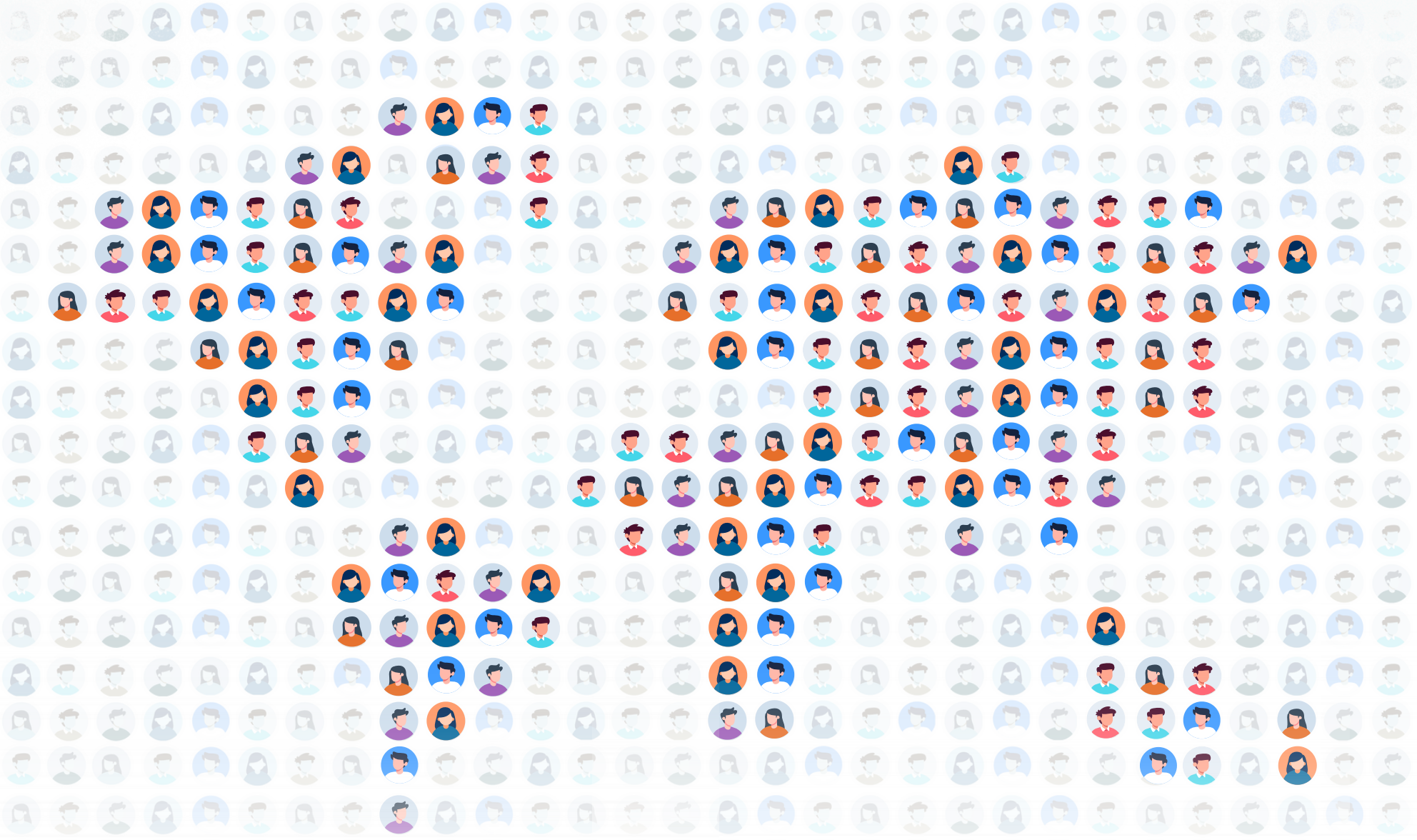


THE DIGITAL SECURITY MANUAL

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 3

DATA PROTECTION BEST PRACTICES:

How to securely store and manage sensitive data (backups)

Prepared by:
Digital security expert
Bahaa Nasr

How to Securely Store and Manage Sensitive Data and Backups

The protection of sensitive data is crucial for everyone specially journalists and activists... Backups are an important pillar of data management and protection strategy, **ensuring that your information is available, safe, secure, and recoverable in the event of loss or damage.** Whether it's documents, pictures and videos, financial records, personal information, or intellectual property, data loss can have significant impact, as well financial, and reputational consequences. Users often don't think of backups until a disaster hit, that is why **adopting robust data protection practices helps minimize these risks**.

1 Data Loss Prevention

Data can be lost due to **hardware failures, device theft, accidental deletions, cyberattacks** (such as malware and ransomware), **natural disasters, or even user error.** A **backup ensures that you have a copy of your data** to restore from in case any of these events occur.

- Ransomware attacks can encrypt your files and demand payment to restore them.
- Hard drives, SSDs, and servers can fail without warning.
- Natural disasters such as floods, fires, or earthquakes can destroy physical data storage.
- Users may accidentally delete or overwrite important files.
- Devices loss or theft

Backups provide an easy way to recover from this type of disasters and restore your files and data in short time.

2 How to Backup?

First you need to decide what you want to backup. Usually, your important files like work documents, pictures, videos, contacts, database... You don't need to backup anything available online and can be downloaded like installation software or similar files.

1

Backup Frequency: Determine **how often you need to back up your data** based on its criticality and the frequency of changes. **For critical data, frequent backups (daily or weekly) may be necessary**, while less critical data may require less frequent backups.

2

Backup Retention: Determine **the numbers of backup copies you want to retain** depending on how sensitive and valuable is your data. You can maintain **multiple versions of your files over time**, enabling you to revert to an earlier version if needed. And decide **how long you need to retain backup copies, based recovery objectives, and storage capacity.**

2 How to Backup?

The method you use to backup data depends on your needs, the sensitivity of your data, and the technology available.

Select Backup Storage location:

Your backup storage options are important for your strategy. A mix of local and off-site storage provides comprehensive protection. You should store backups in a secure location separate from your primary data storage.

Local Storage: External hard drives, USB sticks, or Network Attached Storage (NAS) can store backups onsite. This provides quick access to data for immediate recovery, but is vulnerable to physical damage or theft.

Off-Site Storage: Storing backups in an off-site location, such as a data center or on external hard drives, USB sticks and storing them in a different geographic location, can protects against local disasters like fires, theft or floods.

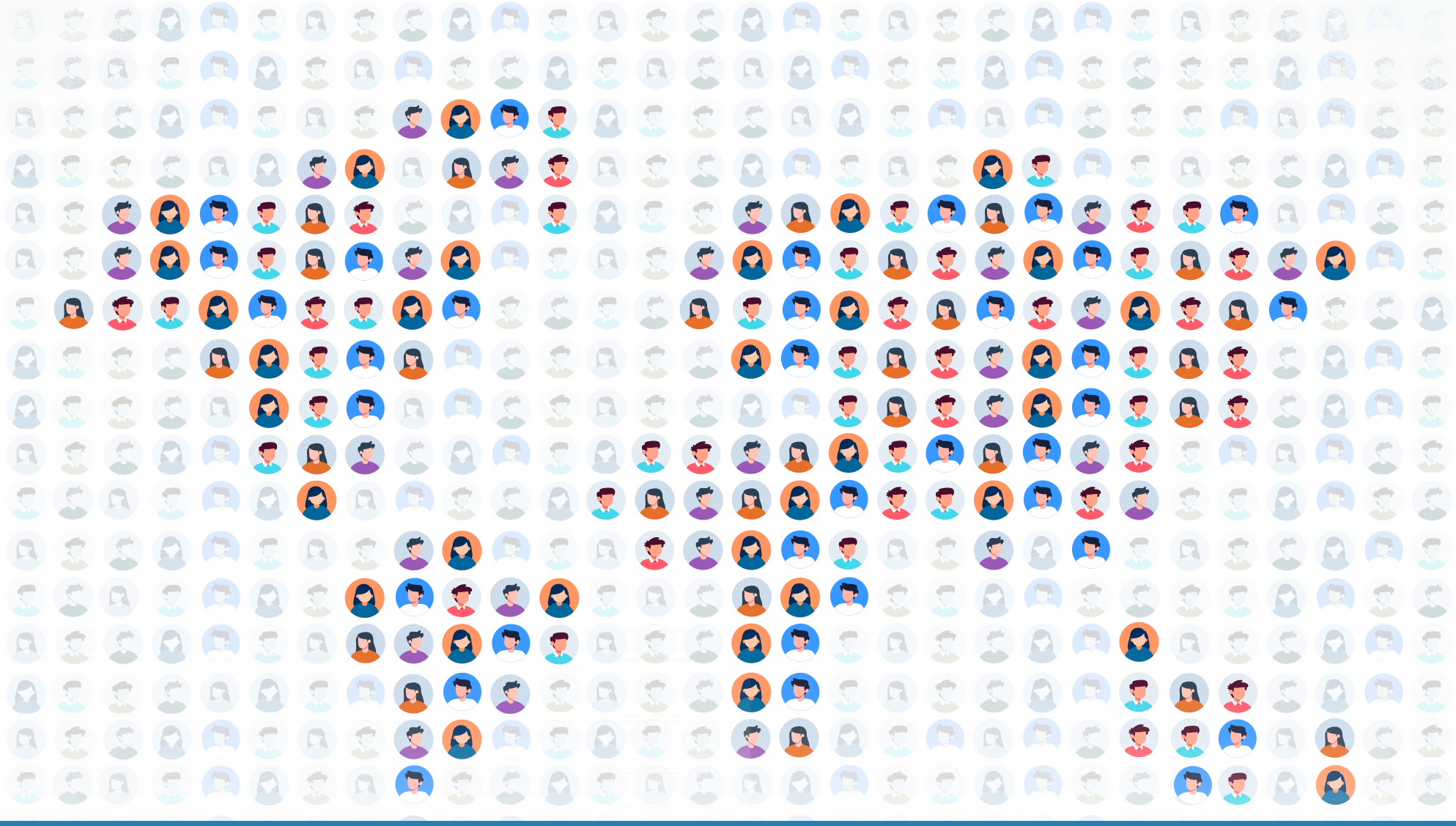
Cloud Backup: Cloud services provide scalable, secure backup options. Data is stored on remote servers managed by cloud providers, offering redundancy and easy access from anywhere.

3 Recommendations

If possible, a combination of local storage, off-site storage, and cloud backup offers a comprehensive, layered approach to data protection. This combination provides redundancy, accessibility, and resilience against various threats like hardware failure, cyberattacks, and natural disasters. Each method has its strengths, and when used together, they create a robust backup strategy.

Regularly verify the integrity and completeness of your backups to ensure they are reliable and can be restored when needed.

Ensure that your backups are stored securely and encrypted for both local and cloud backups to protect them from unauthorized access during storage and transmission.



Maharat Foundation

Address:
Jdeideh, Metn
Beirut, Lebanon

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

مهارات
Maharat