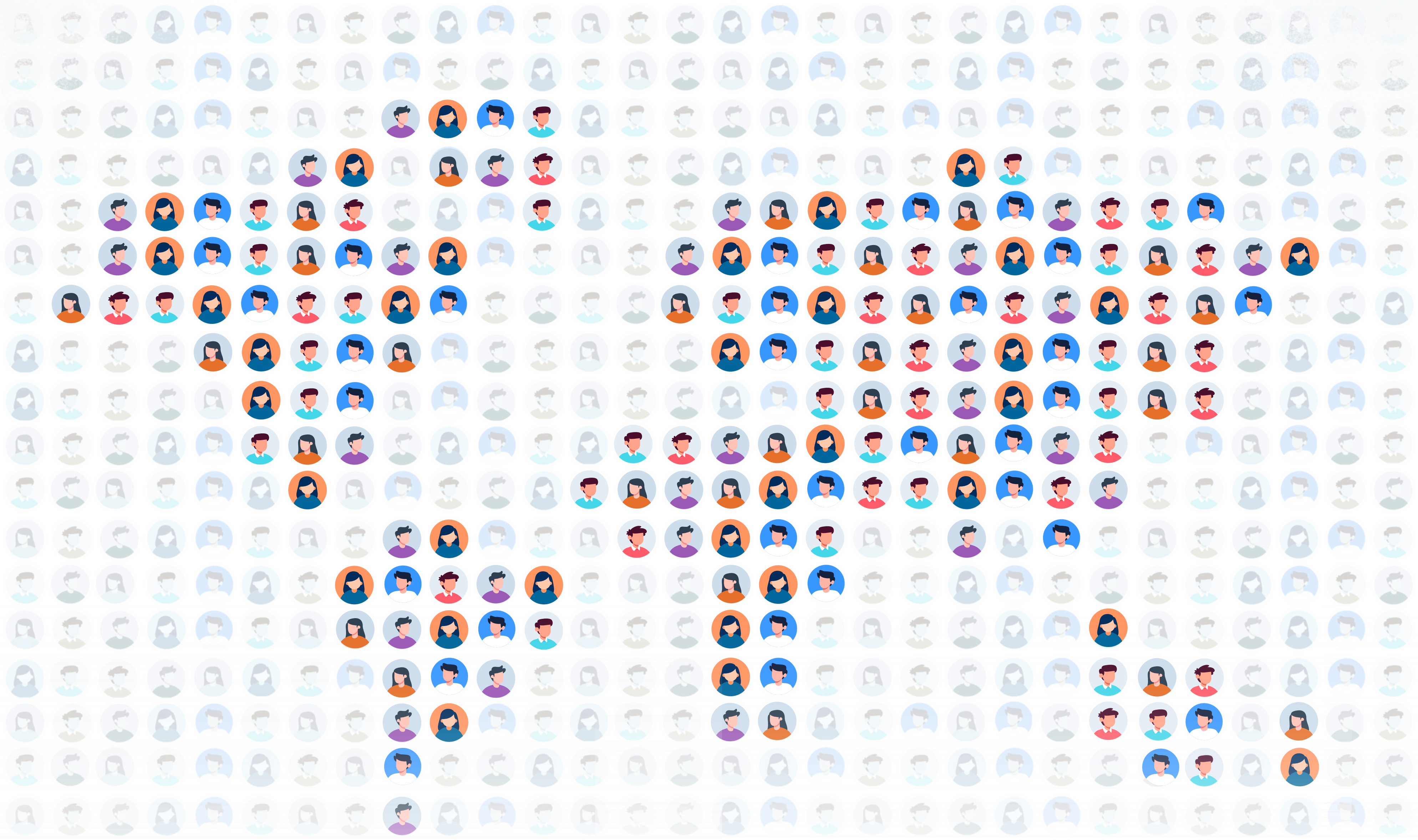


THE DIGITAL SECURITY MANUAL

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.

© Beirut 2025

MODULE 8

Incident Response Planning: Developing a plan for responding to digital security incidents.

Prepared by:
Digital security expert
Bahaa Nasr

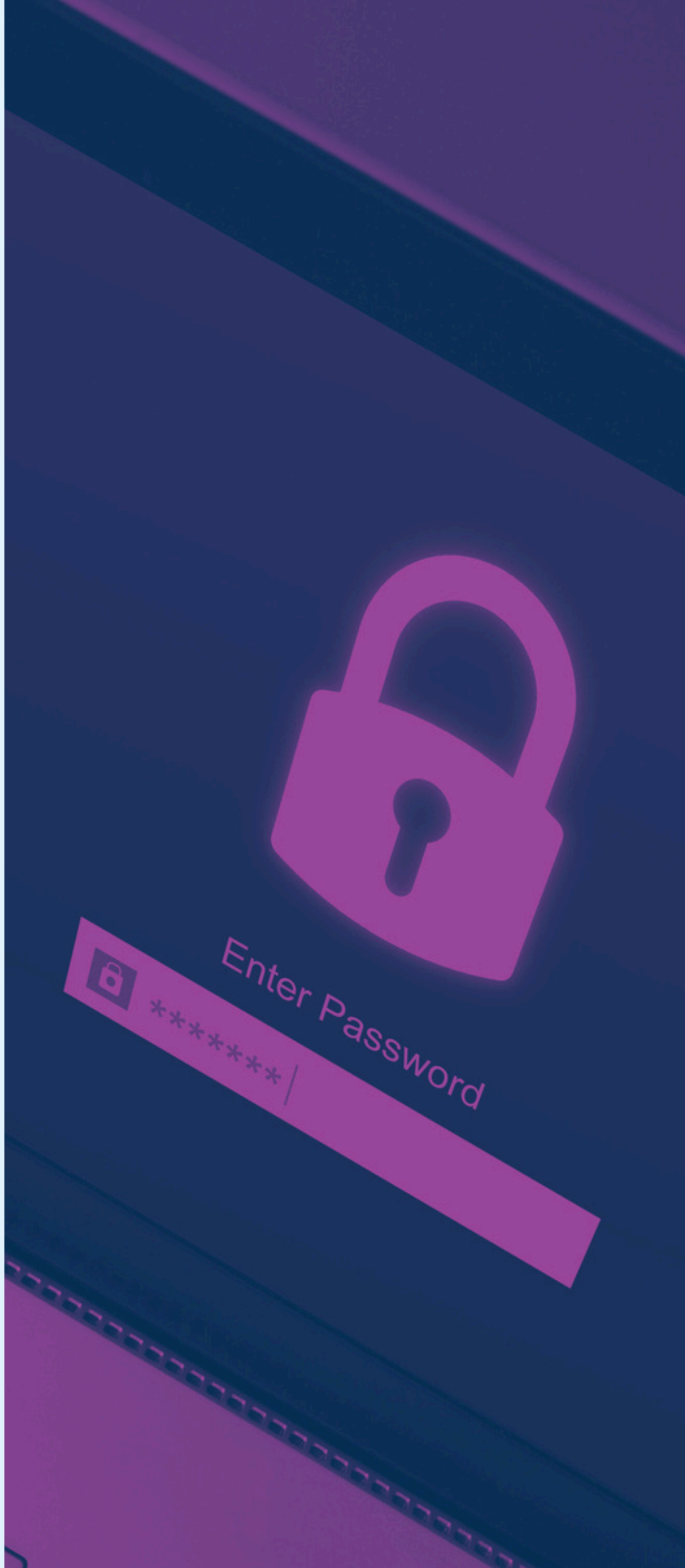
In today's digital age, we conduct most of our work on computers, and when we're not working, our mobile devices are often within arm's reach. **From professional to personal activities, we heavily rely on digital platforms.** As a result, the **digital risks we are exposed to have multiplied**, and adhering to digital security best practices is more important than ever to protect our personal information, our work, our assets and our well-being.

Following the below advice will significantly enhance your digital security and lower the risk of falling victim to malign forces while being online.

1. Use Strong Passwords and Manage Them Securely

Create Strong Passwords

- Use at least **15 characters** with a **mix of upper- and lower-case letters, numbers, and symbols**. Consider using a passphrase that is easy to remember like: Ne5na we zou7al jiran!
- Strictly stick to “one unique password for each account”. Never reuse passwords.
- Use a Password Manager: To help you store and generate complex passwords securely, use tools like KeepassXC or Bitwarden. This will allow you to use complex, unique passwords for each account while only having to remember one single Master password.
- Enable Multi-Factor Authentication (MFA): Setting up a second authentication method like mobile app or biometrics (fingerprint / Face ID) adds an extra layer of security to your accounts and devices. Examples are Google Authenticator or Twilio Authy Authenticator.



2. Protect Your Devices

- Stay up to date: Regularly update the operating system (OS), all applications and software on all your devices. The updates are provided to patch known security vulnerabilities which hackers often exploit.
- Enable automatic updates whenever possible to ensure your devices are always running the latest security patches and fixes.
- Download original software only from official websites, even for free software. Stay away from pirated software – you might pay a steep price for trying to save money. Pirated software usually doesn't update and also could be manipulated and contain malwares.
- Use antivirus software to protect against malicious attacks. Check from time to time that the antivirus is up to date and working properly to ensure it detects and removes the latest threats. Use the built-in Windows Defender or install a reputable well-known antivirus program.
- Lock devices with strong passwords or biometric authentication to prevent unauthorized access, even when leaving the device unattended for just a minute.
- Encrypt Your Devices: Ensure data is encrypted to prevent unauthorized access in case of theft. Encrypt sensitive files with tools like BitLocker or VeraCrypt.

In case your device needs maintenance or repairs, only take it to a trusted person. All devices contain a lot of personal and sensitive data, and the repair person will have access to everything on the device while working on it.

3. Use encrypted messaging apps

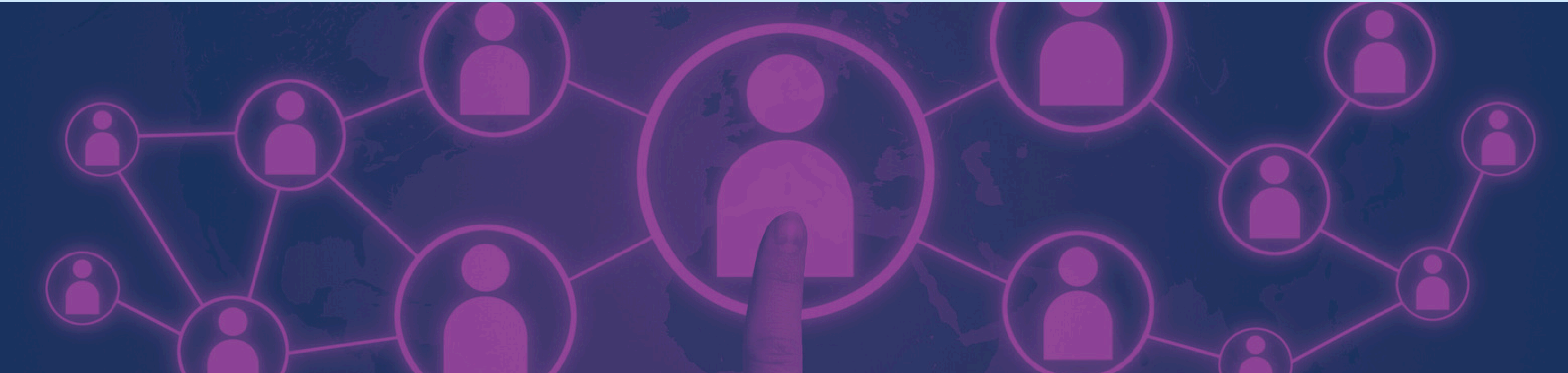
- Use encrypted messaging apps such as Signal, to communicate securely with others.
- These apps use end-to-end encryption, which means only you and the person you're communicating with can read the messages, keeping your conversations private.
- Activate disappearing or auto-delete messages, which minimize the risk of sensitive information being stored or accessed in case your device is confiscated or compromised.

4. Secure Your Internet Connection

- Secure your router: A weak entry point for hackers is often overlooked – the router. Place your router in a secure location where visitors or intruders cannot easily access it to prevent anyone from manipulating it. Always change the default admin password and set your own strong password. Enable WPA3 or WPA2 encryption in the router's settings for better security for your Wi-Fi.
- Don't share your Wi-Fi with neighbors or strangers. Keep in mind: Whoever has access to your network will be able to monitor your online activity.
- Use a VPN especially on public Wi-Fi. VPNs create a secure, encrypted connection between your device and the internet, preventing eavesdroppers from intercepting your data. Known VPNs are Tunnelbear, Psiphon, Proton VPN.

5. Practice Safe Browsing and Social Media Privacy

- Think before you click: Avoid clicking unknown links. Be cautious about links in emails, messages, or websites that may lead to phishing sites.
- Verify websites use HTTPS to ensure information transmitted between your browser and the website you are visiting is encrypted.
- Minimize the personal information you share online. Review and adjust your privacy settings on social media platforms to limit who can see your posts, photos, and personal information. Accept friend requests only from people you know.
- Separate work and personal accounts. If possible, use different devices and accounts for work and personal activities. Monitor your account activity, regularly check account access logs for suspicious activities. Enable account alerts to get notified of logins, password changes, or suspicious activity.



6. Watch out for Phishing Attempts

- Attackers use deceptive emails, messages, or phone calls to trick their victims into revealing sensitive information or perform actions that compromise their security or give away money. These phishing scams and social engineering tactics often target journalists and activists who might be tricked to reveal or share sensitive information or sources. Verify these requests and double-check via a different communication method, i.e. if you are unsure about an email you receive, verify it via a Signal call.
- Verify the sender's email address and check for any inconsistencies or impersonation.
- Avoid clicking on unknown links. Hover over links to check their destination.
- Do not download unknown attachments, especially from unknown sources. They may contain malware.
- Report phishing attempts. Notify your organization or email provider.
- Educate yourself and team members on how to recognize phishing, and stay informed about common phishing tactics used. Practice here or here.

7. Backup Data Regularly

- Use a combination of cloud and physical backups to Store copies of sensitive and important data on encrypted external drives or secure cloud platforms.
- Automate backups, or make schedule to regularly perform a backup to minimize data loss.
- Always test backups to ensure that they are working and you can indeed recover files if needed.

8. Delete Data and Dispose of Devices Securely

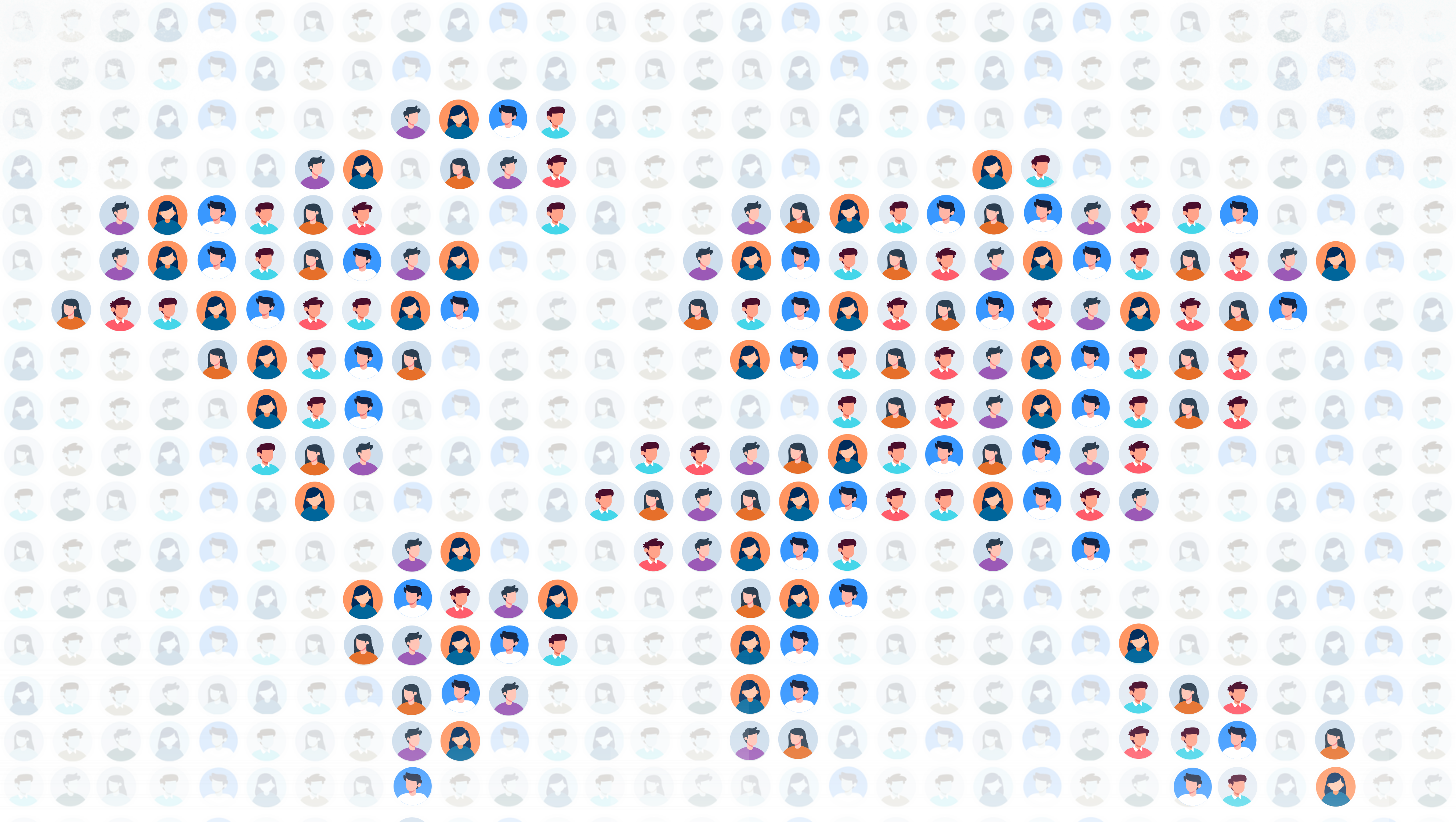
- Most data you delete from your devices can be recovered, if using the ordinary delete function. If you want to delete data permanently you have to use tools like Eraser or BleachBit to delete the data.
- Before disposing, selling or giving away devices you should securely erase all the data.

9. Educate yourself and your contacts

- Stay Updated and informed about the latest cyber threats and security measures.
- If you get the chance, attend in-person workshops or online training sessions specifically designed to address digital threats faced by journalists and activists.

10. Prepare for Incident Response

- Be prepared for worst case scenarios so you don’t get caught off guard. Establish clear protocol what to do in case of data breaches or cyber incidents.
- Have a list of contacts of cybersecurity professionals at hand, as well as organizations you can reach out to in case you need help.
- Regularly review, practice and revise these protocols.



Maharat Foundation

Address:
Jdeideh, Metn
Lebanon

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

© Beirut 2025