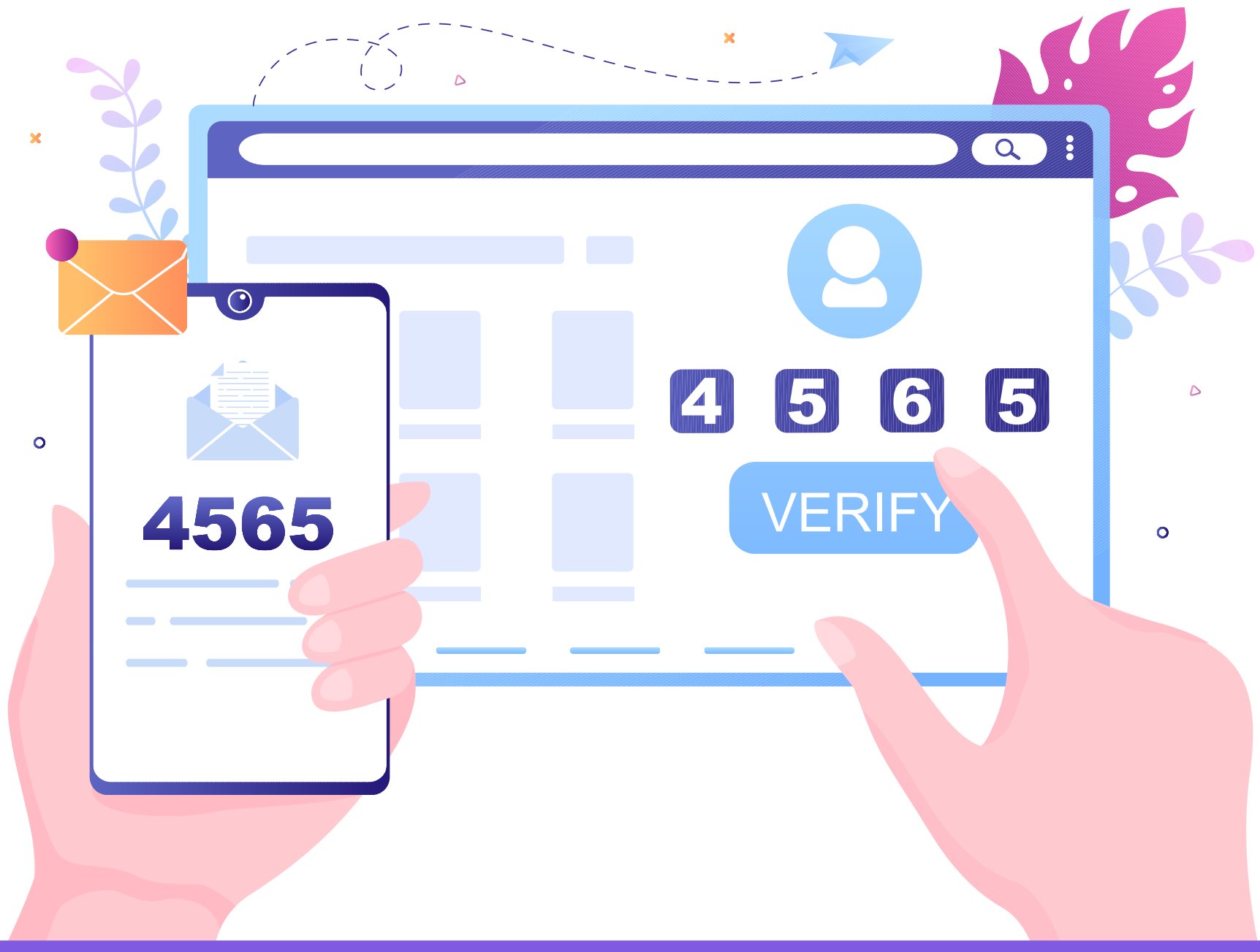
# ONLINE SIGURNOST

# SIGURNO NOVINARSTVO U ONLINE SVIJETU

Danas je gotovo nemoguće zamisliti novinarstvo bez uporabe suvremenih načina komunikacije koji se provode putem interneta. Internet nam je s jedne strane olakšao komunikaciju, dok je s druge strane pred nas postavio nove izazove. Sigurnost u online svijetu jedan je od ključnih izazova s kojim se novinari svakodnevno susreću. Bilo da ste vješti u ovom području ili se prvi put susrećete s ovim pojmom, ovaj bi vam priručnik trebao koristiti kao mali podsjetnik na što trebate obratiti pažnju kada je riječ o online sigurnosti. Informacije u ovom priručniku su općenite i neke ćete stvari morati prilagoditi vlastitom načinu rada ili dodatno istražiti. Imajte u vidu da se različiti alati, aplikacije i načini zaštite koriste u različitim situacijama i oblicima rada. Ne postoje savršeni alati, savršene aplikacije ni načini da ostanemo sigurni u online svijetu. Ovaj priručnik* pruža osnovne smjernice za novinare i novinarke kako bi zaštitili svoje podatke i informacije prilikom rada na internetu.

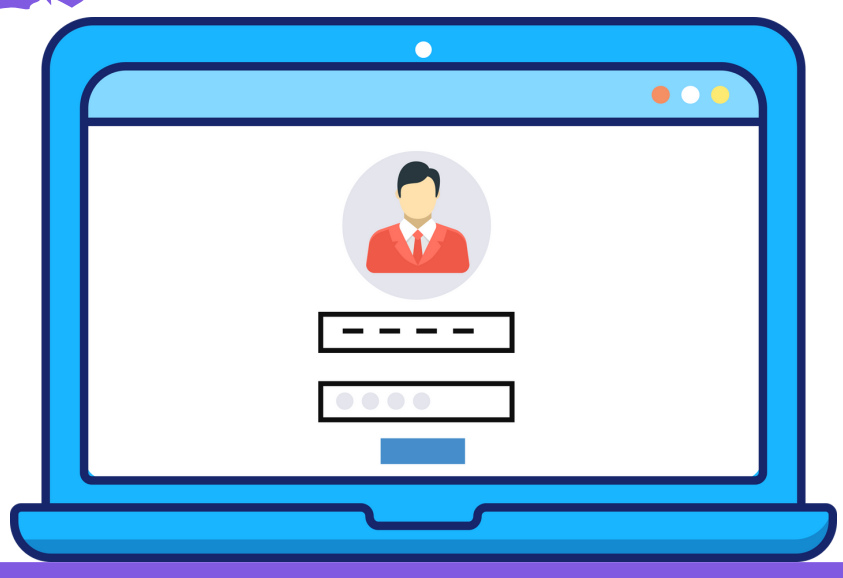

*Ovaj priručnik nastao je kao proizvod niza radionica i predavanja na projektu Journalist Security Fellowship, koji je Internews proveo u Hrvatskoj. Internews je međunarodna neprofitna organizacija koja podupire neovisne medije u više od 100 zemalja svijeta. Priručnik je priredila Monika Kutri, polaznica ovog programa.

# DVOFAKTORSKA AUTENTIFIKACIJA




Koristite dvofaktorsku autentifikaciju (Two-factor authentication) za dodatnu sigurnost. Dvofaktorska autentifikacija je proces provjere identiteta korisnika, koji koristi dva različita načina autentifikacije. Na primjer, kada se prijavljujete na bankovni račun, morate unijeti svoje korisničko ime i lozinku (prvi faktor autentifikacije) i zatim jednokratni kod koji ste dobili putem SMS-a (drugi faktor autentifikacije). To povećava sigurnost prijavljivanja i smanjuje rizik od neovlaštenog pristupa računu. Mnoge usluge danas nude dvofaktorsku autentifikaciju kao opciju pa bi bilo dobro aktivirati je za sve račune na kojima je dostupna.

# JAKE LOZINKE



Koristite jake i jedinstvene lozinke za svaki račun koji imate. Lozinka bi trebala biti dugačka, sadržavati kombinaciju velikih i malih slova, brojeva i posebnih znakova. Dužina je ono što je najvažnije u izradi lozinki. Lozinka sastavljena od nekoliko nasumičnih riječi je odlična. Također, koristite različite lozinke za svaki račun, tako da ako jedna bude kompromitirana, vaši drugi računi neće biti ugroženi. Najjednostavniji način da vaše lozinke budu različite, kompliciranе i da stoje na jednom, sigurnom mjestu, je uporaba Password Managera.

Password Manager je aplikacija koja skladišti sve vaše lozinke, predlaže vam nove i kompliciranе lozinke, a jedino što tada trebate upamtiti je glavna lozinka za vaš Password Manager.

**Prijedlozi:**

- **1Password (besplatan za novinare)**
- **KeePassXC**
- **Bitwarden**

# ENKRIPCIJA

Enkripcija (šifriranje) je postupak pretvaranja običnog teksta u nečitljivi oblik (šifrat) uz pomoć matematičkih algoritama i ključeva. Enkripcija se koristi za zaštitu podataka i privatnosti korisnika na različitim područjima, između ostalog uključujući:

1. Komunikacije: enkripcija se često koristi u komunikacijskim aplikacijama (poput e-pošte, chatova, VoIP-a) kako bi se zaštitili podaci koje korisnici razmjenjuju. Enkripcija sprječava neovlašteni pristup i osigurava da samo primatelj može dešifrirati poruke. Whatsapp i Signal koriste end-to-end enkripciju.
2. Pohrana podataka: enkripcija se koristi za zaštitu osjetljivih podataka poput financijskih podataka, medicinskih zapisa, osobnih identifikacijskih dokumenata i drugih osjetljivih informacija koje se čuvaju u bazi podataka ili na uređajima.
3. Mrežna sigurnost: enkripcija se koristi u mrežnoj sigurnosti kako bi se osiguralo sigurno slanje i primanje podataka preko mreže. Na primjer, protokol HTTPS koristi enkripciju SSL/TLS kako bi se zaštitio web promet, a VPN usluge koriste enkripciju da bi se zaštitio promet preko interneta.

Koristite enkripciju za zaštitu osjetljivih podataka poput privatnih poruka, datoteka ili e-pošte. Postoje različite usluge i alati za enkripciju koji će vam pomoći da zaštitite vaše podatke. End-to-end enkripcija je proces šifriranja podataka tijekom komunikacije između dviju strana tako da samo te dvije strane mogu vidjeti sadržaj razgovora. To znači da čak ni servis koji pruža komunikacijsku uslugu neće moći pristupiti šifriranim podacima. Aplikacija za razmjenu poruka mogu koristiti end-to-end enkripciju kako bi osigurale sigurnu razmjenu poruka između dviju osoba.

Imajte u vidu da je korištenje ovog sustava sigurno sve dok su uređaji kojima komunicirate fizički sigurni. Osoba s kojom komunicirate može napraviti snimku zaslona i poslati dalje prepisku ili uživo nekome pokazati o čemu komunicirate. Budite svjesni ovoga kada komunicirate povjerljive stvari. Također, ako radite back up, imajte u vidu da na nekim aplikacijama treba dodatno uključiti enkripciju za back up.

# UPOTREBA SIGURNOSNOG SOFTVERA

Koristite antivirusne programe, antimalware i druge sigurnosne alate koji će pomoći zaštititi vaše računalo od zlonamjernog softvera. Redovito ažurirajte softver kako biste imali najnoviju zaštitu. Ako koristite Windows, uključite Windows Defender.

# SIGURNO PRETRAŽIVANJE

Kada radite na internetu, koristite samo sigurne mreže koje su zaštićene lozinkom i enkripcijom. Pokušajte izbjegavati besplatne ili javne Wi-Fi mreže koje su otvorene za sve jer su vrlo osjetljive na napade hakera i prisluškivanje.

Koristite Virtualnu privatnu mrežu (VPN) kada se povezujete na internet. VPN enkriptira vašu internetsku vezu i omogućava vam da anonimno i sigurno pregledavate internet. To je posebno važno kada se povezujete na internet preko javnih Wi-Fi mreža. VPN uspostavlja privatnu vezu preko javne mreže (kao što je internet), koja šifrira sve podatke koji se prenose između vašeg računala i mreže. To pomaže zaštititi vašu privatnost i sigurnost jer će vaša IP adresa biti zamijenjena IP adresom VPN-a i zato što se svi vaši podaci koji putuju preko interneta šifriraju.

Prijedlog za VPN:

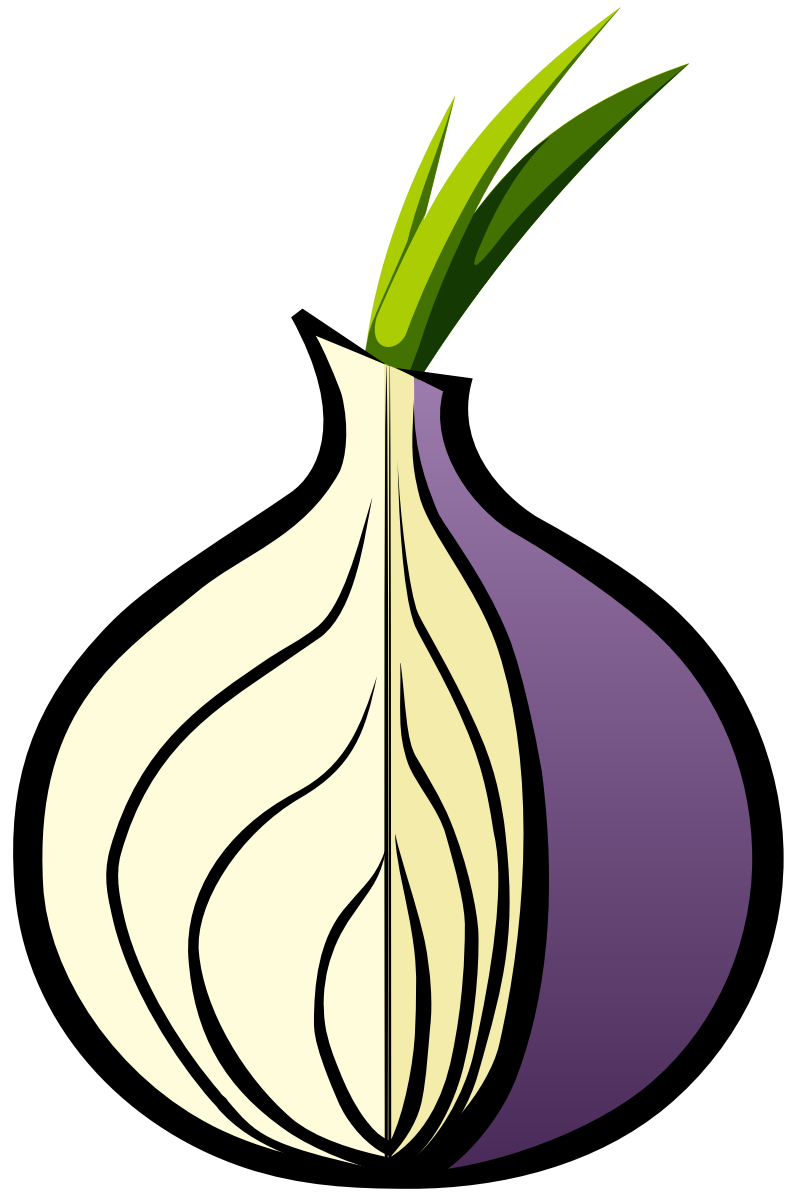
Tunnel Bear

Mullvad

ProtonVPN


**TOR** je besplatan softver za anonimno surfanje internetom koji se sastoji od mreže privatnih računala koja omogućava anonimni pristup internetu. TOR koristi posebnu tehnologiju enkripcije i preusmjeravanja prometa kako bi se sakrio identitet korisnika i omogućio siguran pristup internetu. Mreža TOR djeluje tako da promet korisnika kroz mrežu prolazi kroz niz čvorova prije nego što dođe do krajnjeg odredišta. Svaki čvor zna samo o čvoru s kojim je povezan i ne zna tko je korisnik ili gdje se promet konačno šalje. To omogućava korisnicima da posjećuju web stranice, razmjenjuju poruke i podatke na internetu anonimno i sigurno.

Važno je napomenuti da se TOR često povezuje s nelegalnim aktivnostima kao što su trgovina drogom i oružjem, prodaja informacija ili pružanje usluga hakiranja. Iako se TOR može koristiti za legitimne svrhe, uvijek je važno koristiti ga odgovorno i u skladu s važećim zakonima i propisima.




Prije nego što unesete osjetljive informacije kao što su korisnička imena, lozinke ili brojevi kreditnih kartica, provjerite da li je URL web stranice siguran i poznat.

**HTTPS (HyperText Transfer Protocol Secure)** je sigurna verzija protokola HTTP koji se koristi za komunikaciju između web preglednika i web servera. Kada koristite HTTPS, vaša veza s web stranicom je šifrirana, što znači da se svi podaci koji se prenose između vašeg preglednika i web servera šifriraju i tako su zaštićeni od neovlaštenog pristupa.

Kada pregledavate web stranice koje koriste HTTPS, vaš preglednik će vam obično prikazati zeleni ili zatvoreni lokot na vrhu preglednika kako bi naznačio da se koristi sigurna veza. To vam daje povjerenje da je veza između vašeg preglednika i web servera sigurna i da se vaši podaci šifriraju.

# RAZMJENA PODATAKA

## Aplikacije za razmjenu poruka i poziva

Neke od aplikacija koje imaju razvijen dobar sigurnosni sustav za komunikaciju i koriste end-to-end enkripciju su:

**Signal** - aplikacija za razmjenu poruka koja je poznata po svojoj visokoj razini sigurnosti i privatnosti. Signal također koristi end-to-end enkripciju kako bi se osigurala sigurnost poruka. Signal također nudi mogućnost samouništenja poruka nakon određenog vremena i podržava razmjenu datoteka i glasovne pozive.

**WhatsApp** - jedna od najpopularnijih aplikacija za razmjenu poruka diljem svijeta. Omogućava korisnicima slanje tekstualnih, glasovnih i video poruka, kao i dijeljenje datoteka i pozive putem interneta. WhatsApp koristi end-to-end enkripciju kako bi se osigurala sigurnost poruka. WhatsApp je, međutim, u vlasništvu Facebooka, zbog čega postoji zabrinutost za privatnost podataka.

**Telegram** - aplikacija za razmjenu poruka koja se često uspoređuje s WhatsAppom. Telegram nudi nekoliko značajki koje WhatsApp ne nudi, kao što su grupne poruke do 200 tisuća članova, mogućnost dijeljenja datoteka do 2 GB i mogućnost slanja samouništavajućih poruka. Telegram također koristi end-to-end enkripciju za šifriranje poruka, ali nije u potpunosti otvorenog koda, što je izvor zabrinutosti za privatnost podataka.

**Wire** - aplikacija za razmjenu poruka koja je poznata po svojoj otvorenosti, transparentnosti i visokoj razini sigurnosti i privatnosti. Wire koristi end-to-end enkripciju za sigurnu razmjenu poruka, kao i za glasovne i video pozive. Wire također nudi mogućnost dijeljenja datoteka i grupne poruke do 10 tisuća članova. Wire se ističe svojim otvorenim kodom i transparentnom praksom upravljanja podacima, što znači da su korisnici potpuno svjesni kako se njihovi podaci prikupljaju, koriste i dijele.

Važno: aplikacije za komuniciranje kao i druge aplikacije za vaš telefon uvijek instalirajte s ovlaštenih mjesta kao što su na primjer google play store ili apple store.

# Sigurno slanje elektroničke pošte

Elektronička pošta (e-pošta ili e-mail) jedan je od najčešćih načina komunikacije na internetu. Međutim slanje e-pošte može biti nesigurno jer se poruke mogu lako presresti i mogu ih čitati neovlaštene osobe. Na sreću, postoje neki načini na koje možete sigurno slati e-poštu:

- **Pretty Good Privacy** (PGP) - program za enkripciju koji omogućava sigurno slanje i primanje šifrirane e-pošte.
- **ProtonMail** - besplatna i sigurna e-pošta koja pruža end-to-end enkripciju. To znači da poruke ostaju šifrirane tijekom prijenosa i samo primatelj može dešifrirati poruku.


**Phishing** - oblik napada u kojem se korisniku šalje e-mail ili poruka s lažnim linkom ili privitkom koji je obično dizajniran da izgleda autentično, ali koji će, ako se klikne, otvoriti vrata za hakere. Ako primite mail u kojem se od vas traži da nešto potvrdite ili se negdje registrirate, uvijek provjerite s koje adrese dolazi taj email.

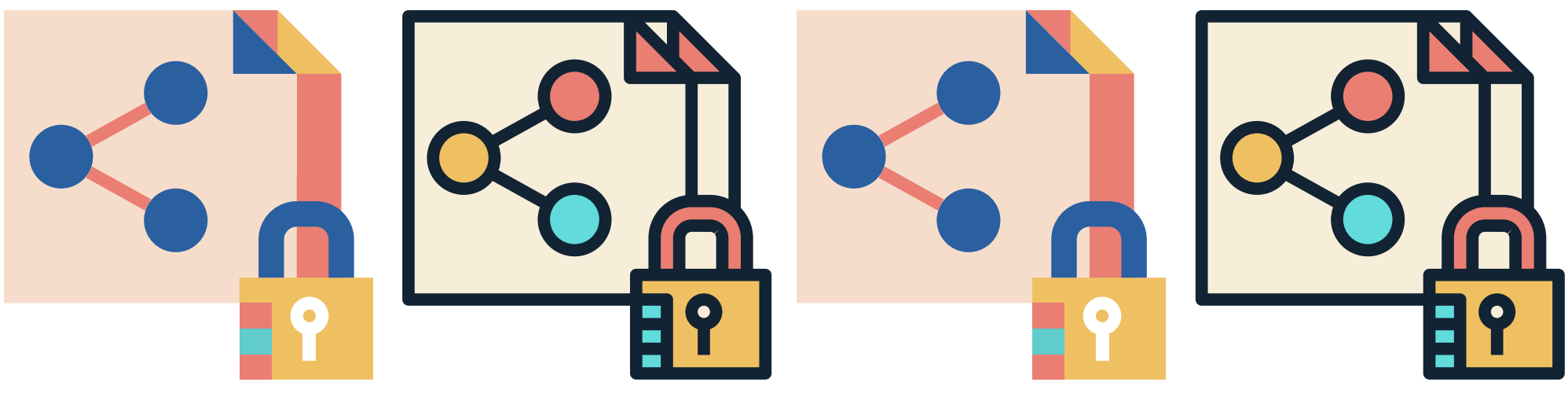
# Sigurno dijeljenje datoteka

Kada dijelite osjetljive datoteke, koristite sigurne usluge dijeljenja, koje štite vaše podatke od neovlaštenog pristupa. Izbjegavajte slanje osjetljivih podataka putem e-pošte ili društvenih mreža.

Ako putem e-pošte primite dokument za koji sumnjate da je zaražen virusom, nemojte ga skidati na uređaj, nego ga otvorite online putem **Google diska** ili **Office 365** (ne putem desktop aplikacija), a možete koristiti i aplikaciju **Dangerzone.**

Za još sigurnije dijeljenje datoteka koristite **OnionShare** i **SecureDrop**

OnionShare je alat za anonimno dijeljenje datoteka i poruka putem mreže TOR, dok je SecureDrop sustav koji omogućava sigurnu razmjenu informacija između izvora i novinara. Oba alata pružaju visoku razinu sigurnosti i anonimnosti kako bi zaštitili privatnost korisnika i potaknuli slobodno dijeljenje informacija.



# I JOŠ...

## Privatnost na društvenim mrežama

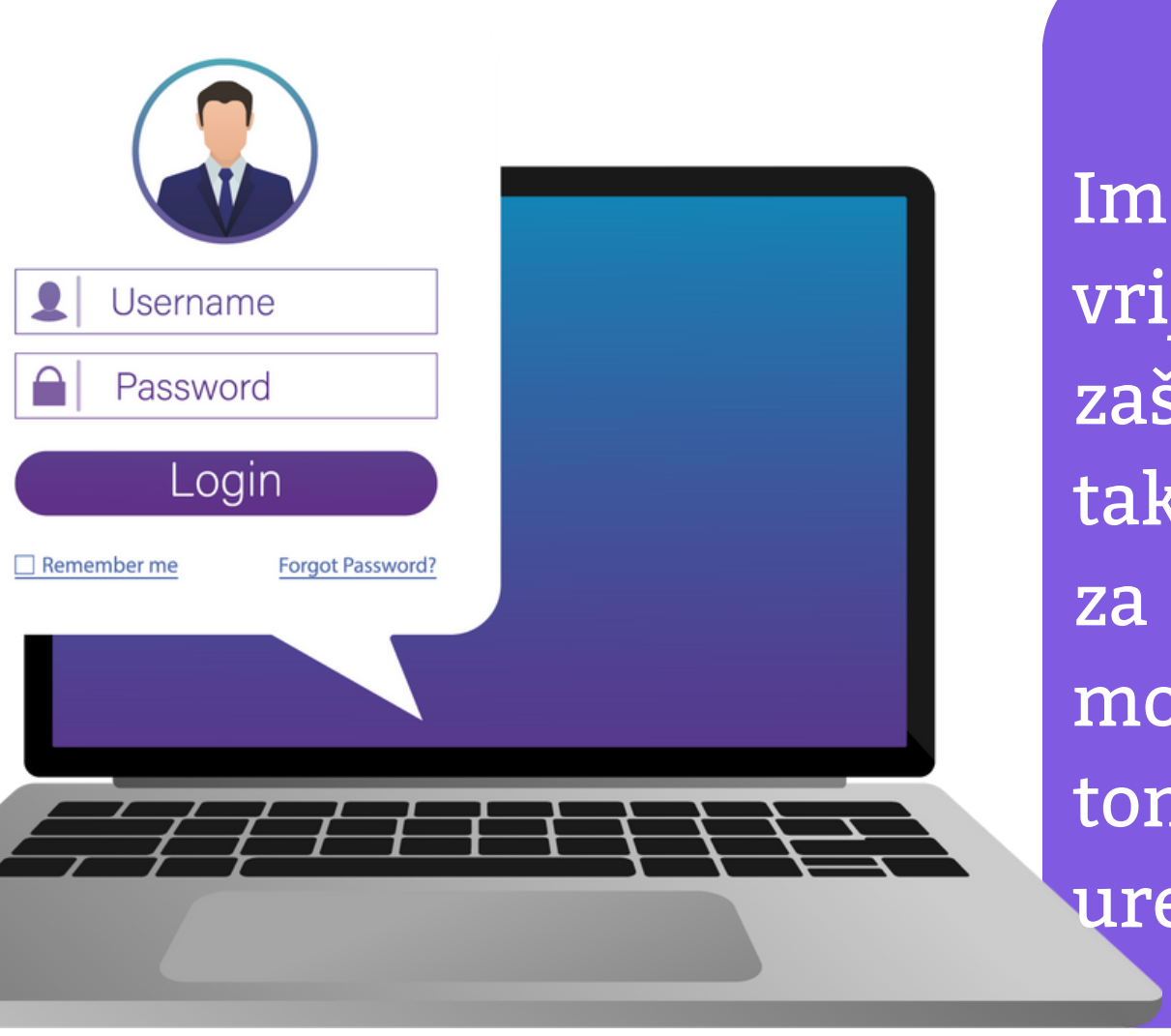
Ova kategorija vrlo je škakljiva tema za pojedine novinare/ke. S jedne strane se od novinara i novinarki očekuje da budu prisutni na mrežama, a s druge strane im se stalno prigovara o sigurnosti. Trebate li se onda skrivati ili biti prisutni na svim mrežama? U ovom slučaju nema točnog odgovora - sve ovisi o vrsti posla kojom se bavite te o potrebama da kao javna medijska ličnost budete prepoznati i zastupljeni i na društvenim mrežama. Pazite na postavke privatnosti na društvenim mrežama. Razmislite o tome biste li trebali imati dva profila, jedan javan i jedan privatan. Svakako ograničite količinu osobnih podataka koje dijelite i ne dijelite osjetljive informacije poput adresa, telefonskih brojeva i drugih privatnih podataka. Provjerite je li vaš profil postavljen na privatno kako bi samo ljudi koje ste odabrali mogli vidjeti vaše objave. Izbjegavajte razmjenu povjerljivih informacija i dokumenata putem društvenih mreža.

## Edukacija

Edukacija je ključna za sigurnost na internetu. Stoga je važno da se stalno educirate o novim prijetnjama i rizicima te kako se zaštititi od njih. Postoje mnogi besplatni online resursi koji će vam pomoći da saznate više o online sigurnosti.

## Redovito ažuriranje softvera

Redovito ažurirajte softver na svojem računalu i mobilnom uređaju kako biste imali najnoviju zaštitu. Ažuriranja često uključuju popravke sigurnosnih propusta i poboljšanja zaštite.


## Oprema

Imajte u vidu da sve upute vrijede samo ako i fizički zaštitite svoje uređaje pa tako uvijek imajte lozinku za ulaz u vaše računalo ili mobitel te vodite računa o tome gdje ostavljate svoje uređaje.

# PRIDRŽAVATE LI SE OVIH SIGURNOSNIH MJERA U RADU?

Priručnik priredila Monika Kutri

Zagreb, svibanj 2023.