SMERNICE ZA DIGITALNU BEZBEDNOST

Ovde su smernice za digitalnu bezbednost koje aktivisti mogu da koriste u represivnom okruženju poput Srbije. Fokus je na zaštiti komunikacija, anonimnosti i sigurnosti podataka kako bi se smanjio rizik od praćenja i represije od strane državnih agencija.

SADRŽAJ

UVOD

Reč 2024. godine u Srbiji je solidarnost. Nažalost, nju ne razumeju sve naše komšije. U trenutku kada se zajedno trudimo da probudimo institucije na ulicama, određeni pojedinci, organizovane grupe i institucije rade protiv nas. Njihov najveći adut, koji u ranijim aktivističkim (omladinskim) pokretima, blokadama i protestima (1968, 1996, 2000) nisu imali jesu upravo nove tehnologije.

Infrastruktura koja im je na raspolaganju zahvaljujući agencijama poput BIA je ogromna i vrlo lako je moguće pratiti skoro sve što radimo svaki momenat. Bitno je da smo i mi pametni, ali i solidarni unutar naše zajednice. Zato su nastale ove smernice - kako bi svi bili podjednako zaštićeni i bezbedni u naporima za ostvarivanje zajedničkog cilja - ispunjenja zahteva.

I OPŠTA DIGITALNA BEZBEDNOST

1. Sigurna komunikacija

- **Koristite šifrovane aplikacije za poruke:** Koristite aplikacije poput **Signal** ili **Wire**, koje nude end-to-end enkripciju. Signal ima opciju automatskog brisanja poruka, što dodatno povećava sigurnost.
- **Izbegavajte SMS i pozive:** Tradicionalne metode komunikacije (SMS, pozivi) lako su dostupne za prisluškivanje. Umesto toga, koristite VoIP servise poput Signala ili Jitsi.
- **Kreirajte anonimne naloge:** Kreirajte naloge koristeći pseudonime i e-mail adrese koje ne mogu biti povezane s vašim pravim identitetom.

---

2. Bezbedno korišćenje interneta

- **Koristite VPN:** VPN-ovi maskiraju vašu IP adresu i lokaciju. Preporuke uključuju **Mullvad**, **ProtonVPN**, ili **NordVPN**.
- **Koristite Tor mrežu:** Pregledanje interneta putem Tor-a omogućava anonimnost. Preuzmite Tor Browser i koristite ga za osetljive aktivnosti.
- **Blokirajte praćenje:** Instalirajte dodatke poput **uBlock Origin**, **Privacy Badger**, i **HTTPS Everywhere** na vaš pregledač.

---

3. Anonimnost na mreži

- **Izbegavajte javne Wi-Fi mreže:** Ako ih koristite, uvek se povežite putem VPN-a.
- **Koristite uređaje kupljene u gotovini:** Ako je moguće, nabavite odvojeni telefon i laptop koji ne mogu biti povezani sa vašim identitetom.
- **Koristite anonimne SIM kartice:** Nabavite SIM kartice bez registracije i koristite ih za jednokratne svrhe.

---

4. Zaštita podataka

- **Šifrujte uređaje:** Aktivirajte šifrovanje diska na laptopu (npr. BitLocker za Windows, FileVault za macOS) i telefonu.
- **Koristite sigurne lozinke:** Koristite menadžere lozinki poput **Bitwarden** ili **KeePass** i generišite jake, jedinstvene lozinke.
- **Redovno pravite bekape:** Sačuvajte podatke na šifrovanim eksternim uređajima i redovno ih ažurirajte.

---

5. Fizička sigurnost uređaja

- **Koristite fizičke brave:** Uvek čuvajte uređaje pod ključem kada ih ne koristite.
- **Onemogućite biometriju:** Umesto otiska prsta ili prepoznavanja lica, koristite PIN ili lozinku. Biometrijski podaci mogu biti prisilno uzeti.
- **Aktivirajte kill switch funkcije:** Ako vaš telefon ili laptop ima opciju brzog brisanja podataka, upoznajte se s njom i koristite je u hitnim situacijama.

---

6. Aktivnosti na društvenim mrežama

- **Izbegavajte lične informacije:** Nikada ne delite podatke koji vas mogu identifikovati. Koristite pseudonime i izbegavajte fotografije lica.
- **Razvijte mrežu poverenja:** Komunicirajte samo s osobama koje su prošle proveru i s kojima imate osnovano poverenje.
- **Redovno brišite naloge:** Kreirajte naloge za jednokratnu upotrebu za specifične kampanje, a zatim ih obrišite.

---

7. Proaktivna odbrana od napada

- **Pazite na phishing:** Budite oprezni sa sumnjivim e-mailovima, linkovima ili aplikacijama. Proverite svaki URL pre nego što ga otvorite.
- **Koristite antivirus i firewall:** Instalirajte i ažurirajte softvere za zaštitu od virusa i malvera, poput **Malwarebytes**.
- **Pratite ažuriranja:** Redovno ažurirajte operativne sisteme i aplikacije kako biste se zaštitili od sigurnosnih propusta.

---

8. Edukacija i vežba

- **Trenirajte svoj tim:** Organizujte obuke o digitalnoj bezbednosti i delite smernice sa svim članovima.
- **Testirajte sigurnost:** Redovno testirajte svoje sisteme na ranjivosti (npr. kroz simulacije napada).

---

9. Reakcija u slučaju opasnosti

- **Plan za hitne situacije:** Razvijte protokole za brisanje podataka i zaštitu identiteta u slučaju opasnosti.
- **Koristite signalne reči:** Dogovorite se o signalnim rečima koje označavaju opasnost ili potrebu za povlačenjem.
- **Improvizujte mrežu za evakuaciju:** Ako dođe do kompromitovanja, imajte plan za sigurno napuštanje lokacije.

II PLANIRANJE AKCIJA

1. Koristite sigurne aplikacije za komunikaciju

Za planiranje akcija na daljinu, potrebni su alati koji omogućavaju sigurno razmenu poruka, glasovne pozive i zajednički rad. Predlažem sledeće aplikacije:

- **Signal:**
  - End-to-end šifrovanje za poruke, pozive i video pozive.
  - Opcija samouništavajućih poruka.
  - Otvoreni kod i redovno proveravan od strane zajednice.
- **Wire:**
  - Pogodan za timsku komunikaciju.
  - End-to-end šifrovan tekst, glas i deljenje fajlova.
- **Element (Matrix):**
  - Decentralizovana i šifrovana platforma za čuvanje komunikacija.
  - Pogodna za grupe i kolaboraciju.
- **Jitsi Meet:**
  - Besplatna, otvorenog koda, šifrovana aplikacija za video konferencije.
  - Može se koristiti bez registracije.

---

2. Planirajte akcije putem anonimnih platformi

- **Padovi:**
  - Koristite alate kao što je **CryptPad** ili **Etherpad** za kolaboraciju na dokumentima bez otkrivanja identiteta.
  - Svi unosi su šifrovani i podaci se ne čuvaju na serverima duže nego što je potrebno.
- **Proton Drive:**
  - Bezbedno deljenje dokumenata sa šifrovanjem.
  - Mogućnost deljenja linkova sa lozinkama.

---

3. Organizujte sigurne online sastanke

- Koristite **Jitsi Meet** ili **BigBlueButton** za šifrovane video konferencije.
- Sastanke organizujte uz jedinstvene lozinke i menjajte linkove nakon svakog sastanka.
- Onemogućite snimanje sastanaka.

---

4. Deljenje dokumenata i fajlova

- **OnionShare:**
  - Omogućava sigurno deljenje fajlova putem Tor mreže.
  - Vaši fajlovi nikada ne prolaze kroz centralizovani server.
- **ProtonMail/Proton Drive:**
  - Šifrovana e-mail i skladišna platforma za deljenje fajlova.

---

5. Izbegavajte praćenje lokacije

- **Izbegavajte deljenje fizičke lokacije:**
  - Nemojte koristiti aplikacije koje prate lokaciju ili omogućavaju "check-in".
  - Isključite GPS na uređajima tokom osetljivih aktivnosti.
- **Koristite aplikacije koje ne otkrivaju identitet:**
  - Telegram može biti opcija, ali samo uz podešavanje tajnih četova (ne koristiti regularne grupe).

---

6. Planirajte na decentralizovan način

- **Koristite PGP šifrovanje za e-mail:**
  - Ako morate koristiti e-mail za komunikaciju, koristite PGP za šifrovanje poruka.
- **Kreirajte mrežu poverenja:**
  - Delite informacije samo sa ljudima koje poznajete i u koje imate poverenja.
  - Koristite pseudonime i šifrovane kanale.

---

7. Fizički sastanci (kada su neizbežni)

- Planirajte sastanke na neutralnim mestima i ne nosite elektronske uređaje koji vas mogu identifikovati.
- Pre sastanaka dogovorite "code words" za proveru identiteta.

III KREIRANJE I DISTRIBUCIJA FAJLOVA

1. Fajlovi na računaru

Na lokalnom računaru, metapodaci fajla mogu sadržavati informacije o kreiranju fajla. Evo šta je moguće:

- **Metapodaci fajla:**
  - Operativni sistemi (Windows, macOS, Linux) beleže vreme kreiranja fajla i često čuvaju informacije o korisničkom nalogu koji je fajl kreirao.

    - Na Windows-u, kliknite desnim klikom na fajl > *Properties* > *Details*. Na macOS-u, koristite *Get Info*.
    - Metapodaci mogu sadržavati i informacije o autoru, pogotovo ako je fajl napravljen u aplikacijama poput Worda ili Excel-a.
- **Ograničenja:**
    - Metapodaci se mogu izmeniti ili obrisati pomoću specijalizovanih alata.
    - Ako se fajl kopira, originalni metapodaci mogu biti izgubljeni.

---

2. Google Drive, Google Docs i Google Sheets

Google Drive i povezane aplikacije beleže detaljne informacije o fajlovima i njihovim vlasnicima.

- **Ko je napravio fajl:**
    - Google beleži vlasnika fajla (osobu koja je prva kreirala fajl ili ga uploadovala).
    - Informacije su dostupne u okviru opcije *File Details*:
        - Kliknite na fajl desnim klikom.
        - Izaberite *View Details* ili *Manage Access*.
        - Videćete ime vlasnika fajla i datum kreiranja.
- **Rekordi o uređivanju:**
    - Google Docs/Sheets čuvaju istoriju verzija (*Version History*), gde se vidi ko je kreirao fajl, kao i sve izmene koje su usledile.
    - Kliknite na *File* > *Version History* > *See Version History* da biste videli detalje.
- **Ograničenja:**
    - Ako je fajl preuzet sa Google Drive-a, informacije o vlasniku se ne prenose na fajl van sistema.
    - Fajlovi koji su javno deljeni (npr. sa opcijom "Anyone with the link") ne prikazuju uvek detalje o vlasniku ako su izvan vašeg domena.

---

3. Kako zaštititi privatnost fajlova?

Ako ne želite da drugi saznaju ko je kreirao fajl:

- **Google Drive:**
    - Postavite fajl kao anoniman pre deljenja. To možete postići tako što ćete kopirati sadržaj u novi dokument kreiran pod pseudonimom ili na drugom nalogu.
- **Lokalni fajlovi:**
    - Očistite metapodatke pre deljenja fajla. Na primer:
        - Na Windows-u: *Properties* > *Remove Properties and Personal Information*.
        - Koristite alate kao što je ExifTool za detaljnije uklanjanje metapodataka.

Evo detaljnih uputstava kako da pronađeš informacije o tome ko je napravio fajl i kako da zaštitiš privatnost metapodataka ili ukloniš informacije koje ne želiš da deliš.

---

1. Pronalaženje informacija o fajlovima na računaru

Windows

1. **Pregled metapodataka fajla:**
    - Desnim klikom na fajl, izaberi *Properties*.
    - Idi na karticu *Details*. Ovde možeš videti:
        - Vreme kreiranja i izmene fajla.
        - Informacije o autoru (ako postoje).
        - Verziju fajla i program u kojem je napravljen.
2. **Kako izmeniti ili ukloniti metapodatke:**
    - Otvori *Properties* > *Details*.
    - Klikni na *Remove Properties and Personal Information* (nalazi se pri dnu).
    - Izaberi:
        - *Create a copy with all possible properties removed* (kreira novu verziju bez metapodataka).
        - *Remove the following properties from this file* (omogućava ti da selektivno ukloniš određene informacije).

---

macOS

1. **Pregled metapodataka:**
    - Klikni na fajl desnim klikom i izaberi *Get Info*.
    - Pregledaj polja poput *Created*, *Modified* i *More Info*.
2. **Kako očistiti metapodatke:**
    - macOS nema ugrađen alat za uklanjanje metapodataka.
    - Koristi softvere kao što su **ExifTool** ili **Preview** (za slike).

---

2. Pronalaženje informacija na Google Drive-u

Prikaz vlasnika i detalja fajla:

1. Otvori Google Drive i pronađi fajl.
2. Desnim klikom na fajl, izaberi *View Details*.
3. Videćeš:
    - Ko je kreirao fajl.
    - Datum i vreme kreiranja.
    - Poslednjeg urednika i vremenske oznake.

Pristup verziji fajla:

1. Otvori Google Docs/Sheets fajl.
2. Klikni na *File* > *Version History* > *See Version History*.
3. Videćeš detalje o tome ko je kreirao i menjao fajl.

---

3. Uklanjanje informacija sa fajlova

Google Drive:

- **Kopiraj sadržaj u novi fajl:**
  - Kreiraj novi fajl koristeći drugi Google nalog ili pseudonim.
  - Kopiraj sadržaj iz originalnog fajla u novi fajl kako bi uklonio informacije o vlasniku.
- **Preuzimanje i uklanjanje metapodataka:**
  - Preuzmi fajl u formatu kao što je DOCX ili PDF.
  - Ukloni metapodatke koristeći alate opisane ispod.

Alati za uklanjanje metapodataka:

1. **ExifTool (za napredne korisnike):**
   - Instaliraj **ExifTool** (besplatan alat za uklanjanje metapodataka).

Komanda za uklanjanje metapodataka:
bash
Copy code
```
exiftool -all= ime_fajla
```

   -
   - Ova komanda briše sve metapodatke iz fajla.
2. **GIMP (za slike):**
   - Otvori sliku u GIMP-u.
   - Klikni na *Export As...* i isključi opciju *Save EXIF Data*.
3. **PDF dokumenti:**
   - Koristi besplatan alat kao što je **PDF24** ili **Adobe Acrobat**:
     - Otvori fajl i idi na *Properties*.
     - Ukloni informacije o autoru, naslovu i slično.

---

4. Saveti za zaštitu privatnosti pri kreiranju fajlova

- **Koristi pseudonime:** Ako aplikacija traži ime autora, unesi pseudonim ili generički naziv.
- **Isključi automatsko čuvanje metapodataka:**

    - U aplikacijama poput Microsoft Word-a ili Excel-a, idi na *File* > *Options* > *Trust Center* > *Privacy Options* i uključi opciju *Remove personal information from file properties on save*.
- **Anonimni nalozi:** Kreiraj Google nalog pod pseudonimom za planiranje ili deljenje fajlova.

IV MALO VIŠE O IMEJL SIGURNOSTI

1. Koristite šifrovane e-mail platforme

Ako želite visok nivo privatnosti, razmotrite platforme koje nude end-to-end enkripciju:

- **ProtonMail:**
    - Švajcarski servis sa jakom zaštitom privatnosti i end-to-end enkripcijom.
    - Vaša komunikacija se ne može čitati čak ni od strane ProtonMail-a.
    - Besplatan osnovni paket; plaćeni paketi nude više prostora i funkcionalnosti.
- **Tutanota:**
    - Nemačka platforma koja nudi šifrovanje i visok nivo privatnosti.
    - Dolazi sa ugrađenim kalendarom i alatima za organizaciju.
- **Skiff Mail:**
    - Fokusiran na privatnost i šifrovanje, integrisan sa kolaborativnim alatima.

---

2. Koristite dodatke za šifrovanje sa postojećim e-mail servisima

Ako želite ostati na Gmail-u ili sličnom servisu:

- **PGP (Pretty Good Privacy):**
    - Koristite dodatke poput **Mailvelope** ili **FlowCrypt** za šifrovanje e-mailova u vašem pregledaču.
    - Zahteva deljenje javnih ključeva sa primaocima, ali pruža visok nivo sigurnosti.
- **ProtonMail Bridge:**
    - Omogućava korišćenje šifrovanih ProtonMail naloga unutar klijenata kao što su Thunderbird ili Outlook.

---

3. Dodatni koraci za zaštitu e-maila

a) Dvofaktorska autentifikacija (2FA):

- Aktivirajte 2FA na svim e-mail nalozima kako biste zaštitili nalog čak i ako su vaše lozinke ugrožene.
- Koristite aplikacije kao što su **Google Authenticator**, **Authy**, ili **Yubico** (za fizički ključeve).

b) Snažne i jedinstvene lozinke:

- Koristite menadžer lozinki (npr. **Bitwarden**, **LastPass**, **1Password**) za generisanje i čuvanje jakih lozinki.
- Nemojte koristiti istu lozinku za više naloga.

c) Izbegavajte sumnjive linkove:

- Ne klikćite na linkove ili otvarajte priloge iz nepoznatih izvora, čak i ako izgledaju legitimno.
- Proverite URL pre nego što unesete lozinku.

d) Koristite privatne e-mail adrese:

- Kreirajte posebne adrese za komunikaciju koja zahteva visok nivo privatnosti. Ne koristite ih za registraciju na javnim servisima ili aplikacijama.

---

4. Izbegavajte servise koji narušavaju privatnost

- **Gmail i Outlook:** Pouzdani su, ali nisu idealni za visoku privatnost jer podaci mogu biti dostupni državnim institucijama (posebno u SAD).
- **Yahoo Mail:** Ima istoriju ozbiljnih povreda privatnosti, uključujući hakovanja.

---

5. Sakrivanje e-mail identiteta

- **Alias adrese:** Koristite servise kao što su **SimpleLogin** ili **AnonAddy** za kreiranje privremenih ili maskiranih adresa koje preusmeravaju poruke na vaš glavni e-mail.
- **Privremeni e-mail:** Koristite privremene servise (npr. **10minutemail**) za jednokratne registracije.

---

6. Praćenje neovlašćenog pristupa

- Redovno proveravajte aktivnosti na nalogu:
    - Gmail: *Security Checkup* nudi pregled prijava i uređaja.
    - ProtonMail i Tutanota: Beleže sve sesije i IP adrese.
- Postavite obaveštenja za pokušaje prijave ili promene lozinki.

---

7. Koristite odvojene uređaje

- Ako je moguće, koristite poseban uređaj ili operativni sistem za pristup osetljivim e-mailovima, npr. **Tails OS** ili **Qubes OS**, koji su dizajnirani za maksimalnu privatnost.

V ZAKONSKA ZAŠTITA

1. Ustav Republike Srbije

- **Član 42 – Zaštita podataka o ličnosti:**
  - Garantuje pravo na zaštitu ličnih podataka i privatnosti.
  - Obrada podataka može se vršiti samo uz saglasnost ili na osnovu zakona.
- **Član 41 – Tajnost pisama i drugih sredstava komunikacije:**
  - Komunikacija je nepovrediva, osim u slučajevima koji su izričito predviđeni zakonom i uz sudski nalog.

---

2. Krivični zakonik Republike Srbije

- **Član 146 – Neovlašćeno prisluškivanje i snimanje:**
  - Neovlašćeno prisluškivanje, snimanje razgovora ili praćenje komunikacija je krivično delo, osim ako postoji sudski nalog.
  - Kazne: Novčane kazne ili zatvorska kazna do tri godine.
- **Član 208 – Povreda tajnosti pisama i drugih pošiljki:**
  - Povreda tajnosti komunikacije može rezultirati zatvorskom kaznom do jedne godine.

---

3. Zakon o zaštiti podataka o ličnosti

- **Prava građana:**
  - Imate pravo da znate kako se vaši podaci obrađuju, ko ih obrađuje i zašto.
  - Možete zahtevati uvid u svoje podatke, tražiti ispravku ili brisanje.
- **Nadležno telo:**
  - Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti može se obratiti ako smatrate da su vaša prava prekršena.

---

4. Zakon o elektronskim komunikacijama

- **Član 128 – Nadzor komunikacija:**
  - Nadzor komunikacija dozvoljen je samo uz sudski nalog.
  - Operateri su dužni da obezbede tajnost komunikacije, osim u slučajevima kada je to zakonom predviđeno.

---

5. Procedura za slučaj špijunskog softvera ili prisluškivanja

Ako sumnjate da ste pod nadzorom, možete koristiti sledeće pravne korake:

1. **Podnošenje prijave policiji:**
   - Obavestite lokalnu policiju ili tužilaštvo o sumnjama na prisluškivanje ili postojanje špijunskog softvera.
   - Insistirajte na pokretanju istrage.
2. **Obraćanje Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti:**
   - Poverenik ima pravo da istraži zloupotrebe podataka o ličnosti i nadzora.
   - Kontaktirajte ih putem zvanične adrese: Poverenik za informacije.
3. **Zahtev za uvid u sudski nalog:**
   - Ako ste prisluškivani, nadležni organi moraju imati sudski nalog. Zatražite uvid u taj nalog preko advokata.
4. **Angažovanje stručnjaka za digitalnu bezbednost:**
   - Ako sumnjate na špijunski softver, angažujte nezavisnog stručnjaka za forenziku da analizira vaš uređaj.

---

6. Međunarodna zaštita

Ako ne možete ostvariti pravdu u Srbiji, možete se obratiti međunarodnim organizacijama:

- **Evropski sud za ljudska prava (ECHR):**
  - Možete podneti prijavu za povredu prava na privatnost (Član 8 Evropske konvencije o ljudskim pravima).
  - Važno je prethodno iscrpeti sve domaće pravne resurse.
- **Amnesty International ili Human Rights Watch:**
  - Ove organizacije mogu pružiti podršku ili podići svest o represivnim praksama u Srbiji.