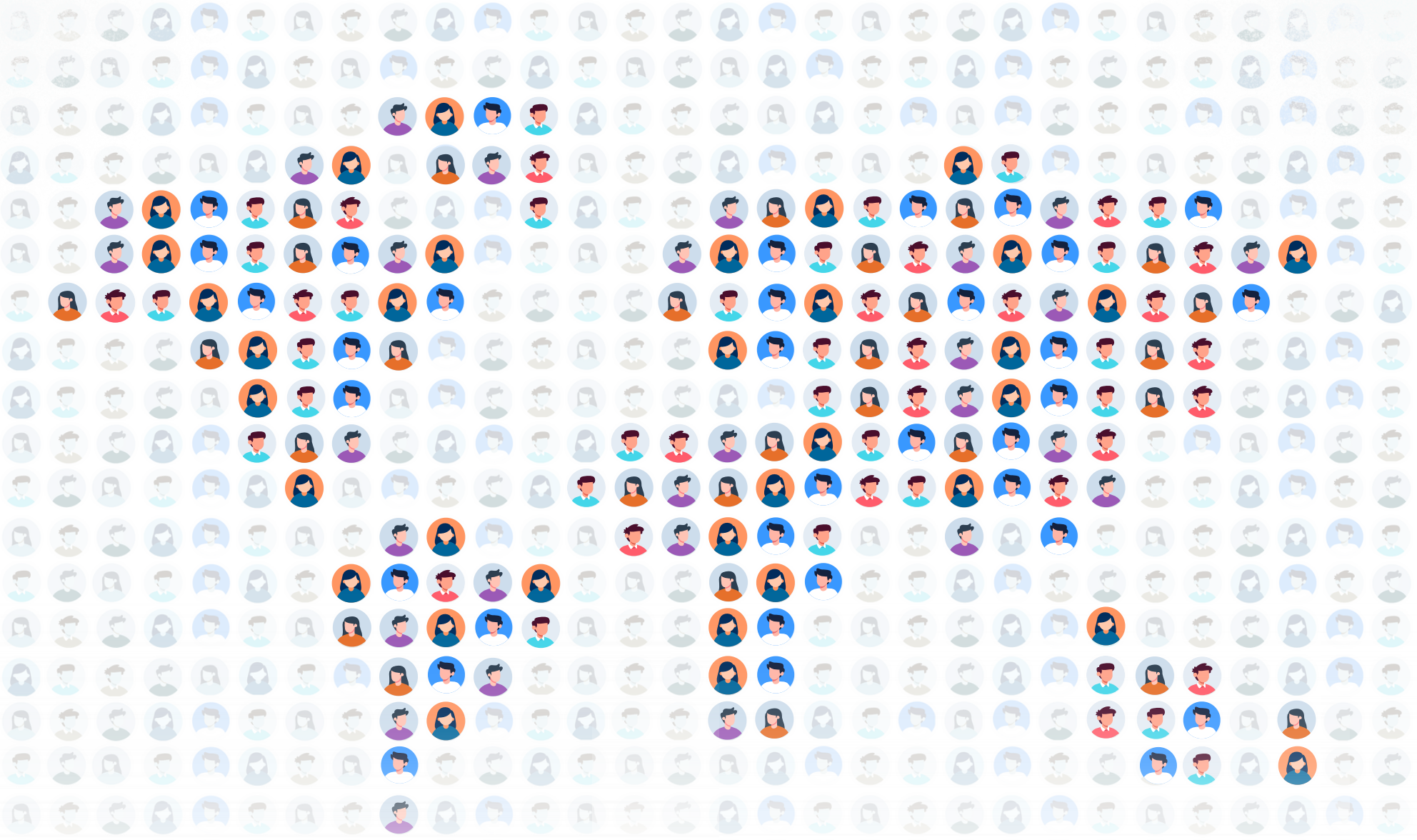


THE DIGITAL SECURITY MANUAL

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 6

Social Media Safety:
Best practices for using social media safely (privacy settings, sharing sensitive information).

Prepared by:
Digital security expert
Bahaa Nasr

Social Media Safety

Social media became part of our daily life. We use it to stay connected and to maintain relationship with family and friends; some use it for **networking, or for access to news and information**, others for **self-expression and creativity as well as for entertainment and leisure**.

The more social media is becoming an integral part of our daily life, the bigger is the risk that this might lead to **oversharing personal information** online, like pictures, our whereabouts, interests, hobbies and other personal details.

To be able to use social media safely, we have to **tighten our privacy settings in each platform** that we use, be mindful about the information we share, and **understand the risks associated with any online interactions.**

Best practices to improve the security and privacy of our social media accounts:

During war time, long before any actual attack, the **military uses special unites for reconnaissance to gather information about the enemy**: readiness, capabilities, explore the area. Cyber criminals and hackers use the same technique of “reconnaissance”. **Reconnaissance** is the first phase of hacking, which involves gathering as much information as possible about the target. The process of reconnaissance is like the work of a detective: The hacker collects data and information to understand their victims. They will use this information, and it will give them leverage to craft a targeted attack against their victims.

1. Be Selective with information you share publicly

Avoid Oversharing Personal Details: Limit information about your location, daily routine. Sharing specifics like your exact location or personal addresses can increase your risk of theft, stalking, or other dangers.

Limit Sensitive Content: Avoid sharing information that could be used for identity theft, such as your full date of birth, address, or financial information. Even small details can be pieced together by cybercriminals to create a comprehensive profile of you.

Be cautious with pictures: Avoid posting images of people without permission.

2. Think Before You Post

Avoid Sharing Location in Real-Time

Wait until you leave a location to share a post or photo taken there. This prevents strangers from tracking your real-time movements.

Consider the Long-Term Impact

Remember that what you post today may affect you in the future. Employers, colleges, and others often check social media profiles as part of background screening.

Stay Mindful of Social Engineering Risks

Cybercriminals use social engineering to gather personal details through social media. For example, seemingly harmless posts about your first pet or favorite teacher can give away answers to security questions.

3. Strengthen Account Security

Use Strong, Unique Passwords

Create complex passwords that include a mix of letters, numbers, and symbols. Avoid using the same password for other accounts.

Enable Two-Factor Authentication (2FA)

Activate 2FA for an added layer of security. This often involves verifying your login with a second method, such as a code generated by an app on your phone.

Regularly Review Connected Devices

Check your account's "logged-in devices" list regularly and sign out from devices you don't recognize or no longer use.

Never open your accounts on the devices of other people or public devices. You never know if these devices are secure.

4. Adjust Privacy Settings

Limit who can see what you post online

Set your profile visibility to "friends only" to restrict who can see your posts, photos, and personal information.

Review Tagging Permissions

Control who can tag you in photos or posts. Many platforms allow users to review tags before they appear on their profile.

Review App installed in your account and their Permissions

Check the permissions granted to third-party apps linked to your social media. Many apps request access to your information, which can compromise your privacy. Remove all the third-party apps installed in your account that you are not using.

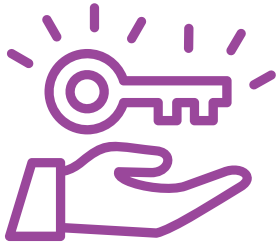
Control Who Can Contact You

Set restrictions on who can send friend requests or messages. For example, only allow “friends of friends” to send you requests if possible.

Limit Searchability

Disable search engine indexing to prevent your profile from showing up on external search engines like Google.

5. Limit Sharing with Third-Party Apps



Restrict Third-Party Access

Limit permissions granted to third-party applications, especially if they request access to your friends list, profile details, or post history.

Review Data Collection Policies

Be mindful of the privacy policies of apps and services that connect with social media. Some apps may use your data in ways you're not aware of or comfortable with.

Turn Off Location Sharing

Avoid sharing location data with third-party applications connected to social media unless absolutely necessary. Some apps collect location information in the background without your active input.

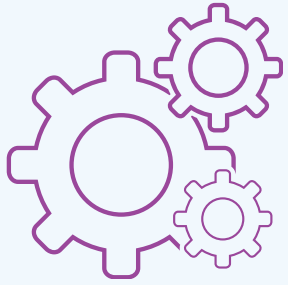
6. Stay Informed About Privacy Updates

Review Privacy Policies Regularly

Social media platforms update their privacy policies frequently. Review these changes to understand how your information is used and make adjustments to your settings accordingly.

Be Aware of Security Notifications

Platforms may notify users of potential security issues or data breaches. Stay alert to these and take action if your account could be affected.



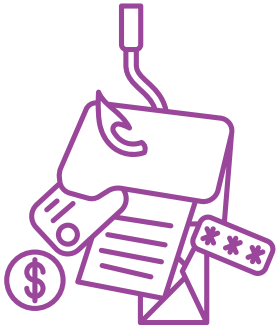
Use Privacy Checkup Tools

Many social media platforms offer tools to review and optimize your privacy settings, guiding you through common privacy and security best practices.

7. Be Cautious with Online Interactions

Avoid Engaging with Unknown Profiles

Interacting with strangers, especially those asking for personal information, can be risky. Avoid friend requests or direct messages from unknown individuals.



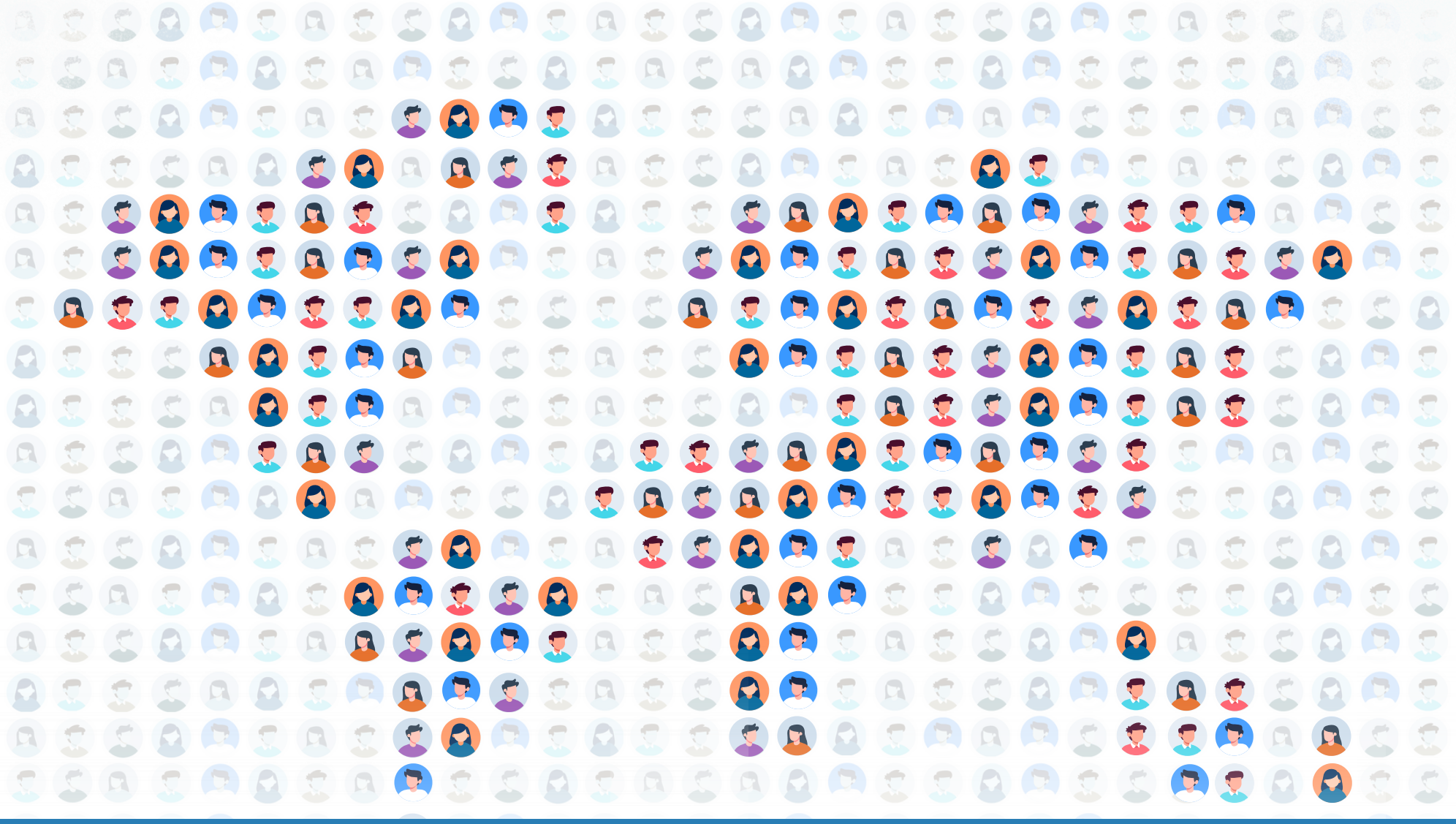
Stay Alert to Phishing Attempts

Watch out for phishing scams that use messages, links, or fake pages to trick you into revealing your login information.

Report Suspicious Content

Report or block users and content that seem suspicious or violate community guidelines. This helps maintain a safer online environment for everyone.

By following these best practices, you will enhance your privacy and better protect your personal information, helping you enjoy social media with greater security and peace of mind.



Maharat Foundation

Address:
Jdeideh, Metn
Lebanon

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

مهارات
Maharat