veze između vašeg web pretraživača i web poslužitelja koji posjetite. Imajte na umu da neke web stranice ne nude takvu vezu. Status određene veze možete vidjeti klikom na ikone s lijeve strane adresne trake preglednika. **https://www.eff.org/https-everywhere**

uBlock Origin: efikasan blokator oglasa i praćenja. Zajedničke su skripte postavljene na vašem računalu kako bi vas identificirale i pratile vaše ponašanje stvarajući vaš profil ponašanja na webu. uBlock Origin blokira sve takve tragače. **https://github.com/gorhill/uBlock#installation**

Napredniji: NoScript Security Suite: većina modernog weba radi na JavaScript-u, skriptnom jeziku koji se može iskoristiti. NoScript omogućava da JavaScript, Flash, Java i drugi izvršni sadržaj budu pokrenuti samo iz pouzdanih domena po vašem izboru (npr. Sa vaše web lokacije za kućno bankarstvo), ublažavajući ranjivosti koje se mogu lako iskoristiti. Ako vam je potrebna veća zaštita, NoScript omogućuje da se ove skripte pokreću samo na mjestima u koja imate povjerenja. U skladu s tim, potrebno je neko vrijeme da se napravi popis web lokacija kojima vjerujete omogućavajući zakonite i potrebne skripte, dok su ostale one blokirane prema zadanim postavkama. **https://noscript.net/getit**



Prikaz dodatka NoScript sa statusom JavaScript-a na veb lokaciji (blokiranje koda sa Facebook i Google servera)

B) KORIŠTENJE VPN-A

VPN označava Virtual Private Network. To je oblik tuneliranja svih vaših podataka na drugi poslužitelj koji se pojavljuje drugima kao da dolaze s tog drugog poslužitelja. Ova tehnika maskira vaš IP koji se može koristiti za identifikaciju vaše lokacije i eventualno vas. Tunel vas štiti i od znatiželjnih očiju u vašoj neposrednoj blizini, poput vašeg davatelja internetskih usluga ili vlade u vašoj zemlji.

VPN bi vam mogla ponuditi kompanija osiguravajući na primjer da se vaše javne WiFi veze ne mogu očitati. VPN također omogućava zaobići bilo koji internetski filtar implementiran u vašoj nadležnosti.
Međutim, čak je i s VPN-om vaš promet i dalje podložan nadziranju i praćenju od strane samog VPN-a, poslužitelja usluge na koju se povezujete i drugih igrača nakon izlaska iz VPN-a na javni internet.

Ključni je odabir izbora dobrog dobavljača VPN-a u prijateljskoj nadležnosti s povoljnim zakonima. Ponašanje VPN-a ovisi o povjerenju i reputaciji koju su izgradili kao usluge i oni nisu uvijek transparentni uprkos onome što mogu tvrditi ili se mogu iznenada promijeniti. Većina VPN-a plaća se kreditnom karticom i mogu izgraditi profil vaših navika pregledavanja koji će vas identificirati.

Stoga su VPN-ovi pogodni samo u određenim scenarijima da spreče prijetnje u vašoj neposrednoj mreži. Dvije dobre VPN usluge su FreedomeVPN sa sjedištem u Finskoj i ProtonVPN sa sjedištem u Švicarskoj, ali trebali biste napraviti vlastito istraživanje kako biste osigurali da dobijete najbolju uslugu. Svi koštaju nekoliko eura mjesečno za upotrebu, ali FreedomeVPN nudi i osnovni besplatni nivo koji ćemo i ovdje pokazati.

Upotreba ProtonVPN Windows aplikacije

ProtonVPN i drugi davatelji usluga objavljuju vlastite aplikacije većinom za Windows, macOS, Android i iOS koji su spremni konfigurirani, pa stoga ne treba nikakvu predkonfiguraciju koja je inače potrebna. Ispod su upute za instaliranje i povezivanje sa Windows PC-a. Pogledajte **https://protonvpn.com/support/** radi dodatne pomoći o ostalim operativnim sistemima (macOS, Linux, Android i iOS).

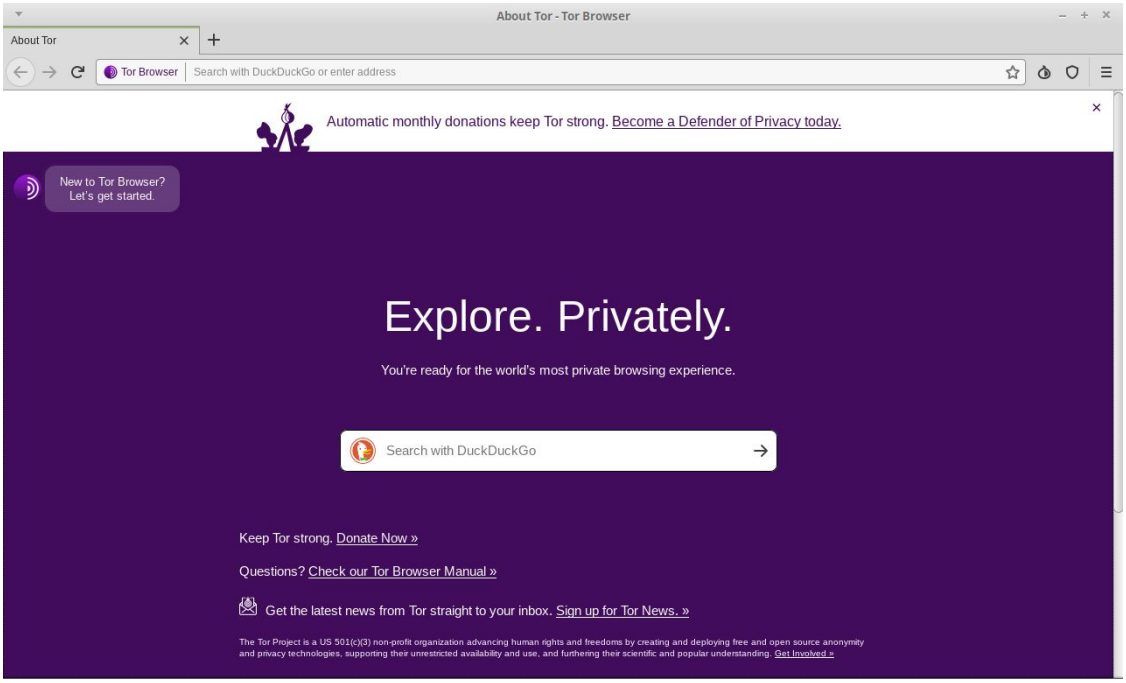
1. Idite na **https://account.protonvpn.com/signup** i prijavite se za ograničeni plan. Ako imate račun ProtonMail, možete ga koristiti.
2. Da biste preuzeli ProtonVPN, idite na https:**//protonvpn.com/download/** i kliknite na Download for Windows.
3. Po završetku instalacije pronađite prečicu i dvaput kliknite na nju da biste pokrenuli aplikaciju. Pojavit će se zaslon za prijavu tamo gdje trebate unijeti svoje ProtonVPN vjerodajnice za prijavu. Unesite podatke svog računa stvoreni u koraku 1.
4. Kad se prijavite, vidjet ćete mogućnosti za brzu i jednostavnu navigaciju i povezivanje.
5. Sada možete vidjeti popis zemalja pri čemu svaki ima popis VPN servera koje možete koristiti klikom na strelicu dolje. Izaberite ga i kliknite Quick Connect.

ProtonVPN ekran za vezu

6. Imajte na umu da besplatni račun omogućava vam pristup samo besplatnim serverima u Holandiji, SAD-u i Japanu. Izaberite onu koja vam je najbliža radi boljih performansi, vjerovatno Holandiju ili druge, ako se želite pojaviti kao pregledavatelje iz te druge dvije države.
7. Gotovi ste.

C) SIGURNIJI PREGLEDNIK: TOR BROWSER

Pregledavanje web stranica podvrgnuto je nadzoru na različitim razinama. Mreža Tor Onion dizajnirana je za zaštitu od praćenja, nadzora i cenzure na mreži. Tor Browser je siguran preglednik koji usmjerava svoj promet preko Onion mreže i ima druga sigurnosna poboljšanja. Svaka sesija preglednika Tor je jedinstvena.



Ekran za otvaranje preglednika Tor

Using Tor Browserg Tor Browser

1. Idite na službenu stranicu Tor Browser-a da biste preuzeli Tor Browser za svoju platformu **https://www.torproject.org/download/** Postoje opcije za Windows, macOS, Linux i Android. Pogledajte donji odjeljak Sigurnije mobilno pregledavanje kako biste ga koristili na mobilnom uređaju.
2. Za Windows preuzmite .exe datoteku i pokrenite je.
3. Kliknite na Start meni i pokrenite Tor Browser.
4. Prvi put kada pokrenete Tor pretraživač, vidjet ćete prozor Tor Network Settings (postavke mreža). To vam nudi mogućnost da se direktno povežete s mrežom Tor koja bi trebala raditi u jugoistočnoj Europi ili konfigurirate Tor preglednik za svoju vezu u slučaju da vaš provajder / zemlja blokira proxy ili Tor veze.

Tor pretraživač pruža korisnicima mogućnost da odrede željenu razinu sigurnosti. U pregledniku Tor kliknite na ikonu značke (s desne strane adresne trake) i kliknite na " Advanced Security Options" (Napredne sigurnosne mogućnosti)da biste vidjeli opcije. Ova opcija je podrazumevano postavljena na Standard, što povećava upotrebljivost. Da biste iskoristili viši nivo privatnosti i anonimnosti koji Tor može ponuditi, postavite klizač na **Safer** (sigurniji) ili **Safest** (najsigurniji) nivo.

SIGURNO SLANJE E-POŠTE

A) SIGURNIJE USLUGE E-POŠTE

Za one koji žele sakriti pravi identitet sebe i / ili drugih s kojima komuniciraju, treba koristiti anonimne račune e-pošte, koji nisu povezani sa bilo kojim drugim aspektom vašeg mrežnog identiteta. Drugim riječima, ne bi trebali biti ni na koji način povezani s vama. Usluge poput Gmail-a i Microsoft Live-a traže telefon ili alternativnu adresu e-pošte, tako da ovi pružatelji usluga nisu idealni za anonimne naloge. ProtonMail, Tutanota i Posteo (plaćeni) omogućavaju korisnicima da stvaraju račune bez takvih identifikacijskih podataka.

B) ŠIFRIRANJE E-POŠTE U PRETRAŽIVAČU S MAILVELOPEOM

Šifriranje e-pošte pomoću OpenPGP standarda uobičajena je praksa da se osigura da se vaše poruke e-pošte ne čitaju ako ih presreću na putu ili u mirovanju na serverima davatelja usluga, kao što je slučaj s većinom komercijalnih dobavljača usluga e-pošte. Šifriranje e-pošte s OpenPGP-om nije najpogodnije za korisnike i ako se ukrade privatni ključ za šifriranje, sve se poruke kojima stranka ima pristup mogu pročitati.

Nadalje, ako se privatni ključ izgubi, te poruke nećete moći dešifrirati. Također, šifrirani e-mail nije savršen jer se adresa i predmetna linija (metapodaci) mogu čitati ako ih presreću, tako da imate na umu prilikom korištenja. Mailvelope je besplatni softver za cjelovito šifriranje sadržaja e-pošte unutar web preglednika (Firefox ili Chrome / Chromium) koji se dobro integrira s većinom najpopularnijih komercijalnih internetskih usluga e-pošte.

Može se koristiti za šifriranje i potpisivanje elektroničkih poruka i privitaka uz izbjegavanje matičnog klijenta e-pošte (poput Thunderbird-a) koristeći OpenPGP standard. Najkorisnije je jer vas ne primorava da pređete na novog klijenta e-pošte.

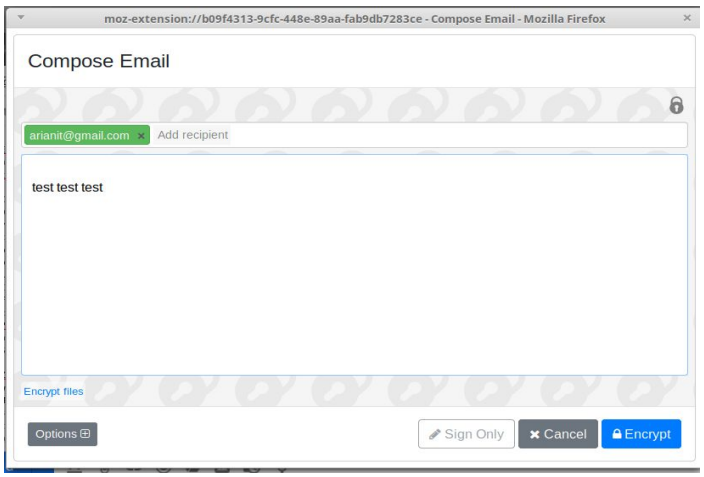
Postavljanje Mailvelope-a i vašeg PGP ključa

1. Idite na Firefox dodatke i potražite Mailvelope.
2. Na alatnoj traci kliknite ikonu Mailvelope. Otvorit će se ekran Dashboard.
3. Kliknite **Manage keys**. Zatim **Generate** ako nemate postojeći ključ ili **Import** ako ga već imate.
4. Unesite polja koristeći ime povezano sa vašim računom e-pošte. Unesite sigurnu lozinku koju nećete zaboraviti jer u suprotnom gubite pristup ključu. Ostale postavke ostavite zadane.
5. Kliknite na **Generate** i pričekajte uskoro. Vaš je ključ sada generisan i spreman za upotrebu. Poslat će vam se poruka da biste mogli da pošaljete svoj javni ključ na server da bi ga drugi mogli pronaći. Vaš javni ključ je ono što drugi koriste za šifriranje poruka za vas. Da biste ih otvorili, koristite svoj privatni ključ.

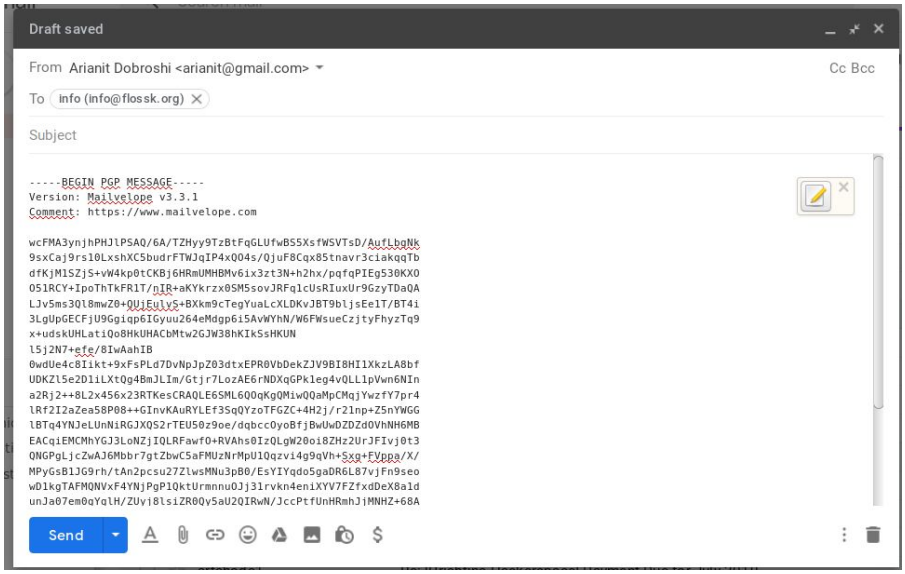
Upozorenje: Vaš privatni ključ treba čuvati u tajnosti. Nikada ga ne delite sa bilo kim.

Slanje šifriranih e-poruka

1. Da biste nekome šifrirali e-poštu, prvo morate da uvezete javni ključ osobe u Mailvelope-u. To možete dobiti direktno npr. putem e-pošte pronađite ga na javnoj web stranici te osobe ili na nekom od poslužitelja ključeva na kojem se nalaze ključevi pod uvjetom poput onih s Ubuntua ili MIT-a.
2. U Mailvelopeu idite na **Key management** (Upravljanje ključevima), zalijepite tekst javnog ključa u okvir ili kliknite **Search** (Pretraži). Pretražite putem e-pošte ili imena i kliknite na šifru ključa, koja bi trebala biti nešto poput ovog E7F3E1D6. Imajte na umu da iako je na javnim poslužiteljima navedeno da ključ pripada određenoj osobi, ova činjenica se može prevariti, to je razlog zašto možda želite potvrditi ključni kôd na neki drugi način s osobom koja posjeduje ključ.
3. Kliknite tipku za uvoz. Sada ste spremni za šifriranje poruka e-pošte i datoteka na tu adresu.
4. Ako je Mailvelope aktivan, na polju za poruke usluge e-pošte (npr. Gmail) dobit ćete ikonu u koju ćete umjesto toga upisati svoju poruku. Ta će poruka biti šifrirana javnim ključem osobe kojoj šaljete pod uvjetom da ste prvo uvezli njihov ključ.



Tekstni okvir poštanskog pisma



Prikaz šifrirane poruke na Gmailu stvorene pomoću Mailvelope-a

SIGURNOST MOBILNOG OPERATIVNOG SISTEMA

Većina vašeg korištenja računara sada se obavlja na mobilnom uređaju, uključujući i ono za osjetljiv rad. Ipak, mobilna sigurnost je u žalosnom stanju, izlažući korisnike mnogim ranjivostima. Od zastarjelih i nepodržanih Android sustava do aplikacija koje traže previše dozvola, trebali biste dobro razmisliti upotrebljavate li mobilne uređaje za osjetljiv rad. Sam Android i određene aplikacije, čak i one navodno zaštićene poput WhatsAppa, tražit će od vas da ažurirate svoje podatke na poslužitelju, koji se pohranjuju na jasnom mjestu i mogu biti lako dostupni putem sudskog naloga ili na neki drugi način.

A) OSNOVE: SIGURNOST ANDROID APLIKACIJA

Iako Apple odobrava mobilne aplikacije prije nego što ih pojedinačno objave u App Store-u, vodeći pažljivu brigu o privatnosti koje te aplikacije nameću korisnicima, to nije slučaj sa Androidovim aplikacijama iz Google Play Store-a.

Ako koristite Android vjerovatno su vas pitali i davali aplikacijama pristup stvarima poput vaše povijesti poziva, poruka, lokacije, kamere, mikrofona i više. Prije verzije 6.0, Android je tražio od korisnika da odobre zahtjeve za dozvolom u paketu, što izaziva sumnju zašto je određenoj aplikaciji potreban pristup mikrofonu ako se bavi samo fotografijama.

Od verzije 6.0 Android omogućuje korisnicima da odaberu dozvole koje će dati aplikaciji. Treba obratiti pažnju na to koje aplikacije instalirate na telefon. Pored toga, ako ne planirate koristiti određenu značajku aplikacije, npr. fotografije označene vašom zemljopisnom lokacijom, a ne dozvolite ih ili ih privremeno privremeno odobrite samo kad su vam potrebne.

Da biste provjerili već data odobrenja:

1. Otvorite Settings (Postavke) uređaja
2. Kucnite na **Apps and notifications** (Aplikacije i obavijesti). Odaberite bilo koju aplikaciju, a zatim dodirnite Permissions (Dozvole) ili App permissions (Dozvole aplikacija) da biste pregledali dozvole na osnovu određenog odobrenja.
3. Dodirnite klizač na položaj **On** (Uključeno) ili **Off** (Isključeno). Ako niste sigurni, onemogućite je. Android će vas pitati za dozvolu kada je to potrebno i vi možete donijeti odluku na osnovu razumnosti zahtjeva u toj situaciji.

B) OSNOVE: AŽURIRANJE ANDROID-A

Većina verzija Androida je zastarjela zbog modela isporuke softvera koji Google (izdavač Android-a) koristi sa svojim klijentima (proizvođačima mobilnih telefona). Google često gubi kontrolu nad ažuriranjem svog softvera, što je sada odgovornost proizvođača ili prijevoznika koji možda nemaju poticaj da podrže vaš određeni uređaj i nakon određenog vremena. Generalno, uređaji s brendom Google i proizvođači vodećih telefona imaju duže periode podrške. Apple iOS uređaji također su duže podržani. Zbog toga biste uvijek trebali tražiti razdoblje podrške s ažuriranjima softvera prije nego što kupite određeni model.

Ažuriranje Android-a

U postavkama možete vidjeti broj verzije uređaja i razinu ažuriranja sigurnosti uređaja. Obavijesti ćete dobiti kada su ažuriranja dostupna za vas ako je sistem i dalje ažuriran. Ažuriranja možete i sami provjeriti. Imajte na umu da se ove upute mogu mijenjati ovisno o Android verziji. Posavjetujte se s web stranicom proizvođača telefona ako imate poteškoća da ih pratite.

Da biste vidjeli koju verziju Androida imate

1. Otvorite **Settings** (Postavke) svog uređaja.
2. Pri dnu dodirnite **System> Advanced> System update** (Sistem> Napredno> Ažuriranje sistema). Ako ne vidite Advanced (Napredno), dodirnite **About phone** (O telefonu).
3. Pogledajte vašu verziju Android-a i nivo sigurnosne zakrpe pod odgovarajućim naslovima.

Dobijte najnovije Android ispravke dostupne za vas

Kada dobijete obavještenje o ažuriranju, otvorite ga i dodirnite akciju ažuriranja.

Ako ste izbrisali obavještenje ili je vaš uređaj van mreže:

1. Otvorite **Settings** (Podešavanja) uređaja.
2. Pri dnu tapnite na **System > Advanced > System update** Sistem> (Napredno> Ažuriranje sistema). Ako ne vidite Advanced (Napredno), dodirnite **About phone** (O telefonu).
3. Vidjećete status ažuriranja. Sljedite bilo koje korake na ekranu.

SIGURNOSNO KOMUNICIRANJE

A) OSNOVE: PORUKA SA SIGNALOM

Pogledajte ove sigurnosne značajke dok ocjenjujete klijenta za razmjenu trenutnih poruka kojeg koristite:

- da li su poruke šifrovane tokom tranzita?
- da li su poruke šifrirane davatelju usluga ako ih ima (tj. Da nisu ravnopravne)?
- da li su identiteti kontakata ovjereni?
- je li komunikacija sigurna ako su ukradeni ključevi?
- je li softverski kod otvoren za nezavisni pregled?
- je li sigurnosno dizajniran pravilno dokumentiran?
- da li je bilo nedavno nezavisnih revizija koda?

U ovom je aspektu WhatsApp bolji od Vibera, a Signal bolji od WhatsApp-a.

Signal ispunjava većinu gore navedenih kriterija i prilično je blizu točke upotrebljivosti do one koju već upotrebljavate. Preporučuje se. Signal je dostupan besplatno na Android-u, iOS-u i Desktop-u (Windows / Mac / Linux), otvoren je izvor i pregledan je, obuhvaća tekstualne, glasovne i videopozive i datoteke, svi su krajnje šifrirani i dok odmaraju na uređaju . Međutim, to čini određene sigurnosne kompromise kojima se ovdje nećemo baviti.

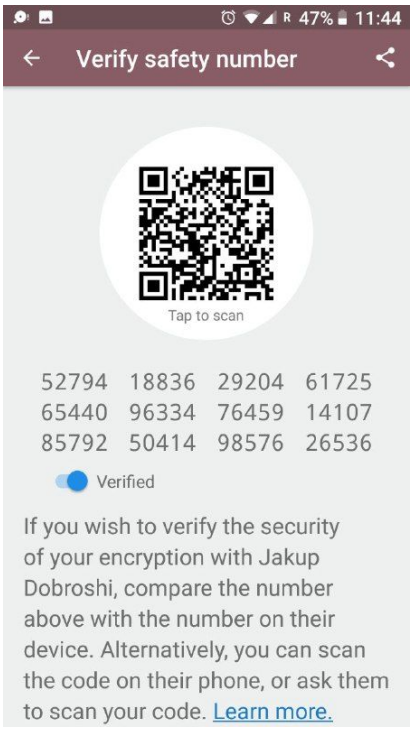
Da biste instalirali signal na svoj Android / iOS telefon,

1. Potvrdite da vaš telefon ima *Android 4.4 / iOS 10.0* ili noviji.
2. Potražite Signal Private Messenger na Google Play / App Store i instalirajte ga.
3. Sledite uputstva na ekranu da biste dovršili postupak registracije slično kao i drugi glasnici koji zahtevaju da registrujete svoj telefonski broj.

Provjera kontakata

Na Signalu ste u mogućnosti da potvrdite svoj kontakt kako biste bili sigurni da račun s kojim razgovarate zaista pripada osobi za koju tvrdi da pripada i da vaš sigurni komunikacijski kanal nije ugrožen.

1. Kad je riječ o signalu, i vi i vaš kontakt trebate ići na ekran na kojem biste obično razgovarali sa svojim kontaktom.
2. Kucnite na ikonu okomite tri točke (gornji desni ugao), a zatim **Conversation settings > Verify safety number** (Postavke razgovora> Provjerite sigurnosni broj).
3. Uporedite dane brojeve ili pritisnite **Tap to scan** (Da biste skenirali) drugi uređaj sa Signalom za usporedbu. Možete je također pročitati naglas ili poslati na zabavu. Ako su isti, dodirnite **Verified** (Provjereno).

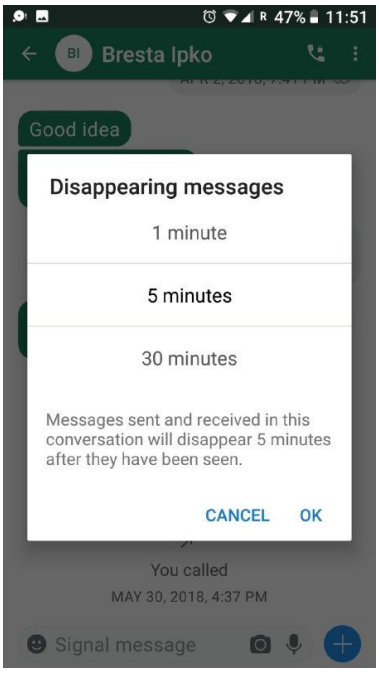


Ekran za potvrdu o signalu

Poruke koje nestaju

Možda želite da poruke nestanu nakon određenog vremenskog perioda.

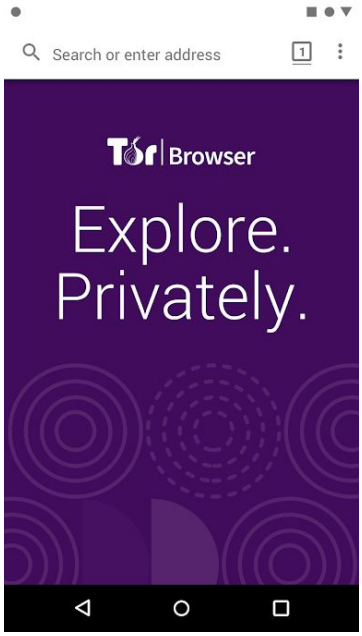
1. Na Signalu idite na ekran na kojem biste obično razgovarali sa svojim kontaktom.
2. Dodirnite ikonu okomite tri okomite točke (gornji desni ugao), a zatim poruke koje želite da nestanu.
3. Na novom ekranu odaberite period. U razgovoru će se pojaviti poruka koja navodi ovaj period.



Zaslon za nestajanje poruka na Signalu postavljen na 5 minuta

B) SIGURNIJE PREGLEDAVANJE PUTEM MOBILNIH UREĐAJA: TOR BROWSER

Tor Browser je dostupan i za Android i iOS. Ako koristite Android, možete ga preuzeti u Google Play trgovini traženjem Tor pretraživača za Android. Na Apple App Store potražite Onion Browser.



Tor pretraživač na Androidu

DIJELJENJE DATOTEKA

Dijeljenje velikih datoteka sigurno je svakodnevna borba. Već su pokrivena dva načina za sigurno slanje datoteka, putem šifrirane e-pošte putem OpenPGP-a i trenutnih poruka, poput signala. Za veće datoteke možda će biti potrebna druga rješenja. U nastavku su navedena dva druga načina. Firefox Send je pogodan za scenarije niskog rizika i praktičan je dok je OnionShare sasvim siguran, pogotovo ako su datoteke prvo šifrirane.

A) OSNOVNO: POŠALJI FIREFOX

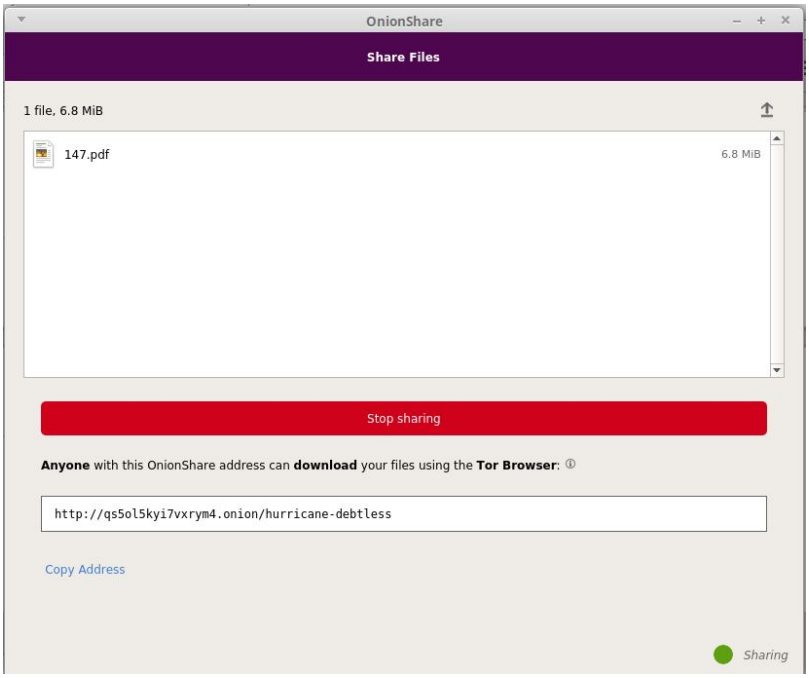
Firefox Send je novije rješenje jednostavno za korištenje. Možda biste htjeli prvo da šifrirate datoteku pomoću opcije Šifriraj datoteku na Mailvelope-u (postoji ograničenje od 50 MB) ili na drugi način prije prijenosa datoteke. Da biste ga poslali, idite na **http://send.firefox.com,** odaberite datoteku za učitavanje i podesite opcije. Imajte na umu da veće datoteke i više vremena na poslužitelju zahtijevaju da se registrirate.

B) SIGURNIJE DIJELJENJE: ONIONSHARE

OnionShare vam omogućuje vrlo sigurno i anonimno dijeljenje datoteka bilo koje veličine. Stvara privremeni nevidljivi web server. Generira se nekorisna adresa i dijeli se primatelju da se otvori u pregledniku Tor za preuzimanje datoteka. Iako je vrlo siguran, nedostatak ovog alata je taj što datoteke nalazite na vlastitom računalu, pa ih morate držati u radu dok ih druge strane ne dobiju. Primalac također mora pokrenuti Tor pregledač kako bi primio datoteke.

Da biste ga koristili:

1. Započnite instalacijom OnionShare za svoju platformu sa **https://onionshare.org**
2. Nakon instaliranja otvorite OnionShare.
3. Dodajte datoteke i kliknite Start share (započni dijeljenja). Ne postoji ograničenje veličine datoteke. Na kraju postupka OnionShare će vam dati adresu poput ove **http://qs5ol5kyi7vxrym4.onion/hurricane-debtles** koju biste trebali predati primatelju preko sigurnog kanala. Imajte na umu da svi s adresom mogu dobiti pristup datotekama pod uvjetom da je vaš OnionShare s dijeljenjem i dalje pokrenut



Snimak ekrana OnionShare

KUDA ODAVDE

Ako ste prerasli ovaj priručnik i želite više savjeta ili se suočite s prijetnjama višeg nivoa, drugi dobri vodiči dostupni su besplatno putem interneta, iako su uglavnom na engleskom jeziku i ponekad zastareli.

- **Sigurnost u kutiji - Digitalni sigurnosni alati i taktike**

  https://securityinabox.org/

  Sigurnost u kutiji projekat je kolektivnih taktičkih tehnologija i branitelja prve linije. Taktički vodiči u ovom priručniku pokrivaju osnovne principe, uključujući savjete o sigurnijoj upotrebi društvenih medija i mobilnih telefona. Vodiči za alate nude detaljne upute za pomoć pri instaliranju, konfiguriranju i korištenju nekih bitnih softvera i usluga digitalne sigurnosti. Alatke zajednice fokusiraju se na određene grupe ljudi - ponekad u određenim regijama - koje su suočene sa značajnim prijetnjama digitalne sigurnosti. Oni uključuju prilagođene savjete o alatima i taktikama koji su relevantni za potrebe ovih određenih grupa.

- **Nadzorna samoobrana: savjeti, alati i upute za sigurniju internetsku komunikaciju**
  https://ssd.eff.org/
  To je popis vodiča i planova lekcija zaklade Electronic Frontier.

- Sigurnost informacija novinarima, priručnik Centra za istraživačko novinarstvo
  https://tcij.org/sites/default/files/u11/InfoSeczanovinare V1.3.pdf
  Priručnik osmišljen da poduči novinare i medijske organizacije o tome kako prakticirati sigurnost informacija u digitalnom dobu, štiteći svoj rad, izvore i komunikacije na različitim razinama rizika uključujući **najvišu** razinu rizika.
- **Digitalna sigurnosna služba za novinare reportera bez granica**
  https://helpdesk.rsf.org/
  Počevši od jula 2019. RSF će redovito nuditi besplatne online videozapise i online savjetovanja o digitalnoj sigurnosti. Ovi se seminari mogu vidjeti ili uživo ili kasnije. Seminari će se fokusirati na to kako zaštititi račune na društvenim medijima od hakiranja, kako zaobići cenzuru pomoću VPN-a i koje su aplikacije za razmjenu poruka na pametnim telefonima najbolje za novinarski rad. U budućnosti će se nuditi više individualizirane usluge podrške.

O AUTORU

Arianit Dobroshi je predsjednik Izvršnog odbora FLOSSK-a, nevladine organizacije koja promiče besplatni softver otvorenog koda na Kosovu. Obučio je novinare i članove civilnog društva o alatima za privatnost i lobirao protiv zakona o digitalnom nadzoru na Kosovu. Do njega se može doći na **arianit.dobroshi@flossk.org**

Ovaj priručnik je objavljen u sklopu projekta InfoSec za Balkan koji finansira Radio Slobodna Azija kroz Fond za otvorenu tehnologiju, a provode Open Data Kosovo i FLOSSK.

Originalna verzija napisana je na engleskom jeziku. Također je dostupan na albanskom, bosanskom, makedonskom, crnogorskom i srpskom jeziku


OPEN
TECHNOLOGY
FUND


RFA
Radio Free Asia


ODK
OPEN DATA KOSOVO


Free Libre Open Source Software Kosova