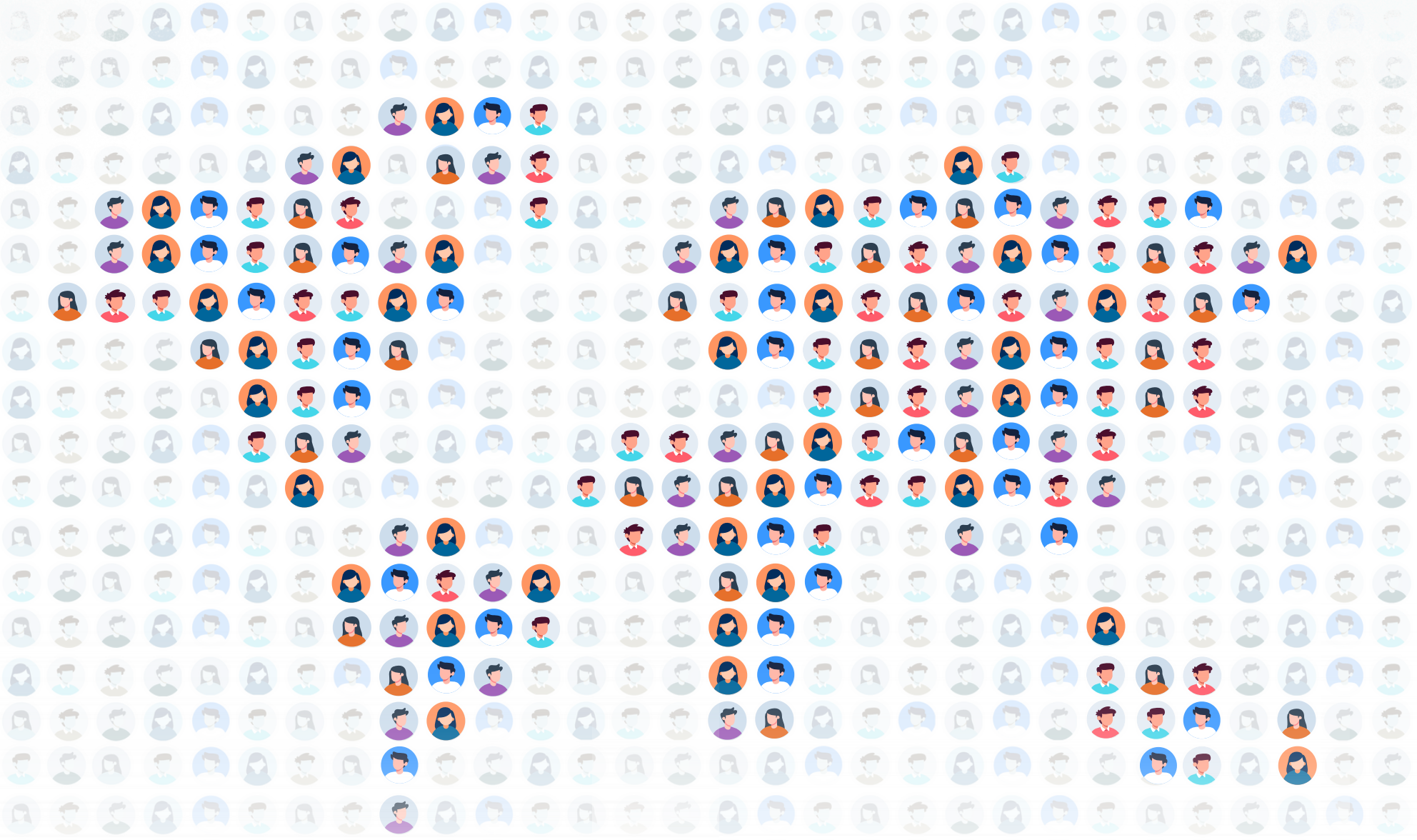


THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

مهارات
Maharat

THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

This manual was prepared by Maharat Foundation, with the support of UN Women and the French Embassy in Beirut.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

مهارات
Maharat

UN WOMEN

MODULE 7

Protecting Sources and Whistleblowers:

Strategies for maintaining the anonymity and safety of sources.

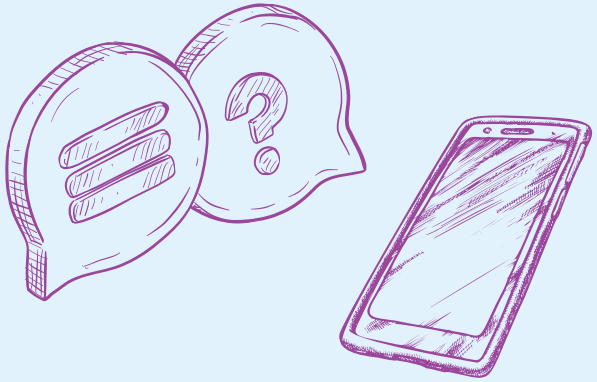
Specific for Journalists

Prepared by:
Digital security expert
Bahaa Nasr

Journalists often rely on confidential information and whistleblowers to expose wrongdoing. **Protecting sources and whistleblowers is essential for maintaining trust,** thus journalists need to make sure to **not accidentally expose where the information came from** and to preserve the anonymity and physical security of their sources.

How to protect journalists, sources and whistleblowers

Please note: The advice listed below is equally important for both the journalists and the whistleblowers.



Establish Secure Communication Channels

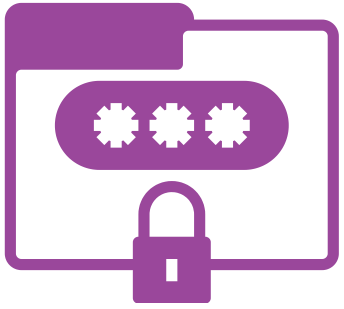
Use Encrypted Messaging Apps:

- Use end-to-end encrypted messaging apps like Signal for communication with sources, to keep conversations private. Signal is particularly recommended for its strong security practices and lack of metadata retention.
- Enable disappearing messages to automatically delete conversations after a set period of time.

- Avoid using email or landline telephone or mobile calls and SMS for sensitive communications, as these are less secure and can be easily monitored / intercepted.
- Establish a safe way for sources to make initial contact through secure encrypted email or a Signal account. There are also specialized Whistleblower apps that provide “secure mailboxes”.
- Whistleblowers need to be able to submit information anonymously without fear of tracing or identification. Tools like SecureDrop or GlobaLeaks are great for this purpose. Investigative journalists should install such tools on their website, along with an easy to understand tutorial on how to use them and a well visible warning for potential whistleblowers not to submit information through other, insecure channels.
- Whistleblowers should avoid using work devices or the internet at work to leak information. Work devices and networks may be monitored. Use personal devices and secure, private networks whenever possible.

Use Encrypted Email Services

- If email communication is necessary, use encrypted services like ProtonMail, which offer end-to-end encryption. For better security, both parties should be using ProtonMail.



Digital Security practice

Learn and implement strong digital security practices to protect your devices and data

These include but are not limited to using strong passwords, performing regular updates, activate multifactor authentication for all your accounts, encrypt sensitive files on your device.

Save Data securely

Use encryption to secure files and documents when storing sensitive information. You can use application like Veracrypt to create an encrypted container to save all your sensitive data inside this encrypted container (it is like putting your files in a safe).

Minimize Digital Footprints

Avoid using work devices for anything related to the whistleblowing topic, clear browsing history, and disable location tracking on devices to reduce potential traceability.

It is also important to permanently and securely delete data provided by sources when requested, or when it is not needed anymore. You can use tools like Bleachbit which will permanently delete files and make them irrecoverable. Deleting files through the computer bin will not permanently delete them, the files will still be recoverable with digital forensic tools.

Use Pseudonyms

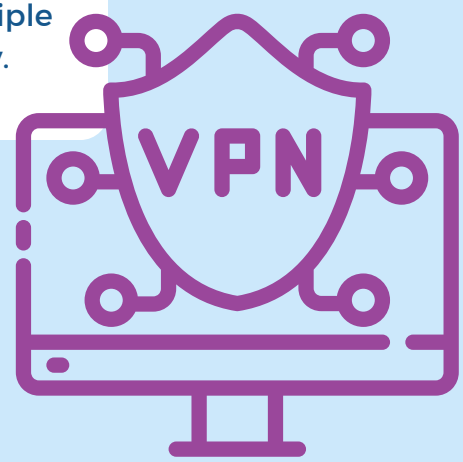
Avoid using real names in communications and use pseudonyms or aliases to keep identities more secure.

Use Virtual Private Networks (VPNs)

VPNs mask IP addresses and encrypt your internet, making it harder for hackers or government agencies to monitor your internet activities and trace locations. Use a VPN, especially when accessing the internet in public places. It is important to know the data retention and sharing policies of the VPN used, as some service providers store sensitive data and hand it over to authorities upon request.

Use Tor Browser for better Anonymity

The Tor browser offers enhanced anonymity by routing traffic through multiple servers. Journalists and sources alike can use it to access the internet anonymously.



Anonymity Protection

Defend anonymity when requested by sources. Take extra precautions when giving away any information, handling communications or meetings with whistleblowers to avoid accidentally revealing their identity. Make sure that the story published based on information provided by whistleblowers does not contain any personal identifiable information that would reveal the source of the information.

Practice “Need to Know” Basis: Limit discussions about sensitive information to only those who are essential to the story, even within your own organization, or the closest people.

Avoid using identifying information in shared workspaces, remove all personal identifiers, such as names, addresses, or specific work-related details that could expose a source's identity from documents shared between sources and journalists. If working within a team, avoid storing sources details in collaborative digital workspaces or unsecured databases.

Practice Metadata Hygiene

Strip Metadata from Files:

Photos, documents, and videos often contain metadata that could reveal: the name of the person who created the file, who last edited or saved the file, brand and model number or type of the device used, location, time and date created, and other identifying information which might give clues that lead back to the whistleblower. Remove the Metadata from the properties of the files before sharing or publishing them.

Limit Digital Trails and Record Keeping

Avoid Cloud Storage for Sensitive Files:
Store sensitive files on local devices or secure, encrypted storage rather than mainstream cloud services that could be accessed by third parties.

Delete Communication Logs:
Regularly delete messages, call logs, and communication histories to reduce the risk of exposure in case of device confiscation or hacking.

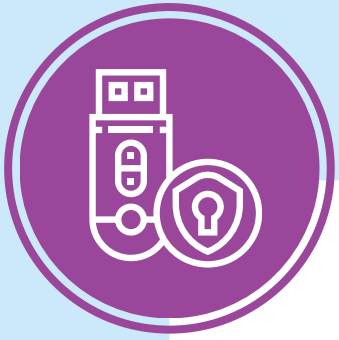
Separate Devices for Sensitive Work:
If possible, use dedicated devices solely for communication with sources to keep sensitive work separate from personal or less sensitive work activities.

Use Burner Phones:
Burner phones can help reduce traceability and protect against phone tapping.

Protect Physical Safety and Location Privacy

Disable Location Services:
Make sure that location tracking on mobile devices is turned off.

Meet in Secure, Private Locations:
For highly sensitive conversations, meet in person rather than communicating electronically. Choose private, discreet locations that aren't associated with either the journalist or the source. Avoid places where CCTV or public surveillance is likely to capture interactions. Use secure communication channels to agree on the meeting place.



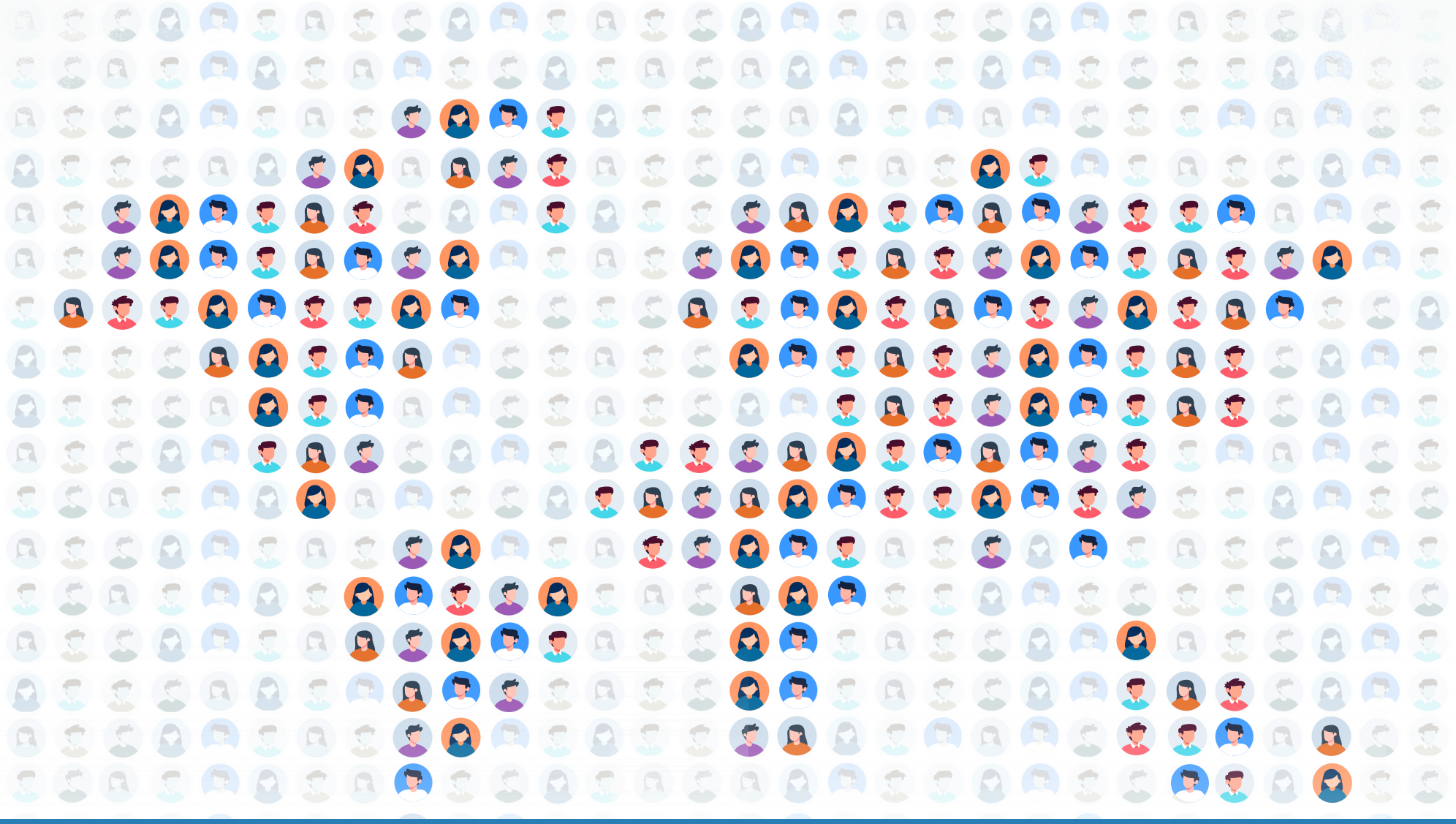
Create Data Backup and Emergency Plans

Store Backup Data in Secure Locations:
Always make backup copies of important files, documents, and recordings, and store them in secure encrypted external device. This ensures that you will always have a copy of critical information if primary data sources are compromised, confiscated or stolen.

Establish Contingency Plans:
Plan for situations where either the journalist or source may face legal risks or get arrested. Agree on specific actions, such as deleting sensitive data or contacting trusted legal aid, if either party is at risk.

Understand Legal Protections and Risks

Familiarize yourself with relevant whistleblower protection laws, as they vary depending on the sector and jurisdiction.
Understand that there is no universal global whistleblower law, and protections may differ between private and public sector employees as well as by country.



Maharat Foundation

Address:
Jdeideh, Metn
Lebanon

Contact Information:
Website: maharatfoundation.org
Email: info@maharatfoundation.org

مهارات
Maharat