RECIPE

Recentering The Civic Internet Through Partner Engagement

A Practical Guide

Digital Security Tools User Guide

2025

OXFAM Alkhatt ROSE

RECIPE
Recentering The Civic Internet Through Partner Engagement

This 30-day plan is a guiding manual for journalists, through sequential daily training

Each unit contains practical instructions, hands-on exercises, and review checklists aimed at strengthening understanding, consolidating acquired skills, and tracking progress toward safer digital practices.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Program

Week one ► Protection of accounts

Week two ► Protection of devices

Week three ► Securing communication and safe browsing

Week four ► Protection of data and privacy

RECIPE
Recentering The Civic Internet Through Partner Engagement

Week One

Protecting Accounts

Securing digital accounts is a fundamental step to protect your identity and your sensitive information.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #1

Reviewing Accounts

Inventory of digital assets from digital accounts

Start by creating a comprehensive list of all your digital accounts, such as email accounts, social media accounts, and accounts on digital services and other website.

You must verify **passwords** and review **the phone numbers and email addresses** linked to each account. This data is essential in account recovery operations when you lose access to it.

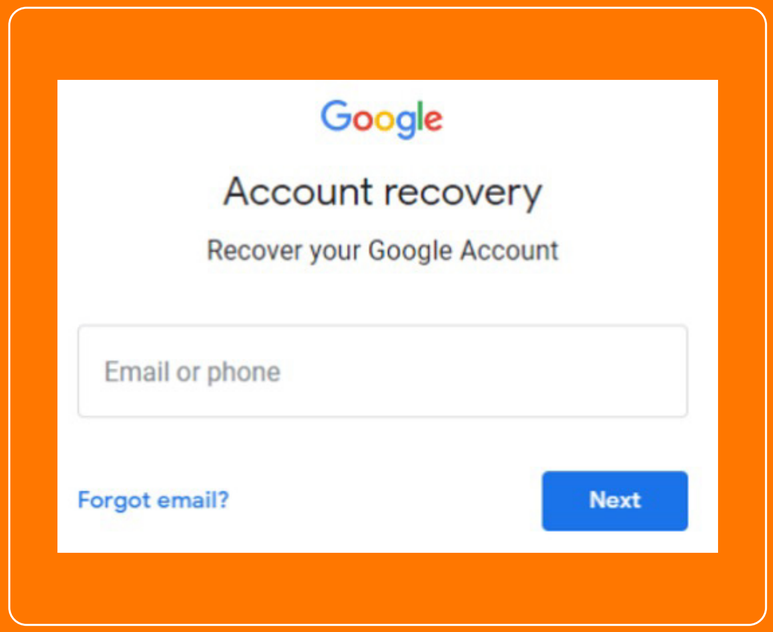
RECIPE
Recentering The Civic Internet Through Partner Engagement

RECIPE
Recentering The Civic Internet Through Partner Engagement

In Google accounts, for example, you can add:

- Trusted phone number to receive verification codes.
- Backup email addresses used in emergencies.
- Security questions or alerts that help verify your identity.

In this way, you ensure that all your accounts have safe, continuously updated recovery methods.



RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #2

Protecting Digital Accounts

Protect digital accounts, especially the email account, with strong and updated passwords

Email is considered the main gateway to your digital life, as it is used to recover most other accounts. Therefore, you must give it top priority in protection.

- Changing your password regularly: It’s best to update your email password periodically (for example, every 3–6 months) to reduce the risk of hacking.
- Choosing a strong password: It should be long and include a mix of letters, numbers, and special symbols.

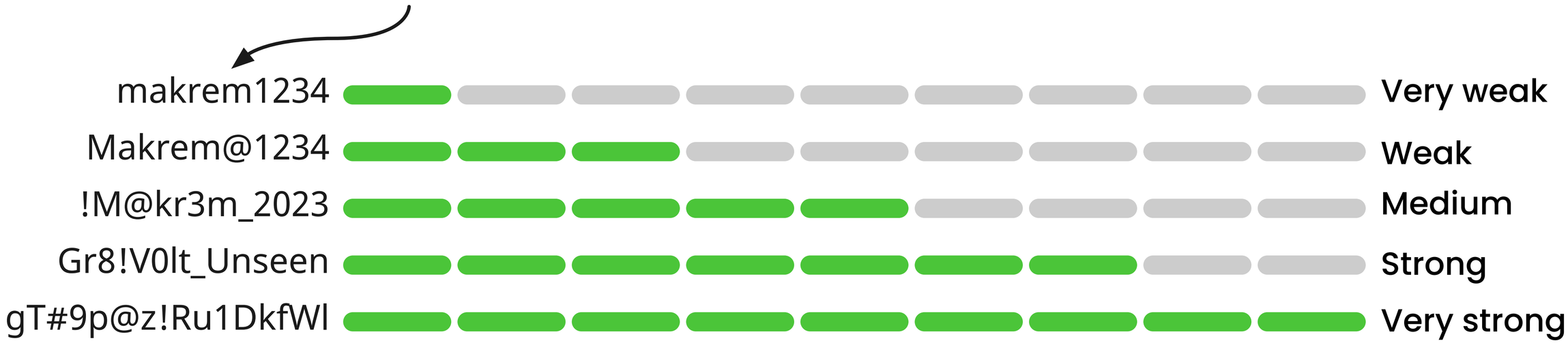
Avoid using common words or personal information that can be easily guessed.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Choosing passwords

Choosing a strong password is one of the basic steps to protect accounts and personal information. The password should consist of more than 16 characters and include a mix of letters, numbers, and symbols. Avoid reusing the same passwords across multiple accounts, and do not use personal information that is easy to find online, such as date of birth or name of a relative.

Use **How Secure Is My Password** to evaluate the strength of your password

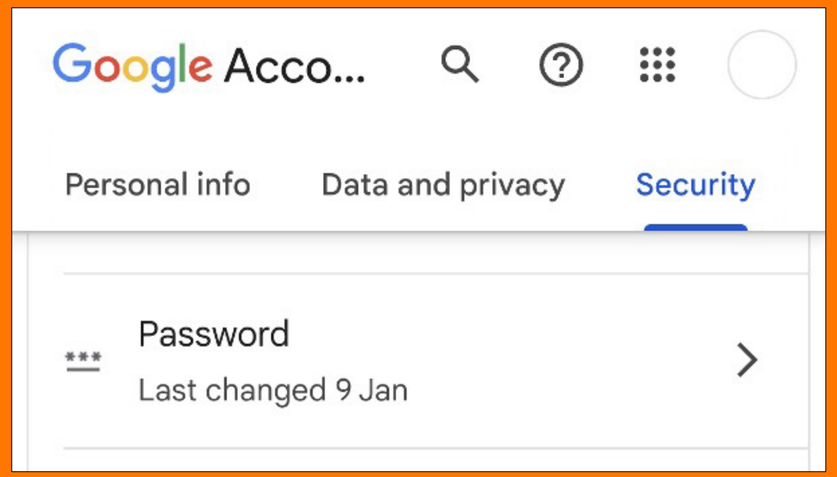


Password strength meter (5 levels)

Changing Google Account Password

1. Open myaccount.google.com
2. From the Security section, choose “Sign in to Google“.
3. Click on “Password” and enter the current password.
4. Enter a new strong and unique password, then save it in the password manager.
5. Make sure to update stored passwords on your phone/browser.

With these steps, ensure that your email is protected with a strong password.



RECIPE
Recentering The Civic Internet
Through Partner Engagement

Day #3

An Extra Layer of Protection (MFA)

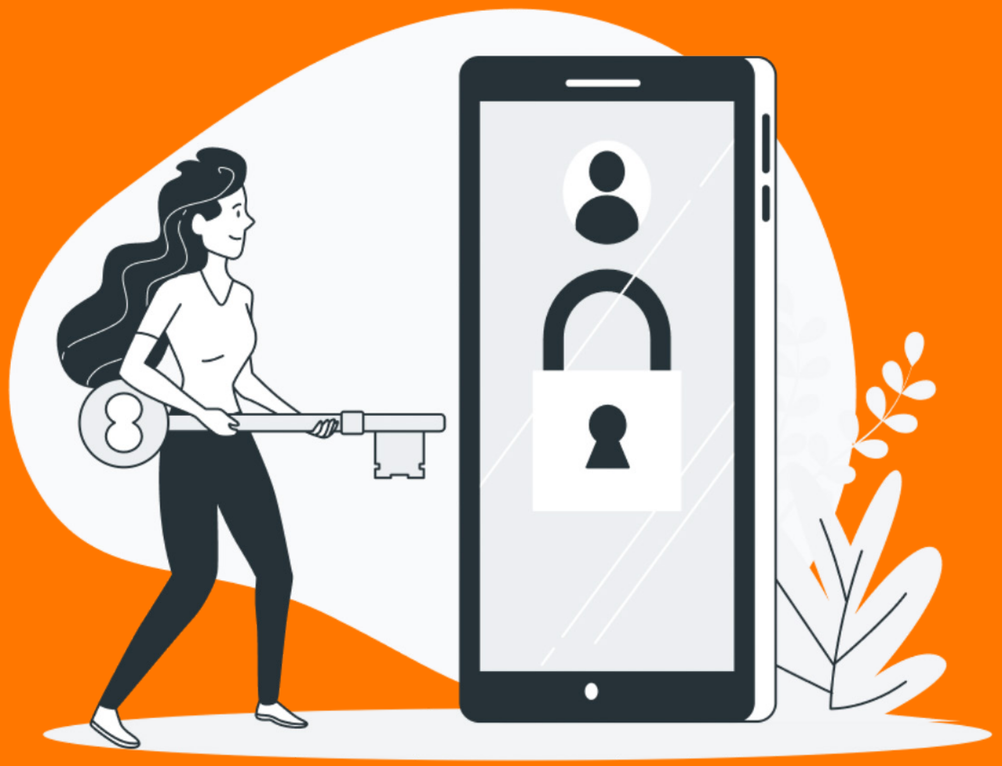
Adding an Extra Layer of Protection (MFA)

Multi-Factor Authentication (MFA) is one of the strongest digital protection methods, because it adds an extra security layer on top of the password. Instead of relying only on the password (which may be leaked or hacked), you need a second or third factor to verify identity.

Common MFA factor :

- Temporary codes (OTP) that arrive via SMS or an authenticator app such as “Authenticator“.
- Notifications on the phone to confirm login.
- Physical security keys such as YubiKey.
- Fingerprint or face recognition when using the phone.

RECIPE
Recentering The Civic Internet Through Partner Engagement



MFA activation in Meta account settings

1. Launch the application Instagram or Facebook, navigate to Settings and Privacy.
2. Choose Security and Login (Security and Authentication).
3. Locate the two-factor authentication option, Multifactorial/(2FA / MFA).
4. Select a protection method:
   Approval application (recommended).
   Physical safety essential (for enhanced security).
5. Incorporate a dependable authentication device or application.

It is always advisable to utilize authentication applications or security keys rather than text messages, as they offer enhanced security and reduced susceptibility to hacking.

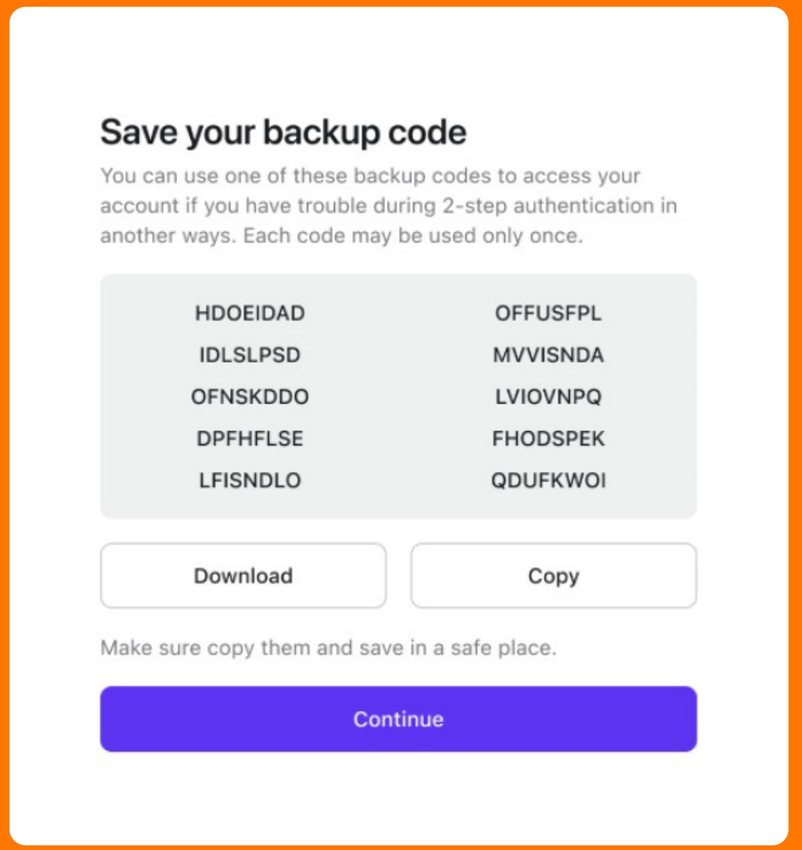
RECIPE
Recentering The Civic Internet Through Partner Engagement

Retrieval codes are regarded as “Backup Codes“, an optional yet significant last resort for regaining access to your account in the event that you lose your phone or you are unable to utilize Multi-Factor Authentication (MFA). Tokens provide the capability to log in once per token.

Why are retrieval codes significant?

- A supplementary security measure in the event that the phone is lost or the authentication application fails.
- It functions even in the absence of internet connectivity or a card.

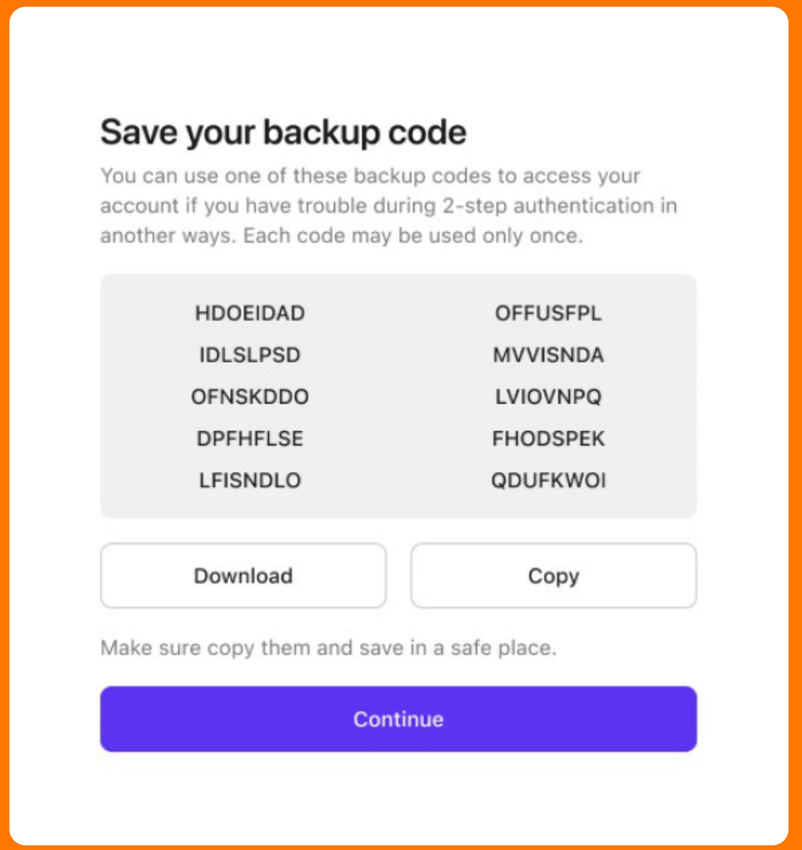
RECIPE
Recentering The Civic Internet Through Partner Engagement



Generate and preserve backup Codes

1. Access the security settings within your account (Example: Meta and Google).
2. Locate the "Refund Codes" option Backup Codes.
3. Develop a new collection of symbols (typically 8–10 symbols).
4. Download it as a text file or print it immediately.
5. Keep the codes in a secure location:
   - Paper secure or encrypted document.
   - Refrain from saving it as an image on your phone or in your email.

RECIPE
Recentering The Civic Internet Through Partner Engagement



RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #4

Utilizing the symbols of the return

For the enduring safeguarding of digital accounts

Utilizing a password manager is among the most crucial practices for bolstering digital security, as it allows you to generate robust and distinct passwords for each account, eliminating the necessity to memorize or reuse them.

Advantages of a password manager:

- Generate robust, random passwords that are challenging to decipher.
- All passwords are securely stored in an encrypted vault.
- Seamless account access without the necessity of memorization.
- Synchronization (devices).

RECIPE
Recentering The Civic Internet Through Partner Engagement

RECIPE
Recentering The Civic Internet
Through Partner Engagement

Day #5

Password administration

Secure storage
and management
of credentials

RECIPE
Recentering The Civic Internet Through Partner Engagement

Use Bitwarden Password Manager

1. Create an account on bitwarden.com, the application is installed on your phone.
2. Generate a robust new master password, because it is the sole key to access to all of your passwords.
3. Add your accounts sequentially.
4. Use the password generator tool within Bitwarden to generate robust and distinctive passwords.
5. Download Bitwarden extension in the browser to activate autofill feature.
6. Regularly monitor the password safe and remove old passwords.

RECIPE
Recentering The Civic Internet Through Partner Engagement

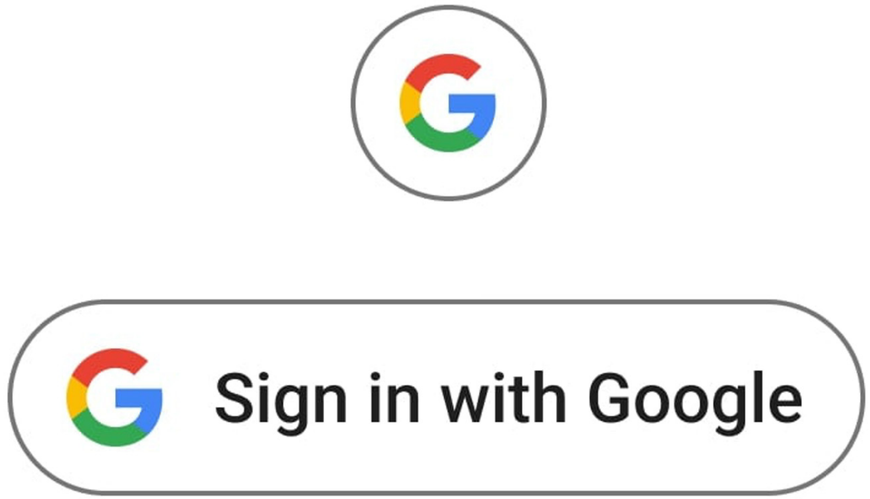
Day #6

Eliminate superfluous hyperlinks

Disabling superfluous permissions and links

RECIPE
Recentering The Civic Internet Through Partner Engagement

Numerous digital accounts, such as Facebook, are linked to your social media profiles. Over time, you may amass connections that are unhelpful or potentially hazardous, jeopardizing your data security. Consequently, it is crucial to assess these links and remove any that are unnecessary.



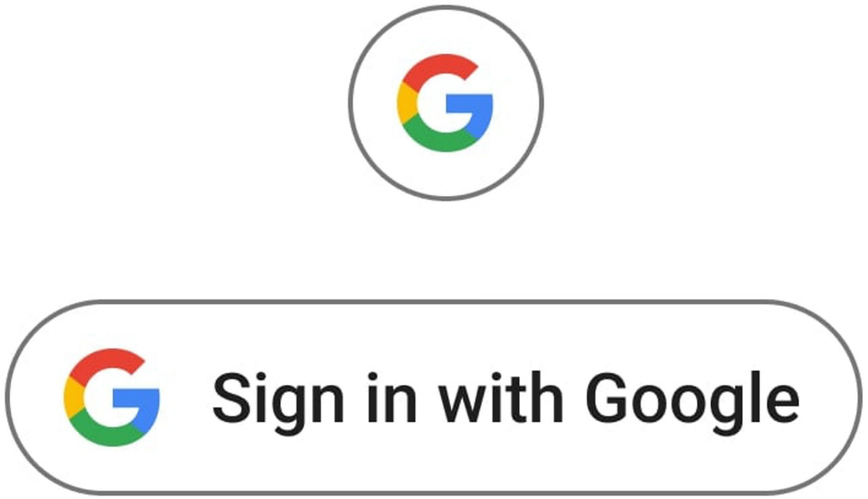
Why is this significant?

- Certain legacy applications may compromise your data in the event of a security breach.
- At times, you grant more permissions than required (access to email, photos, contacts).
- Safeguard your privacy by limiting the number of individuals linked to your account.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Review the provided links on Google

1. Open myaccount.google.com
2. From the list, choose Safety (Security).
3. Continue scrolling until you arrive at the section.
4. Applications authorized to access the account.
5. Select any superfluous application. Or unknown, and opt to revoke access.



RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #7

Assessment and Appraisal

First week

Account Security Assessment

RECIPE
Recentering The Civic Internet Through Partner Engagement

At the conclusion of the first week, it is essential to perform a self-assessment to safeguard your digital accounts. This session will assist you in evaluating your current circumstances and establishing priorities for the days ahead.

Please respond to the following questions using a rating scale from 1 to 5 (1 = Very Weak, 5 = Proficient).

After responding, compile a list of tasks requiring enhancement.

RECIPE
Recentering The Civic Internet Through Partner Engagement

1. Have you compiled a thorough list of all your significant digital accounts (email, social media, digital services)?
2. Are the passwords for all your primary accounts robust and distinct?
3. Have you recently updated your primary email password to a robust one?
4. Has multi-factor authentication (MFA) been activated on social media platforms?
5. Have you generated and stored the backup codes?
6. Do you use a password manager (such as Bitwarden)?
7. Have you assessed the applications and services associated with your accounts and eliminated those that are not beneficial?

RECIPE
Recentering The Civic Internet Through Partner Engagement

Second Week

Device security

Securing digital accounts is a crucial measure in safeguarding your identity and sensitive information.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #8

Operating system upgrade

Review the security protocols and verify their adherence

Updating applications and browsers mitigates security vulnerabilities, ensures the functionality of new features, and safeguards your data.

Practical steps:

1. Activate automatic updates for all applications on your mobile device and computer.

2. Launch the applications and browsers, then verify ppdates are available.

3. Following any significant update, please restart the application or the browser to ensure that the modifications are implemented.

- Always ensure that you are using a legitimate, licensed version of the operating system, as pirated copies are frequently insecure and do not receive updates.

- A secure and efficient alternative is to use a system which is regarded as an Open-source software, such as **Ubuntu** that is more secure and provides enhanced control over your privacy.

Updated + Original Operating System

=

A Device More Secure Against Attacks

RECIPE
Recentering The Civic Internet
Through Partner Engagement

Day #9

Applications security

Review the security protocols and verify their adherence.

Updating applications and browsers mitigates security vulnerabilities, ensures the functionality of new features, and safeguards your data.

Practical steps:

1. Activate automatic updates for all applications on your mobile device and computer.

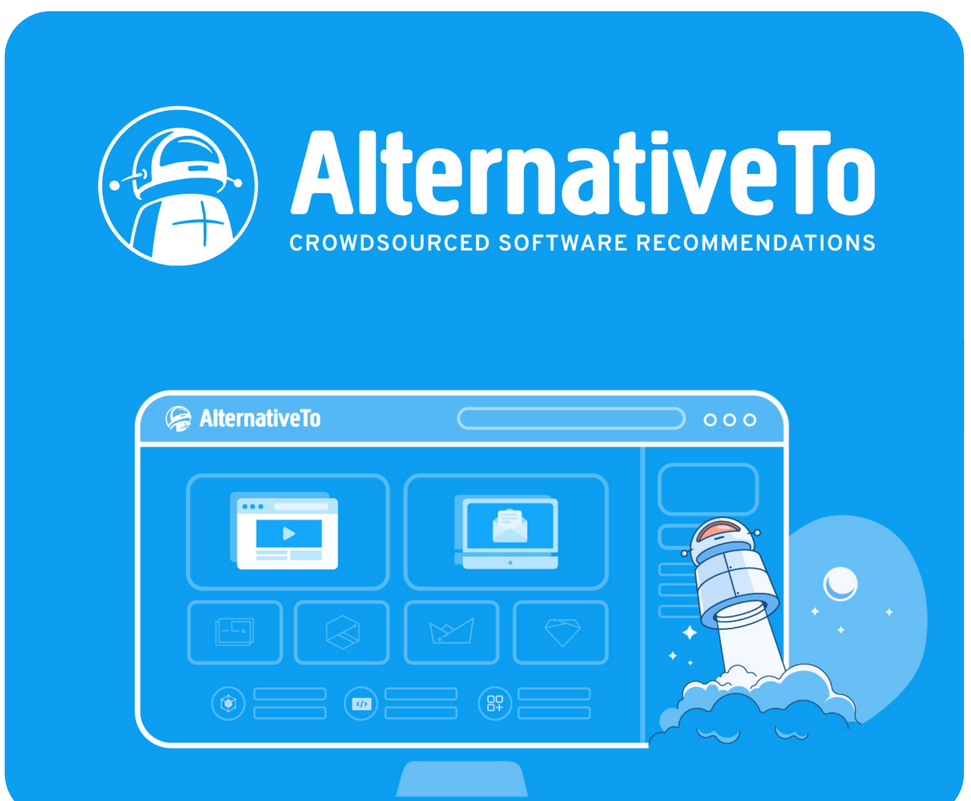
2. Launch the applications and browsers, then verify ppdates are available.

3. Following any significant update, please restart the application or the browser to ensure that the modifications are implemented.

- Use secure and complimentary alternative programs when specific applications are required. For instance the website **Alternativeto.net** is a reliable and open-source platform for popular software.

- It is advisable to refrain from installing software from untrusted or unfamiliar sources, as it may harbor malware.

Updating applications and selecting secure software
=
Substantially mitigates risks to your device and data



RECIPE
Recentering The Civic Internet
Through Partner Engagement

Day #10

Safeguarding the device against viruses and malware

Review the security protocols and verify their adherence

RECIPE
Recentering The Civic Internet Through Partner Engagement

Using an effective antivirus program is an essential part of device protection, as it helps to discover and prevent malicious software before it harms your device or your data.

Practical steps:

- **Windows Defender:** Antivirus for malware integrated in Windows, providing good essential protection without needing additional software.

- Adding an antivirus like **Bitdefender**, with the purpose of moment-to-moment protection and advanced features to maintain safety.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Important Notes

1. Enable Real-Time Protection in your antivirus software.
2. Schedule a periodic full scan of your device at least once a week.
3. Do not rely solely on antivirus; combine it with operating system and application updates to provide comprehensive protection.
4. Be cautious when downloading files or applications from untrusted sources, even if you have antivirus software.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #11

Device storage encryption

Review the security protocols and verify their adherence

RECIPE
Recentering The Civic Internet Through Partner Engagement

Storage encryption protects your data if your device is lost or stolen, by making access to the files impossible without the password or security key.

Activating Encryption on **Windows** using **BitLocker:**

1. Open Control Panel > System and Security> BitLocker Drive Encryption
2. Select the drive you want to encrypt and click Turn on BitLocker.
3. Follow the instructions to create a password or use a security key to fully encrypt the drive.

Keep a copy of the recovery key in a safe place, do not save it on the encrypted safe itself.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Storage encryption protects your data if your device is lost or stolen, making access to the files without the correct password or key impossible.

Use **VeraCrypt** for encrypted disks or folders on any system:

1. Download VeraCrypt from the official website.
2. Create an encrypted container (Encrypted Container) to store sensitive files.
3. Choose a long, strong password, and mount the container to access files when needed.

Keep a copy of the recovery key in a secure place; do not save it on the same encrypted device.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #12

Securing the mobile device lock

Review the security protocols and verify their adherence.

RECIPE
Recentering The Civic Internet Through Partner Engagement

A phone lock is the first line of defense to protect your data from unauthorized access. Using a strong method reduces the risks of theft or hacking.

Activating Encryption on **Windows** using **BitLocker:**

- Use a long PIN instead of simple lock patterns or short codes.
- It is preferable to use a passphrase of 4-6 random words that are easy to remember and hard to guess.
- Enable fingerprint or facial recognition (Biometrics) as an additional security layer, but do not rely on it alone.
- Make sure to disable any simple lock options (like the simple pattern or 1234).

Passphrase + Biometrics
=
Strong and easy-to-use protection for your phone and data

Windows BitLocker

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #13

Enable remote scanning

Review the security protocols and verify their adherence

RECIPE
Recentering The Civic Internet Through Partner Engagement

Activating Remote Wipe lets you protect your data if your phone is lost or stolen, by erasing the device content and locating it.

Steps for each Operating System:

Android

1. Open Find My Device or go to google.com/android/find.
2. Sign in with the Google account linked to the phone.
3. You can locate the phone, play a sound, lock the device, or wipe data remotely.

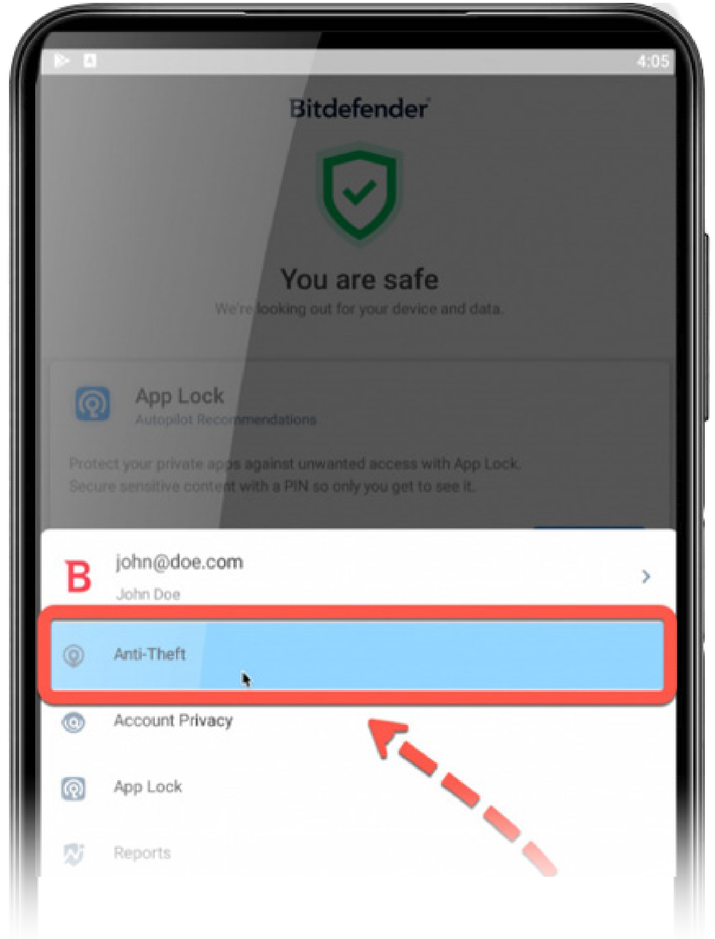
iPhone

1. Open Find My iPhone from iCloud or another device app.
2. Turn on Send Last Location to send the last known location before the battery runs out.
3. You can remotely lock the device or wipe all data.

The Anti-theft feature in Bitdefender Mobile Security provides advanced features such as:

- Pinpoint the phone's location accurately.
- Remote device locking.
- Wipe content if necessary.
- Alerts when switching SIM cards or attempting unauthorized access.

Combining Find My Device + an Anti-Theft app like Bitdefender provides comprehensive protection for your sensitive devices and data.



RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #14

Assessment and Appraisal

Device Protection Audit

Second week

Review the security protocols and verify their adherence

At the conclusion of the second week, it is essential to perform a self-assessment of your device security. This session will assist you in evaluating the robustness of your device security settings and identifying areas that require enhancement.

Please respond to the following questions using a rating scale from 1 to 5 (1 = Very Weak, 5 = Proficient).

After responding, compile a list of tasks requiring enhancement.

RECIPE
Recentering The Civic Internet Through Partner Engagement

RECIPE
Recentering The Civic Internet Through Partner Engagement

1. Have you recently updated your operating system?
2. Are all your applications and browsers updated to the latest version?
3. Do you use a licensed version of the operating system or an open-source system like Ubuntu?
4. Do you have a reliable antivirus that works effectively?
5. Have you secured your phone's lock using a strong password or code along with biometrics/face recognition?
6. Have you activated encryption on your device to protect sensitive files?
7. Have you activated the 'Find My Device' feature or its equivalent?
8. Have you reviewed the installed applications and removed unnecessary or suspicious ones ?

RECIPE
Recentering The Civic Internet Through Partner Engagement

Week Three

Secure browsing and communication

Educational objective: To cultivate awareness regarding protection against digital threats (phishing, tracking), to improve privacy during online browsing and messaging, and to establish a safer digital environment for everyday use.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #15

Transitioning to encrypted messaging

Review the security protocols and verify their adherence

Most popular messaging applications fail to provide sufficient privacy protection, as messages can be readily intercepted or monitored if they lack full encryption. This vulnerability permits the interception of messages and the analysis of a user's digital fingerprint, facilitating the tracking of their activities. Utilizing encrypted and reputable messaging applications enhances the security of personal data and sensitive conversations while minimizing your digital footprint.

Supplementary advice:

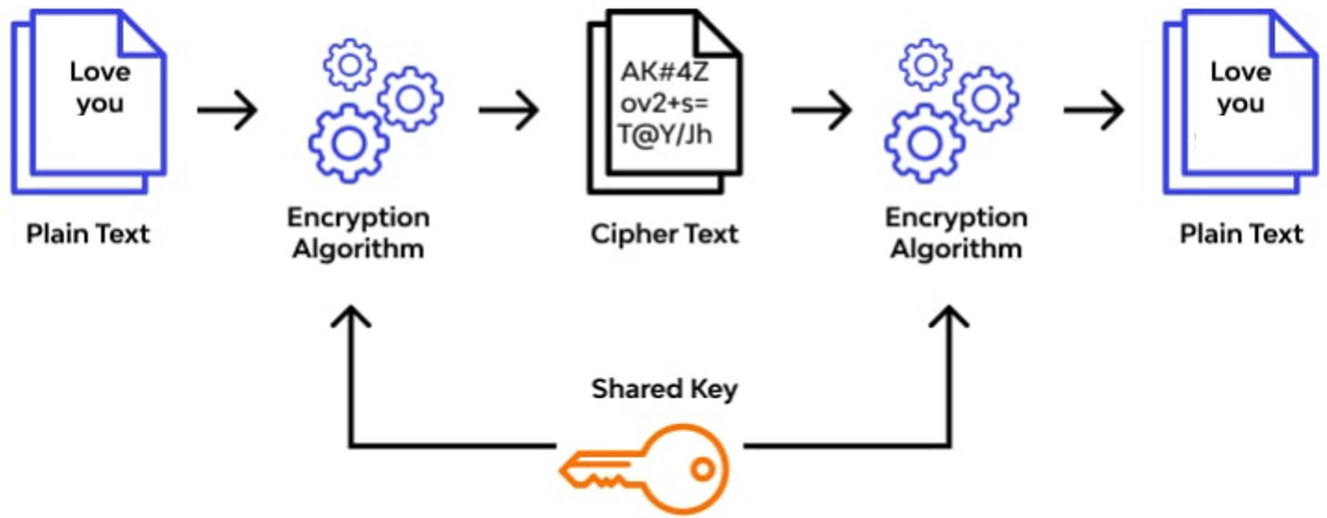
- It is advisable to utilize a robust password to safeguard the messaging account.
- Avoid unfamiliar applications or those that fail to clarify their encryption policies.

Encryption is a technique for transforming data into incomprehensible codes, ensuring that only authorized individuals can interpret them. Whether transmitting a message, storing a file, or backing up your device, encryption offers a fundamental layer of security for your data, even in the event of interception or device theft.

End-to-end encryption signifies a more sophisticated level of security. It guarantees that only the sender and recipient can access the message content, preventing the service provider, platform, or any third party from gaining access.

Consequently, end-to-end encryption is regarded as one of the most dependable methods for safeguarding private conversations, particularly in high-risk settings.

End-to-end encryption

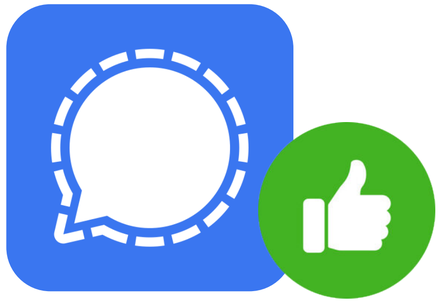


*Ciphertext: is the text produced by encrypting the original content with an encryption algorithm.

Not all messaging applications provide the same degree of protection for conversations. Some do not enable encryption by default and necessitate additional configurations, while others offer robust security automatically. Comprehending these distinctions is crucial for selecting the appropriate tool for secure communication, particularly when handling sensitive information or confronting cyber threats.

Secure messaging platforms

Signal



Encrypted and securely automated

Endorsed by the open-source community and overseen by a non-profit organization

Whatsapp

Automated encryption with affitional configurations

Owned by Meta

Messenger

Not encrypted automatically

Owned by Meta

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #16

Privacy and security configurations on social media platforms

Review the security protocols and verify their adherence

RECIPE
Recentering The Civic Internet Through Partner Engagement

Today, we concentrate on enhancing the security of WhatsApp by examining its settings and utilizing concealed features that improve privacy.

Examine privacy configurations:

- Access Settings > Privacy.
- Conceal Last Seen & Online
- Limiting access to the profile picture and personal information.
- Disable read receipts (blue tick) if you prefer not to disclose whether your messages have been read.

WhatsApp

RECIPE
Recentering The Civic Internet Through Partner Engagement

Backup Management:

- If you use backups on Google, iCloud or Drive, enable the full backup encryption option with a strong password.

Unencrypted backups may expose your messages to risk if the cloud account is compromised.

- Regularly review whether you actually need to keep a backup or if it is enough to retain only important conversations.

WhatsApp

RECIPE
Recentering The Civic Internet Through Partner Engagement

Activate confidential discussions :

- Open any chat > Tap on the contact's name > Choose Chat Lock
- Access will be granted exclusively through fingerprint or password authentication.

WhatsApp

RECIPE
Recentering The Civic Internet Through Partner Engagement

Enable automatic message deletion:

- Open the chat > Tap on the contact's name > Choose self-disappearing messages.
- Indicate the duration (24 hours, 7 days, 90 days).
- This safeguards you from amassing unnecessary old messages that could potentially be used against you.

WhatsApp

RECIPE
Recentering The Civic Internet Through Partner Engagement

Encryption confirmation:

Every WhatsApp conversation is encrypted by default; however, you may confirm this by:

- Open the chat > Tap on the contact's name > Encrypt > Compare the code with the other individual.

WhatsApp

RECIPE
Recentering The Civic Internet Through Partner Engagement

Strategies for safeguarding your account:

- Enable Two-Step Verification on WhatsApp configurations to enhance security and safeguard your account against theft.

- Ensure that the retrieval methods utilizing telephone numbers and email addresses are employed.

WhatsApp

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #17

Exercise caution regarding unsolicited phishing attempts

Recognizing phishing attempts

RECIPE
Recentering The Civic Internet Through Partner Engagement

Recognize and evade becoming a target of phishing attempts through email, text messages, or deceptive links.

What constitutes random phishing?

- Deceptive messages or links intended to mislead individuals for the purpose of acquiring passwords, personal information, or financial data.

- It typically originates from an unfamiliar email address or an unknown number, requesting that you click on a link or download a file.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Essential Tips for Protection from Phishing:

1. **Check the sender's identity:** Do not trust messages from unknown addresses or those with spelling errors.
2. **Avoid clicking on suspicious links:** Hover the mouse or long-press to see the link before opening it.
3. **Do not share your personal data:** (passwords, bank details) via email or messaging apps.
4. **Use verification tools like:**
   - VirusTotal to check links.
   - PhishTank to confirm reported sites.
5. **Enable two-step verification** on your important accounts to minimize damage if your password is revealed.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #18

Exercise caution regarding unsolicited phishing attempts

Recognizing phishing attempts

RECIPE
Recentering The Civic Internet Through Partner Engagement

Using a secure browser reduces the risks of tracking and hacking and helps you protect your personal data during daily browsing, as well as preserving privacy and minimizing the collection of data and tracking of the user's digital footprint.

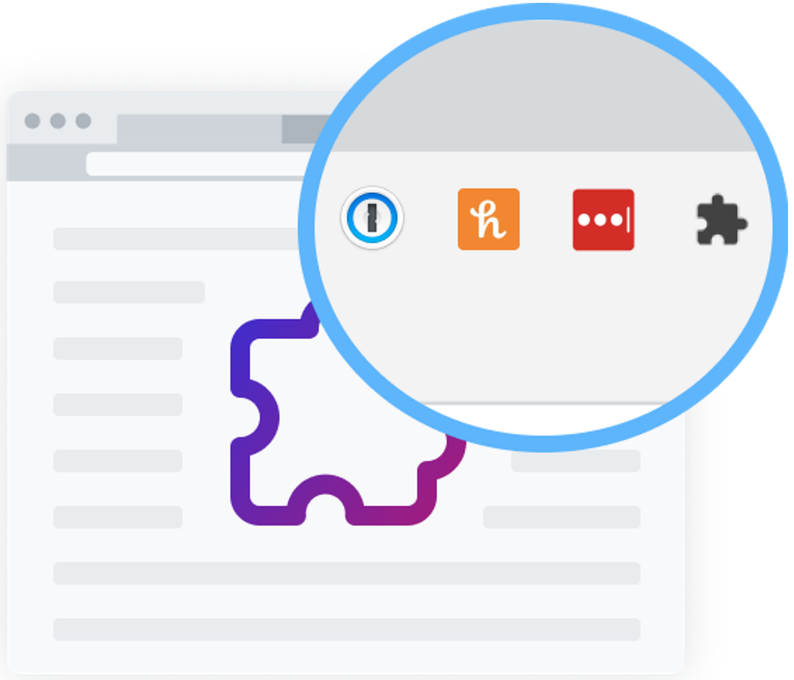
Adoption of secure browsers:

- **Brave:** Provides built-in ad and tracking blockers.
- **Firefox:** With privacy extensions such as uBlock Origin and Privacy Badger.
- **Tor Browser:** For anonymous browsing and accessing blocked content (preferred only when needed)...

RECIPE
Recentering The Civic Internet Through Partner Engagement

Add-ons Administration (Extensions):

- Only essential and trusted additions have been installed.
- Please provide the text you would like me to update.



RECIPE
Recentering The Civic Internet Through Partner Engagement

Activating Privacy Features:

- Disable the option to save passwords within the browser.
- Enable Do Not Track and delete cookies and regularly delete cookies and browsing data.
- Instead of Google, try search engines like DuckDuckGo or Startpage that respect privacy more.
- Use a separate browser for your personal accounts and another for work or other uses.

Startpage

DuckDuckGo

Choosing a secure browser + configuring its settings

=

The first line of defense against tracking and phishing is the first line of defense against tracking and phishing

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #19

Safe browsing

Recognizing phishing attempts

Verify the link :

- Ensure that the website name is accurately spelled. For instance: **facebook.com** and not **faceb00k.com**

- Avoid dubious shortened links, and utilize tools to decrypt them prior to clicking, such as **CheckShortURL**.

RECIPE
Recentering The Civic Internet Through Partner Engagement

When navigating the internet, it is essential to assess the credibility of the websites you visit to prevent becoming a victim of fraud or data theft.

Always use https protocol:

- Do not input any personal or financial information on a website that does not start with **https://**
- While having a padlock icon 🔒 next to the link does not guarantee the site's safety, it is a fundamental prerequisite.

When navigating the internet, it is essential to assess the credibility of the websites you visit to prevent becoming a victim of fraud or data theft.

RECIPE
Recentering The Civic Internet Through Partner Engagement

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #20

Blocking trackers

Recognizing phishing attempts

RECIPE
Recentering The Civic Internet Through Partner Engagement

Trackers are used by websites and ads to collect data about you, such as: the sites you visit, your interests, and even your daily online habits.

Blocking these trackers protects your privacy, prevents building a personal profile about you, and reduces your digital footprint in general.

Activating Anti-Tracking Features in Browsers:

- In **Firefox:** Enable 'Enhanced Tracking Protection
- In **Safari:** Enable Prevent Cross-Site Tracking
- In **Chrome:** Activate Do Not Track' setting + use extensions for blocking trackers, like uBlock Origin and Privacy Badger.
- Or use **Brave:** It blocks trackers automatically.

The less data you share, the harder it is for companies and trackers to build a complete profile of you.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #21

Assessment and Appraisal

Secure Browsing Assessment

Week Three

The most challenging aspect is to provoke sniping attempts and to engage with the public

At the conclusion of the third week, it is time to conduct a self-assessment of your digital communications and internet browsing habits. This session will assist you in evaluating your current status and establishing priorities for the upcoming days.

Please respond to the following questions using a rating scale from 1 to 5 (1 = Very Weak, 5 = Proficient).

After responding, compile a list of tasks requiring enhancement.

RECIPE
Recentering The Civic Internet Through Partner Engagement

RECIPE
Recentering The Civic Internet Through Partner Engagement

1. Have you started using an encrypted messaging app (like Signal) instead of relying on traditional apps?
2. Have you reviewed the security and proivacy settings in messaging apps?
3. Have you become more aware of phishing messages and links, and can you identify signs of fraud?
4. Have you started using a secure browser and reviewed the privacy settings in browsers?
5. Do you always check URLs before entering your data, and have you confirmed the use of HTTPS?
6. Have you activated extensions or tools to prevent tracking?

RECIPE
Recentering The Civic Internet Through Partner Engagement

Week Four

Data classification for secure storage

Educational objective: To cultivate awareness regarding protection against digital threats (phishing, tracking), to improve privacy during online browsing and messaging, and to foster a safer digital environment for everyday use.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #22

Examine your personal information disclosure

Recognizing phishing attempts

Protect yourself from Social Engineering (Hacking, Doxing, and Defamation) by being aware of information available about you on the Internet and reducing your exposure.

Search for yourself online:

- Use search engines like Google, Bing, and DuckDuckGo to search for your full name, email address, phone numbers, and usernames.
- Categorize the information by its sensitivity:
  High: National ID number, phone number, home address, financial data.
  Medium: Pictures, workplace, friend list.
  Low: General interests, public posts on Social media.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Request to remove your personal data

- Find the sites that display your data, send them a removal request.
- Request removal of the page from Google search results.
- Review the privacy settings in your digital accounts.

Check for data breaches

- Use breach checking tools, like **"Have I Been Pwned"**, to see if your email has been breached

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #23

Privacy configurations on digital platforms

Recognizing phishing attempts

Following an assessment of the extent of disclosure of your personal information, we will now concentrate on adjusting privacy settings to avert unauthorized access and safeguard your data on social networks.

Practical measures to safeguard your accounts

1. Assess who has access to your personal content.
2. Control who is able to search for and follow you.
3. Examine the permissions and applications associated with the account.
4. Configuration for messages and conversations, including automatic deletionand confidential discussions.
5. Update passwords and activate multi-factor authentication (MFA).

Consistently review your privacy settings, as updates to the platform may alter them automatically.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #24

Data Governance Policy

Establish a straightforward and transparent data management policy

Establish a systematic framework for managing sensitive data that mitigates risks such as data loss, leakage, or unauthorized access.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Classify Data	Store Securely	Limit Access	Back Up Regularly	Overall Protection
Identify the classification of data as public, internal, confidential, or highly sensitive. Categorize each file or document based on its sensitivity level to establish the suitable protection measures.	Utilize encrypted and access-controlled storage solutions. Keep sensitive data separate from unsecured devices.	Adhere to the principle of minimal authority. Grant access solely to individuals who require it to fulfill their responsibilities.	Establish automated, encrypted backups for critical data. Store the backup copies in a secure location.	Effective data management safeguards your business, your information sources, and your organization or project. The policy should undergo periodic review to adjust the level of protection as necessary.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #25

Data Security Strategy

Data classification for secure storage

Organize your personal and professional data in a way that enables you to store it safely, while determining the appropriate level of protection for each type of data.

Identify your data types:

- **Highly Sensitive:** words, passwords, financial data, ID files, digital certificates.
- **Moderate:** business documents, personal notes, important emails.
- **Low Sensitivity:** general information, non-confidential family photos, general educational files.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Low Sensitivity

Public files or backup copies ofnon-sensitive work information.

Using tools such as:

- Google Drive
- Proton Drive (Encrypted Data)

Moderate

Partial encryption or an encrypted container offers security while remaining accessible and easy to update.

Using tools such as:

- VeraCrypt
- Encrypted folders

Highly Sensitive

Comprehensive encryption secured by a robust password and maintained within a segregated environment for long-term storage.

Using tools such as:

- BitLocker
- VeraCrypt
- Bitwarden

RECIPE
Recentering The Civic Internet
Through Partner Engagement

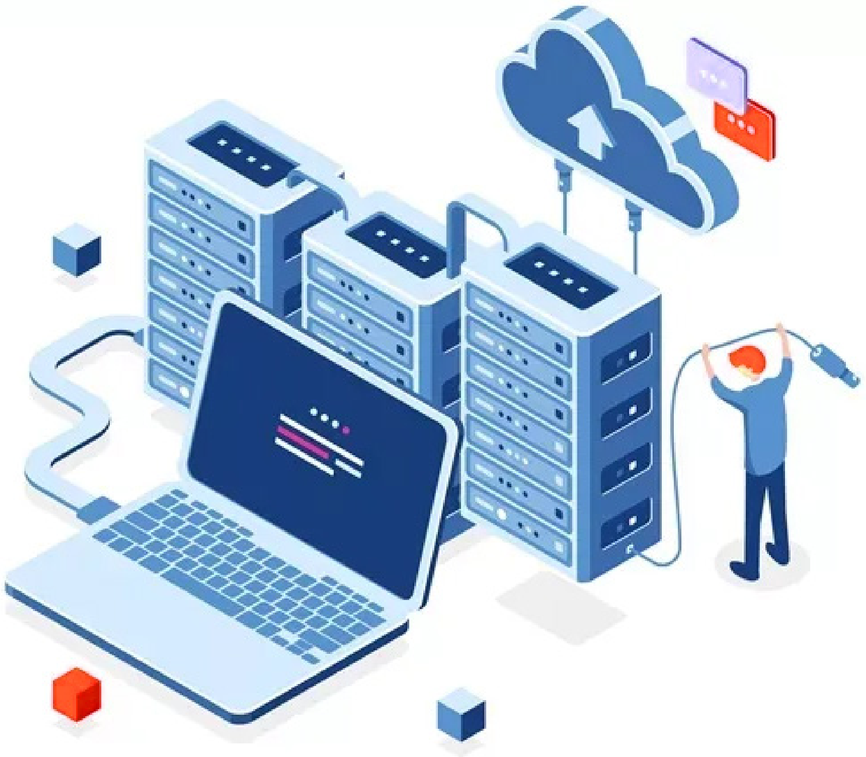
Day #26

Personal security

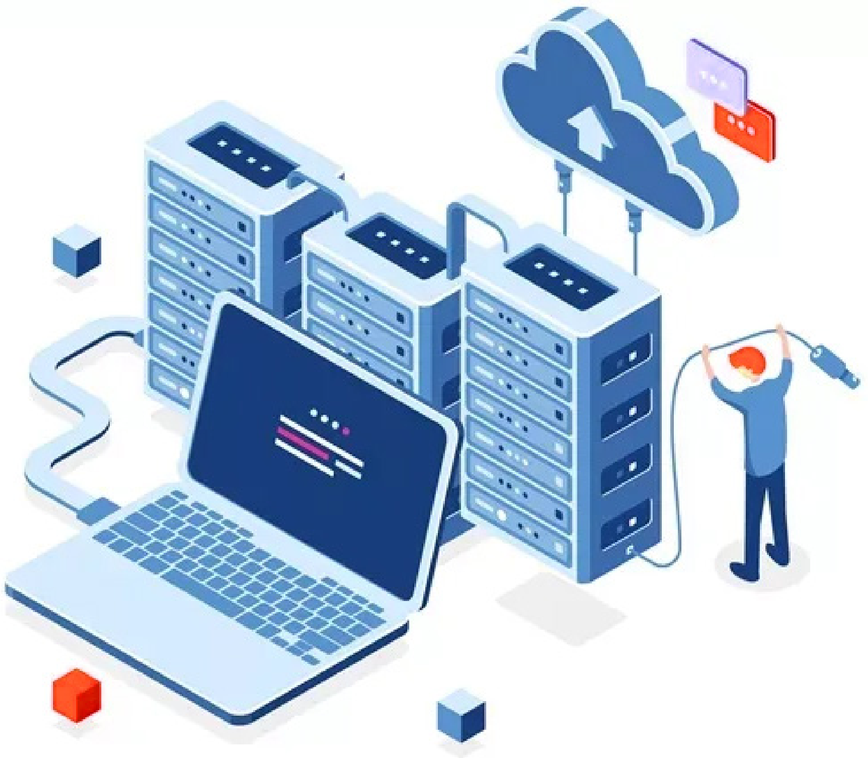
Data classification
for secure storage

To safeguard your digital information, it is essential to consider not only cybersecurity but also the physical security of sensitive devices and documents, as well as the methods employed for their storage and transfer.

- Position laptops and external devices (HDD, USB) in a secure location that is impervious to theft and fire.
- Implement security systems, including surveillance cameras and alarm devices, in critical areas.
- Use encrypted safes whenever feasible.



- Use a dedicated device for travel or public events to reduce the risk of loss or hacking of the main device.
- Minimize the storage of sensitive data on portable devices during travel.
- Be cautious of people around you when working in public places or at events.
- Do not leave devices unattended.



Even the best digital security measures will not be effective if there is physical access to your devices or backup copies. The combination of cyber security and physical security protects you from data loss or leaking.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Day #27

Phishing Verification Assessment

Data classification for secure storage

Phishing Test

phishingquiz.withgoogle.com

RECIPE
Recentering The Civic Internet Through Partner Engagement

RECIPE
Recentering The Civic Internet
Through Partner Engagement

Day #28

Account recovery assessment

Data classification
for secure storage

The account recovery test serves as a practical exercise designed to confirm your readiness and capability to regain access to your accounts in the event of a lost password or a security breach.

Goal:

- Assessing the velocity and efficacy of account recovery.
- Ensure that the recovery methods are current (alternative email, phone number, security keys, etc.).
- Identify any deficiencies or challenges within the process.

This exercise will assist you in assessing your readiness for digital emergencies.

RECIPE
Recentering The Civic Internet Through Partner Engagement

RECIPE
Recentering The Civic Internet Through Partner Engagement

Exercise steps:

1. Select a non-primary account
2. Simulate the loss of your password.
3. Document the duration required to restore the account.
4. Verify the availability of return methods (mail, phone, etc.).
5. Evaluate the preparedness for any event.

This exercise will assist you in assessing your readiness for digital emergencies.

RECIPE
Recentering The Civic Internet
Through Partner Engagement

Day #29

Digital Incident Response Strategy

Data classification
for secure storage

Upon the occurrence of a digital security incident, such as a potential breach or data leak, or a phishing attempt, it becomes necessary to act quickly and calmly to limit damage and start the response and recovery process.

- Immediately disconnect the device from the Internet to reduce the risk of data leakage or remote control.
- Do not delete or modify any files so that the incident
  can be digitally documented or analyzed.
- Immediately report to technical support or a trusted
  security expert to assess the situation.
- Change passwords from another secure device.
- Log everything you know about the incident: time, symptoms, suspicious messages...

RECIPE
Recentering The Civic Internet
Through Partner Engagement

Day #30

Review and standardize the procedures

Data classification
for secure storage

RECIPE
Recentering The Civic Internet Through Partner Engagement

After 29 days of exercises and practical steps, it is time to review and bring together everything you have learned and apply it in an integrated digital security plan. The goal is to have a clear and comprehensive roadmap that you can always refer back to.

Review the list of the previous days (1–29) and write down the most important steps you took:

- **Building a "personal plan"** that includes: protecting accounts, protecting devices, backups, regular checkups, and an incident response plan.
- **Setting priorities**, including points that require continuous follow-up (such as system updates) and those that are done once (such as installing a secure browser).
- **Creating a security routine**, such as monthly reviews of passwords and updates, or annual reviews to ensure the effectiveness of tools.
- **Self-assessment** by answering:
  1. Do I feel more confident in dealing with digital threats?
  2. Can I train or help someone else?