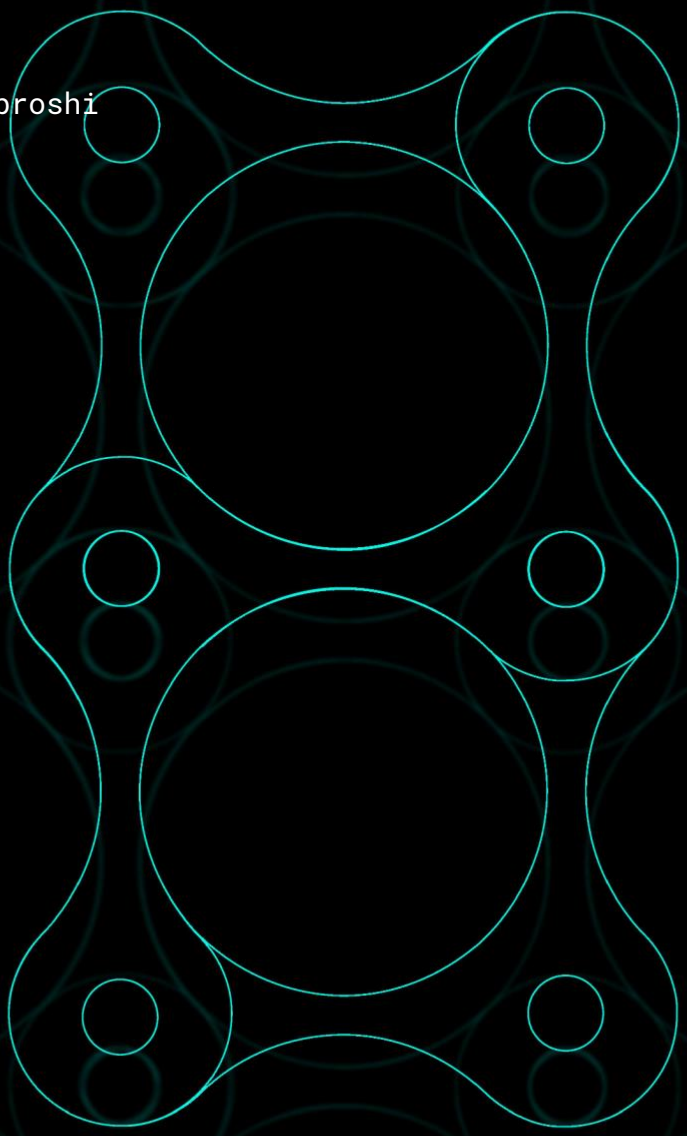
PRIRUCNIK ZA SIGURNOST INFORMACIJA ZA NOVINARE I CIVILNO DRUŠTVO

Autor: Arianit Dobroshi



INFOSEC
for Balkans

Jul 2019

PREGLED SADRZAJA

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 bezbednosnim pretnjama (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 odeljak ovog priručnika pokriva najmanje dva nivoa sigurnosti: osnovni nivo potreban za sigurno računanje koji bi trebalo da praktikuje svako, i odeljak s većim rizikom kojem bi trebali da teže svi istraživački novinari i organizavije civilnog društva koji rade na osetljivim poslovima u regionu. Ipak, neki aktivisti I organizacijama civilnog društva u regionu suočavaju se sa još većim stepenom pretnje i trebalo bi da potraže druge dublje resurse, od kojih su neki navedeni u poslednjem odeljku ovog priručnika.

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

A) ZA KOGA JE OVAJ PRIRUCNIK

Ovaj priručnik je namenjen 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 žele 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 zahtevaju određenu žrtvu upotrebljivosti i praktičnosti iz uobičajene prakse.

B) KAKO CITATI OVAJ PRIRUCNIK

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 odeljke 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 vežba, mada u našem zapažanju to još nije slučaj. drugi podbroj trebalo bi da osigura nadogradnju sigurnosti za većinu osnovnih korisnika.

Deo 2 ovog priručnika pokriva stvaranje jačih lozinki, korisnih za sve platforme. U delu 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 difaultu sigurniji sistem, ali i jednostavan za upotrebu. U delu 4 bezbedno se obraćamo pregledavanju, a u delu 5 sigurno upravljanje e-poštom. U delu 6 pogledamo neke stvari koje se moraju uraditi za bezbednost mobilnog sistema, dok se u delu 7 bavimo bezbednošću komunikacije. Na kraju, u delu 8 se govori o deljenju datoteka, dok se u delu 9 nalazi lista resursa za čitaoce koji žele više.

C) IDENTIFIKACIJA VASIH SIGURNOSNIH POTREBA

Neovlašćeni pristup vašim podacima može podrazumevati njegovu upotrebu, otkrivanje, ometanje, modifikaciju, inspekciju, snimanje ili uništenje. Međutim, pošto su digitalne pretnje nevidljive, složene i često neodredive, one se mogu potceniti ili previdjeti.

Postoji nekoliko načina na koje možete sagledati pretnje sa kojima se suočavate i potrebe za sigurnošću informacija. Najosnovnija pretnja s kojom se suočava cela populacija jesu pretnje mreža sa kojima se susreće svaki građanin regiona, mada se ciljana publika u ovom Priručniku može suočiti sa više specijalizovanih ciljanih prijetnji.

Zemlje regiona primenile su EU direktivu o zadržavanju podataka koja nalaže posedovanje metapodataka (podataka o podacima) o svim obrađenim telekomunikacijama, uključujući liste svih telefonskih poziva, IP adresa, tekstualnih poruka itd. Poslatih ili primljenih u periodu između šest do dvadeset četiri meseca, kojima se može pristupiti sudskim nalogom. Iako sami komunikacioni sadržaji nisu sačuvani, napredovanje od zakonskog mandata do veleprodajnog nadzora nije tako teško i zahtev za sudskim nalogom zavisi od krhkosti sistema vladavine zakona u regionu. Čak su i metapodaci izuzetno otkrivajući jer bi mogli da omoguće onima koji ih poseduju da grade društvene grafikone svog života i indirektno identifikuju sadržaj i izvore sa kojima sarađujete, čak i retrospektivno.

Sa specijalizovanim pretnjama, stranka koja vrši nadzor koristi specijalizovane i sofisticirane alate protiv cilja. Tehnologija za to sve je jeftinija, a pristup njima od strane vlada i privatnih strana postaje sve lakši. Na primer, otkriveno je 2015. godine da je vlada severne Makedonije prisluškivala telefone oko 20.000 ljudi. Takođe postoje dokazi da je srpska vlada preusmeravala internet do određenih tačaka gde je mogao da bude lako prisluškivan. To je bilo pre nekoliko godina i situacija se verovatno pogoršala. Ako verujete da se suočavate sa ovakvom vrstom pretnje, ovaj priručnik nije dovoljan da biste se zaštitili i trebalo bi da potražite posvećenu pomoć.

STVARANJE JACIH LOZINKI

Sigurna lozinka je slučajna, dovoljno dugačka i kombinuje listu gornjih i donjih malih slova, brojevi i drugi znakovi (npr. kkvv3.K3? rrz). Bez obzira na to, moguće je imati sigurne lozinke koristeći kombinaciju reči pod uslovom da je dovoljno dugačka, jedinstvena za uslugu, slučajna i nije povezana sa vama. Kombinacija nasumičnih reči kojih se lako možete setiti je dovoljno sigurna lozinka (npr. WITHIN-WIRE-GRASS-pluto-save).

A) DVA FAKTORA AUTENTIFIKACIJE

Kad god je dostupno, dvofaktorska autentifikacija pruža drugo sredstvo uz vašu uobičajenu lozinku za zaštitu veb 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.

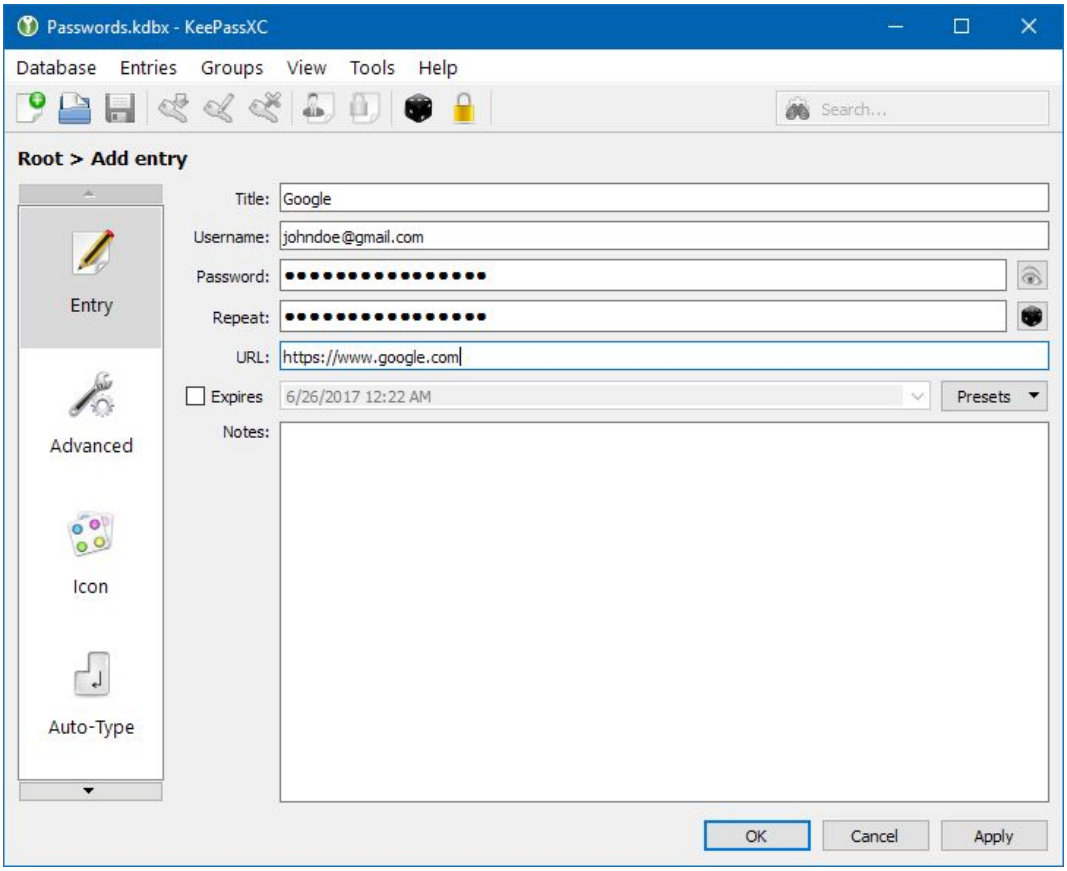
Omogućavanje autentifikacije drugog faktora zavisi od vašeg softvera i potražite ga u Settings>Password (Podešavanja> Lozinka) ili slično da biste ga omogućili. Međutim, još ga ne nude sve usluge.

Na primer, dok koristite Google usluge, možete da posetite **https://miaccount.google.com/signinoptions**, prijavite se sa svojim nalogom, omogućite ga da postoji i odaberete način za primanje drugi put privremene lozinke, obično SMS-om. Imajte na umu da ako izgubite svoj telefonski broj, bićete zaključani sa svog naloga. Zbog toga bi trebalo da postavite i najmanje jednu rezervnu opciju, tako da možete da se prijavite čak i ako vaši drugi koraci nisu dostupni. Jednokratne lozinke za štampanje mogu vam biti najlakši način da se prijavite ako izgubite svoj broj ili putujete.

B) KORISCENJE SOFTVERA ZA KREIRANJE I UPRAVLJANJE LOZINKAMA

Lozinke koje koristite treba da budu jedinstvene za svaku uslugu koju koristite. Memorisanje sigurnih lozinki ubrzo postaje nemoguće, pa je potreban alat za upravljanje njima. Da biste olakšali kreiranje sigurnih lozinki i upravljanje njima, možete koristiti namenski softver. Dobar otvoreni izvor je KeePassKSC (**https://keepassxc.org**) dostupan za Windows macOS i Linux, menadžer lozinki koji čuva korisnička imena i lozinke u lokalnoj šifrovanoj bazi podataka, zaštićen glavnom lozinkom. Takođe dolazi sa PWG-enom, snažnim generatorom slučajnih lozinki.)

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



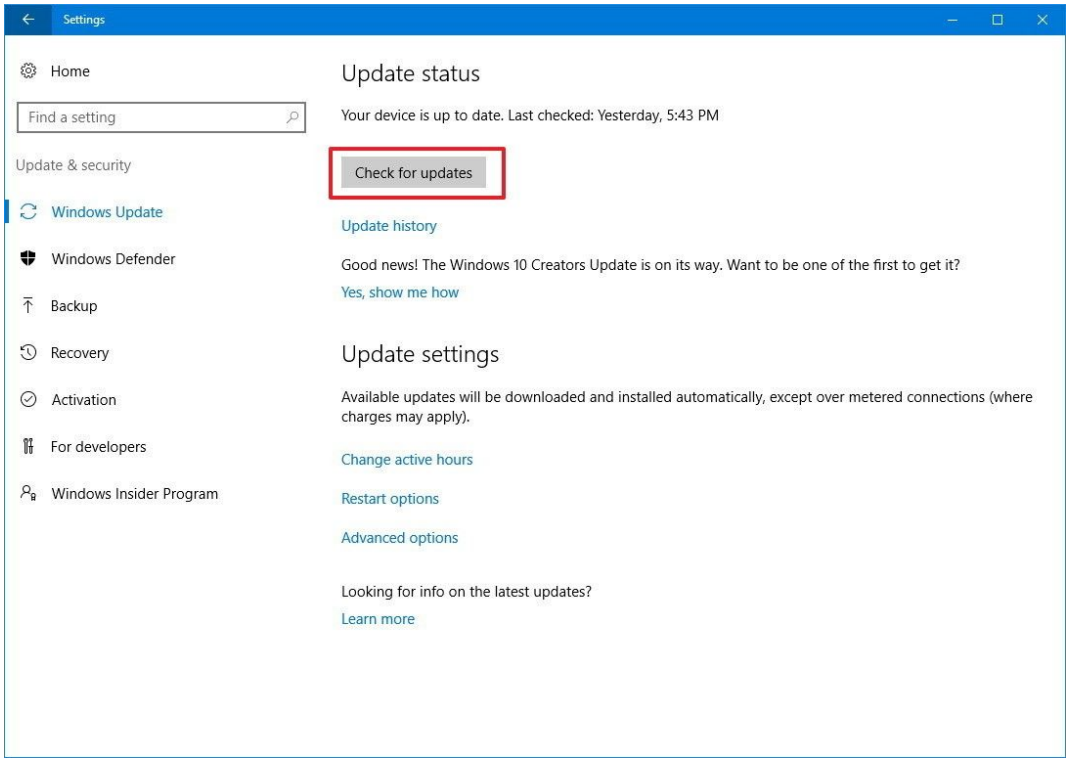
Prikaz ekrana KeePassKSC

KORISCENJE SIGURNIJEG OPERATIVNOG SISTEMA

Operativni sistem za desktop je osnova vašeg svakodnevnog sigurnog korišćenja računara. Uopšte, sigurnost sistema rangiranog od niskog do visokog nivoa je: Windows 7 ili 10 koji su najčešće korišćeni, ali i najmanje zaštićeni, macOS koji je podrazumijevano sigurniji, pa se ovdje ne obrađuje, Linux Mint, ovdje opisan Linux sistemski ukus i Tails, takođe baziran na Linux-u, dizajniran s obzirom na informacionu sigurnost ali sa kompromisima o upotrebljivosti.

A) AZURIRANJE SISTEMA WINDOWS

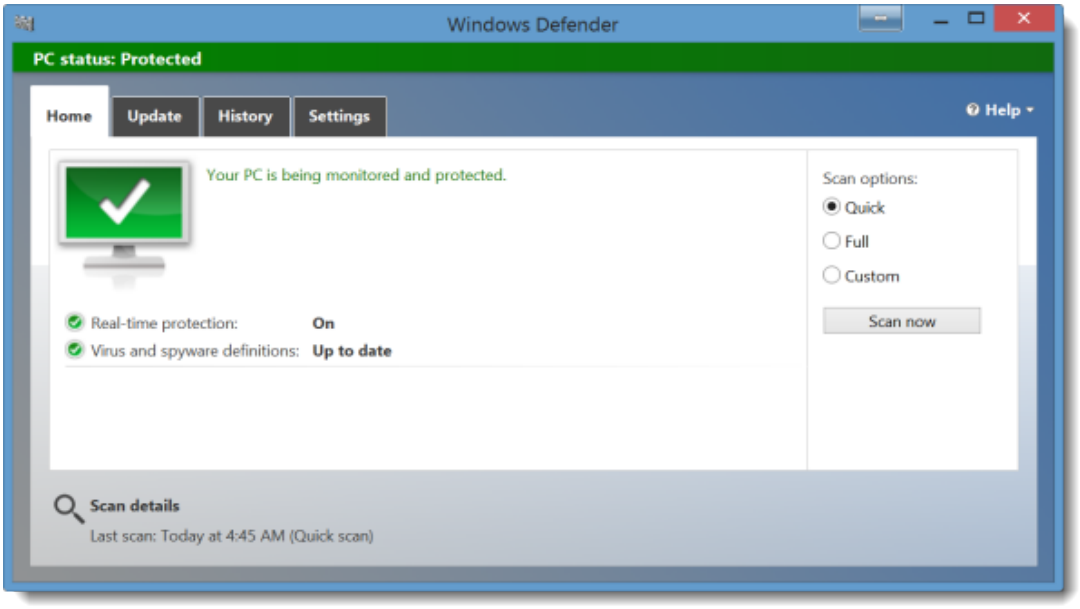
Ažuriranje Windows-a je kritično ako radite na računaru povezanom s internetom. Previše puta, piratske Windows kopije spriječene su da primaju ažuriranja koja vas izlažu svim vrstama zlonamjernog softvera i drugim prijetnjama. Imajte na umu da bi Windows 7 Microsoft izdavač trebao povući do kraja 2019. godine i da posle tog datuma neće biti ažurirani sigurnosnim zakrpama. Trebali biste se nadograditi na Windows 10 posle te tačke.
Da biste osigurali da je vaš Windows ažuriran, trebalo bi da potražite „Windows Update“ na traci za pretragu Windows-a, kliknite Proveri ažuriranja i obezbedite da dobijete ekran poput onog na kome piše „Nema ažuriranja.“ Primijetićete 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 računar ažuriran.



Status ažuriranja Windows-a

Pored toga, potreban vam je softver koji vas štiti od virusa i zlonamernog softvera. U većini slučajeva ugrađeni Windows Defender je adekvatan i ne koristi dodatne resurse na računaru. Da biste ga pokrenuli, deinstalirajte drugi antivirusni softver. Idite na traku za pretragu Windows-a i otkucajte „Windows Defender“. Proverite da li je uključena zaštita u stvarnom vremenu i da li su definicije virusa ažurne. Ako ne, trebalo bi da ih ažurirate na kartici Ažuriranje.

Ako je vaš sistem duže vreme zastareo, pokrenite skeniranje sistema da biste ga očistili što može potrajati nekoliko sati. Ako ne možete sami da rešite bilo koji potencijalni nalaz, trebalo bi da potražite pomoć.

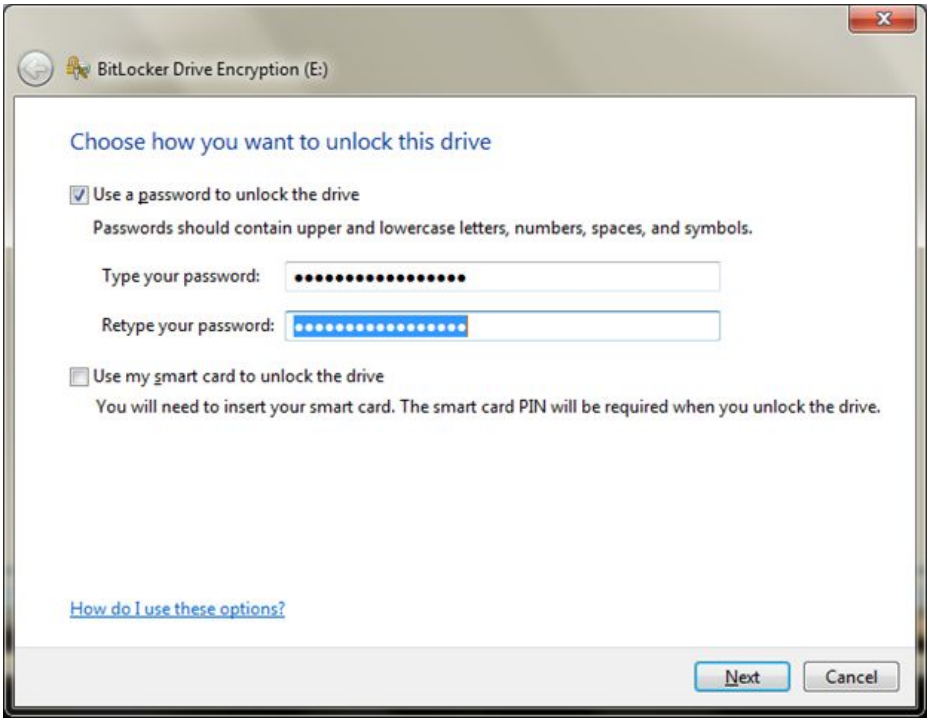


Ažuriran Windows Defender

B) SIFROVANJE DISKA

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

Za šifrovanje punog diska BitLocker-a na sistemskom pogonu potreban je računar sa Trusted Platform Module (TPM) ugrađenim u vaš računar. Ovaj čip generiše i čuva ključeve za šifrovanje koje BitLocker koristi. Ovo možete izbeći korišćenjem grupnih pravila da biste dozvolili upotrebu BitLocker-a bez TPM-a, mada ćete žrtvovati određenu sigurnost.



BitLocker ekran

Možete da šifrujete disk koji nije sistem ili prenosivi uređaj bez TPM-a, tako da je pametno da svoje podatke imate na posebnom pogonu (obično drajv „D“).

Najlakši način da omogućite BitLocker za disk je da otvorite File Explorer i kliknite desnim tasterom miša na disk, a zatim kliknite na Uključi BitLocker. Ako u kontekstnom meniju ne vidite ovu opciju, verovatno nemate Pro ili Enterprise izdanje operativnog sistema Windows-a pa vam je potrebna druga alternativa.

Upozorenje: BitLocker vam pruža ključ za oporavak koji biste trebali čuvati bilo da ga podhranite negdje na sigurno van postojećeg računara ili da ga štampate i fizički sačuvate. U slučaju da zaboravite svoj ključ ili je vaš TPM modul uništen, to će vam omogućiti da ponovo pristupite svojim datotekama.

Ako je sistemski pogon šifrovan lozinkom i imate TPM, nećete ništa primetiti. Ako ste šifrovali nesistemski ili prenosivi uređaj, Windows će od vas tražiti da otključate disk kada prvi put pristupite njemu. Unesite lozinku za otključavanje ako se koristi tokom svakog ponovnog pokretanja.

Ako koristite drugi operativni sistem kao što je Linux, tokom instalacije nudi se opcija šifrovanja diska. Pogledajte deo za instaliranje Linux Mint-a da biste videli kako to omogućiti. Za sve sisteme dobar nezavisni alat otvorenog koda koji poštuju stručnjaci za bezbednost je VeraCript (ranije TrueCript) dostupan ovde **https://www.veracrypt.fr**

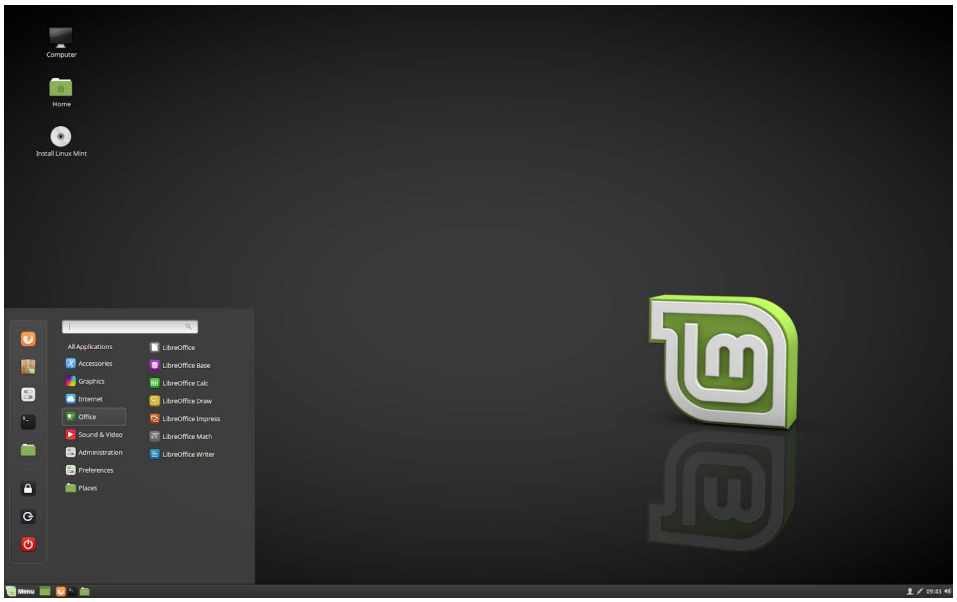
C) LINUK MINT: SIGURNIJI OPERATIVNI SISTEM

Linux je besplatni i otvoreni izvorni operativni sistem. Sigurniji je od Windows-a jer se ne suočava sa nekim bezbednosnim problemima Windows-a, ali zahtevaće da naučite novi operativni sistem i ponekad zahteva da ukucate komande da biste izvršili stvari.

Postoji mnogo „ukusa“ ili iteracija Linuxa: popularniji su Ubuntu, Fedora i Linux Mint, a Tales su namenjeni onima sa većim sigurnosnim potrebama. Trebalo bi da koristite onu verziju koja je najčešća u vašem okruženju, tako da možete potražiti pomoć ako se zaglavite. Ako to nije izvodljiva opcija, onda možete koristiti Linux Mint, što ovde objašnjavamo. Najprikladnija je za korisnike, ima veliku podršku zajednice, nekomercijalna je i ima Windows osećaj za one koji se prebacuju sa nje.

Dok Linux ima pristup skladištu hiljade besplatnog i otvorenog koda softvera, možda ćete morati da naučite 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, Audaciti za uređivanje zvuka itd. Upotrebite **http://alternativeto.net** da biste pronašli alternative softveru koji koristite u Windows ili Mac na Linux-u.

Sledeće ćemo pokazati kako da instalirate Linux Mint na računaru.



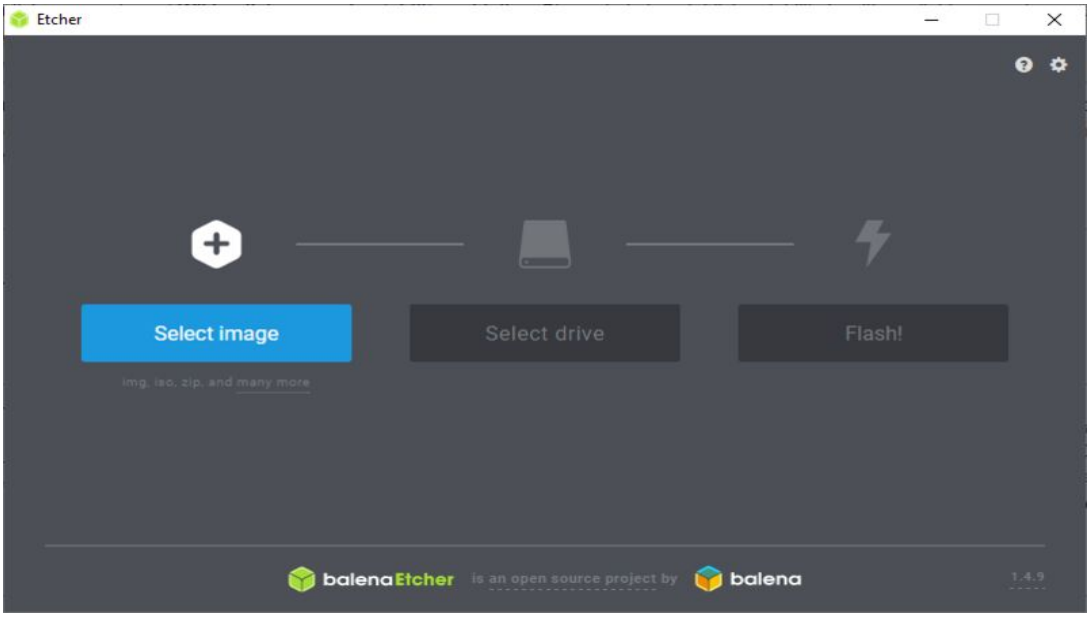
Desktop Linux mint (cimet)

PRIPREMA INSTALACIONI USB

1. Napravite sigurnosnu kopiju podataka sa svog Windows-a sistema na spoljne medije. Najbolje je da potpuno obrišete Windows instalaciju, iako Windows i Linux mogu da rade jedan pored drugog.
2. Preuzmite ISO-ov Linux mint Cinnamon ovde **https://xv.linukmint.com/dovnload.php**. Može biti potrebno oko 30 minuta, u zavisnosti od vaše internet veze.

ZAPISIVANJE ISO NA USB FLES UREDAJU SA ETCHER-OM

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



Etcher ekran

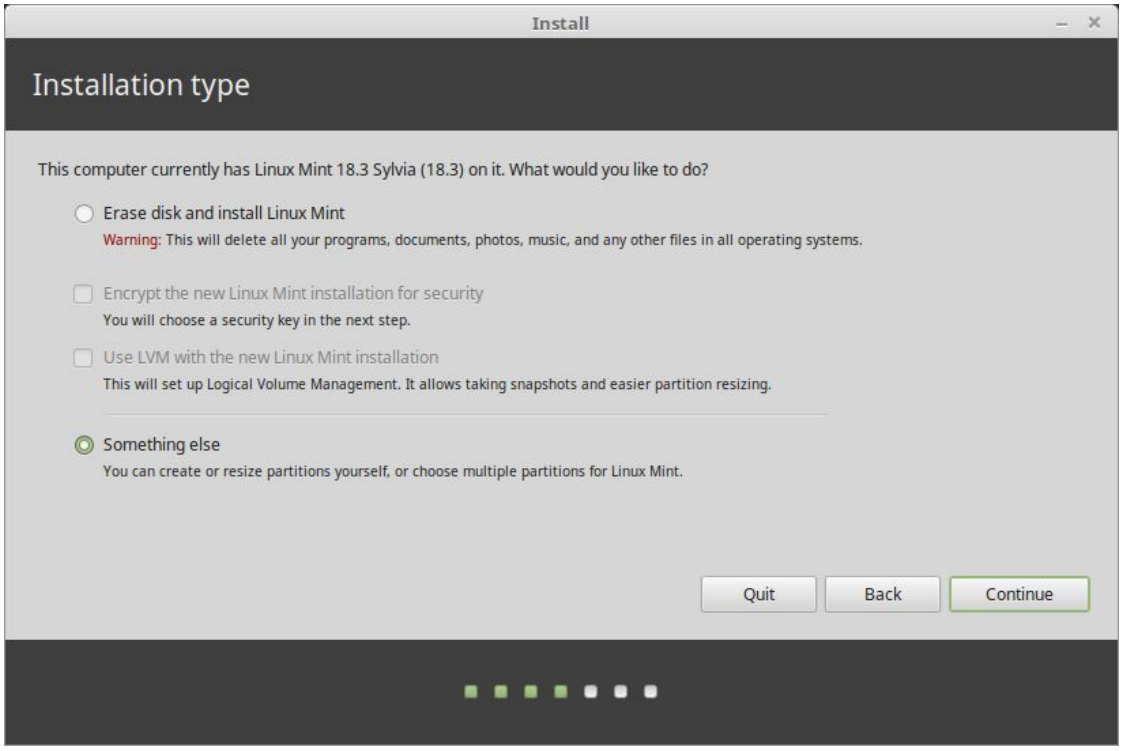
INSTALACIJA LINUX MINT-A

1. Pokrenite računar sa USB uređaja.
2. Kada računar pokrenete sa USB fleš uređaja, Linux Mint započinje sesiju uživo. Automatski se prijavljuje u sistem i prikazuje vam radnu površinu sa instalatorom na njemu. Ovo možete da koristite za testiranje kako vam se sviđa Linux Mint.
3. Live session je sličan uobičajenoj Linux Mint sesiji nakon što se trajno instalira na računar, ali sporije jer se pokreće sa USB uređaja. Izmene koje unesete tokom sesije uživo nisu trajne.

INSTALIRANJE LINUK MINT-A NA RACUNARU

1. Da biste trajno instalirali Linux Mint na svoj računar, na radnoj površini dvaput kliknite Instaliraj Linux Mint
2. Izaberite jezik.
3. Povežite se sa Internetom.
4. Ako ste povezani na Internet, potvrdite okvir da biste instalirali multimedijalne kodekse.
5. Odaberite vrstu instalacije.
6. Ako je Linux Mint jedini operativni sistem koji želite da pokrenete na ovom računaru i svi podaci se mogu izgubiti na čvrstom disku, izaberite Obriši disk i instalirajte Linux Mint

UPOZORENJE



Šifrovanje nove Linux Mint instalacije radi sigurnosti odnosi se na potpunu enkripciju diska. Ako ste novi u Linux-u, umesto toga koristite šifrovanje kućnog direktorijuma (možete ga odabrati kasnije tokom instalacije).

7. Ako je na računaru prisutan drugi operativni sistem, instalater vam pokazuje mogućnost da uz njega instalirate i Linux Mint. Ako odaberete ovu opciju, instalacijski program automatski promeni veličinu vašeg postojećeg operativnog sistema, napravi mesta i instalira Linux Mint pored njega. Postavljen je meni za pokretanje da biste izabrali između dva operativna sistema svaki put kada pokrenete računar.
8. Izaberite svoju vremensku zonu.
9. Izaberite raspored tastature.
10. Unesite svoje korisničke podatke. Vaše korisničko ime je ime vašeg naloga za lokalnu prijavu, dok je ime domaćina ime računara.
11. Da biste zaštitili svoje lične podatke od ljudi koji imaju fizički pristup vašem računaru, označite Šifruj moju matičnu mapu.
12. Izaberite jaku lozinku.
13. Pratite prezentaciju dok je na računar instaliran Linux Mint.
14. Kada je instalacija završena, kliknite na Restart Now (Ponovo pokreni).
15. Računar će se zatim isključiti i tražiti da uklonite USB. Po ponovnom pokretanju računar treba da vam prikaže meni za pokretanje ili pokrene vaš novi instalirani Linux Mint operativni sistem.

D) TALES: JOS SIGURNIJI OPERATIVNI SISTEM

Tails označava 'Amnesic Incognito Live Sistem'. Radi se o otvorenom izvoru, Linux-ovom operativnom sistemu koji štiti privatnost i anonimnost korisnika. Nakon isključivanja sistem ne ostavlja trag upotrebe računara, on je orijentisan na privatnost i bezbednost, podrazumevano pristupa anonimno internetu, čime se zaobilazi svaka cenzura, i dolazi unapred instaliran alatima otvorenog koda koji omogućavaju bezbednost. Ovde nije detaljno obrađeno, ali trebali biste to razmotriti ako smatrate da radite na veoma osetljivim temama, posebno na onima koji se suočavaju sa državnim akterima sa sofisticiranim obaveštajnim agencijama. Pogledajte ovde više **https://tails.boum.org/.**

SIGURNIJE PRETRAZIVANJE INTERNETA

Pretraživanje interneta izlaže vas brojnim rizicima. Ovaj deo govori o rizicima u komunikaciji između računara i servera koji gostuje veb stranicu koju pregledavate. Započinje sa spiskom dodataka koji bi svaki korisnik trebalo da koristi. Zatim objašnjava šta je VPN i kako ga instalirati. I na kraju, za najviši nivo rizika objašnjavaju Tor i Tor pretraživač za sigurnije pregledavanje.

A) DODATNI PAKETI ZA VAS TRENUTNI PRETRAZIVAC

Trebali biste početi instaliranjem nekoliko dodataka ili proširenja na vaš trenutni pretraživač ili Firefox ili Chromium (verzija Chrome-a bez Google-ovih usluga).

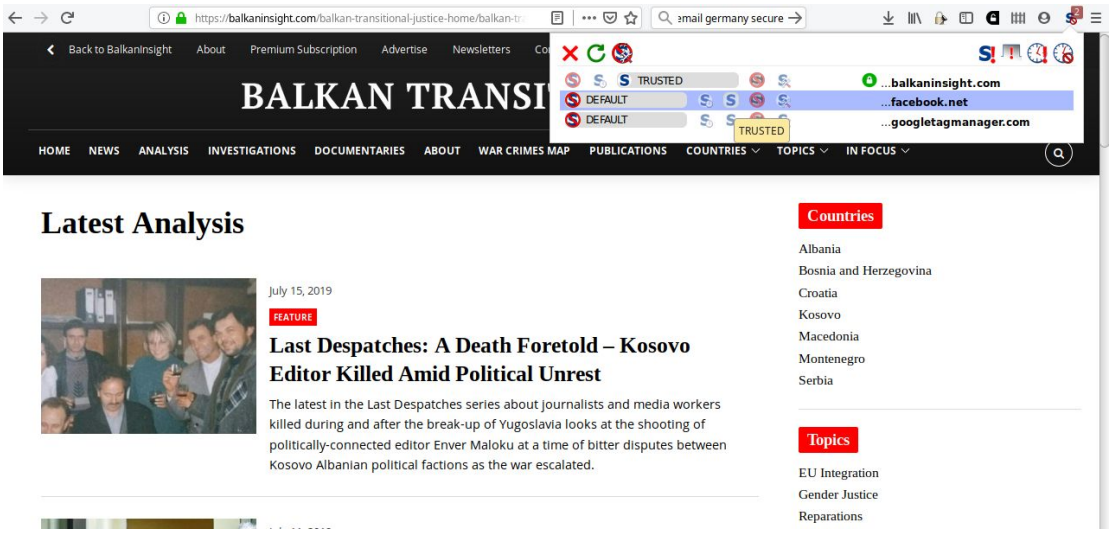
Dodaci

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

HTTPS Everivhere: forsira šifrovanje za sve veze između vašeg veb pregledača i veb servera koji posećujete. Imajte na umu da neke veb lokacije ne nude takvu vezu. Status određene veze možete videti klikom na ikone levo od adresne trake pregledača. https://www.eff.org/https-everivhere

uBlock Origin: efikasan blokator oglasa i pratilaca. Zajedničke skripte postavljene na vašem računaru predstavljaju da bi vas identifikovale i pratile vaše ponašanje stvarajući vaš profil ponašanja na vebu. uBlock Origin blokira sve takve tragače. **https://github.com/gorhill/uBlock#installation**

Napredniji: NoScript Securiti Suite: većina modernog veba 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 veb lokacije za kućno bankarstvo), ublažavajući ranjivosti koje se mogu lako iskoristiti. Ako vam je potrebna veća zaštita, NoScript dozvoljava da se te skripte pokreću samo na veb lokacijama u koje imate poverenja. Uprkos tome, potrebno je neko vreme da se napravi lista veb lokacija kojima verujete omogućavajući legitimne i potrebne skripte, dok su ostale one po difaultu blokirane.
https://noscript.net/getit



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

B) KORISCENJE VPN-A

VPN označava Virtual Private Network. To je oblik tuneliranja svih vaših podataka na drugi server koji se drugima prikazuje kao da dolaze s tog drugog servera. Ova tehnika maskira vaš IP koji se može koristiti za identifikaciju vaše lokacije i eventualno vas. Tunel vas takođe štiti 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 primer da se vaše javne WiFi veze ne mogu očitati. VPN takođe omogućava zaobilaziti bilo koji internetski filter koji je implementiran u vašoj nadležnosti.

Međutim, čak i ako imate VPN, vaš saobraćaj je i dalje podložan nadgledanju i praćenju od strane samog VPN-a, servera usluge na koju se povezujete i drugih igrača nakon što izađe iz VPN-a na javni internet.

Ključni je izbor odabira dobrog dobavljača VPN-a u prijateljskoj jurisdikciji sa povoljnim zakonima. Ponašanje VPN-a zavisi od poverenja i reputacije koju su izgradili kao usluge i oni nisu uvek transparentni uprkos onome što mogu tvrditi ili se mogu iznenada promeniti. Većina VPN-a se plaća kreditnom karticom i oni mogu da naprave profil vaših navika pregledavanja koji će vas identifikovati. Zbog toga su VPN-ovi pogodni samo u određenim scenarijima da spreče pretnje u vašoj neposrednoj mreži.

Dve dobre VPN usluge su FreedomeVPN sa sedištem u Finskoj i ProtonVPN sa sedištem u Švajcarskoj, ali trebalo bi da uradite sopstvena istraživanja kako biste bili sigurni da dobijate najbolju uslugu. Svi koštaju nekoliko evra mesečno za upotrebu, ali FreedomeVPN nudi i osnovni besplatni nivo koji ćemo i ovde pokazati.

Upotreba ProtonVPN Windows aplikacije

ProtonVPN i drugi provajderi usluga objavljuju sopstvene aplikacije uglavnom za Windows, macOS, Android i iOS koji su spremni konfigurisani, pa ne treba drugačije konfigurisanje. Ispod su smernice o tome kako da instalirate i povežete se sa Windows računarom. Pogledajte **https://protonvpn.com/support/** radi dodatne pomoći o drugim operativnim sistemima (macOS, Linux, Android i iOS).

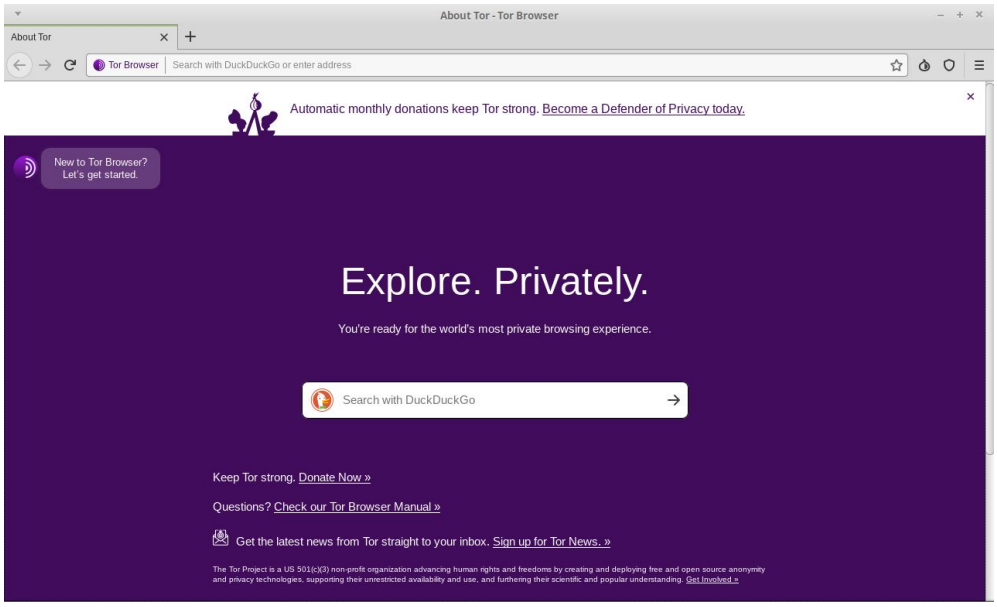
1. Idite na **https://account.protonvpn.com/signup** i prijavite se za ograničeni plan. Ako imate nalog ProtonMail, možete ga koristiti.
2. Da biste preuzeli ProtonVPN, idite na **https://protonvpn.com/dovnload/** i kliknite na dugme Download for Windows
3. Po završetku instalacije pronađite prečicu i dvaput kliknite na nju da biste pokrenuli aplikaciju. Pojaviće se ekran za prijavu tamo gdje je potrebno da unesete svoje ProtonVPN akreditive za prijavu. Unesite podatke za svoj račun kreirani 1. koraku.
4. Kada se prijavite, videćete opcije za brzu i jednostavnu navigaciju i povezivanje.
5. Sada možete videti listu zemalja pri čemu svaki ima listu VPN servera koje možete da koristite klikom na strelicu nadolje. Izaberite ga i kliknite na Quick Connect.

ProtonVPN ekran za vezu

6. Imajte na umu da besplatni nalog omogućava pristup samo besplatnim serverima u Holandiji, SAD-u i Japanu. Izaberite onu koja vam je najbliža zbog boljih performansi, verovatno Holandiju ili druge, ukoliko trebate da se pojavite kao pretraživač iz te druge dve zemlje.
7. Gotovi ste.

C) SIGURNIJI PRETRAZIVAC: TOR PRETRAZIVAC

Pregledavanje veba podvrgnuto je nadzoru na različitim nivoima. Mreža Tor Onion dizajnirana je za zaštitu od praćenja, nadzora i cenzure na mreži. Tor Pretraživač je siguran pretraživač koji usmerava svoj promet preko Onion mreže i ima druga sigurnosna poboljšanja. Svaka sesija pretraživanja Tor-a je jedinstvena.



Ekran otvaranja pretraživača Tor

Korišćenje Tor pretraživača

1. Idite na službenu stranicu Tor Browser-a da biste preuzeli Tor Browser za svoju platformu https://www.torproject.org/dovnload/ Postoje opcije za Windows, macOS, Linux i Android. Pogledajte donji odeljak 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 Browser, videćete prozor Tor Network Settings (Postavke mreža). To vam nudi opciju da se direktno povežete na mrežu Tor koja bi trebalo da funkcioniše u jugoistočnoj Evropi ili da konfigurišete Tor pretraživač za svoju vezu u slučaju da vaš provajder / zemlja blokira proxy ili Tor veze.

Tor pretraživač pruža korisnicima mogućnost da odrede njihov željeni nivo sigurnosti. U pretraživaču Tor kliknite na ikonu značke (desno od adresne trake) i kliknite na "***Advanced Security Options***" (Napredne mogućnosti bezbednosti) da biste videli opcije. Ova opcija je podrazumevano postavljena na ***Standard***, što povećava upotrebljivost. Da biste iskoristili viši nivo privatnosti i anonimnosti koji Tor može da ponudi, podesite klizač na ***Safer***(sigurniji) ili ***Safest*** (najbezbedniji) nivo.

SIGURNO SLANJE E-POSTE

A) SIGURNIJE USLUGE E-POSTE

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

B) SIFROVANJE E-POSTE U PREGLEDACU SA MAILVELOPE-OM

Šifrovanje e-pošte korišćenjem OpenPGP standarda je uobičajena praksa da se osigura da se vaše poruke e-pošte ne čitaju ako se presreću na putu ili u mirovanju na serverima provajdera servisa, kao što je slučaj sa većinom komercijalnih dobavljača usluga e-pošte. Šifrovanje e-pošte pomoću OpenPGP-a nije najpogodnije za korisnike i ako se ukrade privatni ključ za enkripciju, sve poruke kojima strana ima pristup mogu se pročitati. Pored toga, ako se privatni ključ izgubi, nećete moći da dešifrujete te poruke. Takođe, šifrovana adresa e-pošte nije savršena, jer se adresa i predmetna linija (metapodaci) mogu pročitati ako se presreću, tako da imate to na umu prilikom njenog korišćenja.

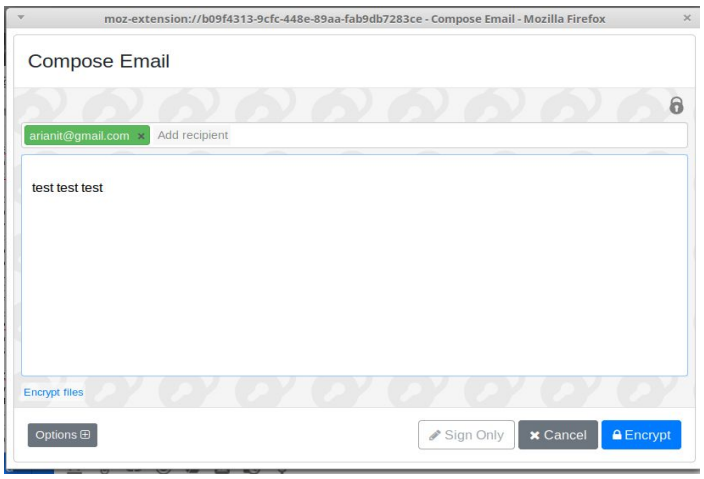
Mailvelope je besplatni softver za šifrovanje sadržaja e-pošte unutar veb pretraživača (Firefox ili Chrome / Chromium) koji se dobro integriše sa najpopularnijim komercijalnim internetskim servisima e-pošte. Može se koristiti za šifrovanje i potpisivanje elektronskih poruka i priloga uz izbegavanje matičnog klijenta e-pošte (kao što je Thunderbird) koristeći OpenPGP standard. Najkorisnija je jer vas ne primorava da pređete na novog klijenta e-pošte.

Podešavanje Mailvelope-a i vašeg PGP ključa

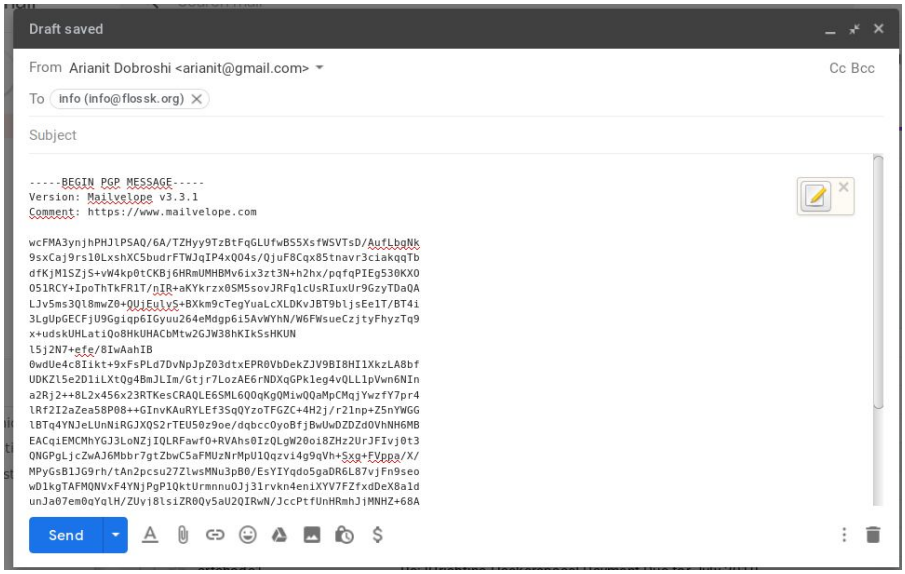
1. dite na Firefox dodatke i potražite Mailvelope.
2. Na alatnoj traci kliknite ikonu Mailvelope. Otvoriće se Dashboard (nadzorna tabla) na ekranu.
3. Kliknite ***Manage keys***. Zatim ***Generate*** ako nemate postojeći ključ ili ***Import*** ako ga već imate.
4. Unesite polja koristeći ime povezano sa nalogom e-pošte. Unesite sigurnu lozinku koju nećete zaboraviti jer ćete u suprotnom izgubiti pristup ključu. Ostala podešavanja ostavite podrazumevana.
5. Kliknite na ***Generate*** i sačekajte uskoro. Vaš ključ je sada generisan i spreman za upotrebu. Poslaće 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 šifrovanje poruka za vas. Da biste ih otvorili, koristite svoj privatni ključ.
6. **Upozorenje**: Vaš privatni ključ treba čuvati u tajnosti. Nikada ga ne delite sa bilo kim.

Slanje šifrovanih poruka e-pošte

1. Da biste nekome šifrovali imejl poruke, prvo morate da uvezete javni ključ osobe u Mailvelope-u. To možete dobiti direktno npr. preko e-pošte, pronađite ga na javnom veb mestu te osobe ili na nekom od servera ključeva na kome se nalaze ključevi koji su obezbeđeni kao što su Ubuntu ili MIT.
2. U Mailvelope-u idite na ***Key management*** (Upravljanje ključevima), zalepite tekst javnog ključa u okvir ili kliknite ***Search*** (Pretraži). Pretražite putem e-pošte ili imena i kliknite na šifru ključa, koja bi trebalo da bude nešto poput ovog E7F3E1D6. Imajte na umu da dok na javnim serverima stoji da ključ pripada određenoj osobi, ta činjenica se može prevariti, zbog čega ćete možda morati da potvrdite ključ koda na neki drugi način sa osobom koja poseduje ključ.
3. Kliknite taster da biste ga uvezli. Sada ste spremni za šifriranje poruka i datoteka e-pošte na tu adresu.
4. Ako je Mailvelope aktivan, na polju za poruke usluge e-pošte (npr. Gmail) dobićete ikonu da umesto toga upišete svoju poruku. Ta će poruka biti šifrovana javnim ključem osobe kojoj šaljete pod uslovom da ste prvo uvezli njihov ključ.



Tekst polje za poštansku poštu



Prikaz šifrovane poruke na Gmail-u kreirane pomoću Mailvelope-a

BEZBEDNOST MOBILNOG OPERATIVNOG SISTEMA

Većina vašeg korišćenja računara sada se obavlja na mobilnom uređaju, uključujući i ono za osetljiv rad. Ipak, mobilna sigurnost je u žalosnom stanju, izlažući korisnike mnogim ranjivostima. Od zastarelih i nepodržanih Android sistema do aplikacija koje traže previše dozvola, trebalo bi dobro razmisliti ako za osetljiv rad koristite mobilne uređaje. Sam Android i neke aplikacije, čak i one koje su navodno sigurne poput WhatsApp-a, od vas će tražiti da ažurirate svoje podatke na serveru, koji se čuvaju na otvorenom i mogu biti lako dostupni putem sudskog naloga ili na neki drugi način.

A) OSNOVE: BEZBEDNOST ANDROID APLIKACIJA

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

Ako koristite Android, verovatno su od vas traženi i dobili su vaš pristup stvarima poput vaše istorije poziva, poruka, lokacije, kamere, mikrofona i još mnogo toga. Pre verzije 6.0, Android je tražio od korisnika da odobre zahteve za dozvolu u paketu, što izaziva sumnju zašto je određenoj aplikaciji potreban pristup mikrofonu ako se bavi samo fotografijama.

Od verzije 6.0, Android omogućava korisnicima da biraju dozvole koje će dati aplikaciji. Treba obratiti pažnju na to koje aplikacije instalirate na telefon. Pored toga, ako ne planirate da koristite određenu funkciju aplikacije, npr. fotografije označene vašom geolokacijom, a ne dozvolite ih ili ih privremeno odobrite samo kada su vam potrebne.

Da biste proverili već data odobrenja:

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

B) OSNOVE: AZURIRANJE ANDROID-A

Većina verzija Androida je zastarela 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 operatera koji možda nemaju uticaj da podrže vaš određeni uređaj i nakon određenog vremena. Generalno, uređaji sa brendom kompanije Google i vodeći telefoni proizvođača imaju duže periode podrške. Apple iOS uređaji takođe su podržani duže vreme. Zbog toga uvek treba da tražite period podrške sa ažuriranjima softvera pre kupovine određenog modela.

Ažuriranje Android-a

U podešavanjima možete da vidite broj verzije uređaja i nivo ažuriranja bezbednosti uređaja. Obaveštenja ćete dobiti kada su ažuriranja dostupna za vas ako se sistem i dalje ažurira. Takođe možete sami da proverite da li postoje ispravke. Imajte na umu da se ova uputstva mogu menjati u zavisnosti od verzije Androida. Posavetujte se s veb stranicom proizvođača telefona ako imate poteškoća da ih pratite.

Da biste videli koju Android verziju imate

1. Otvorite ***Settings*** (Podešavanja) uređaja.
2. Pri dnu kliknite na ***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 obaveštenje o ažuriranju, otvorite ga i dodirnite akciju ažuriranja.

Ako ste izbrisali obaveštenje 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. Videćete status ažuriranja. Sledite bilo koje korake na ekranu.

SIGURNOSNA KOMUNIKACIJA

A) OSNOVE: RAZMENA PORUKA SA SIGNALOM

Pogledajte ove sigurnosne karakteristike dok procenjujete klijenta za instant poruke koji koristite:

- da li su poruke šifrovane tokom tranzita?
- da li su poruke šifrovane provajderu ako ih ima (tj. Nisu jednake)?
- da li su identiteti kontakata provereni?
- da li je komunikacija sigurna ako su ukradeni ključevi?
- da li je softverski kod otvoren za nezavisni pregled?
- da li je bezbednosni dizajn pravilno dokumentovan?
- da li je bilo nedavno nezavisnih revizija koda?

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

Signal ispunjava većinu gore navedenih kriterijuma i prilično je blizu tačke upotrebljivosti do one koju već koristite, preporučuje se. Signal je dostupan besplatno na Android-u, iOS-u i Desktop-u (Windows / Mac / Linux), otvorenog je koda i pregledan je, obuhvata tekstualne, glasovne i videopozive i datoteke, svi od kraja do kraja šifrovani i dok se odmarate na uređaju . Uprkos tome, to donosi određene bezbednosne kompromise kojima se ovde nećemo baviti.

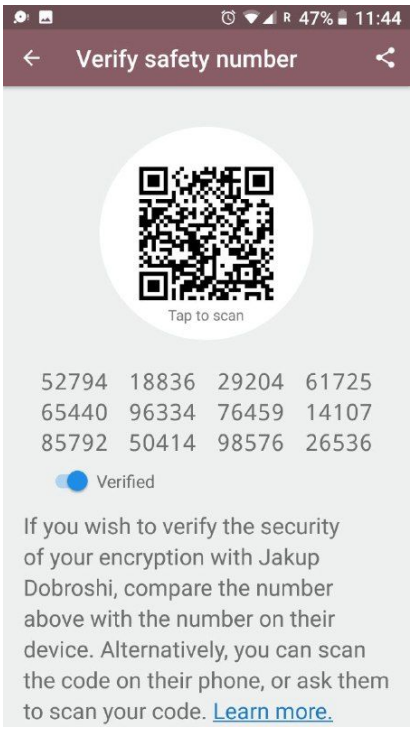
Da biste instalirali signal na svom Android / iOS telefonu,

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

Provera kontakata

Na Signalu ste u mogućnosti da verifikujete svoj kontakt kako biste bili sigurni da nalog sa kojim razgovarate zaista pripada osobi za koju tvrdi da pripada i da vaš bezbedni kanal za komunikaciju nije ugrožen.

1. Kada je reč o signalu, i vi i vaš kontakt trebate da odete na ekran na kojem biste obično razgovarali sa vašim kontaktom.
2. Kucnite na ikonu tri vertikalne tačke (gornji desni ugao), a zatim ***Conversation settings > Verify safety number*** (Postavke razgovora> Proverite bezbednosni broj).
3. Uporedite dane brojeve ili pritisnite ***Tap to scan*** (Da biste skenirali) drugi uređaj sa signalom za poređenje. Možete je takođe pročitati naglas ili poslati na zabavu. Ako su iste, tapnite na Verified (Provereno).

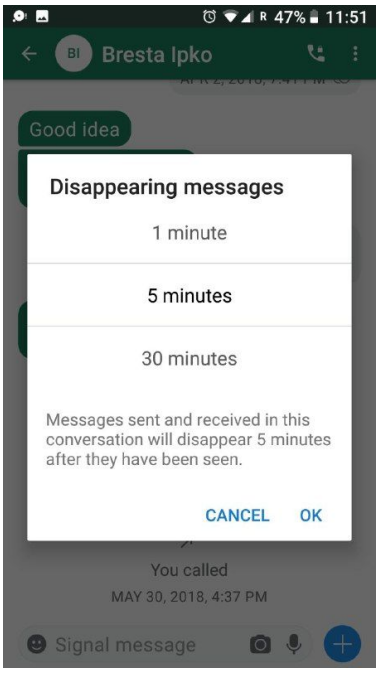


Ekran za potvrdu o signalu

Poruke koje nestaju

Možda želite da poruke nestanu nakon određenog vremenskog perioda.

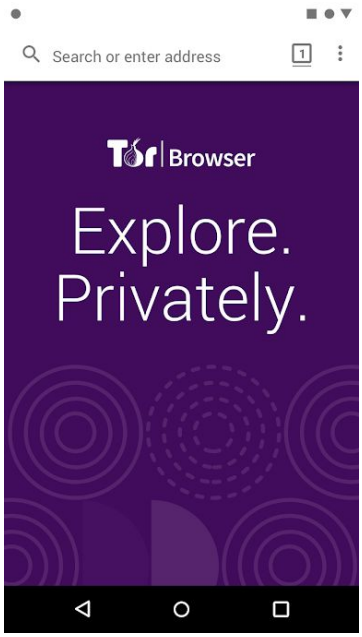
1. Kada je u pitanju signal, idite na ekran na kojem biste obično razgovarali sa svojim kontaktom.
2. Kliknite na ikonu vertikalne tri tačke (gornji desni ugao), a zatim poruke koje želite da nestanu.
3. Na novom ekranu izaberite period. U razgovoru će se pojaviti poruka koja navodi ovaj period.



Zaslon za nestajanje poruka na Signalu postavljen na 5 minuta

B) SIGURNIJE PRETRAZIVANJE PUTEM MOBILNIH UREDAJA: TOR PRETRAZIVAC

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



Tor pretraživač na Androidu

DELJENJE DATOTEKA

Deljenje velikih datoteka sigurno je svakodnevna borba. Već su pokrivena dva načina za sigurno slanje datoteka, putem šifrovane e-pošte putem OpenPGP-a i trenutnih poruka, poput signala. Za veće datoteke mogu biti potrebna druga rešenja. Ispod su dva druga načina da se to uradi. Firefox Send je pogodan za scenarije sa malim rizikom i praktičan je dok je OnionShare sasvim siguran, posebno ako su datoteke prvo šifrovane.

A) OSNOVNO: POSALJI FIREFOX

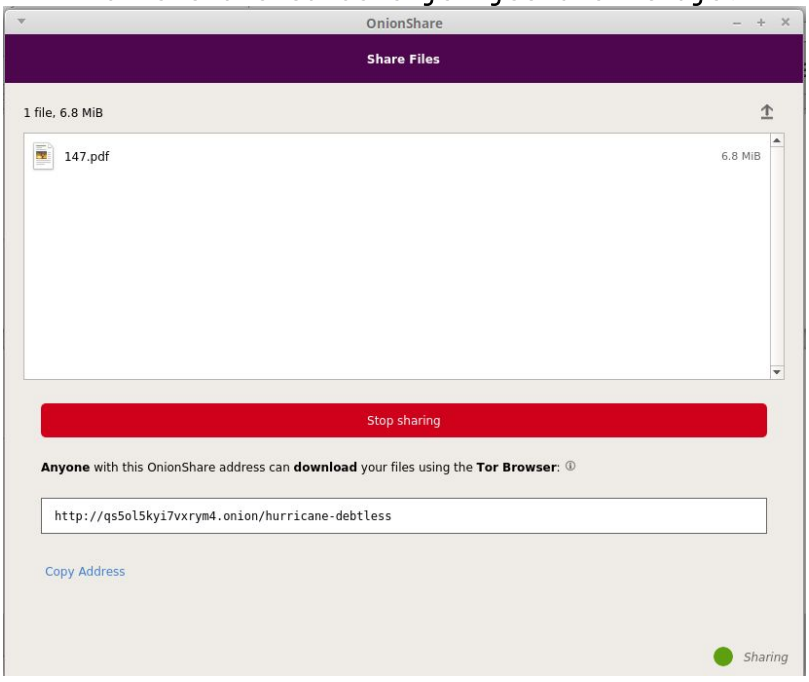
Firefox Send je novije lako rešenje za upotrebu. Možda biste želeli da prvo šifrujete datoteku koristeći opciju ***Encrypt a File*** (Šifruj datoteku) na Mailvelope-u (postoji ograničenje od 50 MB) ili na drugi način pre nego što je otpremite. Da biste ga poslali, idite na **http://send.firefok.com**, izaberite datoteku za učitavanje i podesite opcije. Imajte na umu da veće datoteke i više vremena na serveru zahtevaju da se registrujete.

B) SIGURNIJE DELJENJE: ONIONSHARE

OnionShare vam omogućava da vrlo sigurno i anonimno delite datoteke bilo koje veličine. To stvara privremeni nevidljivi veb server. Generisana je neiskorišćena adresa i deljeno se primaocu otvara u Tor pretraživaču da preuzme datoteke. Iako je veoma bezbedan, nedostatak ovog alata je što hostujete datoteke na sopstvenom računaru, zato ih morate držati u radu dok ih druge strane ne prime. Primalac takođe mora pokrenuti Tor pretraživač da bi primio datoteke.

Da biste ga koristili:

1. Počnite instaliranjem OnionShare za svoju platformu sa **https://onionshare.org**
2. Nakon instaliranja, otvorite OnionShare.
3. Dodajte datoteke i kliknite na ***Start share*** (počni delenje). Ne postoji ograničenje veličine datoteke. Na kraju procesa, OnionShare će vam dati adresu poput ove **http://ks5ol5kii7vkrim4.onion/hurricane-debtles** koju biste trebali da predate primaocu preko sigurnog kanala. Imajte na umu da svako sa adresom može dobiti pristup datotekama pod uslovom da vaš OnionShare sa delenjem još uvek traje.



Snimak ekrana OnionShare

KUDA ICI ODAVDE

Ako ste prerasli ovaj priručnik i želite više saveta ili se suočite sa pretnjama višeg nivoa, druga dobra uputstva besplatno su dostupni na mreži, iako su uglavnom na engleskom jeziku i ponekad zastarela.

Sigurnost u kutiji - Digitalni sigurnosni alati i taktike

https://securitiinabok.org/

Sigurnost u kutiji je projekat kolektivnih taktičkih tehnologija i branitelja fronta. Taktički vodiči u ovom priručniku pokrivaju osnovne principe, uključujući savete o bezbednijoj upotrebi društvenih medija i mobilnih telefona. Vodiči za alate nude detaljna uputstva koja će vam pomoći da instalirate, konfigurišete i upotrebite neke osnovne softvere i usluge digitalne sigurnosti. Alatke zajednice fokusiraju se na određene grupe ljudi - ponekad u određenim regionima - koje su suočene sa značajnim pretnjama digitalne bezbednosti. Oni uključuju prilagođene savete o alatima i taktikama koji su relevantni za potrebe ovih određenih grupa.

Nadzorna samoodbrana: saveti, alati i uputstva za sigurniju internetsku komunikaciju

https://ssd.eff.org/

To je lista vodiča i planova lekcija koju je izdala Fondacija Electronic Frontier.

Bezbednost informacija za novinare, priručnik Centra za istraživačko novinarstvo

https://tcij.org/sites/default/files/u11/InfoSec for Journalists V1.3.pdf
Priručnik osmišljen da poduči novinare i medijske organizacije o tome kako da praktikuju bezbednost informacija u digitalnom dobu, štiteći svoj rad, izvore i komunikacije na različitim nivoima rizika, uključujući najviše nivoe rizika.

Digitalna služba za pomoć novinarima od strane novinara bez granica

https://helpdesk.rsf.org/

Od jula 2019. RSF će redovno nuditi besplatne online video snimke i mrežne konsultacije o digitalnoj sigurnosti. Ove seminare možete videti uživo ili kasnije. Seminari će se fokusirati na to kako zaštititi račune na društvenim medijima od hakovanja, kako zaobići cenzuru koristeći VPN i koje su aplikacije za razmenu poruka na pametnim telefonima najbolje za novinarski rad. U budućnosti će biti ponuđene više individualizovane usluge podrške.

O AUTORU

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

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

Originalna verzija napisana je na engleskom jeziku. Takođe 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