EMPOWERING ACTIVISTS

Digital Security Resource Library

ExpressVPN

Activists, human rights defenders, and members of the media are at the forefront of a wide range of critical global issues. We're thankful for the important work you do and recognize that this work can put you and those you support at risk, especially when it comes to digital security. That's why we've created this resource library.

Digital security refers to the practices and tools used to protect online identities, communications, and data from unauthorized access. We understand that digital security can be complex and intimidating, and we're here to help.

Our goal is to empower you with accessible, affordable, and privacy-focused tools and resources so that you can stay safe and secure online while continuing to make a long-term impact on the causes you believe in, regardless of your technical expertise.

Developed in partnership with experts from organizations such as ExpressVPN and the cybersecurity and digital rights NGO CyberPeace Institute, this resource library has eight sections and provides comprehensive and practical guidance on improving digital privacy and security.

The following resources are not one-size-fits-all: as the Electronic Frontier Foundation's Surveillance Self-Defense resource states, security isn't just about the tools you use or the software you download, it begins with understanding the unique threats you face and how you can counter those threats. Creating a security plan is a crucial step in figuring out which tools to adopt and which are appropriate for your situations. With that in mind, every resource listed in this report might not be appropriate for your unique risks. We encourage you to use these resources judiciously, selecting those that align best with your individual security requirements and challenges.

Utilizing this Library signifies a proactive step in empowering yourself and protecting your work. Thank you for allowing us to be a part of it.

Sections

1

Enhancing your digital security know-how

Activism has increasingly involved digital technology. However, with this shift comes the need for new skills in digital security. By equipping yourself with the necessary tools and knowledge, you can better protect yourself and your movement, ensuring privacy, secure communication, and defense of your digital rights.

We recommend the following resources to enhance your digital security knowledge:

Digital privacy and security fundamentals and best practices

Online cybersecurity education and training resources

- Global Cyber Alliance Toolkit: Free and effective tools for individuals and organizations of any size to reduce their cyber risk. The toolkit includes a range of cybersecurity hygiene resources, organized for ease of use.
- Cybersecurity handbook for civil society organizations: An open-source resource designed to help organizations develop and implement cybersecurity plans. It includes explanations of key security topics, strategies, recommended tools to limit risk, and additional resources. The handbook is also offered as an online course.

- Digital first aid kit: A free resource to help increase protection against the most common types of digital emergencies. It can also be used by activists, human rights defenders, bloggers, journalists or media activists who want to learn more about how they can protect themselves and support others.
- The phishing quiz: An interactive tool presenting realistic phishing scenarios to help develop skills in identifying and avoiding phishing attacks in a safe, controlled environment.
- Harvard University on edX - Introduction to cybersecurity course: A course suitable for both technical and non-technical audiences, covering a wide range of cybersecurity topics, including hacking, social engineering, password security, and encryption. Through real-world examples, you'll learn how to protect your data, devices, and systems from modern threats. The course is self-paced and free to audit.
- The Open University's OpenLearn - Introduction to cybersecurity course: Learn about the threats that individuals and organizations face online, and the steps that can be taken against those threats. The course covers topics such as malware, network security, cryptography, identity theft, and risk management. The course is self-paced, can be accessed for free, and requires no prior technical knowledge. Participants can earn a free digital badge upon completion to demonstrate their knowledge and skills in cybersecurity.
- ExpressVPN's Udemy course on digital privacy: Created by leading cybersecurity and privacy company ExpressVPN, this course has been designed to help educate participants on digital security practices like password hygiene, two-factor/multi-factor authentication (2FA/MFA), and the use of VPNs as tools to safeguard online security, privacy, and anonymity.
- Curricula's non-profit security awareness training program: Provides engaging, budget-friendly security awareness training for non-profits. The program's budget-friendly pricing and automation features are aimed at those with limited resources. Free episodes include phishing, an intro to cybersecurity, and SOC2 compliance.

Safety resources for staying secure amid oppression

A collection of resources for those in challenging circumstances, focusing on online privacy and security, can be found on ExpressVPN's Rights Center.

2

Securing your communications in the field

Implementing secure communications is crucial for safeguarding not only your digital assets but also the data of those you support, whether you're working on the ground or remotely.

While no system can guarantee 100% security, using the right tools and techniques can significantly reduce the risk of interception and compromise.

Recommended communication tools

The top tools that our security experts recommend for high-risk environments are:

- Messaging: Signal
- Privacy-conscious browsers: Tor, Firefox, Brave
- Email: CounterMail, Mailfence, Tutanota
- Secure file sharing: OnionShare

- Search engines: DuckDuckGo, Qwant, Startpage
- Data backup on the Cloud: Google Drive, Dropbox, OneDrive, VeraCrypt, PGP
- Privacy settings: Use Privacy Badger to check all your privacy settings and protect against online tracking.
- Spyware removal: Use Microsoft Defender, Bitdefender, or ESET to detect and remove any potentially malicious software from your device.

Encryption tools

Encryption is the process of converting data into an unreadable format, which can only be decrypted and read by someone with the proper decryption key. By using encryption tools, activists can ensure that their data remains unreadable and secure, even if it falls into the wrong hands. Here are some universally available encryption tools to protect sensitive information:

- Encrypt your device's hard disk: Microsoft BitLocker or Apple FileVault.
- Encrypt your sensitive files on disk: Microsoft OneDrive for file encryption.
- Encrypt your internet traffic: ExpressVPN
- For a comprehensive overview of how a VPN works and the benefits it offers, read more about What Is a VPN? and Top 10 reasons to use a VPN.
- For open-source data protection to encrypt your files, folders, and entire hard disks: VeraCrypt

If you are an organizer, journalist, or individual supporting a cause in an oppressive environment, you can request a complimentary ExpressVPN subscription by writing to safe@expressvpn.com.

Devices for activist operations

For added security, it's advisable to use dedicated devices for activist activities. Below are some cost-effective options:

- Basic browsing and document editing: Consider using a Thinkpad laptop with Ubuntu Linux or an x230 Thinkpad.
- Burner phones: A Nokia 1.3 smartphone or any old phone with a prepaid cell service SIM is suitable. Remember to factory reset before use.
- To maximize privacy and security, these devices should ideally be used in conjunction with Tails OS. You can download Tails and run it off a USB for added convenience.

Protecting your data when crossing borders

- Turn off all your devices: This prevents border agents from accessing your data without your consent, which is crucial when carrying sensitive or confidential information.
- Disable your Bluetooth and your Wi-Fi: Keep Bluetooth and Wi-Fi off to minimize the risk of hacking or tracking. Activate them only when necessary.
- Use a disposable/burner device whenever possible: If you're concerned about your privacy being compromised, consider using a disposable/burner device during your trip. This strategy limits border agents' access to your personal or sensitive data.
- Avoid SMS for 2FA: SMS-based 2FA is vulnerable to interception. Use an authenticator app instead for greater security.
- Stay connected to a VPN at all times: Maintain a VPN connection to protect your online activities. Choose a reputable VPN provider like ExpressVPN and ensure it's active whenever your device is in use.

Securely wiping devices when needed

- When facing surveillance, interrogation, or imprisonment, one effective rapid-response countermeasure is to thoroughly erase your devices. Using third-party apps for this purpose can be unreliable, as they often have limited permissions and may not completely erase the device. Full erasure typically requires permissions not usually granted to third-party apps.
- Additionally, downloading apps from unverified app store developer accounts or third-party websites poses a risk. These apps often need broader permissions to operate, which can compromise your device's security.
- For reliable and secure device wiping, we recommend using native features provided by your mobile operating system.
    - For Android devices, follow the specific steps in the settings menu for a factory reset.
    - For iOS devices, use the built-in feature to erase all content and settings.
    - For older devices, please refer to the manufacturer's documentation for detailed instructions on how to reset the device or erase its data effectively.

Strategies for navigating long-term internet shutdowns

For activists, consistent internet access is essential to stay connected and continue their work. However, long-term internet shutdowns are a common occurrence in oppressive situations. Here are strategies to manage these types of situations:

- Identify the type of internet shutdown: Determine if it's a complete blackout or if only certain sites and services are blocked. This knowledge helps in finding alternative ways to stay connected.
- Use VPNs or proxies: If the shutdown only blocks certain sites or services, accessing them through a VPN or proxy can be effective.
- Consider alternative internet access methods: If standard internet access is disrupted, explore options like satellite internet providers (e.g., Starlink) or mesh networks. Be aware that these alternatives might be more costly and not available in all regions.

3

Open-source intelligence: Tools and techniques for effective investigation

Open-source intelligence (OSINT) is a method of intelligence gathering that focuses on collecting and analyzing information from publicly available sources. These sources include social media, news articles, government records, and other online databases or resources. While freely accessible, they may not be readily searchable through standard methods.

These sources can provide critical information, aiding investigations to uncover the truth behind the actions, activities, intentions, and operations of people, businesses, high-profile figures, governments, and other entities.

OSINT is used by various groups, including law enforcement, intelligence agencies, journalists, and researchers. It serves as a powerful tool for gathering information and gaining insights, enabling informed decision-making. OSINT can reveal details that are not easily accessible through other means.

This section is designed as an introduction for those interested in learning about OSINT. It provides an overview of some effective tools and techniques you can employ in your investigative endeavors.

Introduction to OSINT: Techniques, tools, and resources for activists

- Start with the basics: Master basic OSINT techniques like Google search operators (Google dorks) and advanced social media search filters, and use archive.org for historical website versions.
- Join OSINT communities: Engage with online communities such as Reddit's /r/OSINT or follow the #OSINT on X (formerly Twitter). These platforms are valuable for sharing knowledge, learning from others, and keeping up with the latest tools and techniques.
- Read OSINT blogs for the latest insights:
  - Bellingcat: An independent international collective of researchers, investigators, and journalists. They excel in using open-source information for global event investigations, with a focus on digital forensics and geolocation.
  - Intel Techniques: Specializes in OSINT investigations and digital privacy. They offer tools and resources for those eager to learn more.
- Experiment with OSINT tools:
  - Maltego: A commercial link analysis tool with a freemium version, ideal for OSINT and forensic investigations. It helps in data mining, information gathering, and visualizing complex data relationships.
  - SpiderFoot: An OSINT automation tool that integrates with numerous data sources, facilitating easy data navigation.
  - FOCA (Fingerprinting Organizations with Collected Archives): An open-source tool for finding metadata and hidden information in various document types, capable of using multiple search engines for data analysis.
- Use open-source software: Employ open-source software like Linux, LibreOffice, and GIMP for data editing and analysis. Open-source software is cost-effective, customizable, and benefits from transparent, community-driven development.

Best practices for activists conducting OSINT research

Use multiple sources for verification

Cross-check information from one source with other sources to ensure accuracy and prevent the spread of misinformation.

Maintain records of your sources

Keep detailed documentation of your sources, including dates, times, URLs, or other pertinent details. This practice aids in verifying information, correct citation, avoiding plagiarism accusations, and efficient retrieval of needed sources.

Stay informed about legal and ethical considerations

Understand the legal and ethical frameworks relevant to your research. Being informed about your rights and responsibilities can empower you and help you avoid legal issues. Use this knowledge to conduct more effective and responsible investigations.

Additional resources for those who want to dig deeper

- First Steps to Getting Started in Open Source Research

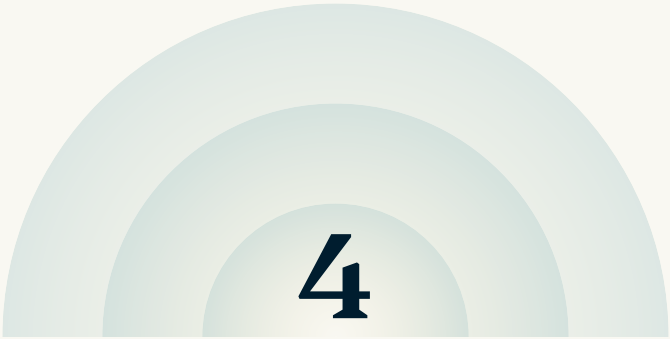
  This introductory guide by Bellingcat, a renowned investigative journalism website, outlines the initial steps for effective OSINT investigations. It covers assessing your skills and interests, connecting with fellow researchers on social media, and engaging with open-source communities.

- GitHub: toolsforactivism

  This GitHub repository offers a curated collection of digital tools tailored for activism. It features both open-source, self-hosted tools and software-as-a-service solutions for individuals, groups, or organizations involved in campaigning, organizing, or communicating for social change.

- GitHub: awesome-osint

  Explore a comprehensive list of OSINT tools and techniques to enhance your investigative work.



4

Protecting activists through pro bono legal services

If you're an activist, you know how important it is to protect your own rights and those of the people and communities you support. However, accessing legal resources can be challenging. Pro bono legal services offer a solution by providing free legal assistance to qualifying organizations and individuals.

Online pro bono legal service providers

- Avocats Sans Frontières: An international organization that offers support to those affected by conflict and human rights abuses. Services include legal representation, mediation, and advocacy.
- Advocates for International Development (A4ID): A global charity that matches international legal expertise with local needs in over 100 jurisdictions, supporting NGOs with legal training and resources.

- TrustLaw: A global pro bono legal service that connects NGOs and social enterprises with law firms, focusing on media freedom, inclusive economies, and human rights. Run by the Thomson Reuters Foundation, its global network covers over 6,500 members in 190 countries.
- LawHelp.org (U.S. only): A directory of legal aid organizations, legal rights information, and self-help resources. Features live chat and a legal aid hotline directory.

Local pro bono legal service providers

- Many bar associations offer pro bono legal services or can refer you to programs in your area. Check yours to see what's on offer.
- Contact local law schools. Some may be able to connect law students or attorneys with people needing legal assistance.
- Search for legal aid organizations in your area that offer free or low-cost services based on eligibility.

Tips for success

If you're considering working with pro bono legal services, there are a few things to keep in mind to ensure the best possible outcome:

- Know your legal rights and obligations, which could involve keeping records of relevant incidents or interactions.
- Be cautious about sensitive information and activities that might lead to legal risks.
- Use secure communication methods to maintain privacy and confidentiality.
    - Refer to Section 2 of this guide, "Securing your communications on the field," for insights on encryption and tools recommended by our security experts.

5

Supporting mental health: Resources and check-ins for activists

Advocating for change can be emotionally and psychologically challenging. Prioritizing self-care is not just an act of self-preservation, but an act of resistance. It ensures you can continue to fight for your cause and effect change over the long term. By taking care of yourself, you're better equipped to support those around you and make a lasting impact.

Here are some well-regarded resources for support:

Apps for meditation or mindfulness practices

- Insight Timer is a free app that offers a variety of guided meditations and mindfulness exercises.
- Forest helps you stay focused and productive by planting trees in a virtual forest as you work. If you stop working, the tree stops growing and dies.
- Headspace offers guided meditation and mindfulness exercises to help you manage stress and anxiety.

- Calm provides guided meditations, breathing exercises, and sleep stories aimed at reducing stress, and promoting a greater sense of calm.

Counseling services and support groups

- Open Path Psychotherapy Collective: An NGO that offers affordable therapy for individuals, couples, and families. The organization's mission is to provide access to affordable mental health services to all, regardless of financial standing.
- Check-in with your local community health center or clinic. Many local organizations provide affordable or free counseling services for those who need specialized support.

Other resources

- The Mindful Path to Self-Compassion: A book by Christopher Germer that discusses mindfulness-based tools for cultivating self-compassion, and freeing yourself from destructive thoughts and emotions.
- The Body is Not an Apology: A website and social media community focused on radical self-love and body positivity. They also offer free online courses, virtual support groups, and events.

Self-care practices

Make time in your day for the basics.

- Exercise or movement: Engage in physical activities like running, dancing, or yoga for mental and physical health benefits.
- Spending time in nature: Go for a walk or hike, spend time gardening, or be in nature. Spending time in green spaces can reduce stress, improve mood, and boost immune function. It's a simple yet powerful way to recharge and feel more connected to the world around you.

- Creative pursuits: Engage in activities that allow you to express yourself creatively, such as painting, writing, or playing music. Whether you're a seasoned artist or a beginner, the act of creating something from scratch can be incredibly satisfying. Give yourself permission to explore your creative side and see where it takes you.
- Mindful breathing: Take a few deep breaths and focus on the sensation of the air moving in and out of your body, noticing any sensations or tension. Focus on each breath through slow, intentional movements. The UCLA Mindful Awareness Research Center has free mindfulness meditations available on its website.

If you're in a crisis or any other person may be in danger, these resources can offer immediate help.

6

Collaboration tools for effective coordination and communication

Collaboration tools enable teams to share information and align with team members with greater efficiency. This section overviews collaboration tools that prioritize privacy and security, enabling confident communication and collaboration.

We focus on decentralized, independent, and Big Tech-agnostic tools to reduce reliance on centralized services and enhance data control while staying connected and organized.

Messaging and communication

- Signal: A free, open-source messaging app emphasizing privacy and security. It offers end-to-end encryption for messages, calls, and files, ensuring only intended recipients have access.
- Element: An encrypted platform for secure, decentralized communication across web, desktop, and mobile. Open-source with flexible hosting, Element allows for public/private groups, file sharing, and voice/video calls.

- Jami: A free peer-to-peer, end-to-end encrypted communication platform. It operates on a distributed architecture, avoiding central servers, and supports voice/video calls, messaging, and file sharing without compromising on privacy.

Project management tool

- Taiga: An open-source, self-hosted project management tool suitable for agile development and other project types. Features include task creation, progress tracking, forums, issue tracking, and chat integration, allowing you to communicate and collaborate with your team.

Video conferencing

- Jitsi: A user-friendly, free, open-source video conferencing platform. It requires no account registration and offers encrypted, open-source, privacy-focused features.

Secure file-sharing

- OnionShare: An open-source tool that allows you to share files securely via the Tor network, encrypting and anonymizing communications, making it difficult for anyone to intercept or surveil your data.

Productivity suite

- CryptPad: An online collaboration suite offering end-to-end encryption for documents, spreadsheets, and presentations. It supports collaborative editing with access controls and privacy settings.

Collaborative text editing

- Etherpad: An open-source text editor for simultaneous document collaboration. It supports real-time collaboration and auto-saving, allowing you to work together with others on documents when you're not in the same physical location.

Scheduling

- Framadate: An open-source online tool for efficient meeting and event scheduling. Features include polls, surveys, multiple languages, privacy settings, and access controls.

7

Translation tools for building an inclusive movement

Incorporating materials in multiple languages can be a powerful way to reach a broader audience and increase accessibility. This approach builds a more inclusive movement, welcoming people from diverse backgrounds who might have been excluded or marginalized due to language or cultural differences.

For more effective localization, consider also the cultural norms and linguistic nuances of the target audience.

Here are some tools to support you in your translation and localization projects:

- DeepL: An AI-powered neural machine translation platform offering high-quality translations in over 30 languages. Known for natural, accurate translations and a user-friendly interface.
- MateCat: A cloud-based tool for translating documents, websites, and other materials into over 100 languages. It's free and supports collaborative translation, allowing simultaneous work on the same project.

- OmegaT: A community-driven, open-source translation memory tool, continually improved by volunteers.
- Crowdin: A cloud-based localization solution with project management tools to streamline the process. It also offers a free option to support non-profit and open-source community projects.
- GIMP: An open-source image editing software suite for localization purposes, such as translating text found in images or creating localized graphics.

8

Cybersecurity and technology assistance for civil society organizations

We understand that civil society organizations often lack the resources to implement comprehensive cybersecurity protection. To address this gap, initiatives like the following programs have been created to provide technological assistance and expertise:

- CyberPeace Builders program: A network of cybersecurity experts from technical and non-technical backgrounds, employed by local and international companies, who volunteer to help civil society organizations (CSOs) protect against online threats. This program offers free cybersecurity expertise to CSOs, ensuring the continued delivery of critical services to vulnerable populations. You can register your CSO and explore the program's services and tools, including policies on cybersecurity, data, and incident response, and awareness of potential cyberattack vulnerabilities.
- TechSoup: Provides technological assistance for organizations, including online consultants, tech support, online courses, and managed IT.

Acknowledgements

We extend our gratitude to the experts who contributed to the original workshop at RightsCon in June 2023, which laid the foundation for the development of this Library. Their valuable insights and participation were instrumental in shaping this resource:

- Francesca Bosco, Chief Strategy and Partnerships Officer at cybersecurity and digital rights NGO CyberPeace Institute
- Rhona Tarrant, Head of Editorial at social news and strategic intelligence agency Storyful
- Shirin Mori, Senior Design & Research Lead of the NGO Electronic Frontier Foundation (EFF)

Contact us

Should you have any recommendations for the Digital Security Resource Library, or if you're an organizer or journalist seeking assistance, please reach out at:

ExpressVPN: safe@expressvpn.com
CyberPeace Institute: assistance@cyberpeaceinstitute.org

ExpressVPN