

DIGITALNA BEZBEDNOST



FLV

FAKULTET ZA
PRAVNE I POSLOVNE STUDIJE
DR LAZAR VRKATIĆ

Tanja Kaurin

- Digitalni način života je nova karakteristika ljudskog iskustva.
- Vrlo intenzivan, dinamičan način života.
- Poslovno stimulativan?
- Privatno ...?
- Većina nas ne zna kako da se pravilno nosi sa tim.
- Nismo o tome slušali od naših baka i deka.
- Bez obzira na sve, voleli to ili ne, koristimo digitalne uređaje i prihvativamo digitalnu realnost.
- I želimo da se osećamo bezbedno. Biti bezbedan na mreži nije luksuz. To je neophodnost.





DA LI SMO BEZBEDNI?

Turkey	19,638,821	Kazakhstan	3,214,990	Denmark	639,841
Morocco	18,939,198	Belgium	3,183,584	Greece	617,722
Colombia	17,957,908	Jordan	3,105,988	Afghanistan	558,393
Iraq	17,116,398	Singapore	3,073,009	Albania	506,602
Africa	14,323,766	Bolivia	2,959,209	Norway	475,809
Mexico	13,330,561	Hong Kong	2,937,841	Bulgaria	432,473
Malaysia	11,675,894	Poland	2,669,381	Japan	428,625
United Kingdom	11,522,328	Qatar	2,526,694	Macao	414,228
Algeria	11,505,898	Argentina	2,347,553	Namibia	409,356
Spain	10,894,206	Portugal	2,277,361	Jamaica	
Russia	9,996,405	Cameroon	1,997,658	Hungary	
Sudan	9,464,772	Lebanon	1,829,661	Ecuador	
Nigeria	9,000,131	Guatemala	1,645,068	Iran	
Peru	8,075,317	Tunisia	1,595,346	Slovenia	229,039
Brazil	8,064,916	Switzerland	1,592,03		
Australia	7,320,478	Uruguay	1,509,31		
United Arab Emirates	6,978,927	Panama	1,502,31		
Syria	6,939,528	Costa Rica	1,464,00		
Chile	6,889				
India	6,162				
Germany	6,054				
Netherlands	5,430				
Oman	5,048				
Yemen	4,617				

1. MediBank: October 2022

Health insurer MediBank revealed on 10/25/2022 that [almost 4 million of their customers' data had been exposed to a hacker](#). The Australian health insurer said the personal information that could have been obtained includes name, address, date of birth, and even insurance card numbers.

2. Uber: September 2022

One of the largest companies in the world, Uber, [discovered they were hacked in mid-September](#)

Microsoft

[Microsoft Security](#) announced in March that its servers were hit by hackers as part of a “large-scale social engineering and extortion campaign” targeting several organizations. This was committed extortion

Red Cross

The International Committee of the [Red Cross](#) said in January that sophisticated hackers had penetrated its network and accessed the personal data of some 515,000 people working with the relief organization as well as the affiliated Red Crescent. According to the Red Cross, the

- Možda da proguglamo i pokušamo da nađemo rešenje sami?

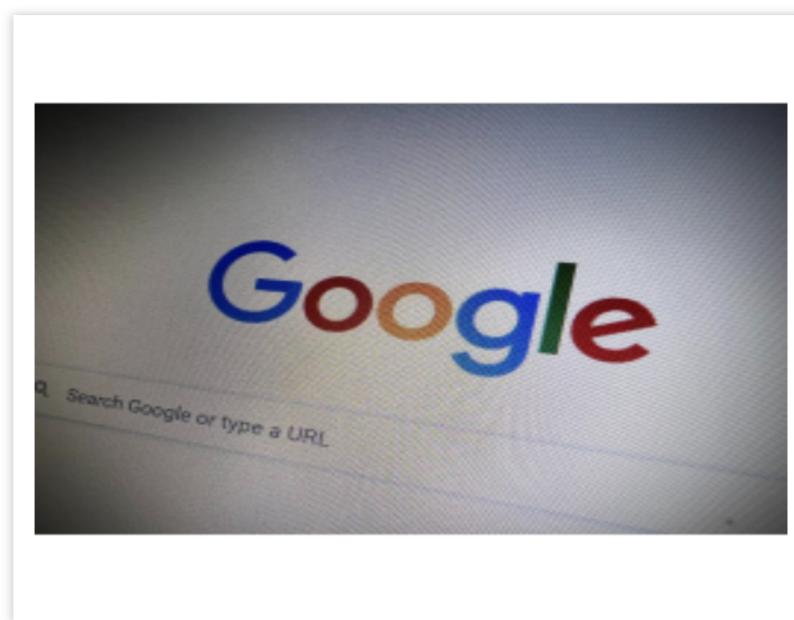
Gugl kažnjen sa 391,5 miliona dolara zbog tajnog praćenja korisnika

Ostale vesti, 15.11.2022, 10:30 AM

Internet gigant Gugl pristao je da plati rekordnih 391,5 miliona dolara za rešavanje spora po tužbi koju su zajedno podneli državni tužioci 40 američkih država zbog toga što je kompanija obmanula svoje korisnike u vezi sa prikupljanjem ličnih podataka o lokaciji.

„Gugl je obmanuo svoje korisnike da misle da su isključili praćenje lokacije u podešavanjima naloga, dok je, u stvari, nastavio da prikuplja informacije o njihovoј lokaciji“, **rekla je u ponedeljak državni tužilac Oregona Elen Rozenblum**. „Gugl je godinama davao prednost profitu u odnosu na privatnost svojih korisnika. Bili su lukavi i varali su“, izjavila je Rozenblum.

Istragu je pokrenuo **izveštaj Asošejted Presa iz 2018.** koji je otkrio da Gugl nastavlja da prati lokacije korisnika na Androidu i iOS-u čak i kada su korisnici isključili „Istoriju lokacija“ u podešavanjima naloga, čime je narušena kontrola privatnosti. Korisnici su bili obmanuti misleći da onemogućavanje „Istorije lokacija“ u podešavanjima onemogućava praćenje lokacije, ali drugo podešavanje naloga nazvano „Aktivnost na vebu i u aplikacijama“, podrazumevano uključeno, omogućilo je kompaniji da prikuplja, skladišti i koristi lične podatke korisnika o lokaciji.



ZAŠTO NISMO BEZBEDNI?

Postoji čitav niz faktora koji utiču na to da li će sistem biti bezbedan ili ne.

1. Pre svega, **tehnološki faktori**, tj. da li je sistem tehnološki kompromitovan ili ranjiv i koji je nivo bezbednosti koji sami uređaji i programi koji su instalirani pružaju.
2. Zatim, **ne-tehnološki faktori**, koji su izuzetno bitni npr. određene navike korisnika.

ZAŠTO NISMO BEZBEDNI?

Važno je znati:

- Bezbednost nije urođena karakteristika digitalnih sistema.
- Da bi sistem bio bezbedan moraju se preuzeti određene aktivnosti.
- Internet je namenjen promovisanju povezanosti a ne bezbednosti.
- Kada je 1969. razmenjena prva poruka niko nije razmišljao o bezbednosti.
- Čak i sada IoT!



DANAS: DIGITALNA BEZBEDNOST

Danas se, za razliku od 1969, ne oduševljavamo kada poruka stigne do primaoca. Danas brinemo da li će stići bezbedno!

Digitalna bezbednost ima za cilj da zaštiti:

- vaše uređaje,
- lične podatke i
- onlajn identitet , od napada na internetu.

Uključuje sve:

- alate,
- tehnike i
- edukaciju.

SVAKI POJEDINAC TREBA DA BUDE SVESTAN

1. Bezbednosti uređaja i mreža koje koristi
2. Neophodnosti zaštite podataka na mobilnim uređajima
3. Zaštite podataka prilikom rada na daljinu
4. Zaštite identiteta
5. Zaštite podataka na društvenim mrežama
6. Zaštita podataka nakon povrede podataka



Претходне 3 године за
сајбер нападе
највише се користила
електронска пошта



OPREZ, PREVARA! U toku je zloupotreba ličnih podataka građana – CERT upozorava na lažnu stranicu Narodne banke Srbije

U toku je prevara građana na lažnoj stranici Narodne banke Srbije gde im se nudi lažna mogućnost da dupliraju iznos na Dina kartici, ukoliko dostave tražene podatke, upozorio je CERT.

**NARODNA BANKA SRBIJE NASELA NA PHISHING -
UKRADENO 175.000 EVRA**

RADI SE O TIPIČNOJ BEC (BUSINESS EMAIL COMPROMISE) PREVARI.

SRBIJA PHISHING MALWARE

**NARODNA BANKA SRBIJE
NASELA NA PHISHING
UKRADENO 175.000 EVRA**

NBS

Send message

24
MAY 2017

<https://phishingquiz.withgoogle.com/>

Can you spot when
you're being phished?

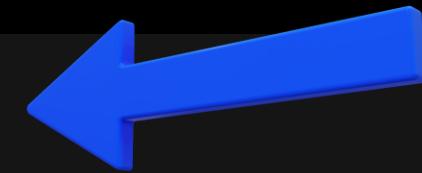
Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ



1. BEZBEDNOST UREĐAJA

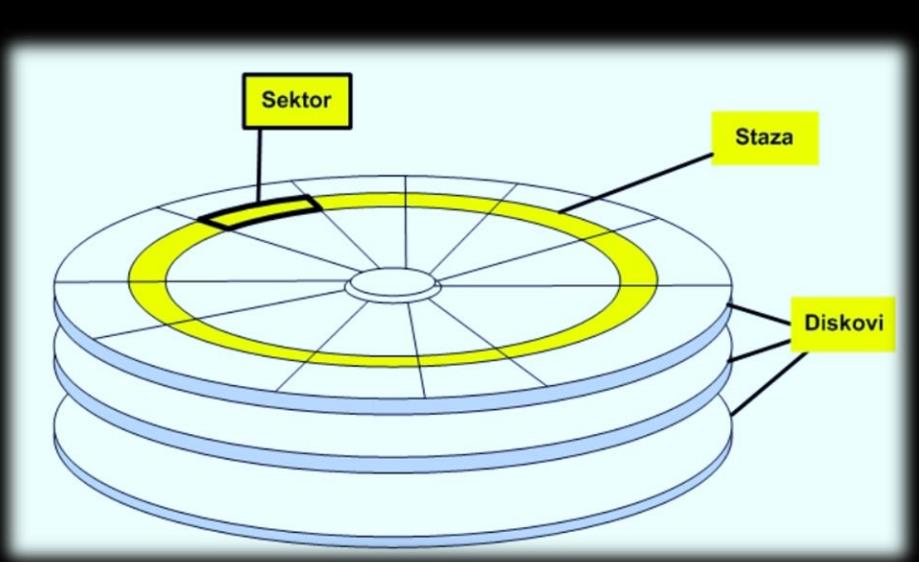
SNIMANJE/BRISANJE PODATAKA



KRIPTOVANJE PODATAKA

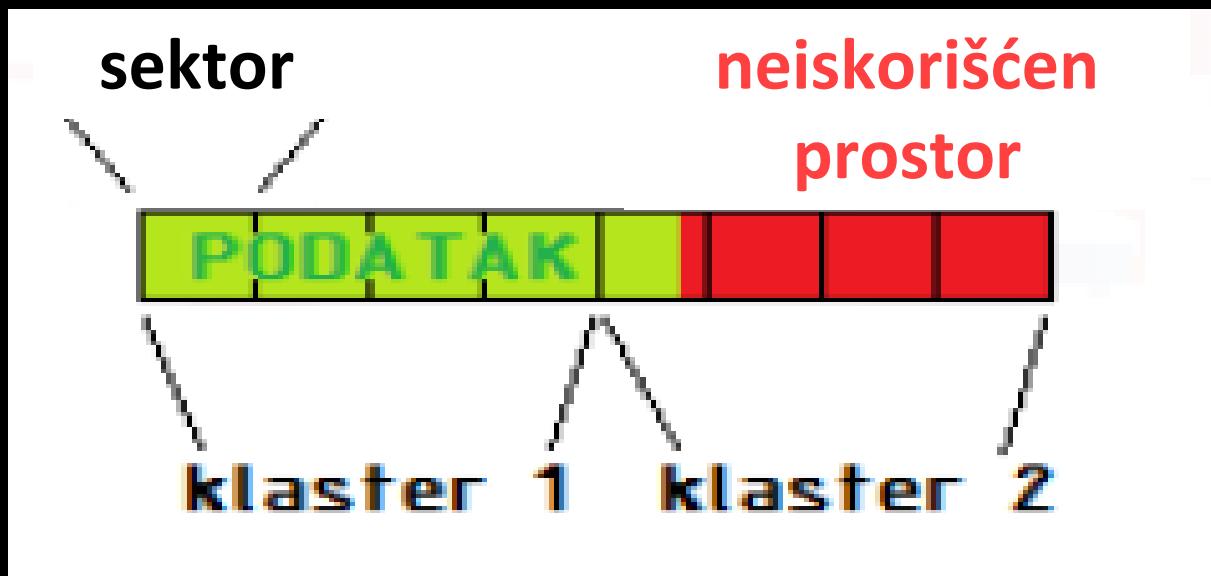
STEGANOGRAFIJA

SNIMANJE/BRISANJE PODATAKA



SNIMANJE PODATAKA

- **Sektor** je najmanja jedinica za pohranjivanje podataka
- **Klaster** sadrži jedan ili više uzastopnih sektora. Broj sektora u klasteruje uvek stepen broja 2 (npr. $2^0=1, \dots, 2^{*3}=8, \dots$).



Kada se podatak pohranjuje, uvek mu se dodeljuje celi broj klastera čak i kada je podatak manji od ukupne veličine dodeljenog prostora.

Podatak veličine 5 sektora, a klasteri su veličine 4, smešta se u 2 klastera.

Prostor u drugom klasteru koji je u tom slučaju ostao prazan se zove neiskorišćen prostor (eng. slack space).

BRISANJE PODATAKA

Fajl A želimo da obrišemo.

Fajl A zauzima 1 klaster (2 sektora)



Kada odlučimo da obrišemo snimljeni fajl:

1. File Allocation Table je „zeroed out“ što znači da je klaster u kome je bio **File A** spremjan za snimanje novog fajla.
2. Prvo slovo ulaznog direktorijuma je promenjeno u specijalni karakter koji govori operativnom sistemu da fajla više nema uprkos tome što on fizički i dalje postoji na tom mestu.

Koji je zaključak?

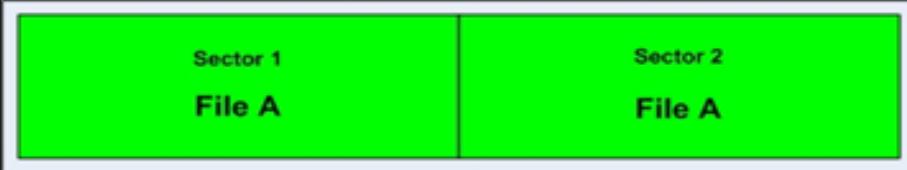
!!! Zaključak je da nakon brisanja fajla on i dalje ostaje na tom mestu!!!

Nije obrisan!!!

Samo je to mesto proglašeno slobodnim za novo upisivanje, i **moguće je povratiti ga.**

BRISANJE PODATAKA

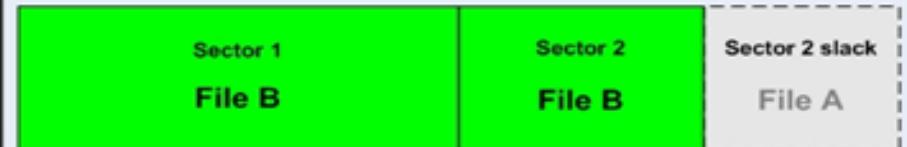
Da bi fajl zaista bio uklonjen pored prethodna dva procesa koji se obavljaju prilikom brisanja mora se dogoditi i:



Sectors 1 and 2 are allocated to File A



File A was deleted – Sectors marked as unallocated



File B written to unallocated space

1. Operativni sistem šalje zahtev za snimanje drugog fajla **File B** baš u istom klasteru.
2. **File B** mora biti bar iste veličine kao **File A** ili će ostati deo prethodnog fajla (*slack space*) koji se može povratiti.



Koji je sada zaključak?

!!!! Pošto je fajl ostao na istom mestu moramo ga „sakriti“ snimanjem novog fajla preko njega!!!

Da li možemo uticati na OS u kom klasteru će snimiti fajl?

NE!

Ne možemo uticati na operativni sistem **da novi fajl snimi baš preko starog.**

Metode sigurnog (!?!) uklanjanja fajlova

Postoji više vrsta metoda za uništavanje zapisa na hard disku. Osnovna ideja je zapisivanje drugih besmislenih (nevažnih) podataka preko njih. Naravno samo jedan prolaz (jedno zapisivanje) nije dovoljno jer navodno neki softveri imaju mogućnost rekonstrukcije podataka i koji su prepisivani čak 21 put.

- **Single Pass**. Ubacivanje jedinica, nula ili pseudoslučjanih podataka;
- **DoD metoda** američkog ministarstva odbrane u kojoj se podaci prepisuju tri puta (jedinicama, nulama pa pseudoslučajnim podacima);
- **PRNG metoda** generisanja niza pseudoslučajnih podataka koji se zapisuju na disk;
- **GUTTMAN metoda** koristi 35 zapisivanja pseudonasumičnih brojeva pri čemu se uzimaju u obzir razni kodirajući algoritmi.

- Besplatan alat za brisanje osetljivih podataka.
- Moguće ga je skinuti sa

<http://freeraser.software.informer.com/download/>

i postoji u dve varijante:

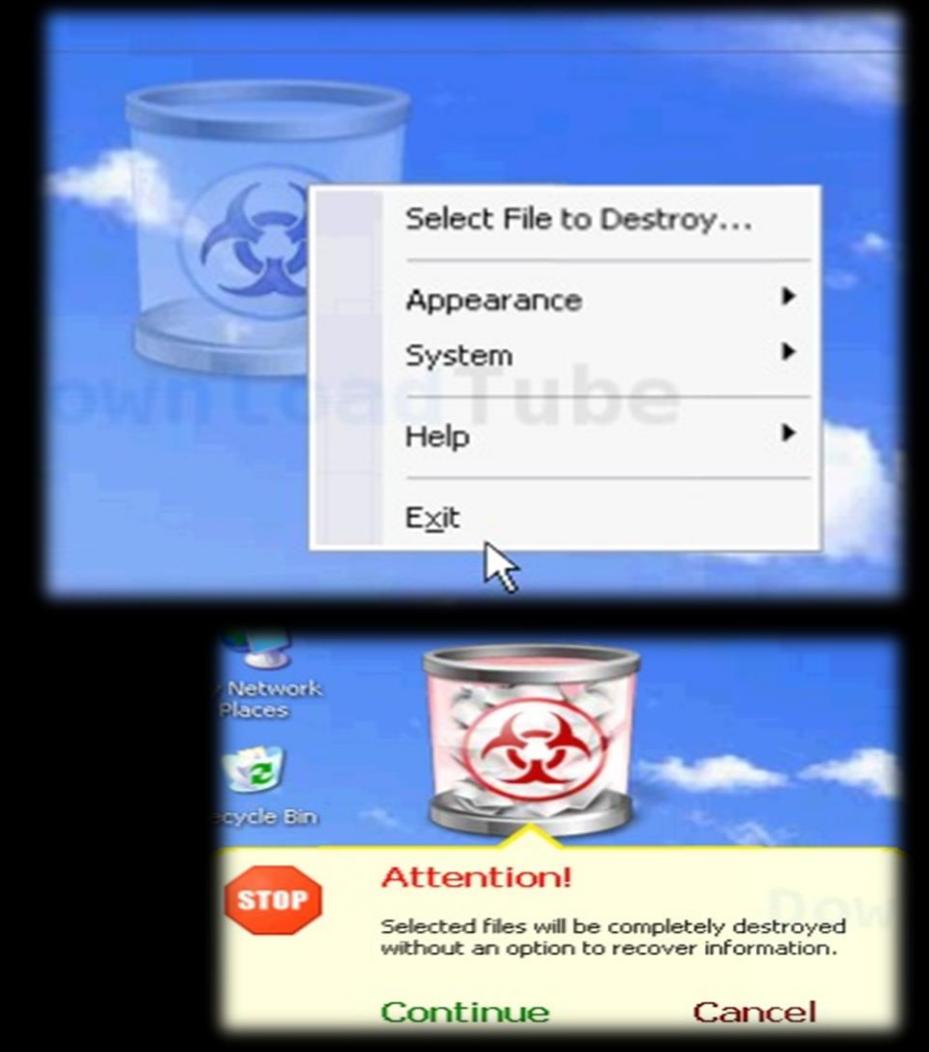
- instalacija i
- prenosiva verzija.

- Ukoliko želimo redovno da čistimo podatke sa naše mašine sigurno ćemo se odlučiti za instalaciju a u koliko želimo da nakon korišćenja zajedničkog računara (na poslu i sl) obrišemo svoje fajlove onda ćemo odabrati prenosivu verziju koja se instalira na USB-u.



- Nakon pokretanja programa pojavljuje kantica ☺
Desnim klikom na nju dobijamo padajući meni sa listom aktivnosti.

- **Appearance** služi da podesimo izgled naše ikone (veličinu, transparentnost...)
- **Opcija System** nam omogućava izbor jednog od tri načina uništavanja fajlova:
 - **Fast** - brzo (jedno prepisivanje nasumičnim podacima)
 - **Forced** - nasilno (tri prepisivanja)
 - **Ultimate** – konačno (35 prepisivanja u skladu sa Guttmanovim algoritmom)



- Još jedan besplatan alat koji radi u Windows okruženju. Brisanje podataka obavlja višestrukim prepisivanjem pažljivo odabralih podataka.
- Pored brisanja podataka, moguće je i obrisati neiskorišćen prostor u klasterima sa mogućnošću izbora metode.
- Briše sve tipove fajlova, foldera i sve njihove delove.
- Nudi mogućnost podešavanja samostalnog pokretanja alata nakon svakog gašenja računara.
- <http://eraser.heidi.ie/download.php>



ERASER®

Brisanje podataka sa računara

01 DBAN (Darik's Boot and Nuke)

of 35



- Odličan alat koji bi svakako trebao biti prvi izbor ako želite da potpuno izbrišete čvrsti disk
- DBAN je besplatan (dostupan je u ISO formatu koji je spreman za upotrebu, tako da sve što treba da uradite je da ga prebacite na fleš disk, i pokrenete sa njega).
- Interfejs je jednostavan za korišćenje.
- radi izvan OS, može da radi sa bilo kojom verzijom bilo kog OS

[How to Erase a Hard Drive Using DBAN \(lifewire.com\)](#)

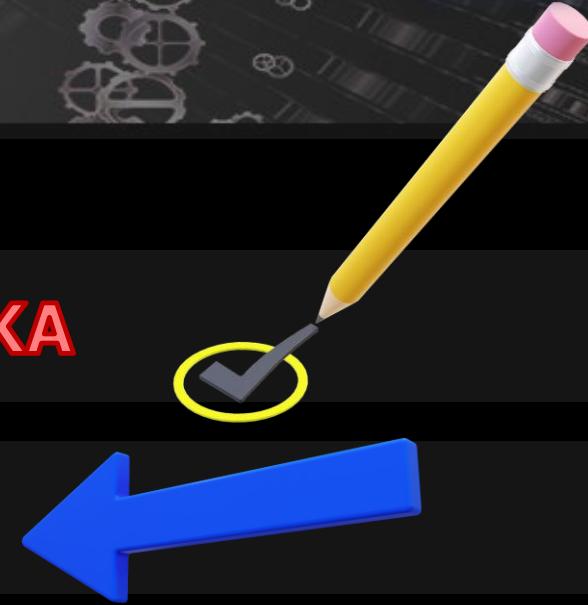
- Pored primene neke od metoda za prepisivanje podataka preko postojećih moguće je koristiti forenzičke alate, pre svega komercijalne koji se vode kao pouzdaniji (npr. Evidence Eliminator) ali i neke od besplatnih.
- Listu besplatnih moguće je videti na
<http://www.softpedia.com/get/Security/Secure-cleaning/>

1. BEZBEDNOST UREĐAJA

SNIMANJE/BRISANJE PODATAKA

KRIPTOVANJE PODATAKA

STEGANOGRAFIJA



KRIPTOGRAFIJA

Suština kriptografije zasniva se na konceptu tajnog komuniciranja (tajne korespondencije) koja podrazumeva da se:

čitljiv (otvoren) tekst, koji treba štititi, transformiše u **nečitljiv** (nerazumljiv) tekst primenom kriptografske transformacije.

Otvoren tekst:	F	A	K	U	L	T	E	T
Šifrovan tekst:	č	G	N	C	O	F	I	F



KRIPTOVANJE PODATAKA NA RAČUNARU

Windows Bitlocker

- Pouzdan alat za šifrovanje koji dolazi sa svakim Windows OS nakon verzije 10,
- Nudi opciju šifrovanja čitavog diska,
- Jednom kada se aktivira šifrovanje svaka nova datoteka koju dodate se šifruje automatski.

Koliko je pouzdan?

- Hakeri su pronašli način da nanjuše ključeve za šifrovanje ako vaša opšta konfiguracija nije sigurna koliko bi trebalo da bude. BitLocker je od pomoći i moćan, ali nije magija; potrebno mu je bezbedno okruženje da bi i sam ostao siguran.

<https://besplatniprogrami.org/kako-uklјuciti-bitlocker-windows-11/>



14 besplatnih softvera za enkripciju

1. BitLocker
2. VeraCrypt
3. NordVPN
4. BCArchive
5. PixelCryptor
6. LastPass
7. FileVault 2
8. DiskCryptor
9. 7-Zip
10. AxCrypt
11. Tor Browser
12. HTTPS Everywhere
13. Silver Key
14. Sophos Free Encryption

KRIPTOVANJE PODATAKA NA RAČUNARU

BCArchive

- Besplatna enkripcija foldera za Windows OS.
- Visok stepen različitih mogućnosti.
- Šifrovanje čitavih foldera ili pojedinačnih fajlova, u zavisnosti od potreba, sa širokim spektrom najboljih poznatih algoritama za šifrovanje.



<https://privacysavvy.com/security/safe-browsing/free-encryption-software/#h-14-best-free-encryption-software-available-today-the-detailed-list>

KRIPTOVANJE PODATAKA NA RAČUNARU

PixelCryptor

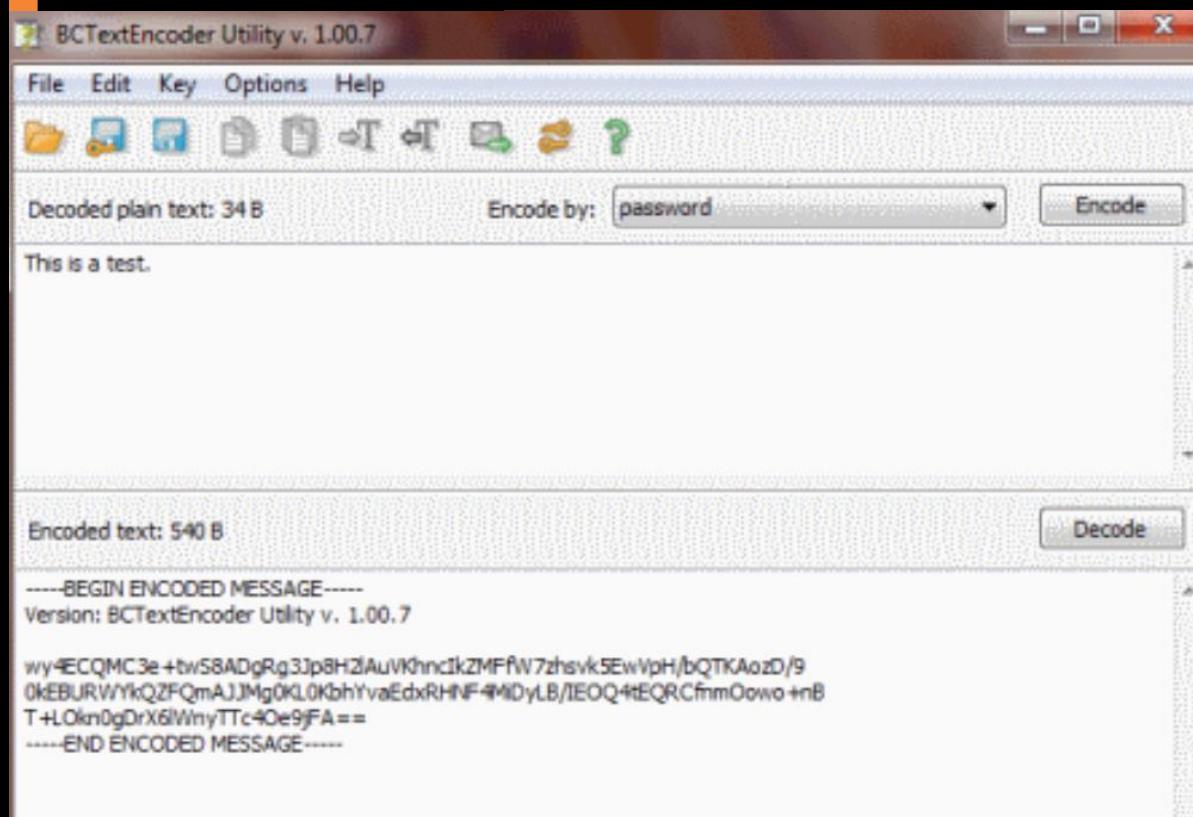
- Jedinstven!
- Kao lozinku birate sliku
(gif, jpeg, tiff, png i BMP)
- Ne pamtite lozinku, ne vodite računa o njenoj sigurnosti i ukoliko dokument šaljete drugoj strani ne morate da razmišljate kako ćete poslati lozinku.
- Softver je userfriendly i lak za korišćenje.
- Koraci: 1. „Encode files“ 2. Izaberite folder koji želite da šifrujete, kliknite na „next“ i dodajte sliku koju koristite kao lozinku i ključ za šifrovanje.
- VAŽNO! Birate svoju najlepšu sliku ☺



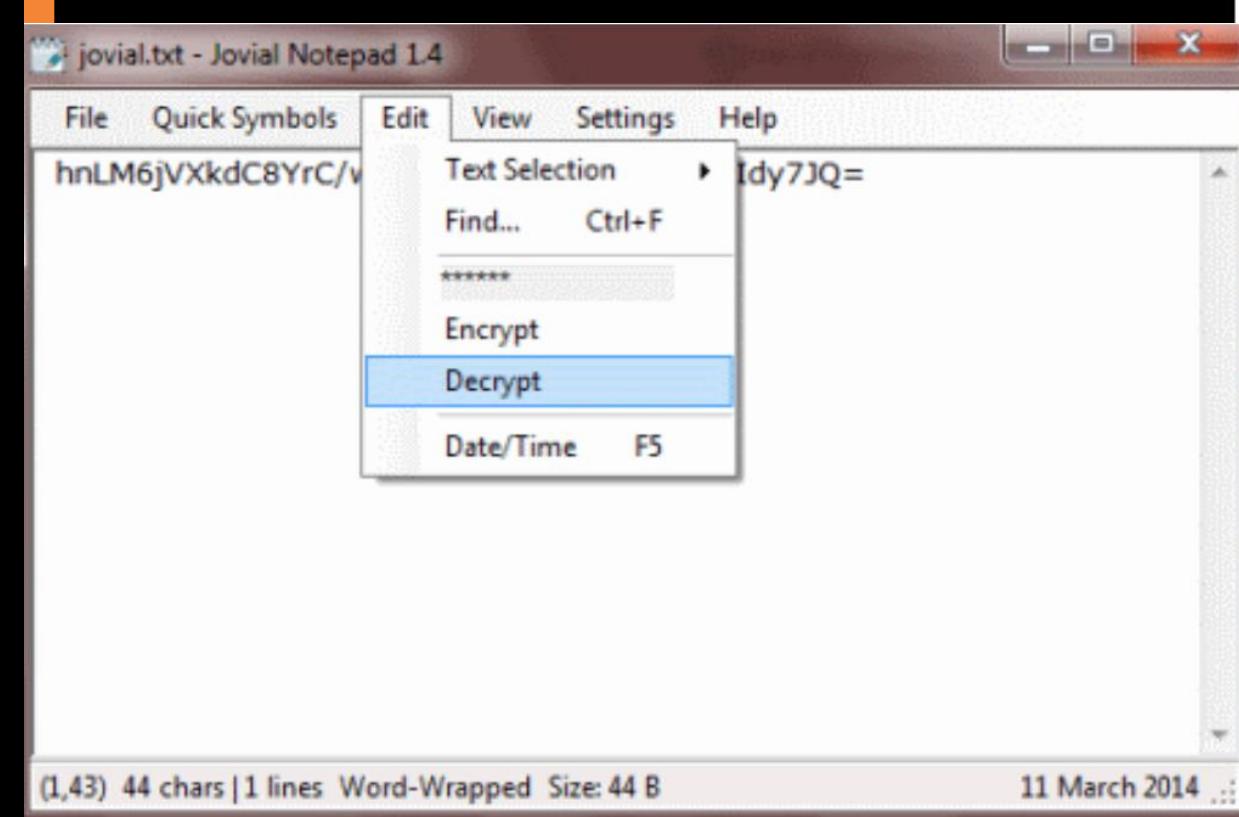
KRIPTOVANJE TEKSTA

<https://listoffreeware.com/list-best-free-text-encryption-software/>

BCTextEncoder



JovialNotepad



KRIPTOVANJE TEKSTA



Cryptography for everybody



The CrypTool Portal (CTP) is the starting page of the CrypTool project. Its aim is to raise awareness and interest in crypto techniques for everyone.

The CT project develops the world's most-widespread free e-learning programs in the area of cryptography and cryptanalysis. All learning programs in the CT project are open source and available for free.

E-Learning Platforms

CrypTool-Online (CTO)

With CrypTool-Online, you can play around with different cryptographic algorithms directly in your browser.



Website

CrypTool 1 (CT1)

With the first version of CrypTool (started in 1998), you can experiment with different cryptographic algorithms on Windows.



Download

CrypTool 2 (CT2)

CrypTool 2 supports visual programming, cascades of cryptographic procedures, and contains lots of cryptanalysis methods.



Download

JCrypTool (JCT)

JCrypTool is implemented in Java and runs under Linux, macOS, and Windows. One focus are post-quantum (signature) algorithms.



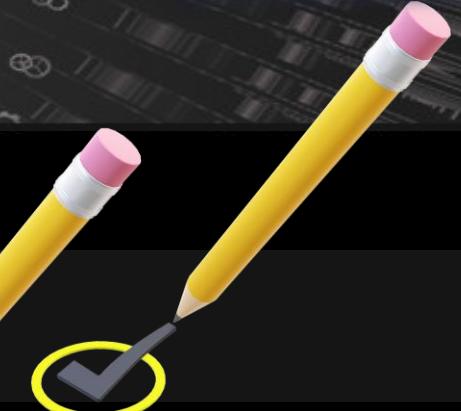
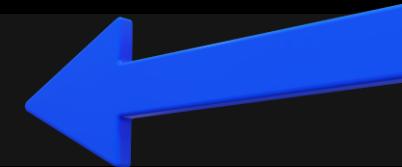
Download

1. BEZBEDNOST UREĐAJA

SNIMANJE/BRISANJE PODATAKA

KRIPTOVANJE PODATAKA

STEGANOGRAFIJA



STEGANOGRAFIJA

Steganografija je naučna disciplina koja se bavi prikrivenom razmenom informacija.

Steganografija je podatak skriven unutar podataka.



STEGANOGRAFIJA

Osnovni princip steganografije počiva na prikrivanju samog postojanja informacije koja se prenosi unutar nekog naizgled bezazlenog medija ili skupa podataka.

Moderna steganografija, koja koristi prednosti digitalne tehnologije, najčešće podrazumeva skrivanje tajne poruke unutar neke multimedijalne datoteke:

- slike,
- audio ili
- video datoteke.

STEGANOGRAFIJA

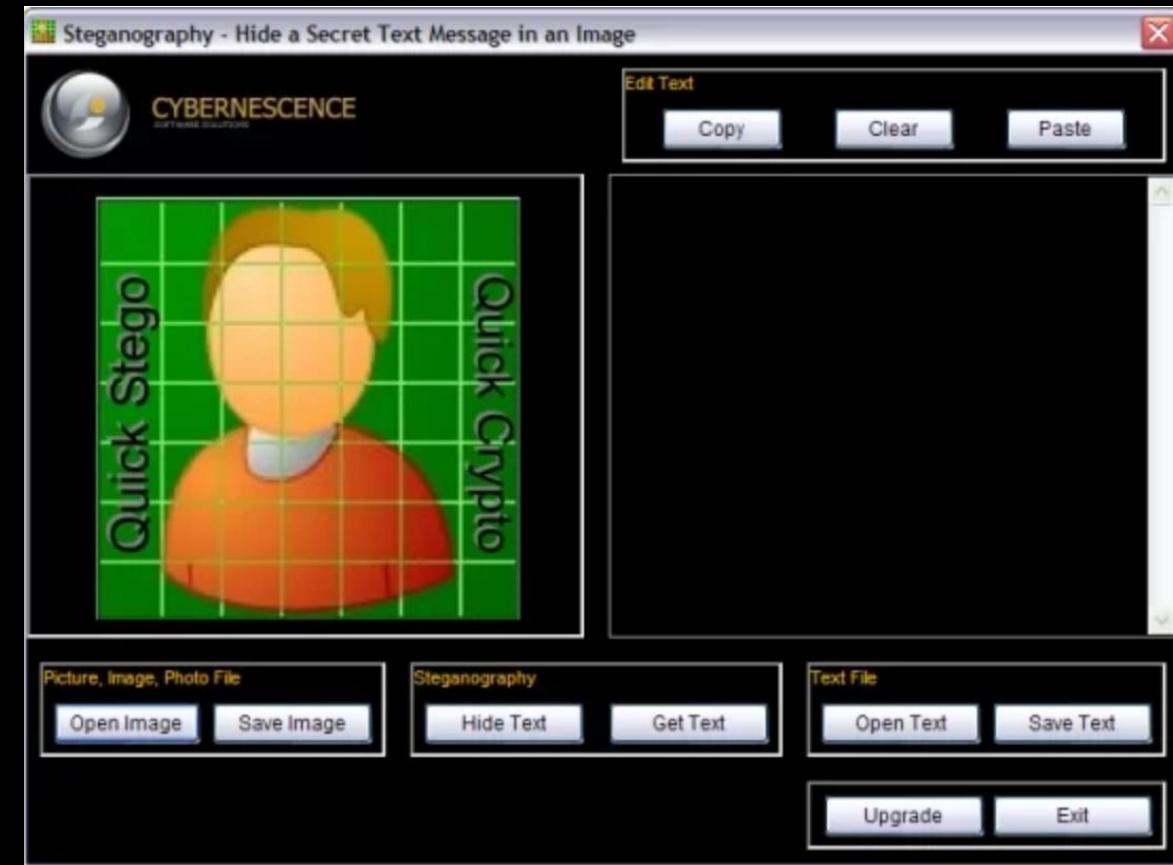
- Napad 11. septembra 2001
- Teroristi Al Kaide organizovali su i izvršili napad na Svetski trgovinski centar i Pentagon komunicirajući putem nekoliko pornografskih Web sajtova.
- Plan terorističkog napada, bio je „utisnut“ u slike koje su prenošene putem Interneta.



STEGANOGRAFIJA

QuickStego

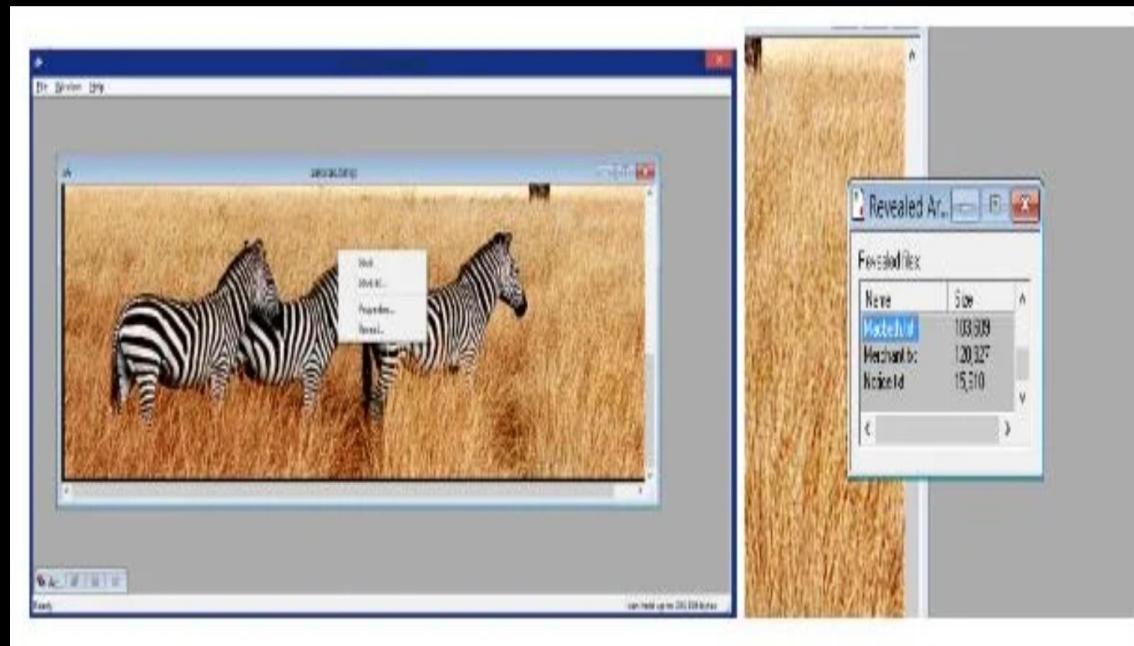
- Skrivanje teksta u sliku.
- Jednom kada je tekst sakriven u slici, sačuvana slika je i dalje „slika“, učitaće se kao i svaka druga slika i izgledati regularno.
- Slika se može sačuvati, poslati e-poštom, postaviti na veb...
- Da bi tajna poruka bila otpakovana primalac mora znati lozinku i imati ovaj program



STEGANOGRAFIJA

S-Tools

- Skrivanje teksta u sliku.
- Izuzetno jednostavan za primenu

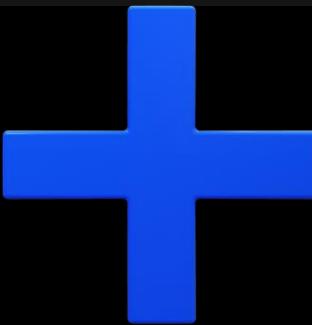


Xiao Steganography

- Skrivanje u tri jednostavna koraka
- Audio fajl ili slika



KRIPTOVANJE TEKSTA



STEGANOGRAFIJA



1. BEZBEDNOST UREĐAJA i MREŽNOG OKRUŽENJA

LOZINKE

KAKO PREPOZNATI WEB SAJT NAMENJEN PREVARI

BEZBEDNO PRETRAŽIVANJE

1. BEZBEDNOST UREĐAJA i MREŽNOG OKRUŽENJA

LOZINKE

- **Sve znate!**
- Podsetnik: Koristite dvofaktorsku autentifikaciju!
- Bez istih lozinki na različitim sajtovima.
- Ne pamtite lozinke u pregledačima.
- Ne zaboravite da je dužina lozinke značajna!
- Provera Password Strength Testing Tool | Bitwarden
<http://www.passwordmeter.com/>
- Savet za lako pamćenje dugačkih lozinki:



Da li je danas 1 amfiteatar pun sudskih tumača? dljd1apST?

LOZINKE

- U januaru 2019. godine, na Dark Web-u, na prodaju se pojavila kolekcija ukradenih email adresa i lozinki.
- Kolekcija je sadržala neverovatnih 773 miliona email adresa i lozinki. Ovaj događaj je nazvan Collection.

<https://haveibeenpwned.com/>

';--have i been pwned?

Check if your email or phone is in a data breach

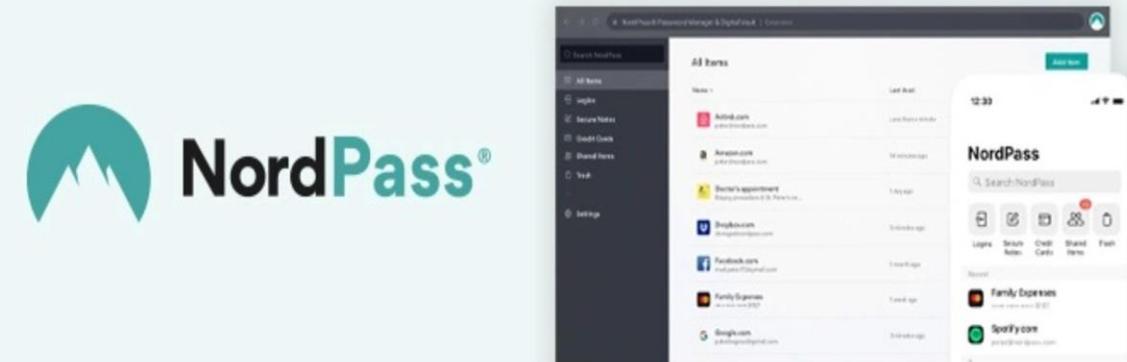
LOZINKE

- Ne koristite akreditive društvenih medija za registraciju ili prijavljivanje na sajtove trećih strana.
- Čini se kao zgodna opcija: logujete se koristeći svoj Facebook ili LinkedIn nalog, i sve dok ste prijavljeni na tu društvenu mrežu, prijavljivanje na sajt treće strane je brz i lak.
- Međutim, **to može ugroziti vašu privatnost**. „lako je to zgodna opcija, prijavljivanje na drugi nalog sa svojim Facebook korisničkim imenom i lozinkom može značiti davanje drugoj veb lokaciji informacije koje je Facebook prikupio o vama.
- Ukoliko neko dođe u posed podataka za prijavu na društvene mreže, takođe dobija pristup ostalim povezanim nalozima
- **Ako koristite istu lozinku za sve, vaš život će se verovatno promeniti 😊**

MENADŽER LOZINKI

- Menadžeri lozinki pomažu da skladištite složene lozinke na jednom mestu bez potrebe da ih pamtite.
- Možete da skladištite i druge osetljive informacije, kao što su podaci o kreditnoj kartici ili beleške.
- nude automatsko popunjavanje (autofill)
- Sprečavaju napade **keylogging** (snimanje kucanja na tastaturi) i **screen logging**

1. NordPass – best password management tool in 2022



Cloud storage:

3 GB (with NordLocker app)

Free version:

Yes

Browser plugins:

Chrome, Firefox, Safari, Opera, Brave, Vivaldi, and Edge

KAKO PREPOZNATI WEB SAJT NAMENJEN PREVARI (Scam Website)

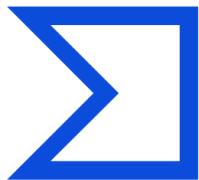
Najčešća upozorenja su:

- Nije **https** već http što znači da nedostaje SSL sertifikat koji ima zadatak da zaštiti vaše podatke šifrovanjem.
- Imaju čudne URL-ove sa sumnjivim kombinacijama slova i brojeva i čudnim domenima
- Često iskači prozori koji traže lične podatke ili neku aktivnost koju niste inicirali.
- Loše organizovan sajt i grafika je niskog kvaliteta.
- Sprečavaju povratak na prethodnu stranicu i u suštini vas zaključavaju na njihovu veb lokaciju.
- Imaju sporije vreme učitavanja ili čak mogu da dovedu do pada pregledača.

**!!! ALI čak i ako veb lokacija ne prikazuje
ove znakove upozorenja, i dalje može da hostuje
zlonamerni sadržaj!!!**

- Zato je mudar izbor da koristite bezbednije načine pretrage na internetu ili digitalne bezbednosne alate, koji automatski filtriraju internet saobraćaj.

PROVERA WEB SAJTA I FAJLOVA



VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other
breaches, automatically share them with the security community.

FILE

URL

SEARCH



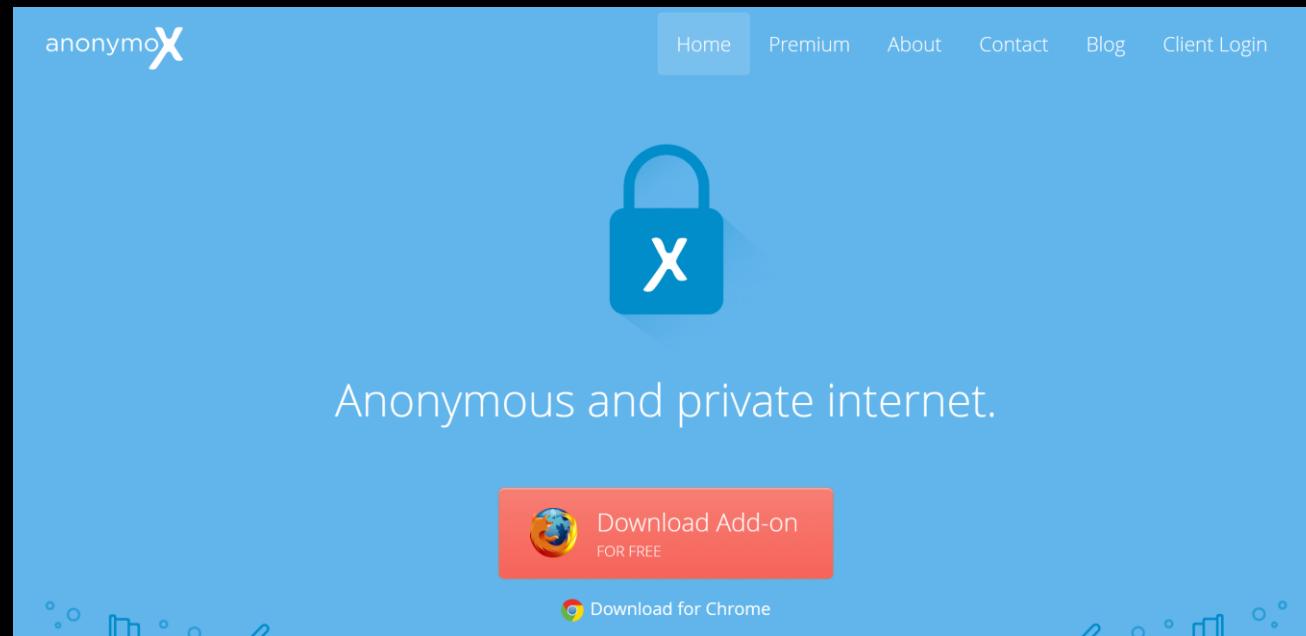
Choose file

<https://www.virustotal.com>

BEZBEDNO PRETRAŽIVANJE

- Anonymox-

Besplatni dodatak za
Firefox ili Chrome.



The screenshot shows the homepage of the Anonymox website. At the top left is the brand logo 'anonymox'. To its right is a navigation bar with links: Home (which is highlighted in blue), Premium, About, Contact, Blog, and Client Login. Below the navigation bar is a large blue banner featuring a white padlock icon with a red 'X' over it, symbolizing security and privacy. The text 'Anonymous and private internet.' is displayed in white. At the bottom of the banner are two download buttons: one for 'Download Add-on FOR FREE' (with a Firefox icon) and another for 'Download for Chrome' (with a Chrome icon).

Zaštitite svoju privatnost

Izaberite željenu IP adresu i zemlju.

Surfujte anonimno

Mreža proksija omogućava da ste zaštićeni i neprepoznatljivi

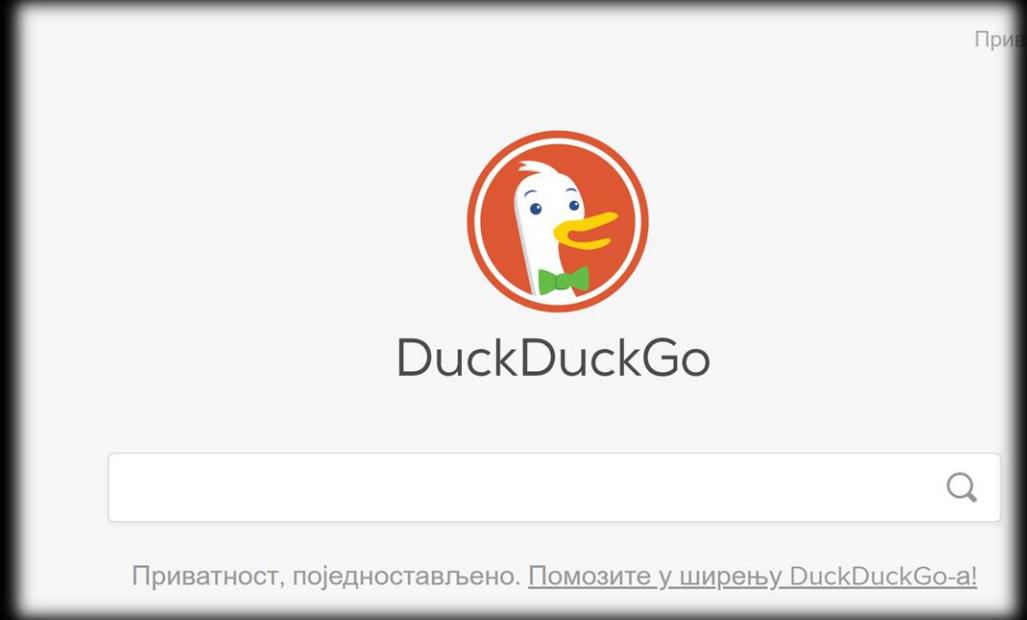
Posetite blokirane sajtove

Promenom IP adrese zaobiđite GEO IP blokove.

Promenite svoj IP

Pristupite veb lokacijama sa jedne od naših IP adresa. Umesto direktnog pristupa veb lokaciji koristite IP adresu jedne od naših proksi mreža.

BEZBEDNO PRETRAŽIVANJE



- Ne prikuplja i ne deli lične podatke
- Ne čuva se istorija pretraživanja
- Nema reklama, ne snima razgovore, ne prati, ne radi s kolačićima (cookies)
- U kombinaciji s TOR-om potpuno je anoniman.

- Tor izoluje svaku veb lokaciju koju istražujete, tako da oglasi i praćenje kretanja nisu mogući. Takođe briše istoriju pregledanja, uklanja kolačiće i obezbeđuje višeslojno šifrovanje.

Download Tor Browser

Protect yourself against tracking, surveillance, and censorship.



Download for Windows

[Signature](#) ⓘ



Download for macOS

[Signature](#) ⓘ



Download for Linux

[Signature](#) ⓘ



Download for Android

[Download in another language or platform](#)

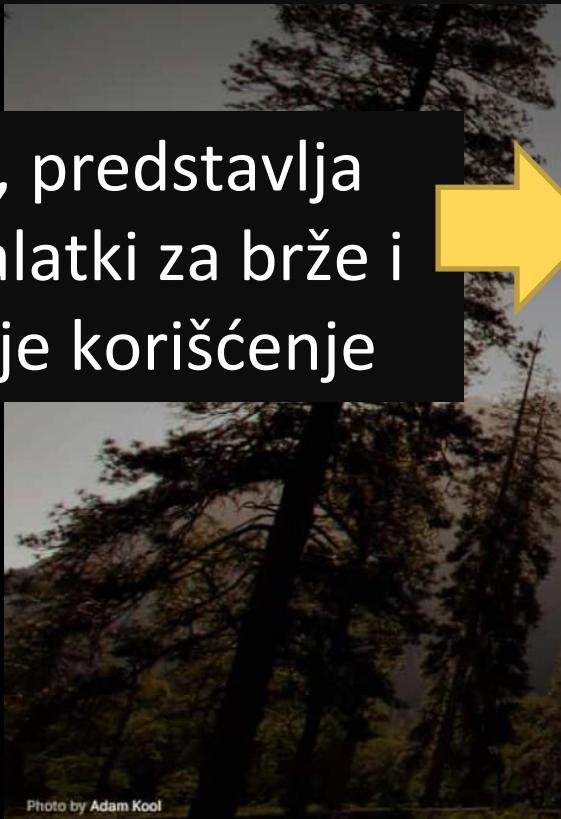
[Download the latest alpha build](#)

[Download Tor Source Code](#)

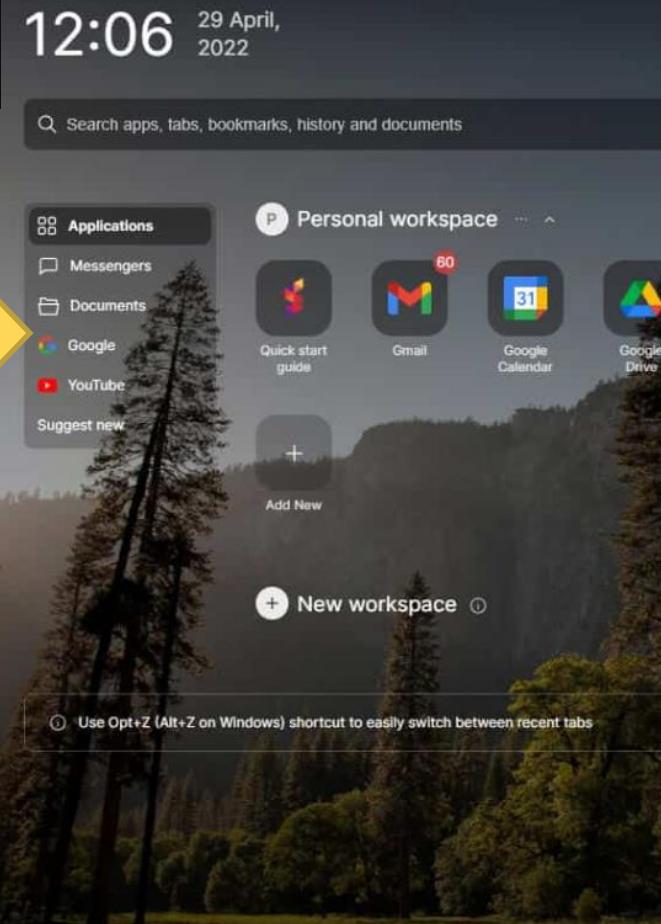
BEZBEDNO PRETRAŽIVANJE - SIDEKICK -

558 MB Saved
memory[Feedback](#) [Help](#) [Pro Plan for free](#)

- Liči na Google Chrome
lak za snalaženje



- Sidebar, predstavlja
paletu alatki za brže i
efikasnije korišćenje



- Premijum (plaćena) verzija
nudi VPN, ugrađenu
opciju za video pozive,
mogućnost deljenja lozinki

...

UKOLIKO DOĐE DO CURENJA PODATAKA

- Hitna promena lozinki!
- Ako je u kompaniji u kojoj radite, promena i privatnih lozinki
- Ako je Vaša banka, insistirajte na novoj kartici
- Ne ignorišite prijave prijatelja o misterioznim mejlovima koji dolaze sa Vaših naloga

Jedan od najčešćih načina na koji ljudi saznaju da su hakovani je kada njihovi prijatelji ili članovi porodice prijave da su primili čudnu e-poštu ili poruku na društvenim mrežama.

- Svaki put kada dobijete novi zahtev za „prijatelja“ od nekoga ko je već na vašoj listi prijatelja na FB, najjednostavnije je da svom pravom prijatelju pošaljete poruku i pitate da li zna za svog dvojnika
- Ukoliko je jedan od naloga hakovan, vaši podaci više nisu bezbedni na drugim nalozima koji koriste iste podatke za prijavu. Pametni haker koji ima kontrolu nad nalogom e-pošte brzo će potražiti vaše druge naloge, društvene mreže, možda, ili bankovne račune.

HVALA NA PAŽNJI



FLV

FAKULTET ZA
PRAVNE I POSLOVNE STUDIJE
DR LAZAR VRKATIĆ

tanja.kaurin@flv.edu.rs