

THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection



THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

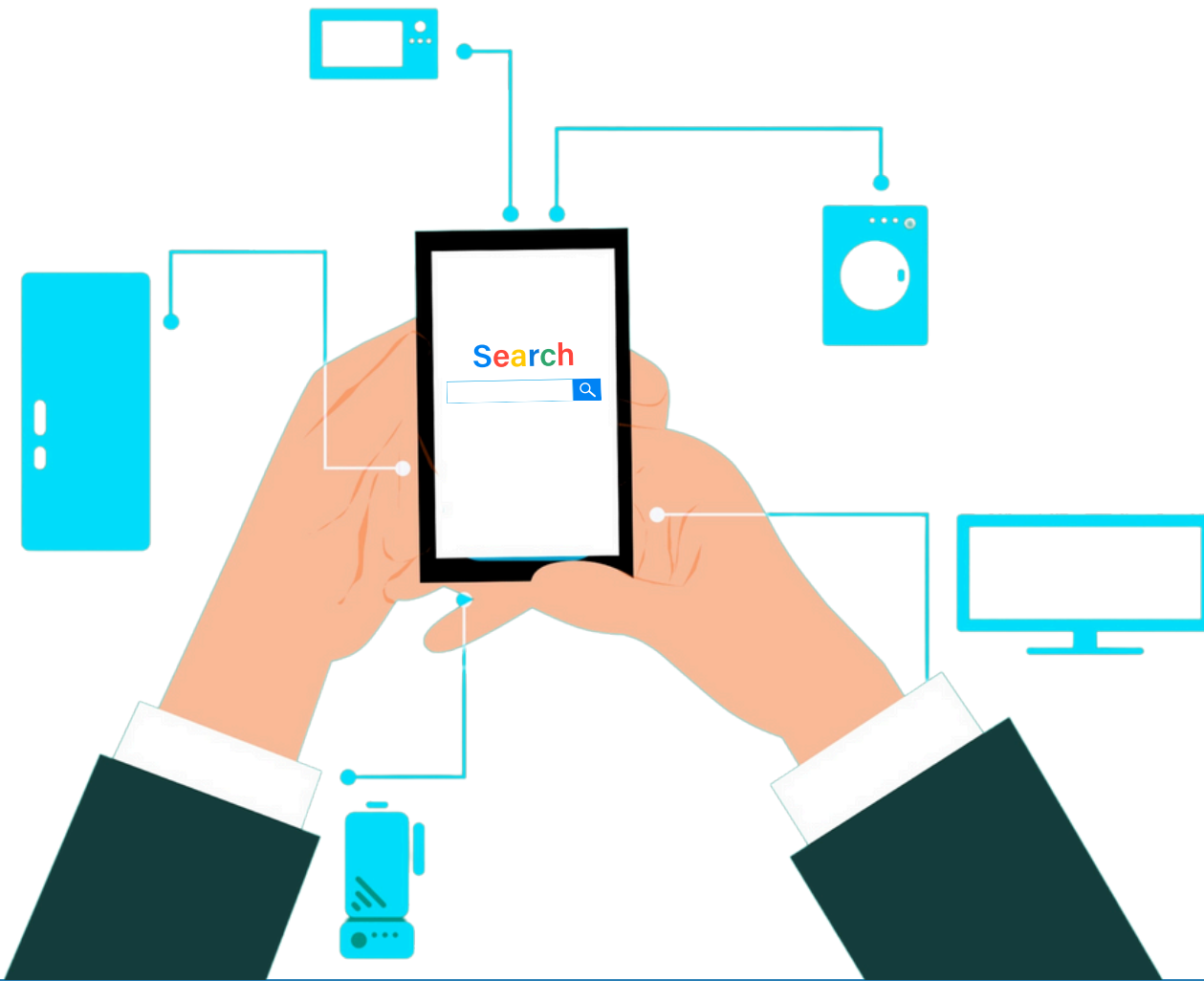
This manual was prepared by Maharat Foundation, with the support of UN Women and the French Embassy in Beirut.

© Beirut 2024



MODULE

4



PRACTICING SAFE BROWSING HABITS IS ESSENTIAL TO PROTECT YOUR PERSONAL INFORMATION, DEVICES, AND OVERALL PRIVACY.

Prepared by:
Digital security expert
Bahaa Nasr

Why is internet safety important?

There is no doubt that the Internet makes our lives easier. Whether you're catching up with the latest news, chatting with friends, browsing social media, or streaming your favorite series. However, with all that the internet has to offer, **it can also be a dangerous place if you're not careful.** Especially in recent years, with the exponential increase in cybersecurity threats and breaches. **Malware, (viruses, remote access tools and Trojans), scammers, malicious emails and inappropriate content** are only a few examples of the potential threats when browsing online. Safe browsing is equivalent to looking both ways before crossing the street. Staying safe online is very important.

Fortunately, **there are several ways to protect yourself and make your internet experience safer and more satisfying,** whether you are browsing on a laptop, tablet or smartphone. Here are some safe web browsing tips:



1

How to browse the internet safely



1. Update your web browser regularly

Hackers frequently target web browser flaws, which is why software manufacturers offer frequent updates to fix any issues and patch vulnerabilities. Installing the most up-to-date version on your system helps to protect your browser and personal data, and provides you with the newest features and latest security measures. Ignoring updates can result in your browser being infected and an easier target for hackers, because many of their attacks exploit outdated software and known vulnerabilities.



2. Think Before you click!

Avoid clicking on suspicious links and attachments, especially in emails and on social media. Phishing links are designed to trick you into revealing personal information or installing malware. A good advice is to type the URL yourself instead of clicking on a link.

Pay attention to the web address. Check the address, and if you click on a link, look to make sure that the address stays the same. If it has changed, then it has taken you to a fraudulent web address where cyber criminals can monitor and access your information. Leave the website immediately and do not enter any personal information.

In the browser, there is a padlock symbol that appears at the beginning of the address line to indicate that the website is genuine. But don't be fooled by a padlock that appears on the web page itself because it is possible for a cyber-criminal to copy the image. So, double check that the padlock is in the window frame of the browser itself.

Double-click the padlock icon for more site information. Under the padlock, you can also find certificate information for the page you are viewing to guarantee that you are on a safe, secure website. Make sure the certificate is current and issued to the web page you are visiting.



3. Use a VPN

A Virtual Private Network (VPN) encrypts your internet connection, creating a secure tunnel between your device and the internet. This hides your IP address and protects your online activities from being monitored by third parties, such as hackers, ISPs, or government agencies. When using a public network, like the ones in hotels, airports, coffee shops, you should always use a VPN because these networks can be dangerous as hackers can use these unsecured networks to snoop on your online activity and direct you to malicious websites. VPNs also help bypass censorship and allow you to visit blocked websites in the country where you are. It is important though that you choose a reliable, trustworthy VPN.



4. Use Strong, Unique Passwords

Create complex passwords that combine letters, numbers, and symbols, and avoid reusing passwords across different sites.

Don't save your passwords in your browser. Use a password manager instead where you can safely store your passwords in an encrypted database, protected by one strong password.



5. Enable Multi-Factor Authentication (MFA)

The best way to protect your online accounts is by activating MFA. This will add an extra layer of security, requiring you to verify your identity through a secondary method (for example an authentication app) to be able to access sensitive accounts, and it will make it a lot harder for hackers who try to get access to your accounts.



6. Avoid Downloading from Untrusted Sources

Download apps and files only from official websites or verified app stores. Third-party sites may offer software bundled with malware, once installed it will open a door for hackers to your device and all the data and information on it.



7. Use a Reputable Antivirus and Firewall

Unsafe web browsing practices can leave you vulnerable to virus attacks, potentially compromising your files, passwords, accounts and devices.

Antivirus software and firewalls provide essential defenses against malware, phishing, and other threats. Ensure these are active and updated on all your devices.



8. Limit Personal Information on social media

Cybercriminals use information shared on social media or available about you online to steal identities or guess security questions. Avoid sharing sensitive details, like your full address, birthday, or family members' names, your interests and whereabouts. Hackers can use information available about you online that might help and give them leverage to craft a targeted attack against you.



9. Educate Yourself About Phishing and Social Engineering

Social engineering attacks are tactics used by cybercriminals to trick or swindle individuals into revealing sensitive information or performing actions that compromise security. Learn to recognize phishing attempts, which often include urgency, unsolicited attachments, or requests for personal information. Educating yourself and others reduces the risk of falling victim to such attacks.

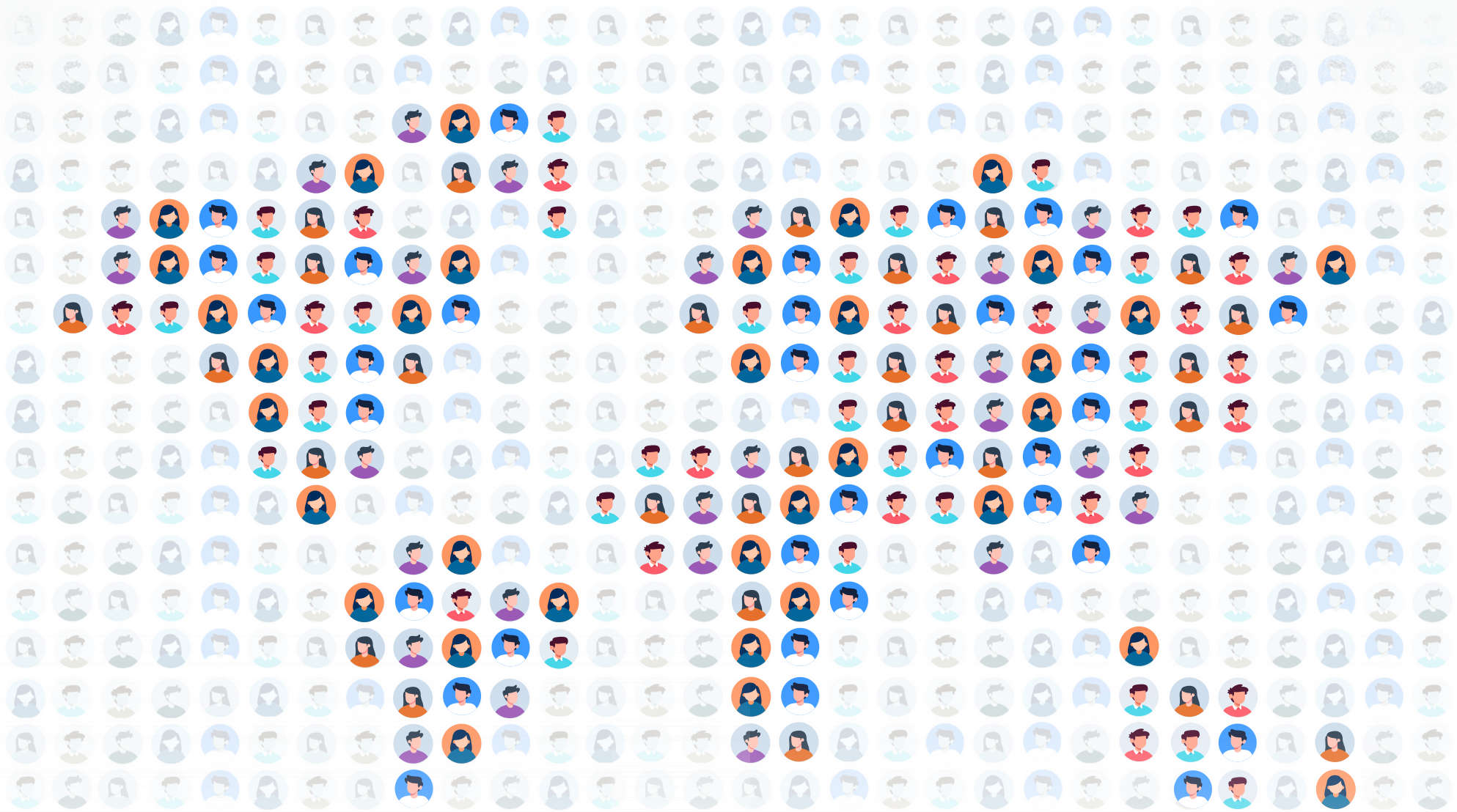


10. Be Careful with Browser Extensions

Browser add-ons or extensions are small software programs that add features to your web browser. It is important to only install the add-ons and extensions that you really need and that are recommended by security experts. Only install them from the official page or the browser's store. Some add-ons and extensions may contain malware or other malicious code, or track your browsing activity.

The internet can be an unpredictable place, and one little mistake might cause you a lot of stress. Following these safe browsing habits can significantly reduce the risks. Safe web browsing practices should be a priority, as keeping your data and privacy protected from common cyber threats. Take your security and privacy into your hands with our 10 tips.





Maharat Foundation

Address:
Jdeideh, Metn
Beirut, Lebanon

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

مهارات
Maharat



© Beirut 2024