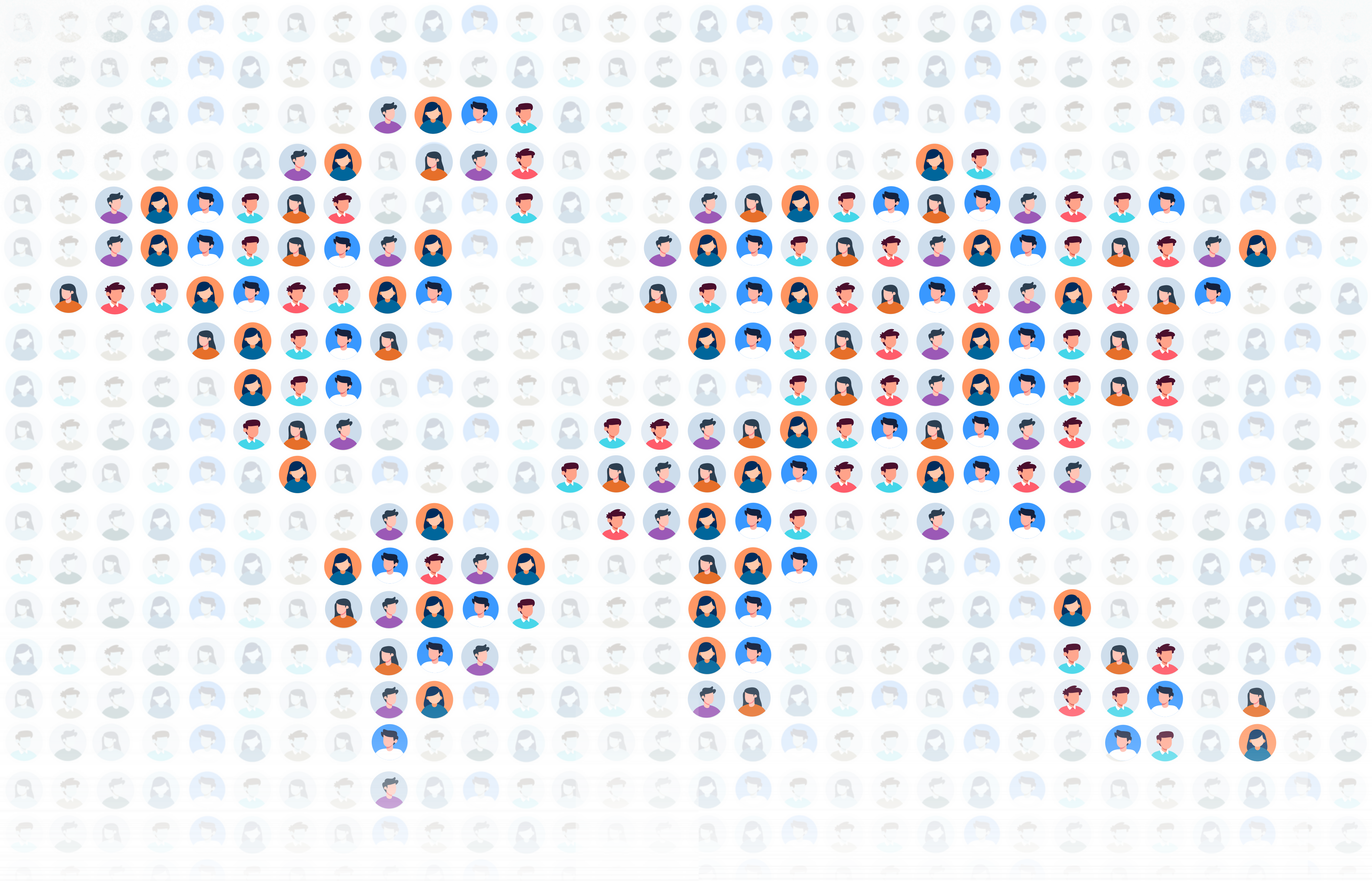


THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

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 9

Best Practices:
Regular updates, strong passwords, use of licensed softwares and two-factor authentication.

Prepared by:
Digital security expert
Bahaa Nasr

Taking in consideration both **physical safety and digital security is essential** for journalists, activists, and anyone working in environments where personal safety and information security are at risk. **Online threats and attacks can have effects on real life.** Likewise, physical attacks can put our digital security at risk, for example when devices are confiscated or searched. Therefore, **it is important to take a holistic approach to enhance overall well-being and personal security.**

The following points will help you improve your physical and digital safety:

1. Start with a Comprehensive Risk Assessment

Identify Potential Threats

Think about both physical risks (like surveillance, detention, or physical attack) and digital risks (such as hacking, device confiscation, or location tracking). Make a list of specific threats that are common in your region and relevant to your situation and risk profile.

Localize your security plan

Different locations present different risks, so assess physical and digital security needs according to each place you'll be working or traveling in.

Evaluate Threat Sources

Map out who you have to worry about: State actors? Corporations? Individuals? Armed parties? It makes a difference whether you are worried about an alienated friend or a powerful government for the precautions taken for both physical and digital security. How much you have to invest in your security depends very much on the resources and determination of your potential attackers.

2. Use Secure, Separate Devices

Dedicated Devices for Sensitive Work

Keep sensitive work on a separate device that is used solely for secure communications or data. This compartmentalization reduces the risk of mixing between personal and professional data, or accidentally leaking information.

Configure Device Security Settings

Set up full-disk encryption, use strong passwords on all devices, and enable two-factor authentication wherever it is available. Ensure location services are turned off unless needed, and limit app permissions to prevent background data leaks.

Consider Disposable or Burner Devices

Use burner phones and temporary email accounts for high-risk assignments. Securely dispose of these devices afterward or keep them off when not actively needed.

3. Ensure Safe and Anonymous Communications

Use Encrypted Channels for Digital Communications

Use end-to-end encrypted apps like Signal for communicating sensitive information, change the settings to use a username instead of your mobile number, and activate disappearing messages. Avoid using social media or other personal accounts for sensitive communication.

Avoid Open Wi-Fi Networks

Public Wi-Fi networks are vulnerable to “Man-in-the-Middle” (MitM) attacks. Use a secure, private network or a Virtual Private Network (VPN) whenever possible.

Regularly Delete Communication Logs

Delete messages and call logs from your devices to reduce exposure if your device is lost, stolen, or confiscated. Activate the disappearing messages feature wherever possible.

4. Coordinate Physical Movement and Location Privacy

Limit Location Tracking

Disable location tracking on devices and avoid social media check-ins that reveal your location. Look for hidden tracking functions in apps where you might not suspect being tracked.

Choose Secure Meeting Places

Plan physical meetings in secure, private locations that are less likely to have surveillance. If concerned, consider changing the location at short notice and do not publicly communicate about meeting places. Avoid using hotels or public venues for sensitive meetings, staff might be compromised and report on you. Use routes and locations that help avoid potential tailing or monitoring.

Have a Contingency Plan

Inform trusted contacts of your whereabouts and expected return times, and establish check-in points for situations where you may be at risk. Use code words for additional security if you are worried about being detained or being surveilled.

5. Practice Strong Operational Security

Use a "Need-to-Know" Approach

Share only essential information with team members or sources. The fewer people know sensitive details, the lower the chance of accidental or forced exposure.

Secure Physical Workspaces

If working in an office or a location that could be compromised, limit physical access to sensitive materials, keep screens facing away from public view, and use privacy screen filters.

6. Mind the Metadata

Remove Metadata from Files

Before sharing files or images, strip metadata that can reveal sensitive information such as sources names, timestamps, location, and device data.

7. Encrypt All Data on Devices and Backups

Encrypt Hard Drives and External Storage

Enable full-disk encryption on all devices (e.g., laptops, phones, USB drives). This ensures your data remains inaccessible even if devices are lost or seized. Always lock your device when you are not using it, and turn it off before handing it over to others for added protection.

Secure Backups with Encryption

Make sure that both your local and cloud backups are securely stored and encrypted to protect them from unauthorized access. In times of war and physical destruction, cloud backup might be the safer option because local storage might get destroyed, lost, or stolen. When selecting a cloud service choose the one that has end-to-end encryption like Tresorit or Proton drive.

Use Strong, Unique Passwords

Set up strong passwords for all devices and accounts. Avoid reusing the same passwords for different accounts. Struggle to remember them all? Use a password manager to create and securely store unique passwords.

8. Plan for Safe Data Transmission

Use Disposable Cloud Storage Links

send files online using secure services like Tresorit. If sharing files online, use secure cloud storage services like Tresorit or Proton drive. Avoid permanently storing sensitive data on mainstream cloud platforms that lack robust security.

Use Secure File Transfer Methods

Use encrypted file-sharing tools like OnionShare, or SecureDrop.

Check Network Security for Sensitive Transmissions

When uploading or downloading sensitive data, avoid using insecure networks. Use VPNs, and consider the Tor browser for added anonymity.

Limit File Access Permissions

Only give file access to essential personnel, and set expiration dates for shared links or files when using online storage platforms.

9. Monitor and React to Emerging Threats

Set Up Threat Alerts

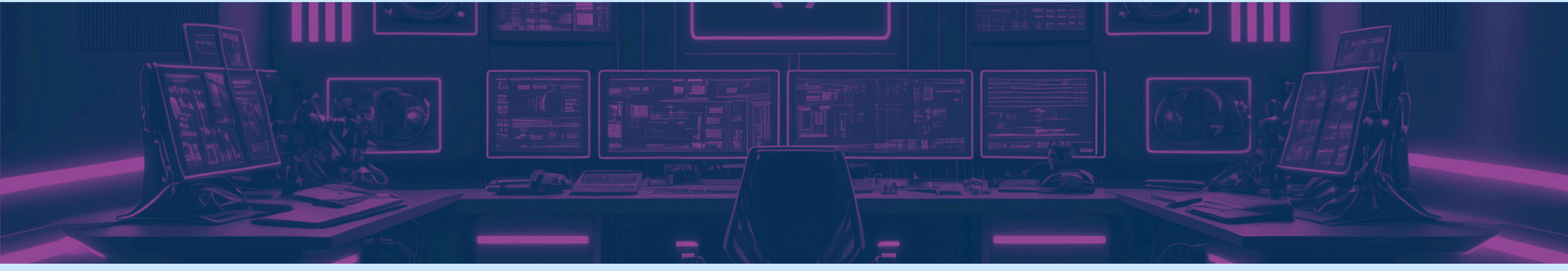
Monitor for news of data breaches, security flaws, or newly emerging threats that might affect you. Cybersecurity alerts or tools like Have I Been Pwned can notify you if one of your passwords is compromised.

Perform Regular Security Check-up

Review security protocols for both physical and digital security regularly, especially when working in high-risk situations. Update passwords, check access permissions, and review communication channels.

Be prepared for worst case scenarios

Plan for potential emergencies (e.g., confiscation of devices, legal risks, physical security threats). For instance, learn how to perform remote wipe for your devices, to protect sensitive data, in case it is lost, confiscated or stolen.



10. Have Legal Support and a Plan for Incident Response

Seek Legal Advice on Digital Privacy Rights

Understand the legal protections and vulnerabilities related to device searches, surveillance, and data retention in your country or any country you'll be working in.

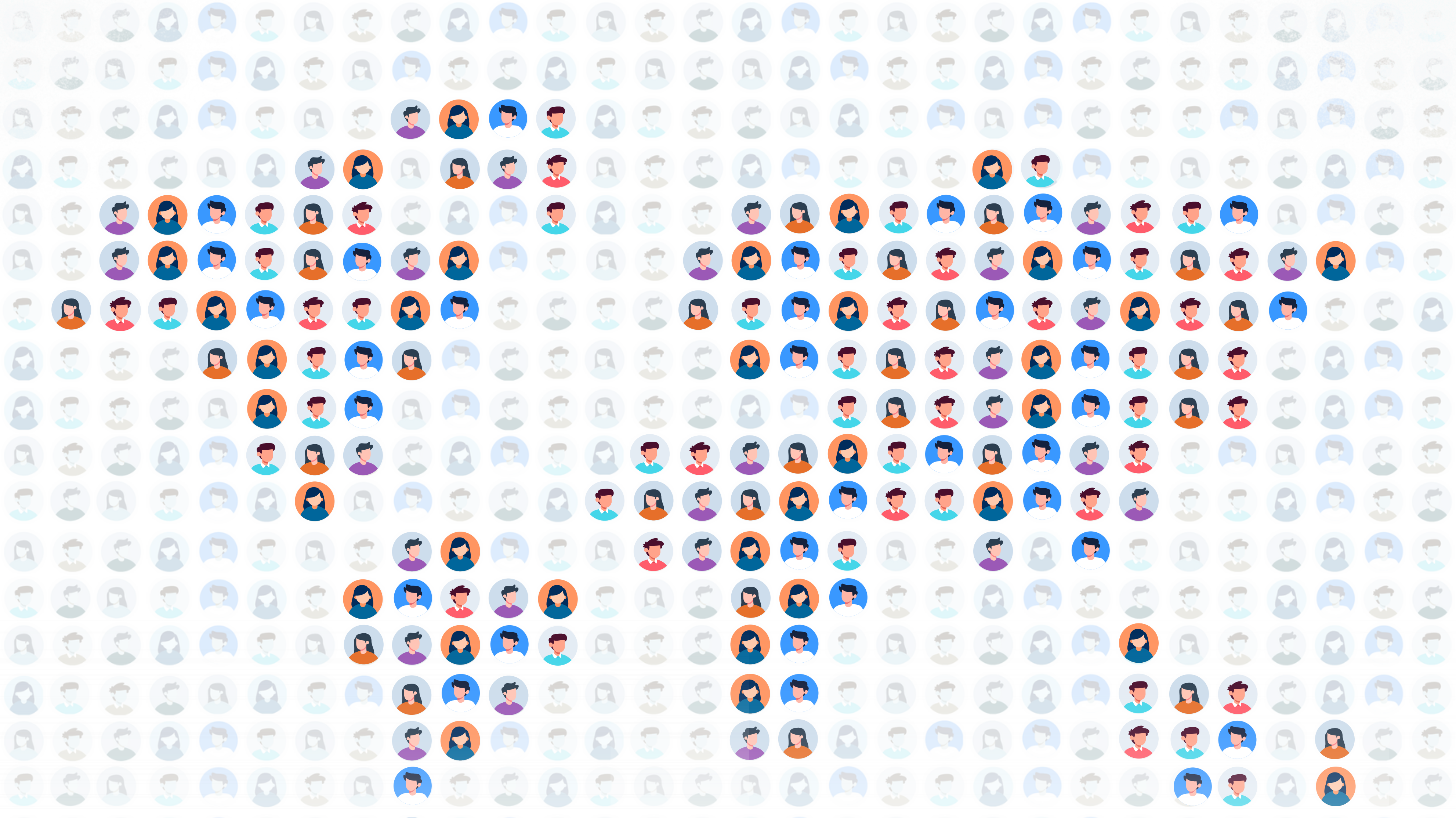
Develop a Response Plan for Confiscations or Detentions

What steps will you take if devices are seized or if you or a team member is detained? Be prepared. Have encrypted backups, accessibility to remote data wipe capabilities, and a list of emergency contacts who can take over in case of an incident.

Consider Using Physical and Digital Decoys

In extreme cases, consider creating decoy devices or accounts that can be shown in emergencies while keeping primary, secure devices or accounts hidden.

Your safety matters. Be proactive, following these strategies will help you and those close to you to operate more securely in high-risk environments. Raise the bar for any potential attacker, avoid being an easy target.



Maharat Foundation

Address:
Jdeideh, Metn
Lebanon

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