

Resource Hub Guidelines for Strengthening Democratic Discourse in Sudan

Technical Guideline for Disinformation



Introduction

This document provides comprehensive guidelines under the Resources Hub of Labs for Development Organization. The Hub aims to empower a wide range of stakeholders, including civil society organizations (CSOs), journalists and media practitioners, youth and students, educational institutions, local media outlets, women's groups, and marginalized and vulnerable communities. By equipping these groups with the necessary tools and knowledge, the Hub seeks to enhance their ability to identify, understand, and combat disinformation effectively. This guideline is designed to foster a more informed and resilient society capable of navigating the complex information landscape with confidence and critical thinking.

Structure Overview

Section One: Media Literacy: Focuses on building skills to analyze and evaluate media content critically.

Section Two: Roles of Social Media Platforms: Explains how social media algorithms work and their policies on Disinformation.

Section Three: Introduction to Fact-Checking: Provides techniques and tools for verifying information.

Section Four: Digital Security for Fact-Checkers: Offers strategies and tools to protect digital communications and data.

Section One: Media Literacy

Introduction

Media literacy is the ability to access, analyze, evaluate, create, and act using all forms of communication. In today's digital age, where information is abundant and sometimes overwhelming, media literacy is crucial for ensuring individuals can discern the quality and credibility of the information they consume, especially in politically and socially charged environments like Sudan. Interactive tools, such as media literacy courses and bias-checking software, can provide practical skills and enhance understanding.

Sudan has experienced significant political upheaval, social unrest, and conflicts, making the media landscape complex and often contentious. In such environments, media literacy becomes not just a valuable skill but a necessary one. In politically charged environments, various groups might use media to disseminate propaganda. Media literacy helps individuals identify and resist manipulative messages designed to sway public opinion unfairly as Media can either inflame tensions or promote peace. Media literate individuals are better equipped to choose media that fosters understanding and cooperation rather than division.

Understanding Media Bias

To navigate the complex landscape of media, it's essential to understand the concept of media bias. Media bias refers to the systematic favoritism or prejudice present in the content produced by media outlets. By recognizing and understanding the various types of bias, individuals can better assess the credibility and reliability of the information they encounter.

Understanding media bias involves recognizing various types of bias that can influence content. Political bias occurs when media content is swayed towards a particular political stance or party. Corporate bias arises from influences by ownership or sponsorship that may affect the portrayal of news to align with corporate interests. Sensationalism involves the use of exciting or shocking stories at the expense of accuracy, aimed at attracting viewers or readers. For instance, during the 2019 Sudanese revolution, media outlets with political affiliations often portrayed events in ways that reflected their biases, influencing public perception.

=Here are some tips on how to define the potential bias in the content:

- **Check the Source:** Understanding the ownership and funding of the news source is crucial in identifying potential biases. Media outlets with affiliations to specific political parties or corporate interests may prioritize certain perspectives over others. By researching the background of a news source, including its ownership structure and financial backers, individuals can gain insights into the potential biases that may influence its reporting.
- **Analyze the Language:** Language is a powerful tool that can reveal biases in media content. Words with strong emotional implications or subjective statements can indicate a particular bias. For example, loaded language that

vilifies or glorifies individuals or groups may suggest a bias towards a specific agenda. Analyzing the language used in news articles or broadcasts can help individuals discern the underlying perspectives and biases present in the content.

- **Look for Balance:** Balanced coverage involves giving equal space to all sides of a story, allowing readers or viewers to form their own opinions based on comprehensive information. When analyzing news coverage, individuals should assess whether all relevant viewpoints are represented fairly. Omissions or disproportionate coverage of certain perspectives may indicate bias towards a particular narrative. By seeking out diverse sources and perspectives, individuals can gain a more nuanced understanding of complex issues.

To be able to verify the resources where the content is published, here are some recommended techniques:

- **Cross-Verification:** Cross-verification involves checking information with multiple trusted sources to confirm its accuracy. By consulting a range of reputable news outlets and fact-checking organizations, individuals can corroborate information and reduce the risk of relying on Disinformation. Cross-verification is especially important in the age of social media, where false information can spread rapidly, and verification is essential to distinguish fact from fiction.
- **Source Expertise and History:** Evaluating the expertise and historical reliability of a source is crucial in assessing its credibility. Individuals should consider whether a source specializes in the topic at hand and whether it has a track record of providing accurate and trustworthy information. Established news organizations with a history of rigorous journalism are generally more reliable than sources with a limited or dubious track record.
- **Source Intent:** Assessing the intent behind a source's reporting can help individuals identify potential biases or motives for Disinformation. Individuals should consider whether a source has a vested interest in promoting a particular agenda or viewpoint. For example, sources that prioritize sensationalism or clickbait may sacrifice accuracy for the sake of attracting attention. By critically evaluating the intent behind a source's content, individuals can better discern its credibility and reliability.

One essential skill needed to verify the authenticity of the published content is interpreting Data and acquiring Data Literacy Skills. For example, understanding charts and graphs (Data visualizations) such as bar charts, line graphs, and pie charts, are essential tools for conveying complex information in a digestible format. Learning to read and interpret these visualizations accurately is crucial for effective data literacy. Also, evaluating data sources to validate

credibility and reliability of data where the sources from which it originates, and the methodologies used to gather and analyze it. Evaluating data sources is essential for ensuring the accuracy and validity of the information being presented.

Finally, spotting misleading statistics as statistics can be manipulated in various ways to mislead or distort the truth. Developing the ability to spot misleading statistics is essential for maintaining data literacy and making informed decisions based on accurate information. These are briefly some of the common manipulation techniques used in publishing unreliable content:

- **Cherry-Picking Data:** Cherry-picking data refers to the selective presentation of data points that support a particular viewpoint while ignoring or omitting other data that may contradict it. This practice can distort the overall picture and lead to biased conclusions. For example, in a debate about the effectiveness of a certain policy, cherry-picking data might involve highlighting only the instances where the policy had positive outcomes while ignoring instances where it failed or had negative consequences. By selectively presenting data in this manner, individuals or organizations can manipulate perceptions and promote a biased narrative.
- **Improper Scale Usage:** Improper scale usage involves manipulating the scale on charts or graphs in a way that distorts the representation of the data. Changing the scale can exaggerate or downplay the significance of the data, leading to misinterpretation. For instance, adjusting the y-axis scale on a line graph to start at a value other than zero can create the illusion of more significant changes than exist. Similarly, altering the scale on a bar chart can make differences between data points appear larger or smaller than they truly are. Improper scale usage can mislead viewers and skew their understanding of the data being presented, ultimately leading to erroneous conclusions.

Learning Resources for Media and Data Literacy

- [The On-ramp to Media Literacy](#)
- [Data Literacy: What is it and why does it matter?](#)
- [Making Sense of the News: News Literacy Lessons for Digital Citizens](#)

Conclusion

Media literacy is a critical skill set for navigating today's complex information environment in Sudan especially during war time and political unrest as Disinformation are more likely to be disseminated. By educating citizens on how to identify media bias, verify sources, and interpret data correctly, we can empower them to make informed decisions and engage responsibly in civic discussions. This section provided the tools and knowledge necessary to enhance the media literacy of individuals and communities across the country.

Section Two: Roles of Social Media Platforms

Introduction

Social media platforms have become integral components of the contemporary information ecosystem, especially in regions like Sudan where access to traditional media might be restricted or inaccessible due to power restrictions. These platforms serve as dynamic channels for the swift dissemination of information, capable of reaching wide audiences in real-time. However, they also pose significant challenges, serving as potent vehicles for the propagation of Disinformation and disinformation. Given their immense influence, it is imperative to comprehend the underlying mechanisms of these platforms to navigate and mitigate the spread of false narratives effectively. Understanding how information spreads, the algorithms shaping content visibility, and the dynamics of online communities are essential for developing strategies to combat disinformation and promote accurate information on social media.

Understanding Algorithms and Content Dissemination

How Algorithms Work

Social media algorithms are complex systems designed to personalize and maximize user engagement. They analyze user behavior—such as likes, shares, comments, and time spent on different types of content—to determine what content is most likely to keep users on the platform. By prioritizing content that elicits strong emotional reactions or confirms users' existing biases, these algorithms aim to create a more engaging and personalized experience. This approach often leads to the amplification of content that evokes emotions like outrage, fear, or joy, as these are more likely to be interacted with.

The nature of these algorithms can inadvertently promote sensationalist and false content. Content that triggers strong emotional responses typically receives higher engagement rates—more likes, shares, and comments—which in turn signals to the algorithm that this content is valuable and should be shown to more users. This feedback loop can result in the rapid spread of Disinformation, as sensational or alarming falsehoods are more likely to engage users than mundane truths. Consequently, Disinformation can gain visibility and traction much faster than accurate information, contributing to widespread false beliefs.

Consider a scenario during political unrest in Sudan. An unfounded rumor about violence and looting by demonstrators might be posted on a social media platform. This type of content triggers emotions such as fear and uncertainty, which are powerful motivators for user engagement. As people react by commenting, sharing, or expressing their concerns, the platform's algorithm interprets these interactions as indicators of valuable content. As a result, the algorithm promotes this rumor to more users, causing it to spread rapidly. The more people

engage with the rumor, the more visibility it gains, perpetuating a cycle of Disinformation dissemination driven by the algorithm's design to prioritize engaging content.

By understanding how these algorithms work, users can become more critical of the content they encounter on social media platforms. Recognizing the role of algorithms in amplifying emotionally charged and potentially false information can help users approach such content with a more discerning eye, seeking verification from reliable sources before accepting or sharing it. Additionally, this understanding can inform efforts to develop more balanced algorithms that prioritize accuracy and reliability alongside engagement.

Major Social Media Platforms and Their Disinformation Policies

Social media platforms have been at the forefront of the fight against Disinformation, developing a range of policies and tools to mitigate the spread of false information. These policies are critical for maintaining the integrity of public discourse, especially in politically sensitive contexts. However, their effectiveness can vary based on local contexts and language support, making it essential to adapt these policies to the specific needs of regions like Sudan. The following are the common social media platforms, and their algorithms policies to prevent and detect Disinformation:

- Facebook:
 - **Content Labeling:** Facebook uses labels for news that fact-checkers have found to be false or partly false. These labels appear directly on posts in the news feed, providing users with a warning before they share or react to misleading information. This labeling system helps users make informed decisions about the content they encounter.
 - **Visibility Reduction:** Posts deemed to be false by verified fact-checkers are less visible in the news feed, significantly reducing their reach. By limiting the exposure of false information, Facebook aims to minimize the potential harm such content can cause.
 - **Removal Policies:** Facebook actively removes content that could lead to imminent physical harm. For Disinformation that doesn't meet the removal criteria, they focus on reducing its distribution and providing additional context. This includes false health information, which can be particularly harmful in the context of public health crises.
- X (Twitter):
 - **Manipulated Media Labels:** X labels tweets that feature manipulated media, such as deepfakes or significantly edited videos that aim to deceive. This label warns users that the content they are viewing may be distorted or taken out of context. This is crucial for maintaining the credibility of information, especially during sensitive times like elections or social unrest.

- **Civic Integrity Policy:** During elections or other major civic processes, Twitter enforces stricter rules against misleading claims that could undermine public confidence in the process. This includes false information about voting methods and election outcomes, which can severely impact democratic processes.
 - **Strike System:** X uses a strike system for repeated violations of its Disinformation policies, where repeated offenses can lead to permanent suspension. This system aims to deter users from consistently spreading false information by imposing escalating consequences.
- Instagram:
 - **Fact-Checking Program:** Like Facebook, Instagram partners with third-party fact-checkers to identify, review, and label false information. This collaborative effort enhances the accuracy of the information presented on the platform and helps users identify misleading content.
 - **Content Demotion:** Content flagged as false is removed from Instagram Explore and hashtag pages to limit its spread. By reducing the visibility of false information, Instagram seeks to prevent the amplification of misleading content.
 - **User Warnings:** When users attempt to share content that has been flagged as false, Instagram shows a warning, informing them of the fact-checkers' findings before they proceed. This proactive approach helps users reconsider sharing potentially harmful Disinformation.

Local Context: Application of Policies in Sudan

In Sudan, the application of policies aimed at countering Disinformation faces unique challenges inherent to the local context, which may impact their effectiveness. One such challenge is the presence of language barriers. Much of the technology used for content moderation and third-party fact-checking services is primarily optimized for English, creating a significant gap in content moderation for Arabic posts or local dialects prevalent in Sudan. This gap potentially allows Disinformation in these languages to circulate more freely, as the tools designed to detect and combat it may not be as effective. Additionally, Disinformation often exploits local contexts and cultural nuances, which may be overlooked by global platforms' moderation policies that are not tailored to specific regional dynamics. This cultural contextualization aspect highlights the need for policies and interventions that consider Sudan's unique sociocultural landscape. Furthermore, the effectiveness of content labels and warnings depends significantly on users' digital literacy levels. In regions like Sudan, where digital literacy is uneven, the impact of these policies may be diminished as users may not fully understand or trust these interventions.

To address these challenges effectively, strategic recommendations are necessary. Policymakers, local NGOs, and community leaders in Sudan should advocate for local language support from social media platforms, engaging with them to improve support for

Arabic and other local languages in moderation tools and fact-checking services. Additionally, there is a need to increase efforts to boost digital literacy through educational initiatives, focusing on teaching users how to critically evaluate information and understand the implications of sharing unverified content. Collaboration with local fact-checkers is also essential, as they can provide culturally and contextually relevant insights, enhancing the accuracy and effectiveness of moderation policies.

In Sudan, where digital discourse heavily influences social dynamics, empowering citizens with knowledge and tools to critically engage with social media is paramount. This involves not only understanding and leveraging platform tools to combat Disinformation but also participating in policy feedback mechanisms to shape more effective governance of digital spaces. By addressing these challenges and implementing strategic recommendations, Sudan can better navigate the complexities of Disinformation and promote a more informed and resilient digital society.

By demystifying the roles of social media platforms in the spread of Disinformation and providing practical tools for engagement and reporting, this section aims to empower stakeholders in Sudan to more effectively navigate and shape their information environments. The goal is to foster a more informed and critical social media user base that can resist manipulation and contribute to a healthier public discourse.

Section Three: Introduction to Fact-Checking

Introduction

Fact-checking is the process of verifying information to ascertain its accuracy and authenticity, playing a pivotal role in combating Disinformation and maintaining the integrity of public discourse. It supports democratic societies by ensuring citizens make decisions based on reliable information. In Sudan, where Disinformation can fuel political instability, robust fact-checking practices are crucial. Fact-checking prevents the spread of false narratives, supports informed decision-making, builds trust in media and institutions, and mitigates political instability. Enhancing these practices through training, international collaboration, public awareness campaigns, and leveraging technology is essential for building and preserving democratic processes in Sudan.

Identification Techniques:

Recognizing Red Flags in News Items

Disinformation often contains several identifiable red flags that can alert a discerning reader to potential falsehoods:

- **Sensational Headlines:** Be wary of headlines that claim shocking or unbelievable events. These headlines often aim to provoke emotional reactions rather than provide informative content. Sensationalism is a common tactic used to attract clicks and shares, sometimes at the expense of truth and accuracy.
- **Mismatched Images:** Images that don't match the story context may be recycled from unrelated events or digitally altered. This tactic is used to give the impression of authenticity and urgency, but a discerning reader can spot discrepancies by checking the source and context of the images.
- **Lack of Credible Sources:** Reliable news stories include quotes from and references to credible sources, such as experts or official institutions. The absence of verifiable quotes or the use of anonymous sources can indicate that the story is not well-substantiated.
- **Example:** Consider a social media post claiming that a specific political party in Sudan has decided to boycott the upcoming elections. The post features an inflammatory headline: "Massive Boycott Threatens Sudan's Electoral Process!" However, it lacks verifiable quotes from party leaders and uses an outdated image from a previous protest.

Red Flags in the example above:

- **Sensational Headline:** The thought up headline "Massive Boycott Threatens Sudan's Electoral Process!" can be seen as designed to incite strong emotions, such as fear or outrage, rather than to inform. Its purpose is to capture attention through shock value.
- **Lack of Credible Sources:** A red flag post might not provide any official statements or quotes from the party's leadership. In a legitimate news story, readers would expect to see direct quotes from party officials or references to credible news outlets that have confirmed the story.

Tools and Software for Fact-Checking:

Overview of Available Tools

In the digital age, an array of tools was developed to help verify facts and detect false information. These tools range from simple browser extensions to complex AI-driven platforms that analyze data patterns. Understanding and utilizing these tools is crucial for anyone engaged in fact-checking, especially in a politically charged environment like Sudan.

Here are some recommended tools to assist with fact-checking:

1. AI and Machine Learning Models

Advanced AI models can analyze vast amounts of data to identify patterns indicative of Disinformation campaigns. These tools utilize sophisticated algorithms and machine learning techniques to detect anomalies and patterns that suggest coordinated efforts to spread false narratives. AI models can be particularly useful during election periods or times of civil unrest, when Disinformation tends to be more rampant.

For example, CrowdTangle, a social media analytics tool by Facebook, offers comprehensive features for scanning social media posts to identify and flag potential fake news stories. It allows users to set up custom searches for keywords, hashtags, and URLs, while analyzing user engagement metrics to pinpoint posts gaining traction. Real-time alerts enable immediate action by fact-checkers and moderators when suspicious content emerges, particularly crucial during critical events like elections. With access to historical data, CrowdTangle enables the identification of recurring Disinformation patterns, aiding in the development of effective countermeasures. Additionally, its collaborative features facilitate coordinated efforts among stakeholders in combating Disinformation, making CrowdTangle an invaluable asset in the ongoing battle against false information on social media.

To learn more about the CrowdTangle tool, visit Meta's [Data for Good site](#).

2. Browser Extensions

NewsGuard: This tool provides trust ratings for news websites, helping users to instantly see the credibility of the source directly in their browser. To use the extension install it on your browser, browse the internet, and receive real-time credibility assessments of news sites as you visit them.



Refer to this [Installation guide](#) by NewsGuard for more details on how to install and use the extension.

3. Databases and Websites for Cross-Verification and Fact-Checking

To ensure the integrity of public discourse, individuals and organizations can refer to a variety of reputable databases and websites dedicated to fact-checking. These platforms provide comprehensive tools and detailed analyses that help users cross-verify information and debunk false claims. Here are some recommended sites to consult for effective fact-checking and as reliable news resources:

- **Sudanese Websites/ Networks:**

- [Beam Reports](#) an investigative journalism platform that provides in-depth reports and fact-checking on various issues in Sudan and the region. It offers detailed investigations and fact-checks where local journalists and researchers gather and verify information on critical issues.

 [@BeamReports](#)

- [Ayin Network](#) - شبكة عاين a news network focused on providing in-depth coverage and fact-checking of events in Sudan. It delivers detailed reports and fact-checks on news stories affecting Sudan, with a focus on providing local context. They utilize a network of local journalists to gather accurate information and provide context-specific analysis.

 [@AyinSudan](#)

- [Poynter](#): A comprehensive database of fact-checking websites that can be filtered by country, including those focusing on Sudan. It is a leading journalism institute and home to the International Fact-Checking Network (IFCN), which sets standards and provides resources for fact-checking organizations worldwide.
- [Snopes](#): is one of the internet's oldest fact-checking websites, dedicated to investigating and debunking urban legends, myths, rumors, and Disinformation. It provides detailed analyses and verdicts on a wide range of claims, from viral social media posts to widely circulated news stories, ensuring that the public receives accurate and well-researched information.
- [Africa Check](#): an independent fact-checking organization, which aims to improve the accuracy of public debate and the media in Africa. It provides detailed fact-checks on claims made by public figures and in the media, focusing on topics relevant to African countries. It uses a rigorous fact-checking process to verify claims, including consulting experts and cross-referencing data.

4. Learning Resources:



- [Fact-Check It: Digital Tools to Verify Everything Online](#): A webinar to learn about some of the best tools, tips and methods for verifying information online.
- [Fact-Checking Fundamentals with IFCN](#): With support from Meta, the International Fact-Checking Network (IFCN) offers a free introductory fact-checking course targeted to journalists. Composed of three modules focusing on fact-checking, verification and debunking and mis- and disinformation, the course will prime journalists on how to find fact-checkable claims, the methodology for fact-checking and tools and techniques to assist in their journey.
- [Hands-on Fact-checking](#): A self-directed course or as a resource for classroom instructors, the approximately 90-minute course includes lessons on identifying reliable sources in fact-checking, debunking viral Disinformation, and deciding whether a statement is checkable.
- [How to spot Disinformation online?](#): A short course from MediaWise and IFCN to learn simple digital literacy skills to outsmart algorithms, detect falsehoods and make decisions based on factual information.
- [Data Detox Kit](#): An online resource that provides practical steps for individuals to protect their data and understand digital privacy. It offers tips and tools for digital hygiene and critical evaluation of online information.

5. Tutorials:

- [Using Google Reverse Image Search](#): This tool helps users to quickly find fact-checking articles about specific topics or claims. You only need to enter a claim or topic into the FactCheck Explorer search bar to retrieve related fact-checking articles from reputable sources.

Application in Sudan

In the context of Sudan, where Disinformation can significantly impact social and political stability, these tools are invaluable for journalists, activists, and civil society organizations. They can use these resources to verify information during election cycles, verify claims made by political figures, or counteract harmful rumors during humanitarian crises.

Understanding and leveraging these technical tools and resources empower individuals and organizations in Sudan to become proactive participants in their information ecosystem, enhancing their ability to discern truth from falsehood and contributing to a more informed and resilient society.

Section Four: Digital Security for Fact-Checkers

Introduction

Digital security is paramount for fact-checkers who often deal with sensitive information and can be targets of cyber threats due to their work exposing falsehoods and holding entities accountable. This section provides essential practices, tools, and strategies to safeguard their digital presence and information integrity. In regions like Sudan, where political environments can be volatile, ensuring the security of communications and data is not only about protecting fact-checkers but also about upholding the integrity of their work.

Why It Matters: The importance of using secure communication tools for fact-checkers, especially when discussing sensitive information, cannot be overstated. These tools are crucial in preventing sensitive data from being intercepted by malicious actors, which is a significant risk given the nature of the information fact-checkers often handle. These tools are essential for: maintaining high standards of digital security, fact-checkers to be able to ensure the confidentiality of their sources, the accuracy of their reports, and their own personal safety.

Fact-checkers frequently rely on confidential sources who provide critical information that may expose corruption, Disinformation, or other sensitive matters. The security of these communications is paramount to protect the identities of these sources and the integrity of the information they provide. Tools like Signal and ProtonMail use end-to-end encryption, ensuring that only the sender and recipient can access the contents of their communications, thereby safeguarding the anonymity and safety of sources.

Secure communication tools ensure that the information being exchanged remains intact and unaltered during transmission. This is crucial for maintaining the accuracy and reliability of the facts being checked. Encryption prevents intermediaries from altering messages, ensuring that the data received is exactly as sent.

Fact-checkers often handle data that could be damaging if released prematurely or without proper context. Secure tools prevent unauthorized access to communications and data, mitigating the risk of data breaches. This not only protects the operational security of the fact-checking organizations but also reduces the risk of reputational damage that could undermine their credibility.

In many regions, including places like Sudan, the political environment can be volatile, and the exposure of certain information can lead to legal or political repercussions. Secure communication tools minimize the risk of interception by state actors or other entities that might use the information to suppress dissent or retaliate against fact-checkers and their sources.

Using secure communication tools signals to sources and partners that a fact-checking organization is committed to security and privacy. This builds trust—a crucial element in obtaining high-quality, sensitive information from sources who might otherwise be reluctant to share it.

In some jurisdictions, there are legal requirements to protect personal data and communications. Employing encryption and secure communication tools helps fact-checking organizations comply with these regulations, avoiding legal penalties and demonstrating their commitment to ethical journalism practices.

The use of encrypted and secure communication tools is fundamental for fact-checkers, particularly when handling sensitive information that, if compromised, could have severe consequences. These tools are not merely optional extras but essential components of the infrastructure that supports the critical work of fact-checking, allowing practitioners to carry out their roles safely, responsibly, and effectively.

Secure Communication

For secure communication and protection of sensitive data, these tools and practices can help fact-checkers protect their identities, communicate securely, and access information anonymously, ensuring their safety and the integrity of their work in challenging environments.

A recommended practice for communication is to avoid using public Wi-Fi when transmitting sensitive information, and to use a secure, private network connection (VPNs). VPNs encrypt users' internet traffic and route it through a remote server, masking their IP addresses and providing anonymity online. Fact-checkers can use VPNs to access the internet securely,

Secure tools:

- **Signal:** A secure messaging app that provides end-to-end encryption for text messages, voice calls, and video calls. It is widely regarded as one of the most secure messaging platforms available, and it is open source, meaning its code is publicly available for scrutiny. Fact-checkers can use Signal to communicate securely with colleagues, sources, and whistleblowers, knowing that their conversations are protected from eavesdroppers.

[Download Signal](#)

- **ProtonMail:** An encrypted email service that prioritizes user privacy and security. It offers end-to-end encryption for emails, meaning that even ProtonMail cannot access the contents of users' emails. Fact-checkers can use ProtonMail to communicate securely without fear of their messages being intercepted or surveilled.

[Download ProtonMail](#)

Data Protection



1. Techniques for Safeguarding Data:

- **Regular Backups:** Encourage regular backups of important data to external drives or secure cloud services to prevent data loss in case of cyber-attacks.
- **Use of Strong Passwords and Authentication:** Advise on creating robust passwords and using multi-factor authentication to enhance account security.

2. Tools for Data Security:

- **Encrypted Storage Solutions:** Services like Veracrypt or BitLocker that provide encryption for data stored on devices.
- **Secure Cloud Storage:** Recommend secure cloud storage providers that offer end-to-end encryption.

Anonymity and Safety Online

1. Maintaining Anonymity:

- **Tor Browser:** This Browser is a powerful tool for accessing the web anonymously. It routes internet traffic through a network of volunteer-operated servers, encrypting data multiple times and bouncing it through random nodes, making it extremely difficult to trace back to the user. This can be particularly valuable for fact-checkers working under oppressive regimes where their safety may be at risk.

[Download Tor Browser](#)

- **Anonymous Email Addresses:** Use of disposable or anonymous email services for communications that require identity protection like ProtonMail (see section above).

2. Strategies to Enhance Online Safety:

- **Educate on Digital Footprints:** Raise awareness about how much personal information is accessible online and how to minimize exposure.
- **Regular Security Audits:** Encourage routine checks of digital security measures to ensure they are up to date and effective.

Training and Resources

This [Data Detox workshop](#) on online privacy offers participants an opportunity to delve into the significance of online privacy. Through discussions and practical activities, participants will learn about the data and examine its impact on individuals and societies.

Conclusion



In the digital age, the security of information and communication is crucial for the effective operation of fact-checkers in Sudan. This section of the guidelines equips them with the necessary tools and knowledge to protect themselves and their work from digital threats, ensuring that their valuable contributions to society continue safely and securely.

Guideline Conclusion

This comprehensive guideline, housed within the Resources Hub of Labs for Development Organization, serves as a vital resource for a diverse array of stakeholders. From Sudanese civil society organizations (CSOs) to journalists, educational institutions to marginalized communities, the Hub endeavors to empower individuals and groups with the necessary tools and knowledge to combat disinformation effectively. By fostering critical thinking and resilience, this initiative aims to cultivate a more informed and resilient society capable of navigating the complexities of the modern information landscape with confidence. Through collective action and unwavering dedication, we can work towards a future where accuracy prevails, empowering individuals to make informed decisions and safeguarding the foundations of democracy in Sudan.