LIFELINE

FOR EMBATTLED CIVIL SOCIETY ORGANIZATIONS

DIGITAL SECURITY CHECKLIST FOR CIVIL SOCIETY ORGANIZATIONS

The following information is an excerpt from the Lifeline Toolkit for CSOs in Restrictive Space (www.csolifeline.org/advocacy-toolkit). This provides a brief overview of how civil society organizations can think about digital security in the context of engaging in advocacy campaigns.

Issue	Recommendations	Tip/Resource

Device Security	• Password protect your device
	• Update your operating system when prompted
	• Run anti-virus software
	• Back up your devices regularly
	• Delete sensitive information regularly (consider secure deletion software to wipe the device if applicable)
	• Don't plug devices into public USB ports or plug unknown USB flash drives to your device
	• Don't use untrusted public WiFi networks
	• Don't leave devices unattended in public/hotel/conference
		• Use password manager software to store your passwords: **Keepass**, **LastPass**, **Dashlane**
		• Free Antivirus: **Avira**, **AVG**, **Avast**, inbuilt Windows Defender
		• Delete your Data Securely: **Bleachbit**
		• Cloud backup:
		  • End-to-end encrypted cloud storage: **Tresorit**
		  • **Client-side encryption https://cryptomator.org/** for your cloud files

File / Disk encryption	• Enable full-disk encryption on your device • Use **Bitlocker** for windows, **Filevault** for Mac, or free open source disk encryption software – **VeraCrypt** • Most smartphones come with encryption enabled, check settings to confirm • If applicable, make sure to encrypt flash drives to protect the data in it	• With encryption ON, both your device and your password will be needed to unscramble the encrypted data • Helpful resource: "Keeping your Data Safe" **https://ssd.eff.org/en/module/keeping-your-data-safe**
Email + Social Media Safety	• Use strong passwords: **https://xkcd.com/936/** • Don't use the same password for more than one service • If supported, implement two-factor authentication • Be very careful clicking links or opening attachments	• Two-factor authentication (2FA) strengthens login security by requiring additional method of authentication • List of websites and whether or not they support Two Factor Authentication: **https://twofactorauth.org/**
Web-based end-to-end encrypted email services	End-to-End encrypted email means that only the sender and the recipient can read the messages exchanged and data shared between them.	Some free, web-based options: • **Protonmail** • **Tutanota** • **Hushmail**

The Lifeline Embattled CSO Assistance Fund provides emergency financial assistance to civil society organizations (CSOs) under threat or attack and rapid response advocacy and resiliency grants to support CSOs in responding to broader threats against civic space. For more information, please visit **https://www.csolifeline.org** or contact **info@CSOLifeline.org**. Find us on Twitter **@CSOLifeline**.

Issue	Recommendations	Tip/Resource
Encrypted email communication 	If you're concerned about online privacy and security of your communication, one of the common methods for encryption is called PGP. Based on public key cryptography, PGP can make sure that your data is safe from prying eyes, and that only intended audience can read the content of your communication	• Pretty Good Privacy (**PGP encryption**) explained, Thunderbird guide: **https://guides.accessnow.org/tag_pgp.html** • **Mailvelope** (browser plugin) • List of email applications that **support OpenPGP standard: https://www.openpgp.org/software/**
Encrypted messaging apps 	• Be aware of which apps are the most secure for your particular country/region: **https://securityinabox.org/en/guide/secure-communication/**: user data and privacy, metadata, recent security news. (Signal App has the highest standards as of October 2019) • Review privacy and security settings of each application. • Even if you use the most secure apps, there is a chance someone might get your sensitive conversations or personal files because it was stored somewhere on your device. It is essential to create a process for revising the app content and deleting sensitive messages regularly (e.g. use disappearing message function if possible)	• Secure your mobile device **https://securityinabox.org/en/guide/smartphones/** • Thinking about what you need in a secure messenger **https://www.eff.org/deeplinks/2018/03/thinking-about-what-you-need-secure-messenger** • Signal, the secure messaging app **https://freedom.press/training/locking-down-signal/** • Whatsapp safety tips (has some security issues) **https://www.whatsapp.com/safety** • How to secure messaging apps **https://guides.accessnow.org/IM_Tips.html**
Safe Browsing 	• Update your Browser version regularly. • Check website authenticity (look at the link, HTTPS icon at the start). • Make your browsing more secure: **https://www.eff.org/https-everywhere** • Use VPN to protect your browsing information from prying eyes (especially if using public / shared Wi-Fi).	VPN is an encrypted tunnel between two devices that lets you access every website and online service privately and securely. • VPN comparison guide **https://thatoneprivacysite.net/** • Run your own VPN **https://getoutline.org/en/home**