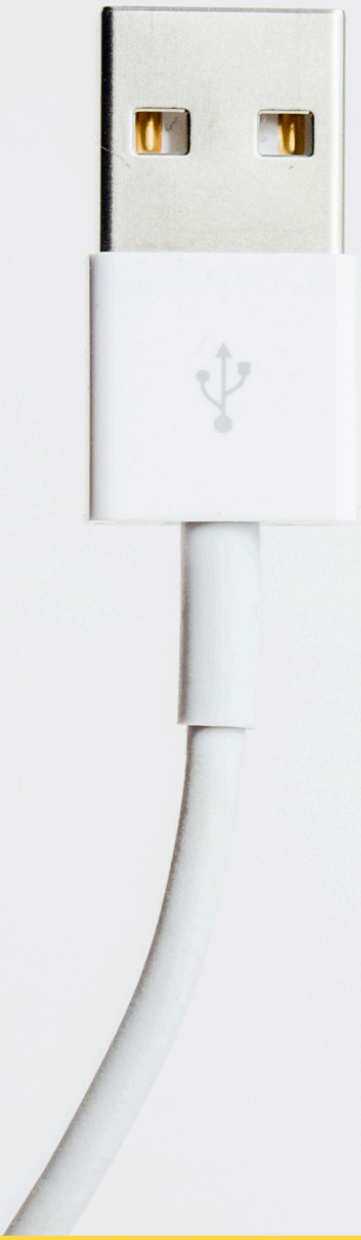
Digital Security Toolkit for Somali Civil Society



Somalia Non-State Actors
SONSA
Jiilayaasha aan Dowliga aheyn ee Soomaaliyeed

OXFAM

Table of Contents

About this Digital Toolkit

Somalia's people are increasingly connected in digital spaces, using technology to express their rights, organize their communities, and share their stories. However, these digital environments also come with risks. From stolen accounts and phishing scams to online harassment and data loss, everyone remains vulnerable in the online world.

This Digital Security Toolkit, created under the EU-cofunded ReCIPE project by SONSA and Oxfam, provides practical, trusted, and easy-to-use tools to help Somali civil society partners operate securely and safely online. It is designed to address critical risks including account takeovers, phishing, malware, and online harassment.

- **What the tool does ?**
- **Why it matters for your safety ?**
- **Where to download or use it ?**

What You'll Find in This Handbook

Essential Digital Security Tools	→	**carefully selected apps and services that protect your communication, data, and devices.**
Simple Guidance for Use	→	**step-by-step notes on where to find each tool and how to get started.**
Quick Safety Standards	→	**practical actions that raise your organization's minimum level of protection.**
Resources for Response & Support	→	**help with phishing, online harassment, misinformation, and peer collaboration.**

Secure, Private Communication

Why This Matters

To operate safely, Somali CSOs must address frequent account takeovers—a primary threat caused by weak or reused passwords. Multi-factor authentication (MFA) is an essential second layer of protection. For teams in sensitive environments, adopting strong passwords alongside MFA is vital to safeguard operations, protect staff, and maintain the trust of your communities and partners.

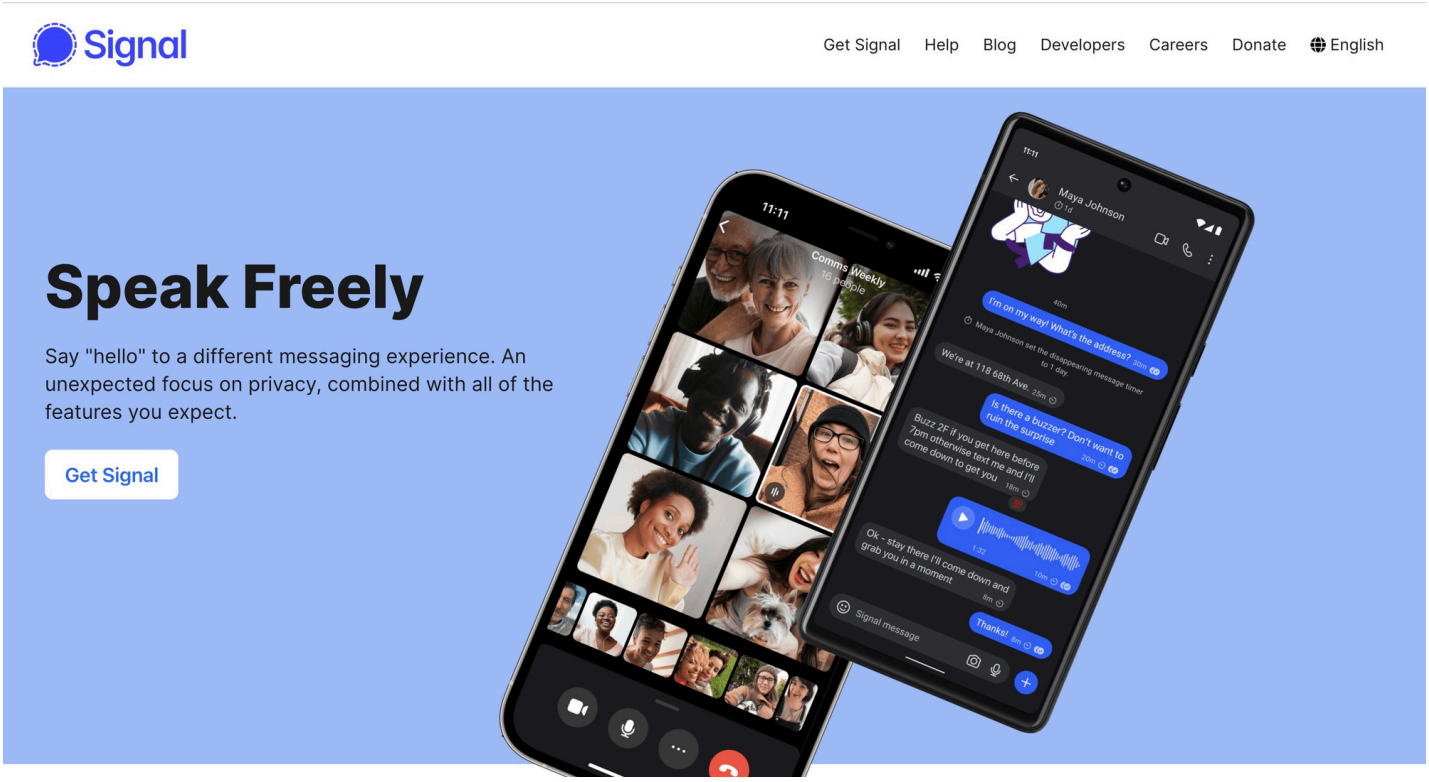
Using simple or repeated passwords across multiple accounts leaves your organization vulnerable, allowing a breach on one platform to compromise critical emails, donor information, or advocacy plans.

Multi-factor authentication (MFA) adds an essential extra layer of protection by requiring not only a password but also a second verification step, such as a code sent to your phone or a physical security key. This significantly reduces the risk of unauthorized access and helps keep your communications and data safe.

For CSOs operating in complex and sensitive environments, adopting strong passwords alongside MFA is vital to safeguarding your operations, protecting staff, and maintaining the trust of your communities and partners.

Below are trusted tools designed to generate strong, unique passwords and manage MFA codes securely, empowering your organization to defend against digital threats with confidence.

Signal



Quick Look

Signal is a free, open-source messaging app that delivers end-to-end encryption for text messages, voice calls, and video calls, ensuring communication remains private and secure.

Built with privacy as its core principle, Signal does not track, collect, or sell user data, earning global recognition as one of the most secure messaging platforms available.

The app is simple to install and works seamlessly across Android, iOS, and desktop devices. Its clean design, strong security protocols, and consistent reliability make Signal a trusted choice for confidential communication. For Somali CSOs: Use Signal for all internal organizational communication and for sensitive conversations with partners to protect against interception.

Features

Signal is a secure messaging app designed to keep your communication private and protected through robust encryption and user-focused features:

- **Offers end-to-end encryption for messages, voice calls, and video calls, ensuring complete privacy.**
- **Supports disappearing messages to automatically delete sensitive content after a set time.**
- **Includes a customizable security PIN to add an extra layer of account protection.**
- **Provides safety numbers to verify contacts, protecting against impersonation and interception.**

How to Use

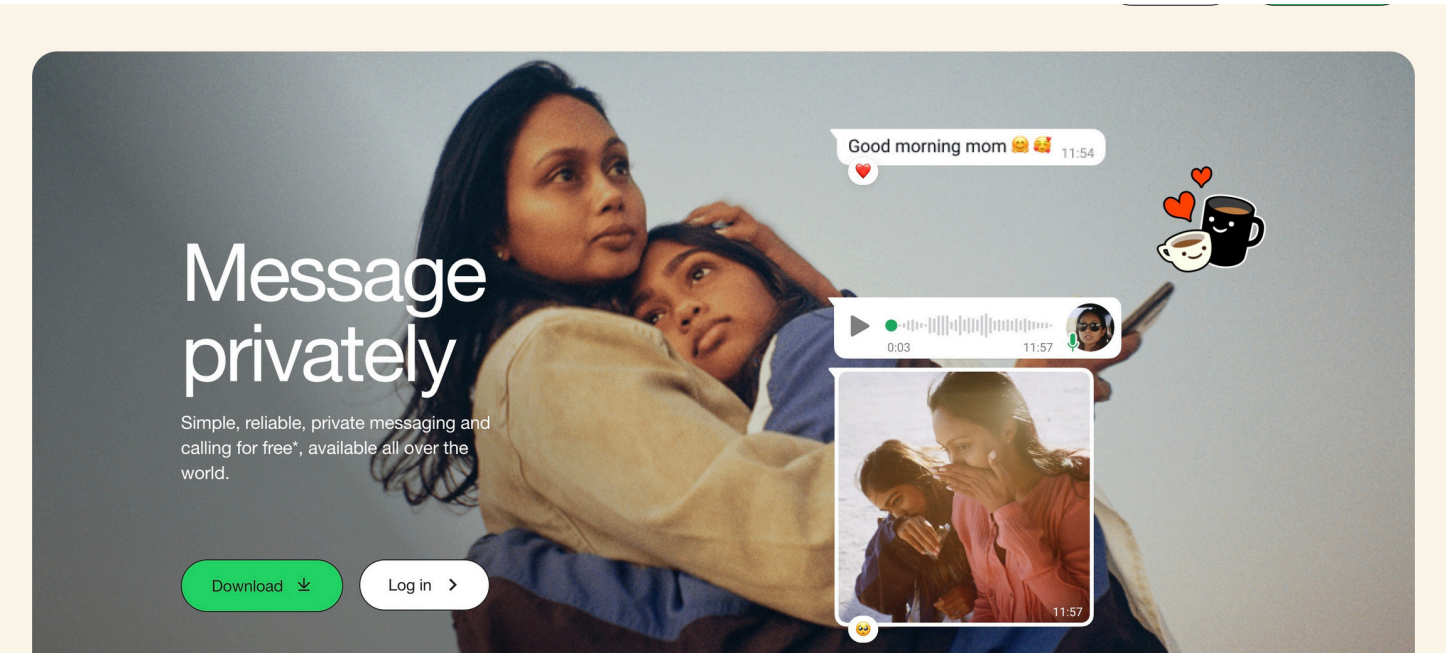
Follow these instruction on your smart phone:

Android

- **Open Google Play Store (Android)**
- **Search for Signal, and then download**
- **Enable safety PIN**

- **Open App Store**
- **Search for Signal, and then download**
- **Enable safety PIN**

WhatsApp



Quick Look

WhatsApp is Somalia's most widely used messaging platform, making it a central tool for everyday communication across communities, families, and organizations.

The app secures chats, voice, and video calls with end-to-end encryption, ensuring privacy while remaining simple and accessible.

Its broad adoption makes it practical for public outreach and general communication. However, for sensitive discussions on advocacy, finances, or beneficiary data, we recommend using more secure tools like Signal to minimize risks. With millions relying on it daily, WhatsApp remains a dependable space for public engagement.

By using the app with care and awareness, it remains a reliable and trusted option for secure interaction across mobile and desktop devices.

Features

WhatsApp is a versatile messaging app designed to enhance communication with powerful privacy, security, and user-friendly features:

- **Offers end-to-end encryption for messages, voice calls, and video calls, ensuring your conversations remain private and secure.**
- **Supports disappearing messages that automatically delete sensitive content after a chosen time to maintain privacy.**
- **Provides direct encrypted chat transfers, allowing you to switch devices quickly and securely without relying on cloud backups.**
- **Enables two-step verification with a safety PIN, adding extra protection against account hijacking and unauthorized access.**

How to Use

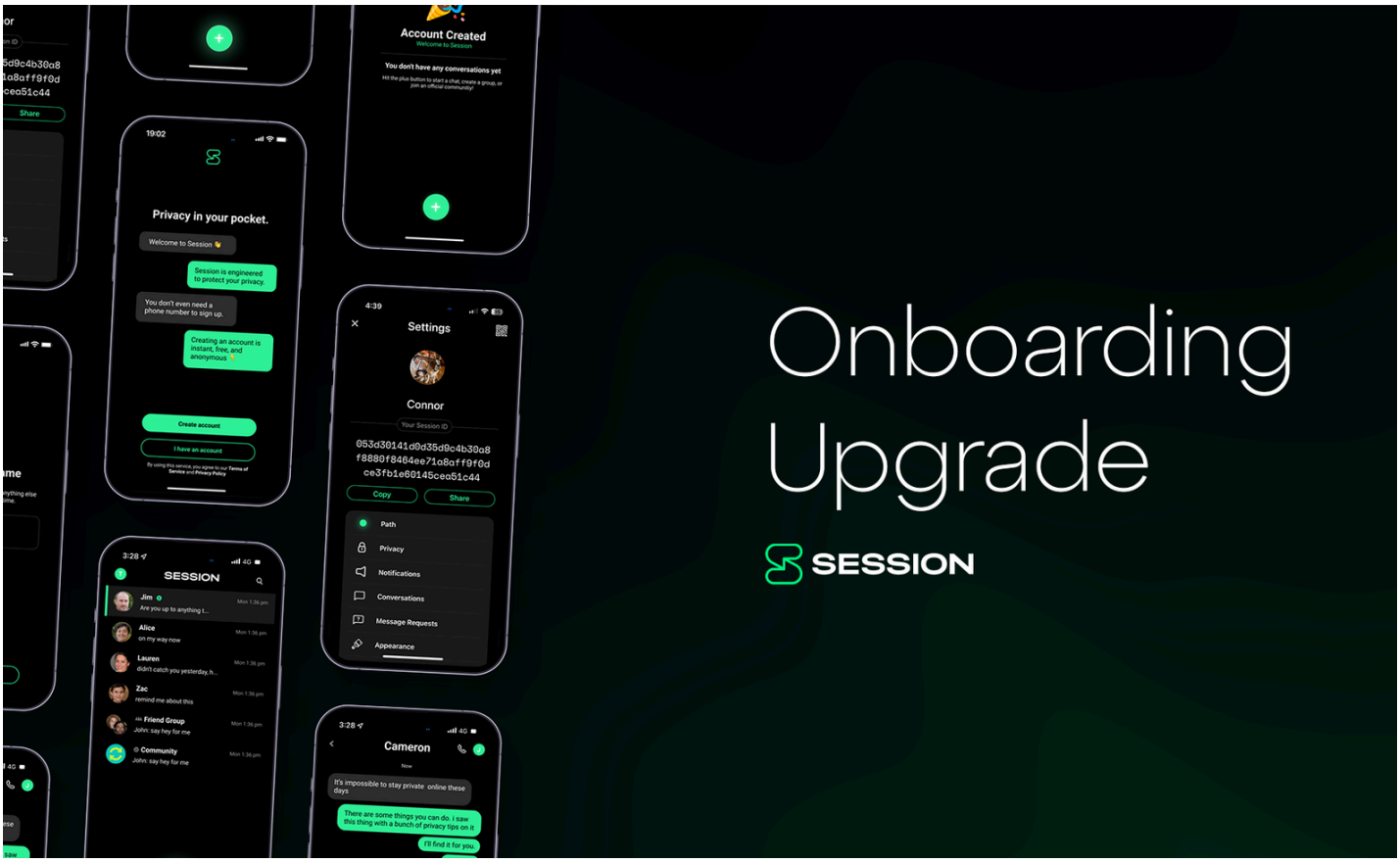
Follow these instruction on your smart phone:

Android

- **Open Google Play Store (Android)**
- **Search for Whatsapp, and then download**
- **Register with your phone number**

- **Open App Store (iOS)**
- **Search for Whatsapp, and then download**
- **Register with your phone number**

Session



Quick Look

Session is a privacy-first messaging app that provides end-to-end encryption without requiring a phone number, email, or any other personal information. Instead, it generates a unique anonymous Session ID, allowing users to communicate securely without linking their identity or personal details.

Built on a decentralized, blockchain-inspired network, Session minimizes metadata collection and protects against surveillance, ensuring private and secure messaging. It supports one-on-one chats, group messaging, encrypted voice calls, and file sharing. Available on desktop and mobile platforms, Session is designed for individuals and organizations that prioritize privacy, anonymity, and secure digital communication.

Features

Session is a private, decentralized messaging app designed to maximize user anonymity and security while eliminating metadata collection:

- **Uses end-to-end encryption with the Signal-inspired Session Protocol and routes messages through a decentralized onion routing network for enhanced anonymity.**
- **Does not require a phone number or email to sign up; users create a unique Session ID for private, anonymous communication.**
- **Supports disappearing messages to automatically delete sensitive content after a chosen time for improved privacy.**
- **Available on desktop and mobile platforms, allowing secure messaging across devices seamlessly.**

How to Use

Follow these instruction on your smart phone:

Android

- **Open Google Play Store (Android)**
- **Search for Session, and then download**
- **Register with your phone number**

- **Open App Store (iOS)**
- **Search for Session, and then download**
- **Register with your phone number**

Element

Quick Look

Element is a secure, privacy-first messaging platform built on the Matrix protocol, designed for individuals, teams, and organizations seeking reliable, end-to-end encrypted communication without surveillance. It provides encrypted one-on-one and group messaging, voice and video calls, and seamless file sharing.

Being open-source and decentralized, Element avoids vendor lock-in and ensures full transparency. It supports federated communication, meaning users can connect smoothly across different servers.

With robust privacy measures and strong encryption, Element is ideal for civil society groups, journalists, and human rights defenders operating in sensitive and high-risk contexts around the world.

Features

Element offers secure, open-source communication designed for both individuals and organizations:

- **End-to-end encryption ensures privacy for one-on-one chats, group discussions, voice and video calls, and secure file sharing across all devices.**
- **Collaboration tools allow users to create large rooms, coordinate projects, and connect with federated Matrix servers for a broader network.**
- **Integration bridges seamlessly link Element with platforms like Slack, WhatsApp, and Signal, providing flexibility while maintaining security and transparency through its open-source foundation.**

How to Use

Follow these instruction on your smart phone:

Android

- **Open Google Play Store (Android)**
- **Search for Element, and then download**
- **Tap Install and follow on-screen setup instructions.**

- **Open App Store (iOS)**
- **Search for Element, and then download**
- **Tap Install and follow on-screen setup instructions.**

Password Hygiene & Multi-Factor Authentication

Why This Matters

To combat account hijacking and data theft—persistent threats for Somali CSOs—using secure communication tools is non-negotiable. When advocacy plans or community data are shared through vulnerable apps, they can be intercepted. This can lead to loss of trust, reputational damage, and compromised safety. The tools below ensure your messages and files remain confidential.

When advocacy plans, community data, or internal communications are shared through weak or vulnerable apps, they become susceptible to interception, unauthorized access, or misuse. This can result in serious consequences such as loss of trust, reputational damage, compromised safety of staff and beneficiaries, or even financial harm.

Using secure communication tools is critical for safeguarding organizational operations and sensitive exchanges.

Whether you are coordinating projects, mobilizing communities, planning advocacy strategies, or engaging with stakeholders, reliable encrypted apps offer peace of mind. These tools ensure that your messages, calls, and shared files remain confidential and fully under your control.

Below is an overview of trusted, widely used communication apps that help CSOs protect their privacy and maintain security in their daily work, empowering you to operate with confidence and safety.

Bitwarden

Quick Look

Bitwarden is a secure, open-source password manager that directly addresses account takeovers caused by weak credentials. It generates, stores, and automatically fills strong, unique passwords across all your devices and browsers, simplifying password management and reducing the risk of password reuse. For Somali CSOs: This tool is your first line of defense against the primary threat of account hijacking.

All data stored within Bitwarden is protected by end-to-end encryption, meaning only you have access to your vault.

As a transparent, auditable, and community-reviewed platform, Bitwarden is an essential tool for closing critical security gaps and protecting sensitive accounts from unauthorized access, data breaches, and cyber threats in today's digital landscape.

Features

Bitwarden offers several key features that make it an effective tool for managing passwords securely:

- **Stores and syncs strong, unique passwords across all your devices.**
- **Includes a built-in password generator for creating secure passwords.**
- **Provides encrypted vaults and browser extensions for quick and easy logins.**
- **Uses end-to-end encryption to keep all stored data private and protected from unauthorized access.**

How to Use

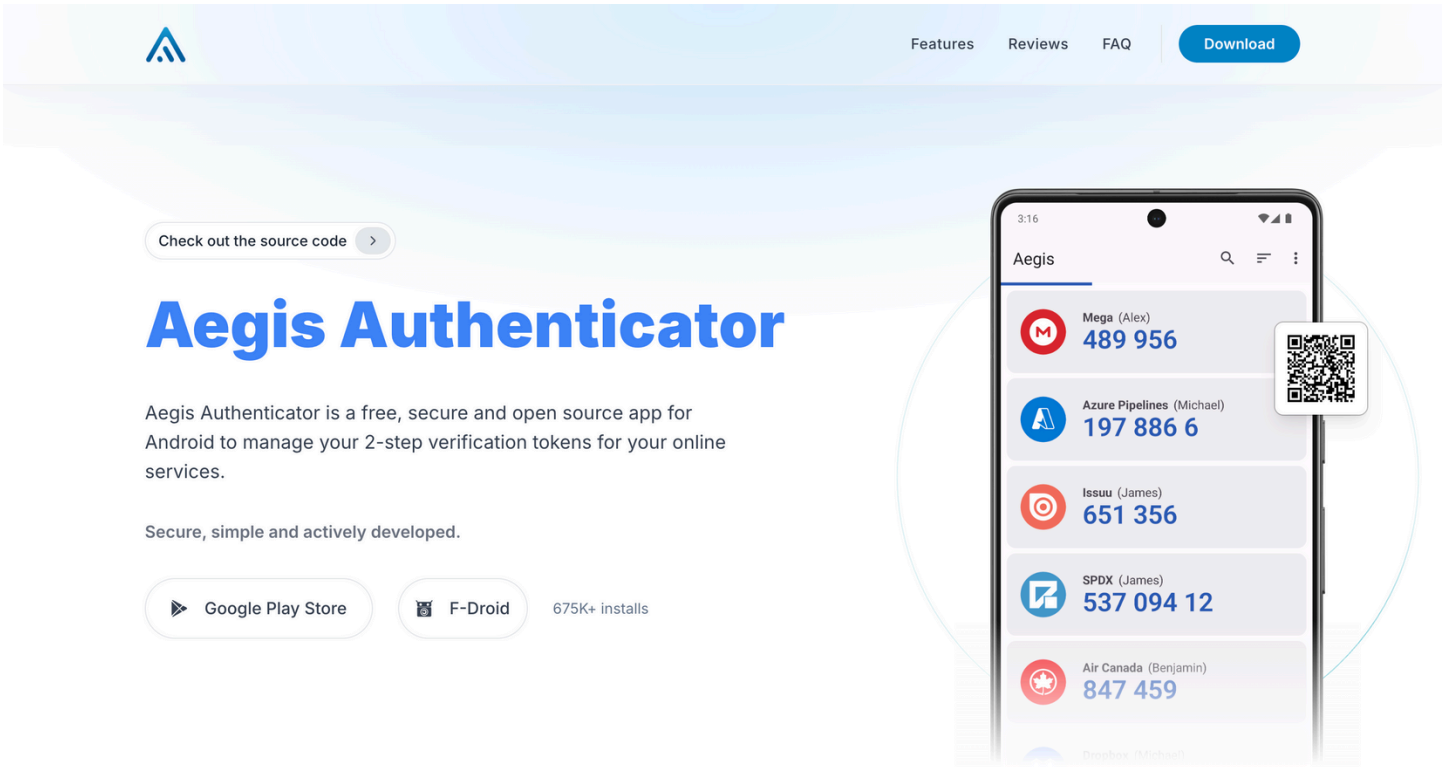
Follow these instruction on your smart phone:

Android

- **Open Google Play Store (Android)**
- **Search for Bitwarden, and then download**
- **Open the app and tap Create Account; enter your email and create a master password**
- **Check your email and click the verification link from Bitwarden.**

- **Open App Store (iOS)**
- **Search for Bitwarden, and then download**
- **Open the app and tap Create Account; enter your email and create a master password**
- **Check your email and click the verification link from Bitwarden.**

Aegis



Quick Look

Aegis is a free, open-source authenticator app for Android that enhances your two-factor authentication (2FA) security by generating offline one-time passcodes.

Unlike SMS codes, Aegis does not require internet or mobile networks, making it more secure against interception and phishing. It encrypts your token vault and allows encrypted backups, ensuring your accounts remain safe and accessible even if your device is lost or replaced.

Aegis offers an easy and reliable way to manage multiple 2FA accounts securely.

Features

Aegis offers key features that make it a reliable and secure authenticator app for managing two-factor authentication (2FA):

- **Generates secure one-time passcodes offline, eliminating dependence on internet or SMS.**
- **Encrypts your token vault to protect sensitive authentication data.**
- **Allows encrypted backups to keep tokens safe and accessible if your device is lost or replaced.**

How to Use

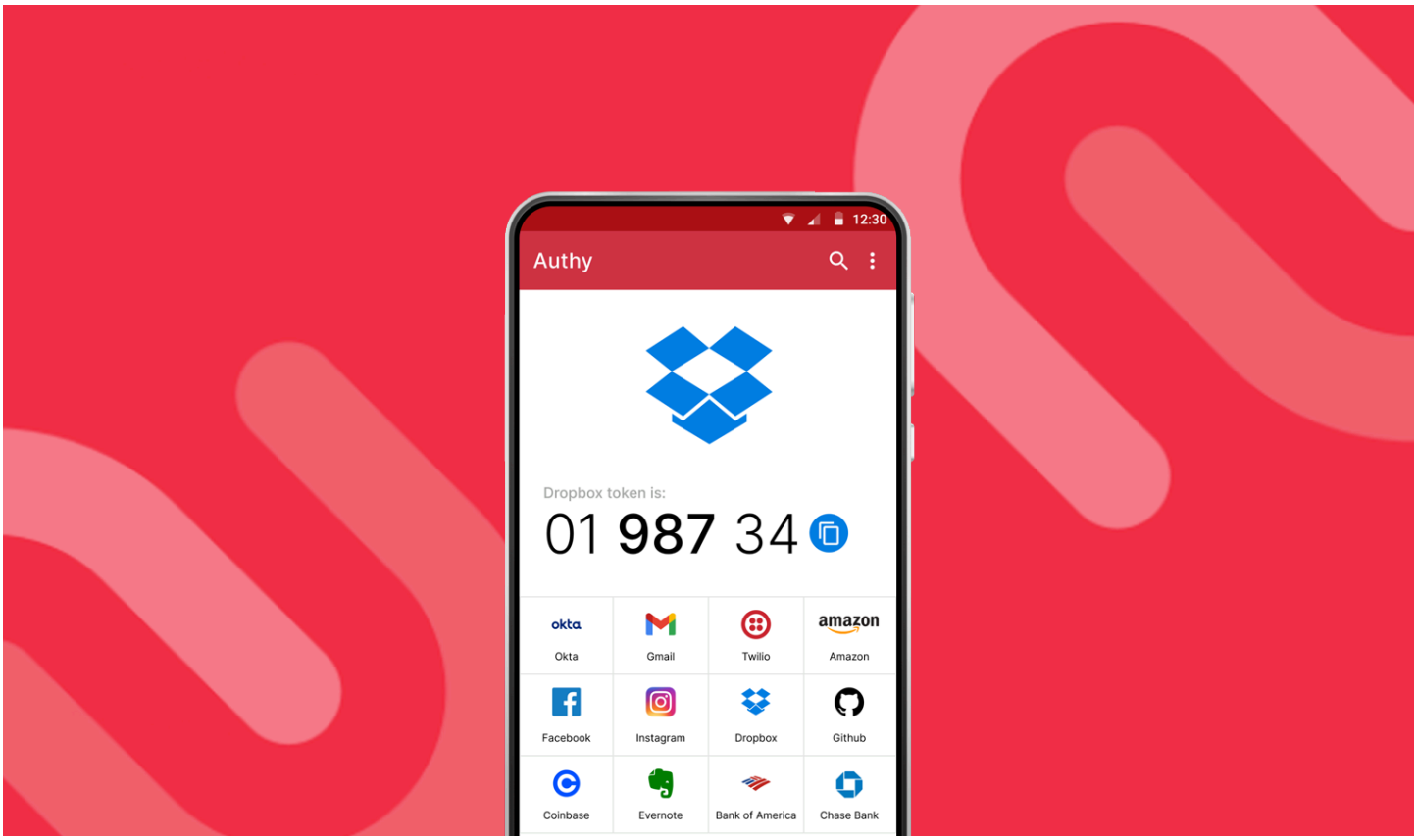
Follow these instruction on your smart phone:

Android

- **Open Google Play Store (Android)**
- **Search for Aegis, and then download**
- **Once installation is complete, open the app from your home screen or app drawer.**
- **Upon opening, you can begin adding your two-factor authentication (2FA) accounts by scanning QR codes or manually entering codes provided by your online accounts.**

- **Open App Store (iOS)**
- **Search for Aegis, and then download**
- **Once installation is complete, open the app from your home screen or app drawer.**
- **Upon opening, you can begin adding your two-factor authentication (2FA) accounts by scanning QR codes or manually entering codes provided by your online accounts.**

Authy



Quick Look

Authy is a free, user-friendly two-factor authentication (2FA) app that enhances your account security by generating time-based one-time passcodes (TOTPs).

Compatible with multiple devices, Authy securely syncs your tokens across smartphones, tablets, and desktops, ensuring access even if a device is lost or replaced. It offers encrypted cloud backups protected by your password, simplifying recovery.

Authy supports offline code generation, eliminating reliance on cellular or internet connectivity. The app provides push notifications for easy approvals and an intuitive interface, making it a reliable solution to protect online accounts from unauthorized access and cyber threats.

Features

Authy provides robust features to simplify and secure your two-factor authentication (2FA):

- **Generates secure one-time passcodes for 2FA across multiple devices.**
- **Supports cloud backups encrypted with your password, enabling easy recovery if your device is lost or replaced.**
- **Syncs tokens securely across smartphones, tablets, and desktops for seamless access.**

How to Use

Follow these instruction on your smart phone:

Android

- **Open the Google Play Store (Android) on your device.**
- **Search for Authy and install the official app by Twilio.**
- **Open Authy, enter your phone number, and follow the on-screen prompts to set up your account.**
- **Authy will verify your number via SMS or call; complete verification to start using the app.**

- **Open the App Store (iOS) on your device.**
- **Search for Authy and install the official app by Twilio.**
- **Open Authy, enter your phone number, and follow the on-screen prompts to set up your account.**
- **Authy will verify your number via SMS or call; complete verification to start using the app.**

Device hardening & Backups

Why This Matters

Inconsistent data-backup practices leave critical organizational information vulnerable to loss or ransom. Without robust device hardening and secure backups, CSOs risk operational interruptions, reputational damage, and financial setbacks that undermine their missions. Implementing these practices is a critical strategic priority for resilience.

When mission-critical data and communications are exposed, organizations risk operational interruptions, reputational damage, and financial setbacks that can undermine their missions. Therefore, implementing comprehensive device protection combined with encrypted, automated backup solutions is not merely a technical requirement but a critical strategic priority for CSOs committed to resilience and trustworthiness.

Whether managing confidential reports, preserving historical documentation, or securing communications, adopting these security practices equips CSOs to operate confidently and sustainably in increasingly hostile digital environments.

Below is an overview of trusted device hardening and backup tools widely used by CSOs to enhance security and safeguard vital information.

VeraCrypt

VeraCrypt

Quick Look

Veracrypt is a free, open-source encryption software designed to secure your data by creating encrypted volumes or encrypting entire disks.
It offers strong protection for sensitive information, making unauthorized access extremely difficult.

Veracrypt supports multiple operating systems, including Windows, macOS, and Linux, providing flexibility for various user environments.

The software uses advanced encryption algorithms to safeguard files, ensuring data confidentiality even if a device is lost or stolen. Veracrypt allows users to create hidden volumes for added privacy and offers plausible deniability features.

Features

Veracrypt is a powerful open-source encryption tool that helps protect sensitive data by encrypting entire disks or creating secure encrypted volumes.

- **Encrypts full disks, partitions, or creates encrypted containers for flexible data protection**
- **Supports Windows, macOS, and Linux for broad platform compatibility**
- **Enables pre-boot authentication to protect system drives before startup**

How to Use

Please follow the instructions for your preferred desktop operating system below.

- **Visit the official website: https://www.veracrypt.fr**
- **Go to the "Downloads" section and choose the version for Windows**
- **Download the installer file for your OS**
  - **Windows: Download the .exe installer.**
- **Install the software:**
- **Windows: Double-click the .exe file, then follow the setup wizard to complete installation.**

- **Visit the official website: https://www.veracrypt.fr**
- **Go to the "Downloads" section and choose the version for macOS.**
- **Download the installer file for your OS**
  - **macOS: Download the .dmg installer.**
- **Install the software:**
- **MacOS: Open the .dmg file, drag VeraCrypt into the Applications folder, and if prompted, allow it in System Settings → Privacy & Security.**

ClamAV

Quick Look

ClamAV is a free, open-source antivirus software specifically designed to detect, identify, and block a wide range of malware threats on multiple operating systems, including Windows, macOS, and Linux.

It provides reliable on-demand and scheduled scanning capabilities, as well as real-time file monitoring to ensure continuous protection. ClamAV maintains an extensive and constantly updated virus definition database to combat the latest malware and viruses effectively.

The software integrates smoothly with email servers to automatically scan incoming and outgoing messages for viruses. Its lightweight design ensures minimal impact on system performance, making it suitable for personal devices and large-scale network environments requiring efficient malware defense.

Features

ClamAV is a free, open-source antivirus software that offers reliable malware detection across multiple platforms. Key features include:

- **Supports Windows, macOS, and Linux operating systems**
- **Offers real-time file monitoring for continuous protection**
- **Integrates with email servers for automated virus scanning**

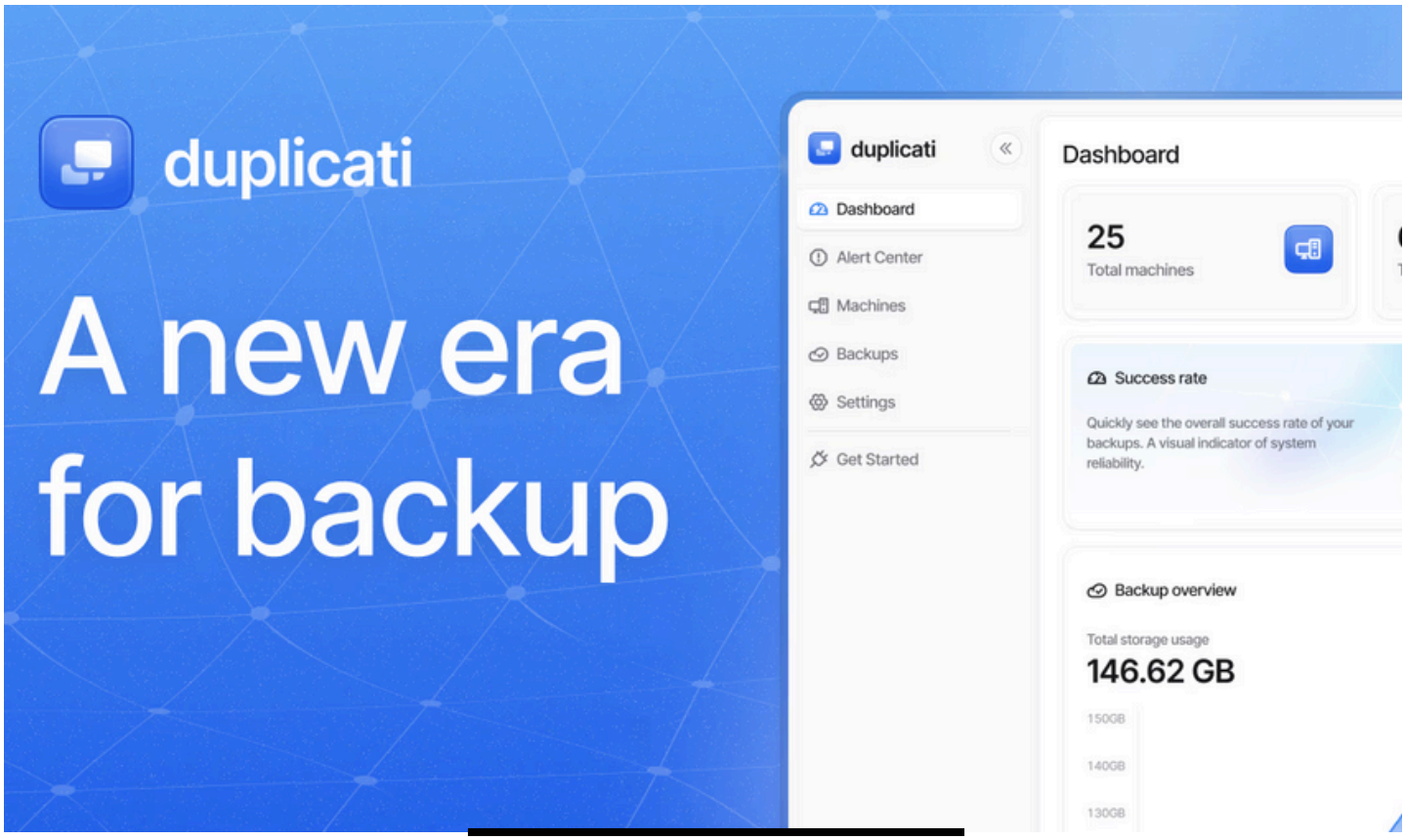
How to Use

Please follow the instructions for your preferred desktop operating system below:

- **Visit the official website: https://www.clamav.net**
- **Go to the "Downloads" section and select the latest Windows version**
- **Download the installer file for your OS:**
  - **Windows: Download the .exe installer.**
- **Install the software:**
  - **Windows: Double-click the .exe file and follow the setup wizard to complete the installation.**
- **Update virus definitions after installation to ensure the latest protection**
- **Run the command or use the built-in updater to download the latest virus signatures.**

- **Visit the official website: https://www.clamav.net**
- **Go to the "Downloads" section and select the version for macOS**
- **Download the installer file for your OS:**
  - **macOS: Download the .pkg installer.**
- **Install the software:**
  - **macOS: Open the .pkg file and follow the installation steps. If prompted, allow installation under System Settings → Privacy & Security.**
- **Update virus definitions after installation to ensure the latest protection**
- **Run the command or use the built-in updater to download the latest virus signatures.**

Duplicati



Quick Look

Duplicati is a free, open-source backup software designed to securely store encrypted backups of your data on local drives, cloud storage services, or remote servers.

It provides flexible, automated backup scheduling and supports incremental backups to save storage space and reduce transfer times. Duplicati uses strong encryption standards to protect sensitive data during storage and transmission, ensuring privacy and security.

The software offers easy restoration of files, versioning support to recover previous file states, and compatibility with multiple platforms including Windows, macOS, and Linux. Its lightweight and efficient design makes it suitable for both personal use and larger network environments that require reliable and secure backup solutions.

Features

Duplicati is a free, open-source backup software that provides secure and efficient data backup solutions for multiple platforms. Key features include:

- Supports Windows, macOS, and Linux operating systems
- Performs encrypted, incremental, and compressed backups to save space and enhance security
- Supports a wide range of storage options, including local drives, NAS, and cloud services (e.g., Google Drive, OneDrive, Amazon S3)

How to Use

Please follow the instructions for your preferred desktop operating system below:

- **Visit the official website: https://www.duplicati.com**
- **Go to the "Download" section and select the latest version for Windows**
- **Download the .msi installer.**
- **Install the software: Double-click the .msi file, then follow the setup wizard to complete installation.**

- **Visit the official website: https://www.duplicati.com**
- **Go to the "Download" section and select the latest version for macOS**
- **Download the .dmg installer.**
- **Install the software: Open the .dmg file, drag Duplicati into the Applications folder, and if prompted, allow it in System Settings → Privacy & Security.**

Privacy & Circumvention

Why This Matters

In environments where online monitoring, censorship, and pervasive tracking threaten operational security, civil society organizations face elevated risks of exposure and compromised confidentiality.

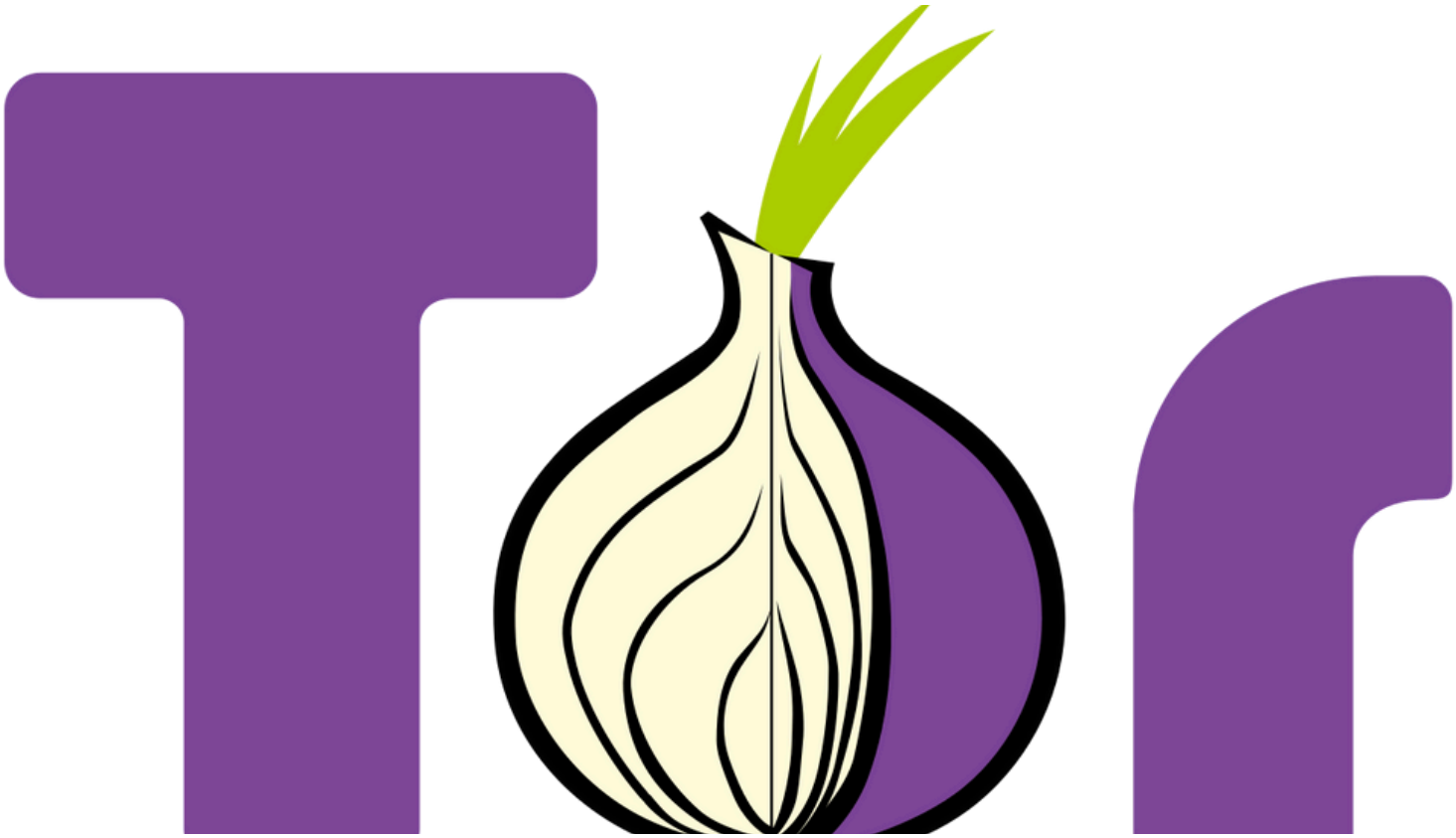
Without robust privacy measures and circumvention tools, CSOs may encounter surveillance, data interception, and restricted access to critical information—jeopardizing both staff safety and advocacy efforts.

When private browsing habits, communications, and research activities are unprotected, organizations risk data leaks, targeted harassment, and loss of stakeholder trust. Therefore, integrating strong privacy solutions alongside reliable circumvention strategies is not simply a technical safeguard but an essential step for CSOs committed to transparency, security, and digital resilience.

Whether safeguarding sensitive communications, bypassing network restrictions, or preventing intrusive tracking, these measures empower CSOs to operate freely, securely, and effectively, even in high-risk or monitored digital spaces.

Below is an overview of trusted privacy and circumvention tools widely recommended for CSOs to maintain confidentiality and ensure unrestricted access to information.

Tor Browser



Quick Look

Tor Browser is a free, open-source web browser designed to provide anonymous and secure internet browsing by routing traffic through the Tor network's onion relays.

It helps protect user privacy by hiding IP addresses and circumventing internet censorship, allowing access to otherwise restricted or monitored content. Tor Browser blocks trackers and defends against surveillance techniques, ensuring safer browsing on monitored or filtered networks.

The browser is built on a modified version of Firefox and is available on multiple platforms including Windows, macOS, Linux, and Android. Its user-friendly design makes it accessible for both personal and professional use, especially for those in high-risk environments requiring strong online privacy protections.

Features

Tor Browser is a free, open-source web browser that prioritizes user privacy and online anonymity. Key features include:

- **Supports multiple platforms including Windows, macOS, Linux, and Android**
- **Routes internet traffic through the Tor network using onion relays to anonymize user location and activity**
- **Blocks trackers, ads, and surveillance scripts to enhance privacy and reduce tracking**

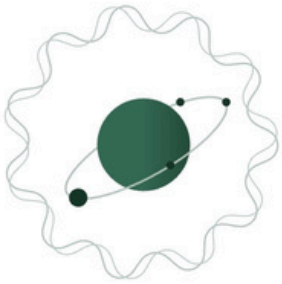
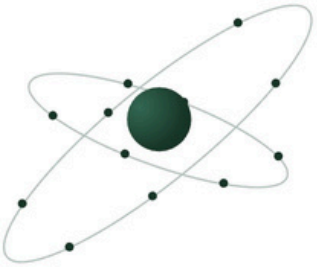
How to Use

Please follow the instructions for your preferred desktop operating system below:

- **Visit the official website: https://www.torproject.org**
- **Click on the "Download" button on the homepage.**
- **Select the latest version of Tor Browser compatible with Windows**
- **Download the installer file for Windows.**
- **Install the software: Double-click the downloaded installer and follow the installation prompts.**
- **Launch Tor Browser and begin browsing anonymously by connecting to the Tor network.**

- **Visit the official website: https://www.torproject.org**
- **Click on the "Download" button on the homepage.**
- **Select the version of Tor Browser compatible with your macOS:**
- **Download the installer file for macOS**
- **Install the software: Open the downloaded .dmg file, then drag Tor Browser into the Applications folder.**
- **Launch Tor Browser and begin browsing anonymously by connecting to the Tor network.**

Outline VPN


Quick Look

Outline VPN is a free, open-source VPN software designed to provide easy and secure access to the internet through a self-hosted Shadowsocks proxy. It allows users to create and manage their own VPN servers without relying on third-party providers, ensuring greater control over privacy and data.

Outline VPN is particularly useful for circumventing internet censorship and enhancing online security by encrypting internet traffic.

The software is simple to set up and manage, with clients available for multiple platforms including Windows, macOS, Android, and iOS. Its lightweight design and user-friendly interface make it suitable for individuals and organizations needing reliable VPN access.

Features

Outline VPN is a free, open-source VPN software that enables users to create and manage their own secure, self-hosted VPN servers with ease. Key features include:

- **Supports Windows, macOS, Android, and iOS platforms**
- **Allows users to set up self-hosted Shadowsocks VPN servers for enhanced privacy and control**
- **Encrypts internet traffic to protect against surveillance and censorship**
- **Offers a simple, user-friendly interface for easy server management and client connection**

How to Use

Please follow the instructions for your preferred operating system below:

- **Visit the official website: https://getoutline.org**
- **Click on the “Get Outline” button on the homepage.**
- **Select the latest version of Outline Client compatible with Windows.**
- **Download the installer file for Windows.**
- **Install the software: Double-click the downloaded installer and follow the installation prompts.**
- **Launch Outline VPN Client and connect using your access key to start browsing securely.**

- **Visit the official website: https://getoutline.org**
- **Click on the “Get Outline” button on the homepage.**
- **Select the latest version of Outline Client compatible with macOS.**
- **Download the installer file for macOS.**
- **Install the software: Open the downloaded .dmg file, drag the Outline Client icon to your**
- **Launch Outline VPN Client and connect using your access key to start browsing securely.**

uBlock Origin

Quick Look

uBlock Origin is a free, open-source browser extension designed to efficiently block ads, trackers, and malicious content to enhance user privacy and web browsing speed.

It offers users control over what content is blocked, reducing intrusive ads and preventing tracking scripts from monitoring online behavior. uBlock Origin is lightweight and highly customizable, making it suitable for both casual users and advanced users who want fine-tuned control over their browsing experience.

The extension supports popular browsers including Chrome, Firefox, Edge, and Opera, and helps protect users working on monitored or filtered networks by blocking unwanted content.

Features

uBlock Origin is a free, open-source browser extension that provides efficient and customizable ad and tracker blocking to improve browsing speed and privacy. Key features include:

- Supports Chrome, Firefox, Edge, and Opera browsers
- Blocks ads, trackers, and malware domains to enhance security and privacy
- Allows use of custom filter lists and user-defined rules for advanced control
- Speeds up page loading by preventing unwanted content from downloading

How to Use

Please follow the instructions for your preferred internet browser below:

- **Visit the official Chrome Web Store page: uBlock Origin for Chrome**
- **Click on the “Add to Chrome” button.**
- **Confirm by clicking “Add Extension” in the pop-up window.**
- **Once installed, you will see the uBlock Origin icon appear in your browser toolbar.**

- **For Mozilla Firefox**
- **Visit the official Firefox Add-ons page: uBlock Origin for Firefox**
- **Click on the “Add to Firefox” button.**
- **Confirm by clicking “Add” in the permission pop-up.**
- **After installation, the uBlock Origin icon will appear in your Firefox toolbar.**

Encrypted Email

Why This Matters

In contexts where email communications are exposed to interception, surveillance, and unauthorized access, civil society organizations face significant threats to their confidentiality and operational integrity.

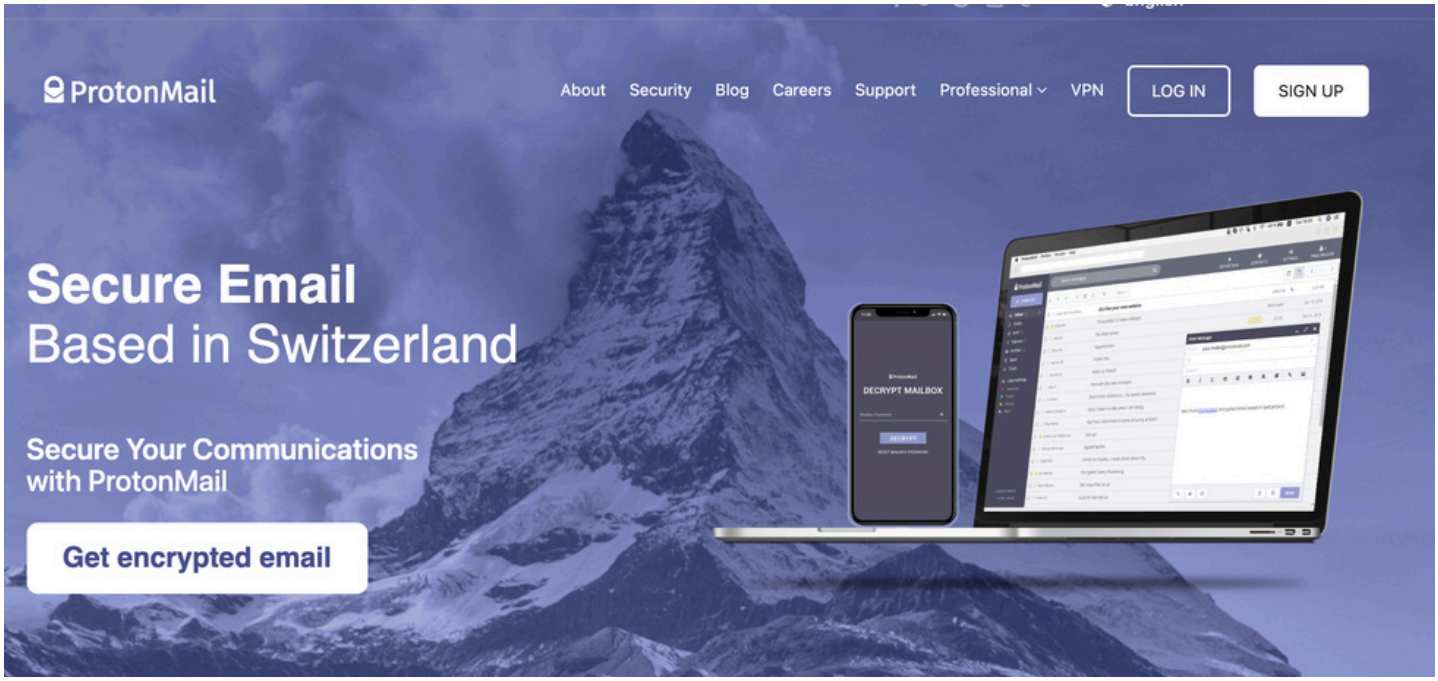
Without reliable encrypted email services, sensitive information exchanged via email—such as advocacy plans, donor data, or whistleblower reports—can be exposed, leading to compromised safety, reputational damage, and legal challenges.

When email communications lack robust encryption, organizations risk data breaches, targeted attacks, and erosion of trust among stakeholders and beneficiaries. Therefore, adopting strong encrypted email solutions is more than a technical necessity; it is a fundamental component of CSO digital security and accountability.

By ensuring end-to-end encryption, secure storage, and access controls, encrypted email services enable CSOs to communicate with confidence, protect sensitive data, and maintain compliance with privacy standards—even in hostile or surveilled environments.

Below is an overview of trusted encrypted email providers widely recommended for CSOs to uphold data confidentiality and secure communication channels.

ProtonMail



Quick Look

ProtonMail is a secure, privacy-focused email service that provides end-to-end encryption to protect users' email communications from unauthorized access.

It is designed to ensure that only the sender and recipient can read the contents of emails, preventing interception by third parties, including ProtonMail itself. ProtonMail offers user-friendly encrypted email with features such as zero-access architecture, open-source cryptography, and strong data protection based in Switzerland.

The service is accessible via webmail and dedicated mobile apps, supporting multiple platforms and making encrypted communication easy for both individuals and organizations.

Features

ProtonMail offers secure and private email communication with the following key features:

- **End-to-end encryption ensuring only sender and recipient can access email contents**
- **Zero-access architecture preventing ProtonMail staff from reading user emails**
- **Open-source cryptographic protocols for transparency and security**
- **Servers located in Switzerland with strong privacy laws**
- **User-friendly web interface and mobile apps for easy encrypted email access**

How to Use

Please follow the instructions for your preferred mobile below:

Android

- **Open the Google Play Store (Android) on your device.**
- **Search for Proton Mail and install the official app by Proton AG.**
- **Open Proton Mail, tap Sign Up or Log In, and follow the on-screen prompts to access your account.**
- **Complete the verification process to start using Proton Mail.**

- **Open the App Store (Apple) on your device.**
- **Search for Proton Mail and install the official app by Proton AG.**
- **Open Proton Mail, tap Sign Up or Log In, and follow the on-screen prompts to access your account.**
- **If creating a new account, complete the verification process to start using Proton Mail.**

Tutanota

Quick Look

Tutanota is a secure, open-source email service designed to provide end-to-end encrypted email communication with a strong focus on privacy and data protection.

It offers automatic encryption of emails and contacts, ensuring that only the sender and recipient can access the message contents. Tutanota features built-in encryption for subject lines and attachments, along with secure calendar and contact management, making it a comprehensive privacy-focused communication platform.

Based in Germany, Tutanota benefits from strict European privacy laws, and its client apps are available across web, desktop, and mobile platforms for easy encrypted email access anytime, anywhere.

Features

Tutanota provides comprehensive encrypted email solutions with the following key features:

- **End-to-end encryption of emails, subject lines, attachments, contacts, and calendar events**
- **Open-source architecture promoting transparency and security audits**
- **Automatic encryption enabling seamless privacy without complex setup**
- **Strict data protection policies supported by German and EU privacy regulations**
- **User-friendly web interface and apps for desktop and mobile devices**

How to Use

Please follow the instructions for your preferred mobile below:

Android

- **Open the Google Play Store (Android) on your device.**
- **Search for Tutanota and install the official app by Tutao GmbH.**
- **Open Tutanota, tap Sign Up or Log In, and follow the on-screen prompts to access your account.**
- **Complete the verification process to start using Tutanota.**

- **Open the App Store (Apple) on your device.**
- **Search for Tutanota and install the official app by Tutao GmbH.**
- **Open Tutanota, tap Sign Up or Log In, and follow the on-screen prompts to access your account.**
- **Complete the verification process to start using Tutanota.**

Digital-Violence Response & Anonymous Reporting

Why This Matters

In digital environments where online violence and harassment are prevalent, civil society organizations and individuals often face significant challenges in accessing timely support and reporting abuse safely.

Without effective digital-violence response and anonymous reporting tools, survivors may encounter barriers that prevent them from seeking help, while organizations may struggle to collect and manage sensitive incident data securely.

When these tools lack confidentiality, ease of use, and robust security features, survivors can be exposed to further harm, and critical evidence may be lost, undermining efforts to combat and prevent online abuse.

Deploying trusted digital-first aid kits, secure incident reporting platforms, and encrypted whistleblowing solutions is vital for protecting vulnerable users and strengthening organizational responses.

Below is an overview of trusted digital-violence response and anonymous reporting tools widely recommended for CSOs to enhance survivor support and secure incident management.

Digital First Aid Kit

Quick Look

Digital First Aid Kit is a comprehensive, survivor-centered resource designed to provide step-by-step guidance and practical support for individuals experiencing digital violence.

It offers survivors clear instructions on how to respond to online harassment, abuse, or threats, including securing devices, documenting evidence, and accessing legal or emotional support. The kit helps users understand their rights and navigate recovery while maintaining privacy and safety.

Developed with input from activists and experts, Digital First Aid Kit empowers survivors to take informed actions against digital harm and supports organizations in offering effective assistance.

Features

Digital First Aid Kit offers essential resources for responding to digital violence, providing the following key features:

- **Step-by-step survivor guidance for recognizing, managing, and mitigating digital violence incidents**
- **Practical advice on securing devices, protecting accounts, and safeguarding private communications**
- **Clear instructions for documenting and preserving digital evidence in a safe manner**
- **Access to emotional support networks, legal aid options, and trusted technical assistance**

How to Use

- **Visit the official website: https://digitalfirstaid.org for direct access.**
- **Explore and use the toolkit online—no installation or special setup required.**
- **Download available resources for offline reference and quick access whenever needed.**
- **Use the materials independently, or incorporate them into organizational training sessions and broader support programs.**

Take Back The Tech

Quick Look

Take Back the Tech is a feminist initiative that supports individuals and organizations in reclaiming technology as a means to promote safety, digital rights, and activism against online violence.

It provides resources and campaigns that empower people to resist and respond to gender-based digital harassment, fostering community-led actions and awareness-raising.

Developed by activists and advocates, Take Back the Tech strengthens efforts to challenge digital violence through education, solidarity, and collective mobilization.

Features

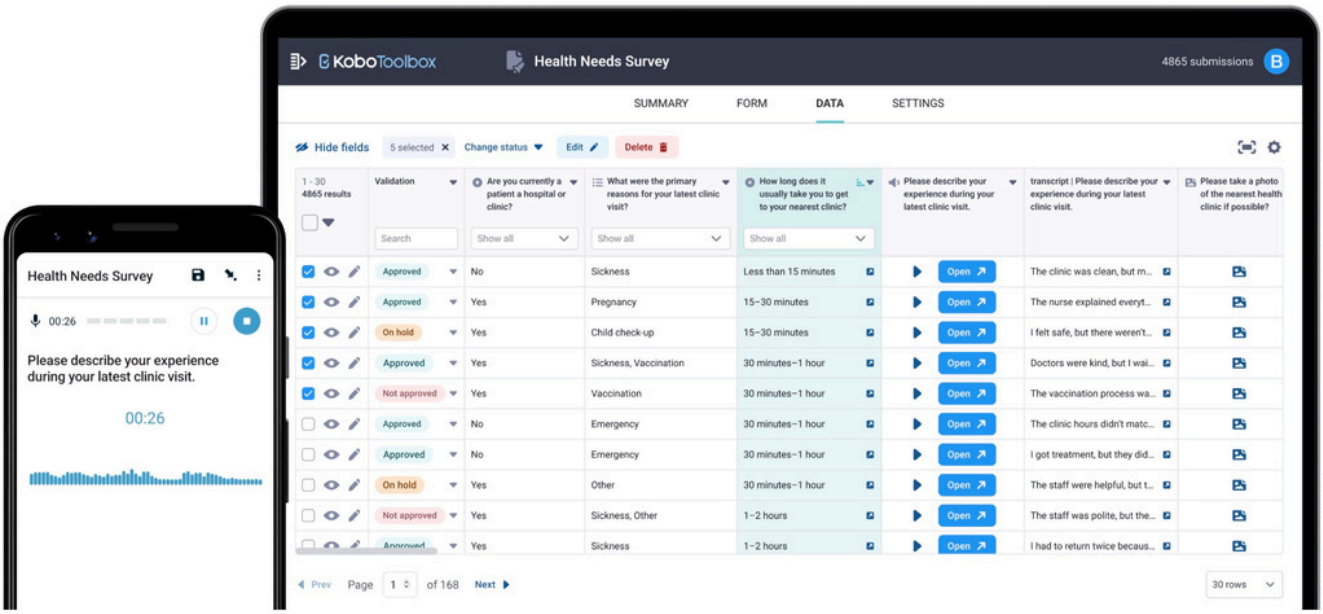
Take Back the Tech provides feminist resources and advocacy tools to challenge and combat digital violence with the following key features:

- **Empowers individuals and organizations to reclaim technology for safety and rights**
- **Supports campaigns and community actions addressing gender-based digital harassment**
- **Facilitates knowledge-sharing on resisting and responding to online abuse**
- **Encourages collaboration among activists, survivors, and organizations to amplify impact**

How to Use

- **Visit the official website: https://takebackthetech.net to explore the initiative.**
- **Access campaign resources, toolkits, and practical guides directly online at any time.**
- **Utilize materials for advocacy, awareness-raising, training, and broader community mobilization efforts.**
- **Actively engage with the community through events, social media platforms, and collaborative local or global projects.**

KoboToolbox



32,000+
Organizations rely use KoboToolbox

220+
Countries & territories

20M+
Surveys collected per month

Quick Look

KoboToolbox is an open-source data collection platform designed for humanitarian, development, and research organizations to efficiently gather and manage field data in challenging environments.

It enables offline-capable, customizable data collection through user-friendly forms, supporting incident reporting, surveys, and assessments even in low-connectivity areas.

Developed with input from global practitioners, KoboToolbox empowers organizations to collect reliable data securely and supports informed decision-making to respond effectively to crises and community needs.

Features

KoboToolbox offers flexible and reliable data collection capabilities with the following key features:

- **Supports offline data collection with automatic syncing when online**
- **Customizable forms for incident reporting, surveys, and research**
- **User-friendly interface designed for low-bandwidth and resource-constrained environments**
- **Secure data storage with options for encryption and access controls**
- **Data export in multiple formats for easy analysis and reporting**

How to Use

- **Create Your Account on the KoboToolbox web platform: https://kf.kobotoolbox.org.**
- **Download the Mobile App**
- **Install KoboCollect from the Google Play Store.**
- **Connect Your Account**
- **Open KoboCollect, enter your server URL, username, and password to link the app with your KoboToolbox account.**
- **Collect and Manage Data**
  - **Use KoboCollect on mobile for field data collection.**
  - **Use the web platform for survey creation, monitoring, and analysis.**

GlobaLeaks

Quick Look

GlobaLeaks is an open-source, secure whistleblowing platform designed to facilitate fully anonymous and strongly encrypted reporting of sensitive information.

It enables organizations, journalists, and activists to create customized digital whistleblowing portals that safeguard reporters' identities, securely manage submissions, and address growing challenges of online violence, corruption, and abuse of power.

Developed with a strong focus on privacy, accountability, and transparency, GlobaLeaks empowers whistleblowers worldwide by offering a reliable, user-friendly, and encrypted channel for safe and confidential disclosures.

Features

GlobaLeaks offers robust features to ensure secure, anonymous reporting:

- **End-to-end encryption to protect the identity of whistleblowers and the confidentiality of submissions**
- **Customizable portals tailored to organizational needs and types of reports accepted**
- **Easy-to-use interface for submitting and managing reports securely**
- **Offline capability with local data encryption before sending**
- **Tools for managing, analyzing, and following up on reports while maintaining privacy safeguards**

How to Use

Visit the official website: https://www.globaleaks.org/download/

Download the GlobaLeaks software and documentation needed to set up a secure whistleblowing portal.

Install and configure the platform on your organization's server to enable anonymous, encrypted reporting.

Access and manage submissions securely through the web interface once your portal is live.

Phishing Drills & Micro-learning

Why This Matters

In digital environments where phishing attacks and cyber threats are increasingly sophisticated, civil society organizations and individuals face critical challenges in building awareness and resilience through effective training and simulations.

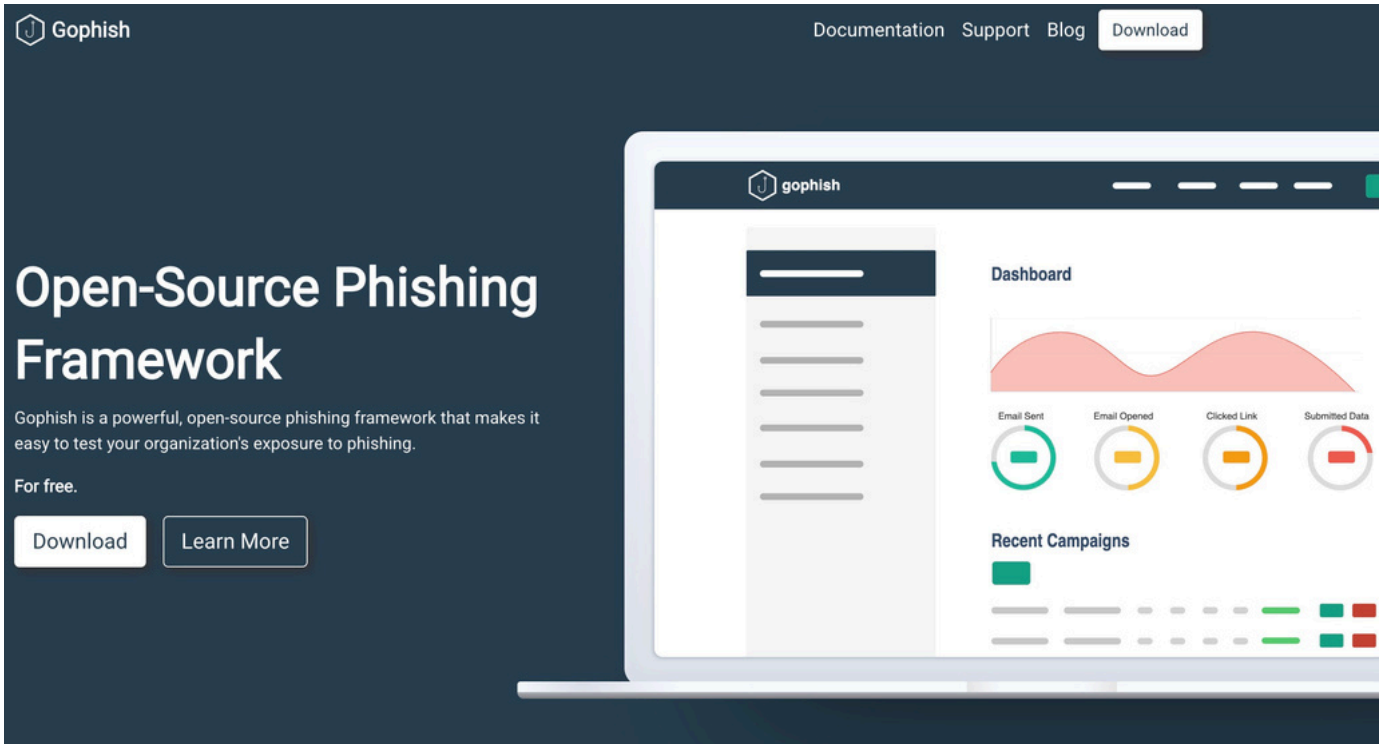
Without accessible phishing drills and micro-learning resources, users may remain vulnerable to deceptive tactics, jeopardizing organizational security and personal data safety.

When educational tools lack interactivity, contextual relevance, and ease of deployment, cybersecurity awareness suffers, increasing the risk of successful attacks and data breaches.

Leveraging trusted phishing simulation platforms and engaging micro-learning quizzes is essential for fostering a security-conscious culture and enhancing defense mechanisms.

Below is an overview of trusted phishing drills and micro-learning tools widely recommended for CSOs to strengthen cybersecurity awareness and incident prevention.

GoPhish



Quick Look

Gophish is an open-source phishing simulation platform designed to help organizations conduct realistic, safe phishing attacks for training and security awareness programs.

It enables civil society organizations to create, launch, and track simulated phishing campaigns to assess user vulnerability and reinforce best security practices.

Developed with ease of use and customization in mind, Gophish provides detailed metrics on user engagement, such as click rates and submitted credentials, allowing organizations to measure the effectiveness of their training programs.

Features

Gophish offers robust features to support effective phishing simulation and cybersecurity training:

- **User-friendly interface to design customizable phishing emails and landing pages**
- **Ability to send safe simulated phishing campaigns to targeted user groups**
- **Real-time tracking of email opens, link clicks, and submitted credentials**
- **Comprehensive reporting to identify vulnerabilities and improve training focus**

How to Use

How to Download:

- **Visit the official website: https://gophish.io**
- **Go to the Downloads section or visit the Releases page: https://github.com/gophish/gophish/releases**
- **Download the latest release compatible with your operating system (Windows, macOS, or Linux).**
- **Extract the downloaded archive and run the Gophish executable.**
- **Follow the official setup guide to configure and access the Gophish dashboard via your browser.**

H5P

Quick Look

H5P Quiz is an interactive content creation tool that enables organizations to develop engaging, multimedia quizzes for training and educational purposes.

It supports civil society organizations in delivering localized, bite-sized learning experiences that reinforce key concepts in a user-friendly format.

Designed for accessibility and ease of use, H5P Quiz allows trainers to create customizable quizzes that can be embedded into websites or learning management systems, enhancing participant engagement and retention.

Its flexibility and multimedia support make it a valuable tool for reinforcing cybersecurity awareness and other essential knowledge areas in a practical, accessible manner.

Features

H5P Quiz offers robust features to create engaging, accessible learning content:

- **Simple drag-and-drop interface to build diverse quiz types**
- **Supports multimedia content including images, videos, and audio for rich interactions**
- **Mobile-friendly and accessible design for diverse user groups**
- **Tracks user responses and progress to monitor learning outcomes**
- **Integrates easily with various content platforms and websites**

How to Use

How to Use:

- **Visit the official website: https://h5p.org**
- **Sign up for a free account to use the H5P Online Editor, or download plugins for popular content management systems such as WordPress, Drupal, and Moodle.**
- **Create interactive content like quizzes, presentations, and videos, then embed them in your website or learning platform.**
- **Leverage these tools for training sessions, security awareness campaigns, and reinforcing cybersecurity lessons in an engaging, accessible format.**

Full Disk Encryption

Why This Matters

In today's digital landscape, where devices are prone to physical loss, theft, and sophisticated cyber threats, securing sensitive data is a critical priority for civil society organizations and individuals alike.

Without comprehensive full disk encryption solutions, confidential information stored on laptops, desktops, and mobile devices remains vulnerable to unauthorized access, risking organizational integrity and personal privacy.

When encryption tools are not integrated seamlessly or lack ease of use, adoption rates suffer, leaving data exposed and undermining security efforts. Therefore, implementing reliable full disk encryption technologies is vital for safeguarding data at rest and ensuring compliance with privacy standards.

By encrypting entire drives, these solutions protect all stored information from unauthorized access, even if the device falls into the wrong hands, thereby reducing risk and bolstering trust in digital operations.

Below is an overview of trusted full disk encryption tools widely recommended for CSOs to enhance data protection and resilience against cyber and physical threats.

BitLocker

Quick Look

BitLocker is a full disk encryption feature integrated into Windows operating systems, designed to protect user data by encrypting entire drives.

It secures information on a device by preventing unauthorized access, especially in cases of device theft or loss.

BitLocker utilizes Trusted Platform Module (TPM) hardware to enhance security by verifying system integrity during startup. It supports encryption for system drives as well as fixed and removable drives, ensuring versatile protection.

BitLocker is user-friendly with seamless integration in Windows, providing transparent encryption without compromising system performance. It is recommended for civil society organizations seeking robust data security on Windows devices.

Features

BitLocker offers robust features to provide comprehensive full disk encryption for Windows users:

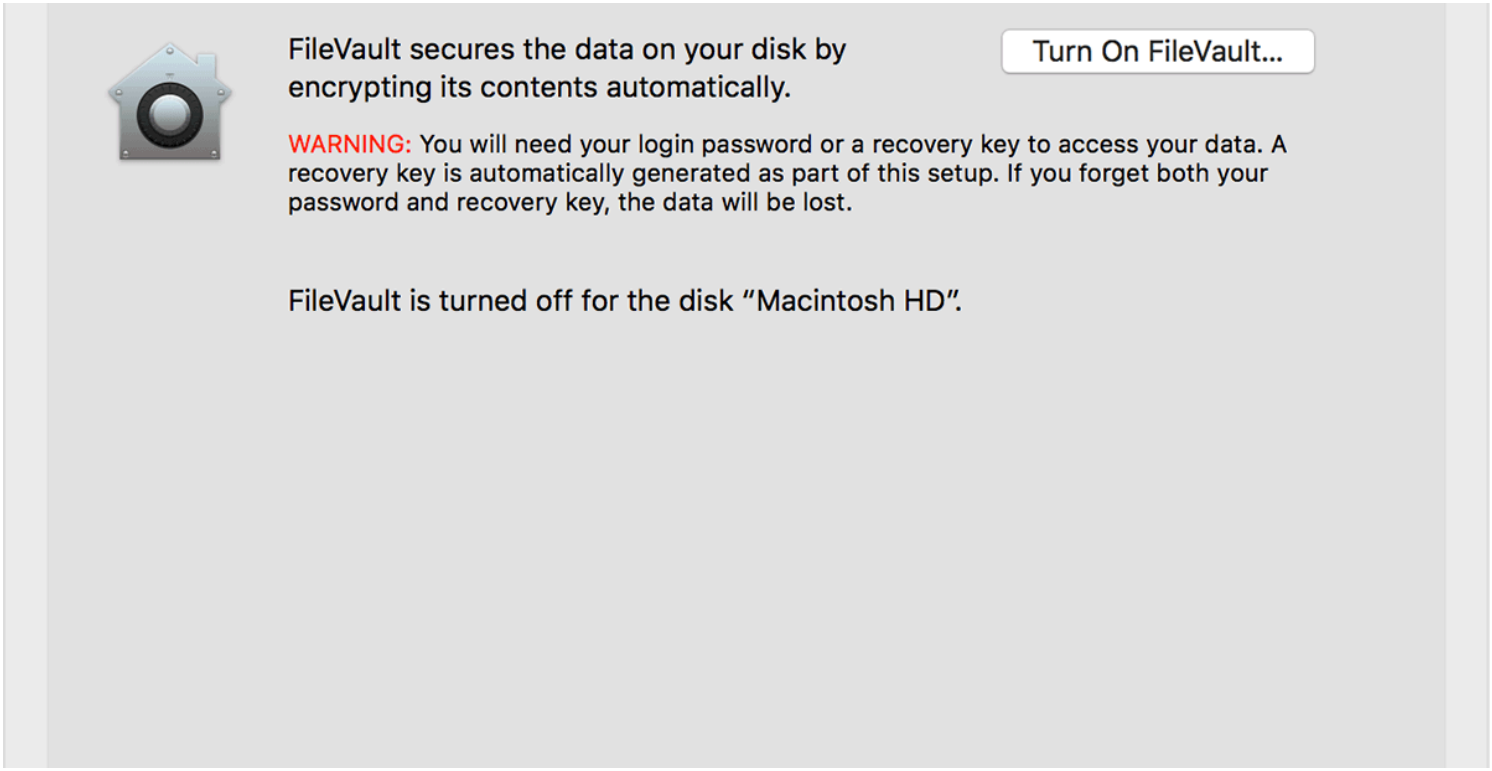
- **Encrypts entire system, fixed, and removable drives to protect data at rest**
- **Integrates with Trusted Platform Module (TPM) hardware for enhanced security**
- **Provides seamless, transparent encryption with minimal impact on system performance**
- **Supports multifactor authentication options like PINs and USB keys**

How to Use

How to use BitLocker on Windows:

- **Access BitLocker through the Control Panel or Windows Settings under "Device encryption" or "BitLocker Drive Encryption"**
- **Select the drive to encrypt and choose encryption options (e.g., full or used disk space only)**
- **Configure authentication methods such as TPM, PIN, or USB key**
- **Save or print the recovery key securely for emergency access**
- **Start the encryption process and monitor progress through the BitLocker interface until completion**

FileVault



Quick Look

FileVault is Apple's built-in full disk encryption feature for macOS, created to safeguard sensitive information by encrypting the entire startup disk.

By requiring a password or recovery key at startup, it ensures that all data stored on a Mac remains protected and inaccessible to unauthorized users, particularly in cases where the device is lost or stolen.

FileVault employs XTS-AES-128 encryption with a 256-bit key, delivering strong security without noticeably affecting system performance.

It integrates smoothly with the macOS environment, offering simple setup, recovery key storage options, and convenient support for multiple user accounts.

Features

FileVault offers strong capabilities to deliver comprehensive full disk encryption for macOS users:

- **Encrypts the entire startup disk to safeguard data at rest**
- **Protects against unauthorized access if a Mac is lost or stolen**
- **Uses XTS-AES-128 encryption with a 256-bit key for robust security**
- **Supports multiple user accounts with individual access permissions**
- **Provides recovery key options to restore access if a password is forgotten**

How to Use

How to use FileVault on macOS:

- **Open System Settings and navigate to Privacy & Security > FileVault**
- **Click Turn On FileVault to begin the encryption setup**
- **Choose to allow iCloud to unlock the disk or create a separate recovery key for secure backup**
- **Ensure each user account with access to the Mac is enabled to unlock the disk**
- **Restart your Mac to activate encryption; FileVault will begin encrypting the startup disk in the background**

Mobile Security

Why This Matters

In today's mobile-first world, where smartphones and tablets serve as primary tools for communication, coordination, and storing sensitive data, protecting these devices is an essential priority for civil society organizations and individuals alike.

Without robust mobile security measures, devices are vulnerable to malware, surveillance, and unauthorized access, especially if lost, stolen, or compromised through malicious apps. Such breaches can expose personal information, endanger organizational operations, and erode trust in digital tools.

When security features are disabled by default or overlooked due to complexity, adoption rates remain low, leaving critical data and communications at risk. Therefore, enabling reliable mobile protection systems is key to ensuring safe usage and resilience in high-risk environments.

By combining built-in protections like Google Play Protect on Android and iVerify on iOS with good digital hygiene, users can reduce exposure to malicious software, phishing, and spyware. These tools provide real-time scanning, app verification, and security alerts that help prevent attacks before they cause harm.

Below is an overview of trusted mobile security tools recommended for CSOs to strengthen defenses and safeguard against evolving mobile threats.

Google Play Protect

Quick Look

Google Play Protect is Android's built-in security system, designed to keep devices and data safe by continuously scanning apps and monitoring for threats.

It works in the background to protect against harmful apps, malware, and suspicious behavior, ensuring that downloaded applications are verified and trustworthy.

Play Protect uses Google's advanced machine learning and threat detection technology, providing real-time protection without interrupting performance or usability.

It integrates seamlessly with the Android ecosystem, offering automatic updates, app verification, safe browsing features, and clear security notifications to keep users informed and in control of their device's safety.

Features

Google Play Protect offers powerful capabilities to ensure comprehensive security for Android users:

- **Scans apps from the Google Play Store and third-party sources to detect harmful software**
- **Continuously monitors devices for suspicious behavior and potential threats**
- **Uses Google's machine learning to identify and block malware in real time**
- **Provides safe browsing protection to warn against dangerous websites**

How to Use

How to Use Google Play Protect

- **Open the Google Play Store app on your device**
- **Tap your profile icon in the top right corner and select Play Protect**
- **Review the latest scan results to see if harmful apps were detected**
- **Tap Scan to manually check all installed apps for threats**
- **Enable Scan apps with Play Protect to allow automatic, continuous protection**
- **Adjust settings to improve detection, such as sending unknown apps to Google for analysis**

iVerify

Quick Look

iVerify is Apple's official security application for iOS, designed to help users strengthen device security and detect potential compromise.

It guides users through best-practice hardening steps—such as enabling strong passcodes, reducing attack surfaces, and securing privacy settings—while monitoring for signs of tampering or jailbreaking.

iVerify uses Apple's secure architecture and built-in protections, providing proactive alerts and expert recommendations without disrupting usability or performance.

It integrates seamlessly with the iOS ecosystem, offering automated checks, step-by-step security guidance, regular updates, and clear notifications to help users stay informed and maintain control over their device's integrity.

Features

iVerify offers powerful capabilities to strengthen iOS device security and privacy:

- **Guides users through comprehensive security hardening steps for maximum protection**
- **Detects signs of compromise, tampering, or jailbreaking on the device**
- **Provides clear, actionable recommendations to address vulnerabilities and reduce risk**
- **Continuously monitors system integrity without impacting performance**

How to Use

- **Download and install iVerify from the App Store**
- **Open the iVerify app and follow the on-screen setup instructions**
- **Run the initial security assessment to check your device's current protection status**
- **Review recommended actions and apply fixes, such as enabling stronger passcodes or adjusting privacy settings**
- **Use the "Security Checklist" to complete all hardening steps suggested by the app**
- **Re-run the scan periodically or after major iOS updates to ensure continued protection**

Counter Dis-Information Kit

Why This Matters

In today's information-driven landscape, where social media and online platforms shape public opinion and influence decision-making, combating disinformation has become a critical priority for civil society organizations and individuals alike.

False narratives, manipulated media, and coordinated misinformation campaigns can undermine advocacy efforts, erode trust, and incite real-world harm. These tactics are often amplified by automated bots and viral sharing, making them difficult to detect and counter in real time.

When verification tools are underutilized or ignored due to complexity, misinformation spreads unchecked, leaving communities vulnerable to propaganda and reputational attacks. Therefore, adopting reliable counter-disinformation strategies and technologies is essential to protect the integrity of information and maintain public trust.

By leveraging trusted verification tools such as InVID, WeVerify, and Hoaxy, users can analyze suspicious content, verify images and videos, and track the spread of harmful narratives across digital spaces. These solutions provide advanced detection capabilities, metadata analysis, and visualization features that enable fact-checking and informed response.

Below is an overview of recommended counter-disinformation tools that can help CSOs strengthen resilience and ensure accuracy in the fight against digital manipulation.

InVID

Quick Look

InVID is a powerful counter-disinformation toolkit designed to help civil society organizations and individuals verify and analyze online multimedia content. It provides a browser plug-in that breaks videos into key frames, checks metadata, and facilitates reverse-image searches.

These features enable users to authenticate the origin and integrity of videos, helping to combat the spread of fake news and manipulated media.

By offering quick verification and detailed analysis tools, InVID supports informed decision-making and strengthens digital literacy in environments prone to misinformation and disinformation campaigns. It is an essential resource for promoting transparency and trust in digital communications.

Features

InVID offers powerful capabilities to verify and analyze digital media content:

- **Guides users through step-by-step checks to assess the authenticity of online videos and images**
- **Detects traces of manipulation, editing, or misattribution using advanced forensic tools**
- **Provides clear, actionable insights to help verify sources and reduce misinformation risk**
- **Supports frame-by-frame analysis and reverse image/video search without compromising usability**

How to Use

- **Download and install the InVID Verification Plugin or access the online tool**
- **Open the tool and upload a video link, file, or image you want to verify**
- **Run the analysis to extract keyframes, metadata, and other verification elements**
- **Review the results, including reverse image search matches and forensic indicators**
- **Use the provided checks (thumbnails, keyframes, metadata, magnifier, and contextual search) to evaluate authenticity**

Hoaxy

HOAXY®

Visualize the spread of claims and fact checking.

Quick Look

Hoaxy is a dynamic counter-disinformation toolkit developed to help civil society organizations and individuals track the spread of online misinformation. It provides a visual platform that maps how hashtags and URLs propagate across social media in real time.

These features enable users to understand the reach and influence of potentially false or misleading content, facilitating timely intervention and response.

By offering clear visualizations and analytics on information diffusion, Hoaxy supports improved media literacy and strategic communication efforts in environments vulnerable to fake news and disinformation campaigns. It is an invaluable tool for promoting awareness and accountability in digital ecosystems.

Features

Hoaxy offers powerful features to track and analyze the spread of online misinformation:

- **Visualizes how hashtags, URLs, and claims propagate across social media in real time**
- **Maps networks of accounts sharing or amplifying disinformation for deeper insights**
- **Provides timeline views to monitor the evolution and reach of misleading content**
- **Enables users to identify influential spreaders and key sources of disinformation**
- **Supports data export and detailed analytics to inform response strategies and media literacy efforts**

How to Use

- **Access the Hoaxy platform through its web interface at https://hoaxy.osome.iu.edu.**
- **Enter hashtags, keywords, or URLs related to the content you want to track.**
- **Explore interactive network graphs showing how the specified content spreads across social media platforms.**
- **Use filters to adjust the time range, domains, and nodes, and export data for deeper analysis if needed.**

Advocacy Content & Scheduling

Why This Matters

In today's fast-paced digital environment, where public discourse unfolds across multiple social media platforms, strategic advocacy and timely engagement are essential for civil society organizations (CSOs). The ability to craft compelling messages and deliver them at the right time can determine whether a campaign gains momentum or fades into obscurity.

Uncoordinated messaging, inconsistent posting schedules, and poorly designed visuals can weaken advocacy efforts, limit reach, and erode credibility. In a world driven by visual storytelling and rapid content cycles, CSOs that rely on manual processes or fragmented tools risk falling behind in shaping narratives and mobilizing supporters.

When content creation and scheduling are treated as secondary priorities, campaigns struggle to maintain visibility and audience engagement. Missed posting windows or low-quality design assets can cause vital advocacy messages to be overlooked. Therefore, adopting professional-grade design and scheduling tools is critical to ensuring consistency, maximizing impact, and amplifying voices in competitive digital spaces.

By leveraging these types of platforms, CSOs can streamline the entire advocacy workflow—from creating visually engaging campaign materials to automating post distribution and monitoring audience response. These tools empower organizations to plan strategically, execute efficiently, and sustain impactful campaigns without overwhelming internal resources.

Below is an overview of recommended advocacy content and scheduling tools designed to help CSOs strengthen their digital presence and drive meaningful engagement.

Canva

Quick Look

Canva is a versatile and user-friendly design platform that empowers individuals and teams to create a wide range of stunning visual content. It provides an intuitive drag-and-drop interface, along with a rich library of templates, images, and fonts, making professional-quality design accessible to everyone, regardless of their level of expertise.

These features enable users to effortlessly produce everything from social media graphics and presentations to posters and videos. By offering a collaborative and streamlined design process, Canva helps users maintain brand consistency and bring their creative visions to life.

By simplifying the design process, Canva fosters creativity and enhances visual communication for businesses, educators, and individuals alike. It is an invaluable tool for anyone looking to create impactful visual content quickly and efficiently.

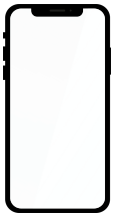
Features

Canva offers powerful features to design and create visually stunning content with ease:

- **Provides an intuitive drag-and-drop interface to customize templates and design elements effortlessly**
- **Offers a vast library of photos, illustrations, icons, fonts, and templates for every type of project**
- **Enables real-time collaboration for teams to create, edit, and share designs seamlessly**
- **Supports export in multiple formats including PNG, PDF, and video for diverse publishing needs**

How to Use

- **Visit the Canva website and log in or create a free account**
- **Select a design type or start from scratch on the dashboard**
- **Use drag-and-drop tools to add and edit photos, fonts, shapes, and more**
- **Access advanced features like resizing, layers, and animation for enhanced designs**



- **Open Apple App Store or Google Play Store**
- **Use the search bar to type "Canva"**
- **Find the official Canva app by Canva and Company in the search results**
- **Tap the Get (iOS) or Install (Android) button to download and install the app**

Flourish

Quick Look

Flourish is a powerful and intuitive data visualization platform designed to help users create engaging and interactive charts, maps, and graphics with ease. It offers a user-friendly interface and a wide range of customizable templates, enabling users to transform complex data into compelling visual stories without needing advanced technical skills.

These features allow users to build interactive content for reports, presentations, and websites, making data more accessible and understandable for diverse audiences. Flourish supports seamless integration with other tools and platforms, enhancing the ability to communicate insights effectively.

By simplifying the creation of dynamic visualizations, Flourish empowers businesses, nonprofits, educators, and analysts to showcase data-driven narratives that inform and inspire action.

Features

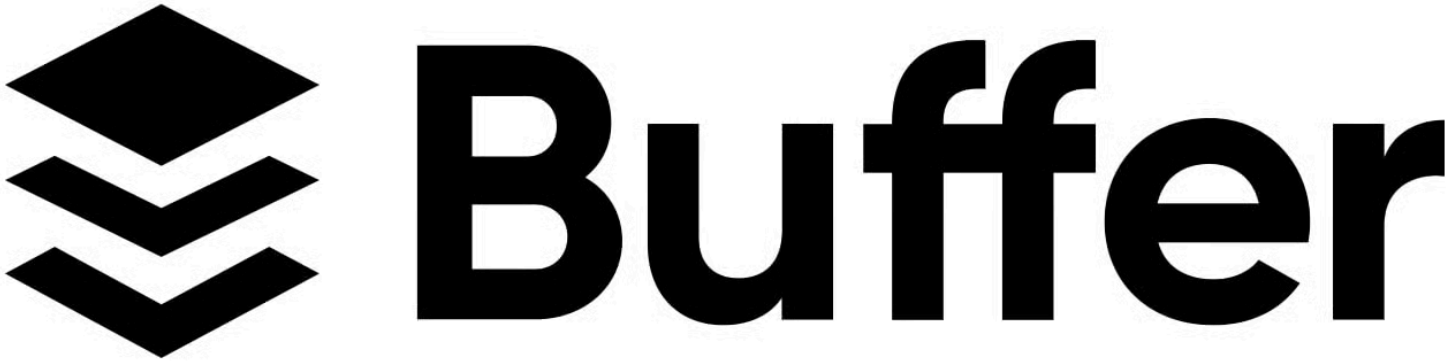
Flourish offers powerful features to create engaging and interactive data visualizations with ease:

- **Provides a user-friendly interface with customizable templates for charts, maps, and graphics**
- **Supports a wide range of visualization types to suit different data storytelling needs**
- **Enables users to add interactivity to visualizations, enhancing audience engagement**
- **Allows embedding and sharing of visualizations across websites, presentations, and social media**

How to Use

- **Access the Flourish platform through its web interface at https://flourish.studio.**
- **Sign in or create a free account to start building your visualizations.**
- **Choose a template or upload your data to create interactive charts, maps, and graphics.**
- **Customize your visualization using the intuitive editor, adding interactivity and adjusting design elements.**
- **Embed, share, or download your completed visualization for use in reports, presentations, or websites.**

Buffer



Quick Look

Buffer is a comprehensive social media management platform designed to help individuals and organizations schedule, publish, and analyze content across multiple social media channels effortlessly. It provides an intuitive interface and powerful tools to plan and automate posts, track engagement, and measure performance.

These features enable users to streamline their social media marketing efforts, maintain consistent posting schedules, and gain valuable insights through detailed analytics. Buffer supports collaboration among team members, making it easy to coordinate campaigns and optimize social media strategies.

By simplifying social media management, Buffer empowers businesses, nonprofits, marketers, and content creators to build stronger online presence and engage their audiences effectively across platforms.

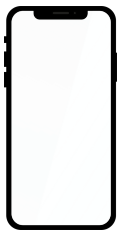
Features

Buffer offers powerful features to manage and optimize social media presence efficiently:

- **Provides a streamlined interface to schedule and publish content across multiple social media platforms**
- **Supports multi-account management, allowing users to handle several profiles from one dashboard**
- **Offers detailed analytics and insights to track engagement, audience growth, and post performance**
- **Enables team collaboration with user roles, approval workflows, and shared content calendars**

How to Use

- **Visit the Buffer website and log in or create a free account**
- **Connect your social media accounts to the dashboard**
- **Schedule posts, manage multiple accounts, and analyze engagement with the web interface**
- **Collaborate with team members using shared calendars and approval workflows**



- **Download and install the Buffer app from the Apple App Store or Google Play Store**
- **Open the app and log in or sign up for a new account**
- **Connect your social media profiles within the app**
- **Schedule, publish, and monitor posts on the go with an intuitive mobile interface**

Shared Resource Hub & Peer Support

Why This Matters

In today's interconnected digital landscape, where collaboration and resource sharing are vital for civil society organizations (CSOs), having reliable and secure platforms for managing knowledge and communication is indispensable. Effective coordination, peer support, and secure information exchange form the backbone of resilient and responsive advocacy networks.

Fragmented communication channels, inconsistent document management, and lack of encryption can compromise both the safety and effectiveness of CSO operations. In an age where sensitive data protection and seamless collaboration are paramount, relying on disjointed or unsecured tools increases risks of information leaks, operational delays, and diminished trust among partners.

When resource hubs and peer support systems are undervalued or poorly integrated, organizations face challenges in maintaining continuity, responding swiftly to emerging issues, and delivering cohesive messaging. Ensuring access to encrypted, easily accessible, and well-organized shared resources strengthens the capacity of CSOs to act decisively and collaborate meaningfully across diverse contexts.

By adopting professional-grade platforms that offer end-to-end encryption, low-bandwidth accessibility, and around-the-clock support, CSOs can safeguard their knowledge assets while fostering inclusive peer networks. These tools empower organizations to maintain operational security, enhance information flow, and build robust support systems that underpin sustained advocacy efforts.

Below is an overview of recommended shared resource hub and peer support tools designed to help CSOs securely manage information, collaborate efficiently, and provide continuous mutual support.

Nextcloud Hub

Quick Look

Nextcloud Hub is a secure, self-hosted collaboration platform designed to give organizations full control over their data while enabling seamless teamwork. It integrates file sharing, communication, and productivity tools in one unified environment, ensuring privacy through end-to-end encryption and compliance with data protection regulations.

With Nextcloud Hub, users can store, sync, and share files securely, collaborate on documents in real-time, and manage workflows efficiently. Its flexible architecture supports integration with existing IT infrastructure, making it ideal for organizations seeking to maintain data sovereignty without sacrificing usability.

By combining robust security features with comprehensive collaboration capabilities, Nextcloud Hub empowers organizations to enhance productivity, safeguard sensitive information, and create a reliable digital workspace tailored to their needs.

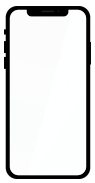
Features

Nextcloud Hub offers powerful features to securely manage and collaborate on digital resources effectively:

- **Provides a centralized platform for file storage, sharing, and synchronization with end-to-end encryption**
- **Supports real-time collaborative editing of documents, spreadsheets, and presentations within the hub**
- **Enables seamless integration with existing IT environments and popular productivity tools**
- **Offers role-based access controls and permissions to safeguard sensitive information and regulate collaboration**

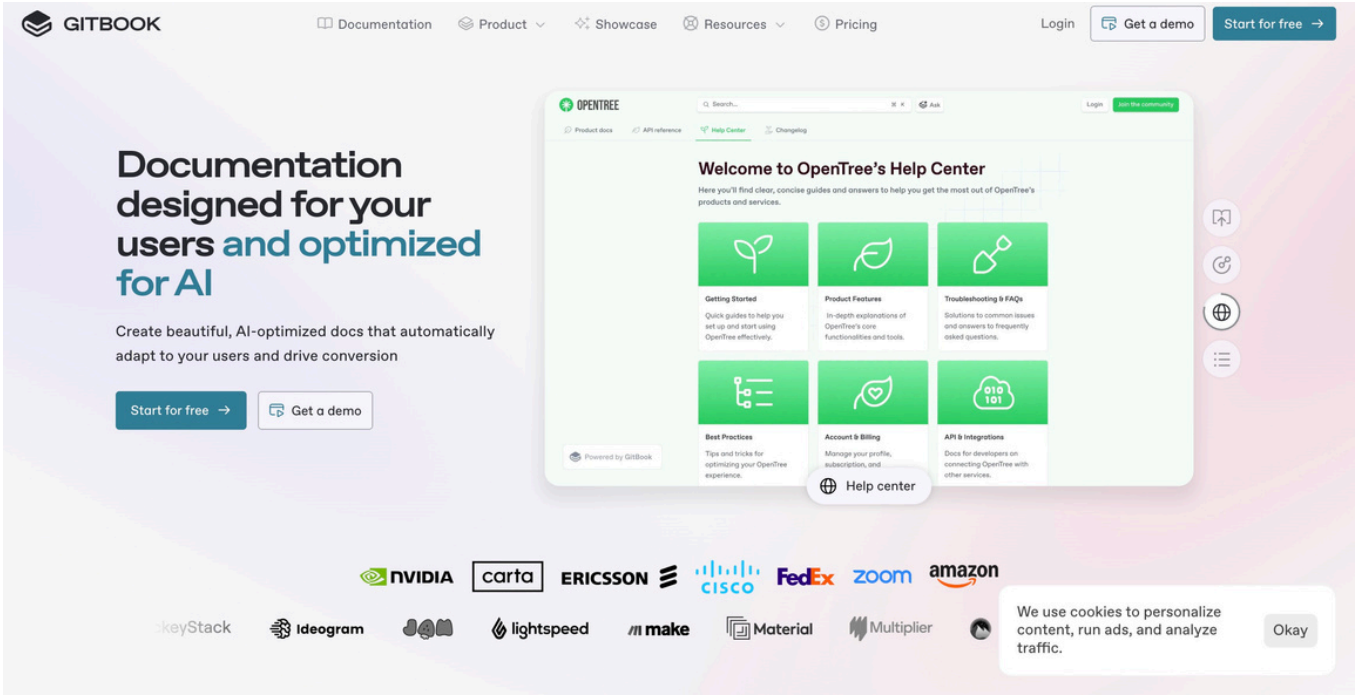
How to Use

- **Visit the Nextcloud website at https://nextcloud.com**
- **Sign in or create an account to access your files through the web interface**
- **Alternatively, download the Nextcloud desktop client for Windows, macOS, or Linux to sync files locally**



- **Download the Nextcloud app from the Apple App Store or Google Play Store**
- **Open the app and sign in to access, upload, and sync files securely on your mobile device**

GitBook



Quick Look

GitBook is a modern documentation and knowledge-sharing platform that allows organizations to create, manage, and distribute content in a structured and accessible way. It combines powerful editing tools with a clean, user-friendly interface, making it easy to maintain living documents that evolve with projects and community needs.

With GitBook, users can publish guides, reports, and resource hubs optimized for both online and offline access, ensuring that critical information remains available even in low-bandwidth environments. Its collaboration features support version control, team contributions, and content updates in real time, fostering transparency and collective knowledge-building.

By offering a reliable and scalable solution for sharing resources, GitBook enables organizations to strengthen peer support networks, preserve institutional memory, and make knowledge accessible to wider audiences in a professional, engaging format.

Features

GitBook offers powerful features to create, manage, and share organizational knowledge effectively:

- **Provides a centralized platform for publishing documentation, guides, and resource hubs in a structured format**
- **Supports real-time collaboration and version control, ensuring content stays accurate and up to date**
- **Enables offline access and low-bandwidth optimization, making resources available in diverse contexts**
- **Offers intuitive editing tools with markdown support and customizable layouts for professional presentation**
- **Integrates with external platforms and workflows, streamlining content sharing across teams and communities**

How to Use

- **Visit the GitBook website at https://www.gitbook.com**

- **Sign in or create a free account to start creating and managing documentation directly through the web interface**

- **Alternatively, invite team members to collaborate within your GitBook workspace and publish resources for online or offline access**

Matrix Server

Quick Look

Matrix Server is an open, decentralized communication platform that enables organizations to host their own secure messaging and collaboration environment. It is built on the Matrix protocol, which ensures interoperability across different chat clients while maintaining strong end-to-end encryption for privacy and trust.

With Matrix Server, organizations can run encrypted chat rooms, voice calls, and video meetings, while retaining full ownership of their data. It integrates seamlessly with clients such as Element, allowing users to communicate across multiple platforms and bridge with external services like Slack, IRC, or WhatsApp.

By offering a resilient, community-driven infrastructure, Matrix Server empowers civil society organizations to establish 24/7 peer support networks, protect sensitive conversations, and build a sustainable communication system free from reliance on centralized providers.

Features

Matrix Server offers powerful features to build secure, decentralized communication networks effectively:

- **Provides a self-hosted platform for encrypted messaging, voice, and video communication under organizational control**
- **Supports real-time collaboration across teams and communities with persistent chat rooms and group spaces**
- **Ensures interoperability through the Matrix protocol, allowing bridges to platforms like Slack, IRC, and WhatsApp**
- **Offers strong end-to-end encryption and granular access controls to safeguard sensitive conversations**
- **Integrates with clients such as Element for user-friendly communication across desktop and mobile devices**

How to Use

- **Visit the Matrix website at https://matrix.org**

- **Choose the Synapse server implementation (the most widely used Matrix server) and follow the installation instructions for your operating system (Linux, macOS, or Windows)**

- **Alternatively, use a pre-configured hosting provider or Docker image to quickly deploy a Matrix Server without complex setup**

- **Once installed, connect through a Matrix client such as Element to create rooms, manage users, and start secure communication across your network**