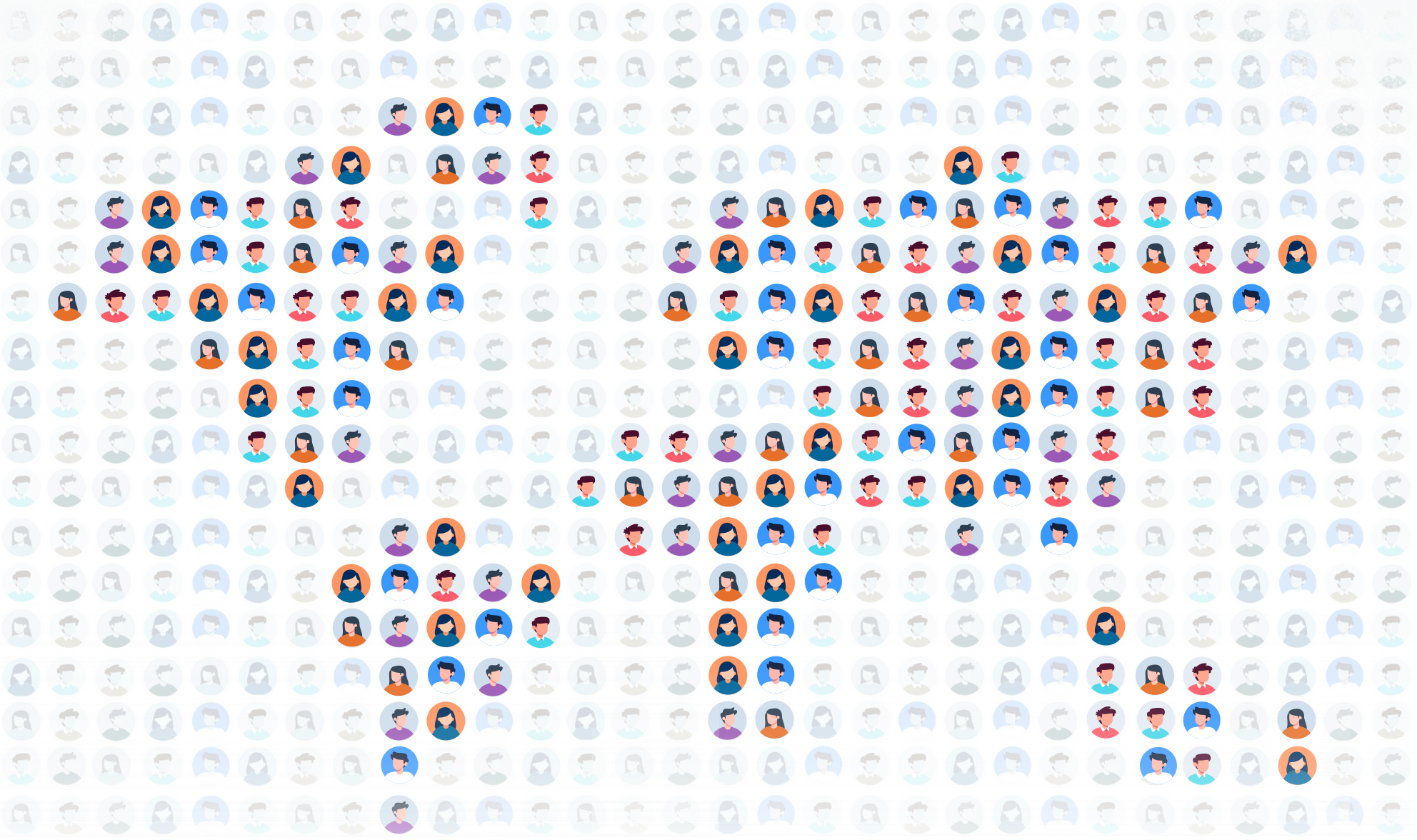


THE DIGITAL SECURITY MANUAL

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

5

Recognizing Digital Threats:

Recognizing threats, responding to breaches, and using security tools

Prepared by:
Digital security expert
Bahaa Nasr

Recognizing Digital Threats

In today's interconnected world, where technology is deeply embedded in our daily lives, understanding and identifying digital threats is more critical than ever. **Cybercriminals employ sophisticated tactics to exploit vulnerabilities, steal sensitive information, and disrupt systems.** These threats often manifest as phishing emails, malicious links, deceptive messages, or unusual device behavior. **To safeguard your digital life, it is essential to recognize these threats early,** respond effectively to breaches, and leverage robust security tools.

The Importance of a Proactive Approach to Digital Security

Being **proactive** means taking action before something bad happens. Taking a proactive approach **minimizes the risk of breaches, and helps mitigate risks associated with digital threats and vulnerabilities.** By identifying potential risks and implementing appropriate safeguards you can reduce your exposure and enhance your overall digital security.

Adopting a proactive approach to digital security involves **empowering yourself with knowledge and skills to navigate the digital world safely**. Taking a proactive approach means acting in advance to prevent potential issues, like locking your door before leaving. While no method is foolproof, proactive security measures discourage attackers by making you a harder target. Simple steps such as using strong passwords, activating multi-factor authentication, updating software, and adjusting privacy settings help keep your information safe and private.

Additionally, **fostering a culture of digital awareness**—both personally and within organizations—can help identify emerging threats and prevent costly mistakes. Staying informed about the latest cyber risks and adopting best practices ensures you remain one step ahead of potential attackers.

Below are some of the most common tactics used by cybercriminals to target individuals and organizations:

Phishing Attempts

Phishing and social engineering attacks rely on psychological manipulation and deceptive tactics to trick individuals into revealing sensitive information, clicking malicious links, or performing actions that compromise their security. These attacks often come in the form of emails, messages, or phone calls that appear to originate from legitimate sources, such as banks or well-known companies.
To protect yourself, it is essential to recognize common signs of phishing attempts:

Suspicious Emails or Messages

Phishing messages often contain slight errors, such as misspellings, unusual grammar, or unexpected sender addresses. They may use generic greetings instead of personalized ones to appear legitimate. Always verify the sender's authenticity.

Urgent Language and Requests

Attackers frequently use urgency to create panic and pressure you into acting quickly without thinking. Phrases like “Your account will be locked if you don’t click this link!” or “Act now to claim your reward!” are common. Be wary of messages about lotteries you didn’t participate in, or unexpected inheritances, these are often scams.

Unusual Links or Attachments

Hover over links before clicking to check the URL. Phishing links may closely resemble legitimate websites but include subtle alterations (like using ".net" instead of ".com" or replacing letters with similar-looking characters). Avoid downloading attachments from unknown sources, as they may contain malware.

Offers That Seem Too Good to Be True

Scammers often lure victims with promises of large sums of money, prizes, or rewards that seem unrealistic.

Requests for Personal Information

Be cautious of unsolicited requests for login credentials, personal details, or financial information. Legitimate websites don't ask for such sensitive data via email or text.

To improve your ability to recognize phishing and social engineering attacks, practice using resources like phishing quizzes

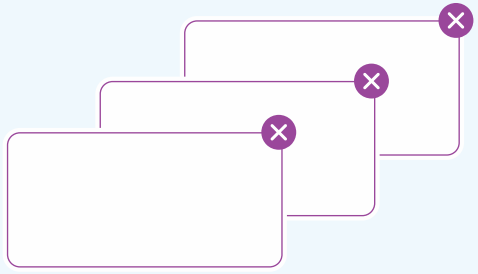
phishingquiz.withgoogle

shira.app

Additionally, watching "social engineering" videos on YouTube can help you better understand these deceptive tactics and how to avoid falling for them.

Malware and Ransomware

Malware refers to any software designed to harm or exploit devices, while ransomware is a specific type of malware that locks your data and demands payment to unlock it. Recognizing the signs of malware or ransomware infections is crucial for protecting your devices and data. Here are some common symptoms to watch out for:



Frequent Pop-ups

If you encounter persistent pop-ups, especially those with warnings or offers that seem too good to be true, it could indicate malware. Some pop-ups may pose as virus alerts, tricking users into downloading malicious software disguised as a solution.

Slow or Malfunctioning Devices

Malware can significantly slow down your device, cause apps to crash, or generate strange error messages. If your device starts behaving abnormally, it may be infected.

Suspicious New Programs or Extensions

Be cautious if you notice unfamiliar programs or browser extensions that you don't remember installing.

Locked Files or Ransom Notes

Ransomware often encrypts files and displays a message demanding payment to restore access.

Browser Hijacking

If your browser's homepage or search engine changes without your consent and redirects you to unintended websites, this could be a sign of malware.

Disabled Antivirus or System Tools

Some malware disables antivirus programs or system tools like Task Manager (Windows) or Activity Monitor (Mac) to avoid detection. If these tools remain disabled despite attempts to enable them, your device may be compromised.

Unexpected Emails or Social Media Activity

Malware infections can result in emails being sent from your account or social media posts you didn't create.

Counter Measures

Scan Devices for Malware

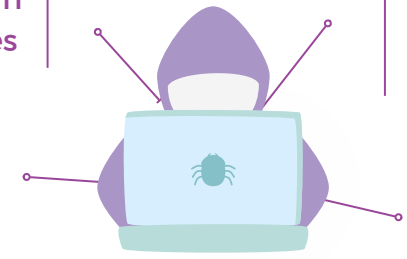
- Use Antivirus or Anti-Malware Software: Run a full scan on your device using reputable software like Malwarebytes, or Windows Defender.
- Isolate Infected Devices: Disconnect compromised devices from the internet to prevent malware from spreading or communicating with attackers.
- If you don't know how to deal with the malware, reach out to trusted organizations who can help you.
- Regularly update software and operating systems.

Unauthorized Account Access

If you notice signs that someone else has accessed your accounts like

Notifications of logins from unknown locations or devices

Changes to account settings (e.g., passwords, recovery emails).

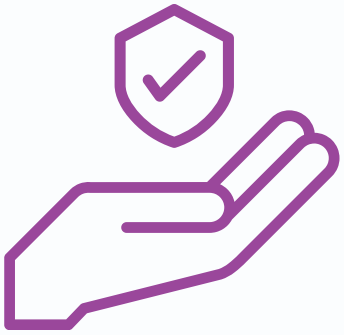


Check in the settings of the accounts what devices are logged in to your account and from what location.

Unrecognized purchases or sent messages.

If a security breach occurs, taking prompt action can limit damage and help secure your accounts and devices.

Secure Compromised Accounts

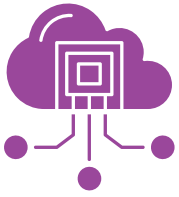


- Change Passwords Immediately: If you can still access the account, change your password to a strong, unique one. Enable two-factor authentication (2FA) for added protection.
- Log Out of All Sessions: Many platforms allow you to log out from all devices. Use this feature to kick out any unauthorized users.
- Alert Contacts of the Breach: If your email or social media is compromised, inform your contacts and colleagues to prevent them from falling victim to any scam messages sent from your account.
- Notify Relevant Platforms: Report the breach to the service provider or platform, as they may have additional recovery steps or advice.

Unusual Network Activity

Abnormal network activity could indicate hacking attempts or malware:

Significant spikes in data usage.



Unknown devices connected to your network.

To protect yourself from such attacks:

- You should always download software from official websites.
- Be very careful with email attachments and files you receive in message or social media.
- Never click on suspicious links.
- Don’t insert USB’s or cables you don’t own yourself in your devices.

Recognize Fake Websites

Cybercriminals often create counterfeit websites that mimic legitimate ones to steal sensitive information.

Check for HTTPS

While HTTPS indicates that the information transmitted between your browser and the website is securely encrypted, it doesn't guarantee the website's authenticity. Hackers can also use HTTPS on fake sites.

Look for Typos and Inconsistencies

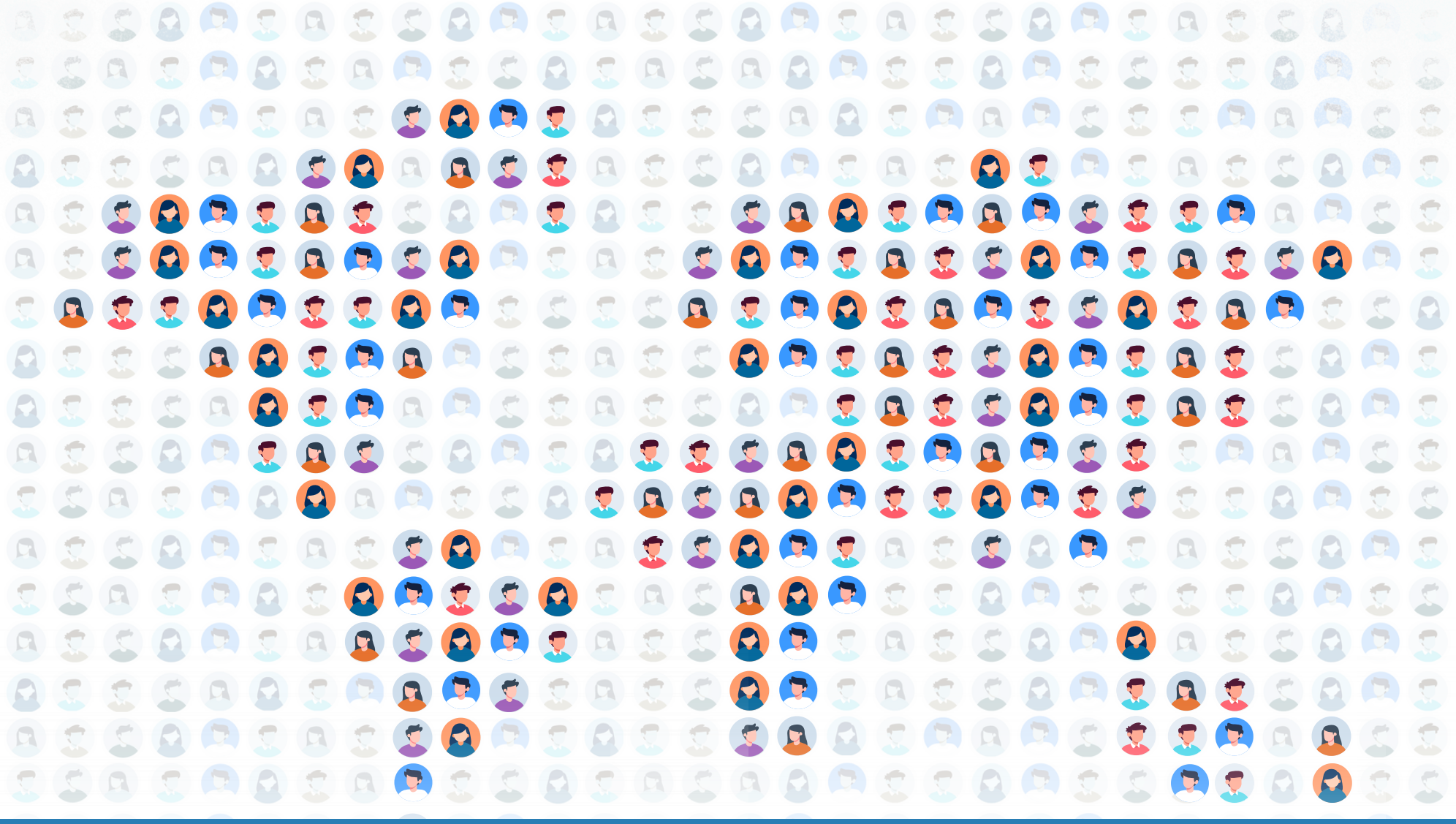
Fake websites often have poorly designed layouts, misspelled words, or unusual colors that don't match the official branding.

Verify the URL Carefully

Cybercriminals often create URLs that mimic real sites by changing a letter or using alternate extensions (like "gmall.com" or "amazon.shop" or "facebouk.com"). Always double-check the spelling of URLs before entering sensitive information.

With the rise of Advanced Persistent Threats (APTs), typically highly skilled hackers often affiliated with states or state-sponsored groups who carry out complex and prolonged attacks, and the increasing use of AI by cybercriminals to automate and enhance attacks, and the increasing use of AI-generated phishing emails and deepfake attacks, recognizing digital threats has become an essential skill in today's technology driven world.

Staying vigilant against phishing attempts, malware infections, and fake websites, while adopting a proactive cybersecurity approach, can significantly reduce your vulnerability to cyberattacks. Remember, cybersecurity isn't just about using the right tools; it's also about raising awareness and good habits. By regularly educating yourself about emerging threats, you can stay prepared in an ever-evolving digital landscape.



Maharat Foundation

Address:
Jdeideh, Metn
Lebanon

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

مهارات
Maharat