foto @gavriloandric

Prošireni vodič za visokorizična okruženja

Kako ostati bezbedan tokom protesta?

Ovaj vodič pruža ključne i napredne savete o tome kako da zaštitite sebe, svoje podatke i druge dok koristite svoje pravo na protest u okruženju sa pojačanim nadzorom.

it SRBIJA

I. BRZA LISTA ZA PROVERU (CHECKLIST)

Za one koji žure, ovo su apsolutno najvažniji koraci:

- [x] Primarni telefon ostaje kod kuće.
- [x] Ako nosite telefon, neka bude "čist" (bez ličnih podataka).
- [x] Isključite biometriju (lice/prst).
- [x] Koristite dugačku, alfanumeričku šifru.
- [x] Koristite Signal za komunikaciju.
- [x] Uključite samouništavajuće poruke.
- [x] Pokrijte lice.
- [x] Maska, naočare, kapa. Nosite neupadljivu odeću.
- [x] Broj advokata napišite na ruku.
- [x] Ne oslanjajte se na telefon.
- [x] Idite sa partnerom (buddy system).
- [x] Dogovorite plan za razdvajanje.
- [x] Ne objavljujte slike sa licima drugih ljudi bez njihove izričite dozvole.
- [x] Isključite telefon ili ga stavite u Faradejevu torbicu kada ga ne koristite.

II. VAŠ TELEFON: NAJVEĆA RANJIVOST

Vaš pametni telefon je uređaj za praćenje koji nosite sa sobom.

Poneti ili ne poneti telefon na protest?

Najbolja opcija:

Ostavite svoj primarni telefon kod kuće.
To je najefikasnija mera zaštite.

Ako vam je potreban telefon:

- **Koristite sekundarni "čist" telefon sa minimalnim ličnim podacima, nalozima ili aplikacijama.**
- **"Burner" telefon (za jednokratnu upotrebu) nije automatski anoniman. Ako ste ga kupili karticom ili dali lične podatke, povezan je sa vama.**
- **Držite telefon isključen što je više moguće kako biste izbegli povezivanje sa lažnim baznim stanicama (IMSI hvatači/stingrays).**
- **Koristite Faradejev kavez (torbicu) da blokirate sve radio signale (GPS, Wi-Fi, mobilnu mrežu) kada ne koristite telefon.**

Obezbedite svoj uređaj

Ukoliko ste primorani da nosite licni telefon na proteste obavezno aktivirajte Lockdown Mode* (iOS) ili Advanced Protection (Android)**

Enkripcija:

iOS:
Enkripcija celog diska je podrazumevano uključena kada koristite šifru.

Android:
Proverite da li je opcija "Sifruj disk" (Encrypt Disk) omogućena u bezbednosnim podešavanjima.

Zaključavanje ekrana:

- **Koristite dugačku, jaku, alfanumeričku šifru.**
- **Onemogućite biometrijsko otključavanje (Face ID, Touch ID) pre protesta. Teže je da vas organi reda primoraju da odate šifru nego da vas nateraju da prislonite prst ili lice na senzor.**
- **Naučite kako da na svom telefonu brzo aktivirate hitnu funkciju za onemogućavanje biometrije (npr. na iPhone-u, brzo pritisnite dugme za uključivanje 5 puta).**

*https://support.apple.com/en-us/105120
**https://support.google.com/accounts/answer/9764949?hl=en

Obezbedite svoju komunikaciju

Koristite End-to-End enkripciju (E2EE):

- Koristite aplikacije poput Signala za sve pozive i poruke.
- Izbegavajte SMS, Telegram (osim "secret chats"), Facebook Messenger itd.
- Omogućite samouništavajuće poruke podešene na kratak vremenski period (npr. 1-6 sati).
- Uverite se da svi sa kojima komunicirate koriste istu bezbedne aplikacije i ako ste u mogucnosti potvrdite Safety Number (signal) sa osobom sa kojom komunicirate i ekvivalente kljuceve u drugim aplikacijama.

III. VAŠ IDENTITET: FIZIČKA I DIGITALNA ANONIMNOST

Fizički izgled na protestu

Pokrijte lice:

Standardna maska za lice i naočare za sunce su minimum. Za veću bezbednost, razmislite o kapi, kapuljači i drugim slojevima.

Odeća:

Nosite neupadljivu odeću bez logotipa. Pokrijte sve prepoznatljive tetovaže ili belege.

Prevoz:

Budite svesni da automatski čitači registarskih tablica (ALPR) prate vozila. Parkirajte dalje od mesta okupljanja ako je moguće.

Digitalni otisak

Društvene mreže:

- **Ne najavljujte javno svoje planove za odlazak na protest.**
- **Nikada ne objavljujte fotografije ili video snimke koji prikazuju prepoznatljiva lica drugih demonstranata bez njihove izričite saglasnosti. Time ih direktno dovodite u opasnost.**
- **Budite izuzetno oprezni prilikom prenosa uživo (livestreaming).**

Metapodaci (EXIF):

Fotografije sadrže skrivene podatke (GPS lokacija, vreme, model telefona). Koristite aplikacije za uklanjanje metapodataka pre deljenja. Mnoge društvene mreže ovo rade automatski, ali ne sve.

IV. PRAVNA I OPERATIVNA PRIPREMA (OPSEC)

Pre nego što krenete na protest

Znajte svoja prava:
Istražite lokalne zakone o javnom okupljanju, pravima prilikom hapšenja i snimanju službenih lica. Potražite resurse od lokalnih pravnih organizacija koje se bave ljudskim pravima.

Pravni kontakt:
Zapišite broj telefona advokata ili grupe za pravnu podršku na svom telu trajnim markerom.

Hitni kontakti:
Zapamtite broj telefona bar jednog hitnog kontakta.

Planirajte izlaz:
Upoznajte područje i imajte isplanirano više izlaznih ruta.

Tokom protesta

Sistem partnera (Buddy System):
Idite sa pouzdanim prijateljem. Dogovorite plan šta raditi ako se razdvojite ili ako neko bude uhapšen.

Ostanite svesni:
Pratite okolinu, kretanje policije i potencijalne agitatore.

V. FIZIČKA BEZBEDNOST I PRVA POMOĆ

Pre nego što krenete na protest

Suzavac:

- **NE KORISTITE MLEKO. Voda je najbolja opcija za ispiranje očiju.**
- **Ponesite flašicu vode isključivo za ovu svrhu. Nagnite glavu u stranu i ispirajte oko od unutrašnjeg ka spoljašnjem uglu.**
- **Ne trljajte oči. Često trepćite da podstaknete suze.**
- **Gas-maska ili plivačke naočare mogu pružiti dobru zaštitu.**

Kettling (Opkoljavanje):

Ako policija formira kordon, ostanite mirni.
Ne gurajte se. Sledite uputstva i tražite siguran izlaz. Često policija ostavi jedan otvoren prolaz.

Prva pomoć:

Ponesite mali paket sa flasterima, gazom i antiseptičkim maramicama.

VI. DIGITALNA HIGIJENA NAKON PROTESTA

Analiza materijala:

Pregledajte sve fotografije i video snimke. Zamutite lica drugih ljudi pre bilo kakvog deljenja koristeći aplikacije poput "Signal Blur" ili "ObscuraCam".

Bezbedno brisanje:

Nakon što ste sačuvali i obradili materijal, bezbedno ga obrišite sa "čistog" telefona. Koristite "file shredder" aplikacije na Androidu. Na iOS-u, vraćanje na fabrička podešavanja je najsigurnija opcija.

Praćenje naloga:

U danima nakon protesta, obratite pažnju na sumnjive aktivnosti na vašim imejl i društvenim nalozima (npr. pokušaji logovanja, phishing poruke).

VII. BORBA PROTIV DEZINFORMACIJA

Državni akteri često koriste psihološke operacije (PSYOPs) da bi diskreditovali proteste.

Prepoznajte taktike:

Lažne vesti:
Izmišljene priče dizajnirane da izazovu bes ili strah.

Manipulisani snimci:
Video ili audio materijal izvučen iz konteksta.

Ubačeni agitatori:
Pojedinci koji namerno izazivaju nasilje da bi protest izgledao nasilno.

Vaša uloga:

Proverite pre deljenja:
Uvek proverite izvor informacije. Da li je kredibilan? Da li i drugi pouzdani izvori prenose istu vest?

Ne širite glasine:
Ako niste sigurni, bolje je da ne delite.

Prijavite dezinformacije:
Koristite alate na društvenim mrežama da prijavite lažne naloge i dezinformacije.

VIII. NAPREDNE MERE, ANTIFORENZIKA I PROTIV-NADZOR

Za one sa višim profilom rizika (novinari, aktivisti, organizatori).

Ojačani mobilni operativni sistemi

GrapheneOS/CalyxOS:
Ako posedujete kompatibilan Google Pixel telefon, razmislite o instaliranju ovih distribucija. One su dizajnirane da minimiziraju praćenje i poboljšaju bezbednost, nudeći više zaštite od standardnog Androida ili iOS-a.

Antiforenzičke mere: Otežavanje analize uređaja

Enkripcija celog diska:
Ovo je vaša prva linija odbrane. Uverite se da je omogućena na svim uređajima.

Aplikacije i podaci za obmanu:
Razmislite o korišćenju aplikacija koje stvaraju skrivene, šifrovane kontejnere za vaše podatke. Neke aplikacije čak mogu imati i "šifru za prinudu" (duress password) koja otkriva lažni skup datoteka umesto vaših pravih.

Bezbednosni skeneri i panik tasteri:

Bezbednosni skeneri (poput iVerify):
Aplikacije poput iVerify su korisne za redovno skeniranje vašeg uređaja kako bi se otkrilo da li je bio neovlašćeno modifikovan (jailbreak/root) ili zaražen poznatim malverom.

Funkcije panike/prinude:
Neke specijalizovane bezbednosne aplikacije, posebno na Androidu, nude "panik taster" ili "PIN za prinudu". Ova funkcija vam omogućava da unesete poseban kod na zaključanom ekranu koji može pokrenuti akcije poput brisanja podataka sa telefona, slanja hitnog upozorenja pouzdanom kontaktu ili skrivanja određenih aplikacija. Ovo je moćan antiforenzički alat ako ste primorani da otključate svoj uređaj.

Bezbedno brisanje i čišćenje:
Jednostavno brisanje datoteke obično samo uklanja pokazivač na nju, ostavljajući stvarne podatke na memoriji dok ne budu prepisani. Za osetljive informacije, ovo nije dovoljno.

Koristite aplikacije za uništavanje datoteka (File Shredder):
Na Androidu potražite aplikacije za "uništavanje datoteka" ili "bezbedno brisanje" koje prepisuju datoteke više puta kako bi postale neoporavljive. Primeri uključuju iShredder, Shreddit i Secure Wipe. (Napomena: Dostupnost i reputacija aplikacija se mogu menjati, pa uvek proverite najnovije recenzije iz pouzdanih bezbednosnih izvora).

Očistite slobodan prostor:

Da biste obrisali ostatke prethodno obrisanih datoteka, koristite aplikaciju koja bezbedno briše slobodan prostor na internoj memoriji vašeg uređaja ili SD kartici.

Ograničenja na iOS-u:

Na modernim iOS uređajima, zbog jake hardverske enkripcije, bezbedno brisanje pojedinačnih datoteka je manja briga jer se ključevi za šifrovanje uništavaju prilikom brisanja. Vraćanje na fabrička podešavanja je najefikasniji način za potpuno brisanje uređaja.

Vraćanje na fabrička podešavanja:

Za maksimalnu bezbednost na sekundarnom uređaju, izvršite vraćanje na fabrička podešavanja pre i posle događaja.

Minimizirajte podatke:

Najbolji način da zaštitite svoje podatke je da ih uopšte nemate. Redovno proveravajte aplikacije i podatke na svom telefonu.

Razumevanje rezervnih kopija u oblaku (Cloud Backups):

Budite svesni koji se podaci automatski čuvaju u oblaku (npr. Google Photos, iCloud).
Organi reda često mogu dobiti ove podatke od tehnoloških kompanija uz nalog. Onemogućite automatske rezervne kopije.

Reagovanje na napredni špijunski softver (npr. Pegasus)

Ako ste **osoba visokog rizika** (novinar, aktivista, advokat) i imate razloga da verujete da ste bili meta **sofisticiranog državno sponzorisanog špijunskog softvera poput Pegasusa**, reakcija je drugačija od suočavanja sa običnim malverom.

Ne paničite, ne brišite!

Odmah prestanite da koristite uređaj za bilo kakvu osetljivu komunikaciju. Isključite ga sa Wi-Fi i mobilnih mreža (npr. uključivanjem avionskog režima ili uklanjanjem SIM kartice). **Ključno je da ne pokušavate da vratite uređaj na fabrička podešavanja ili da sami uklonite malver.** To može upozoriti napadače i uništiće ključne forenzičke dokaze potrebne za potvrdu.

POTRAŽITE STRUČNU POMOĆ!

Ovo nije situacija "uradi sam". Kontaktirajte specijalizovanu organizaciju opremljenu za rešavanje takvih pretnji.

Access Now's Digital Security Helpline: Pruža 24/7 pomoć grupama civilnog društva i aktivistima širom sveta.

Izolujte uređaj!

Držite fizički uređaj na sigurnom i izolovanom mestu dok ga ne predate pouzdanom stručnjaku na forenzičku analizu.

Imaš još pitanja ili dileme?

Znamo da ni najdetaljniji vodiči ne mogu da obuhvate svaku moguću situaciju. Ako i dalje imaš nedoumice u vezi sa digitalnom bezbednošću, korišćenjem tehnologije tokom protesta ili drugim aspektima zaštite u visokorizičnim okruženjima — nisi sam/a.

Slobodno nam se obrati.

Zajednica IT Srbija stoji ti na raspolaganju za savete, dodatna pojašnjenja i tehničku podršku.

Skeniraj QR kod i pridruži se serveru!

ITSRBIJA.ORG