RECIPE

Recentering The Civic Internet Through Partner Engagement

Digital Security Tools User Guide

A Practical Guide

OXFAM Alkhatt ROSE

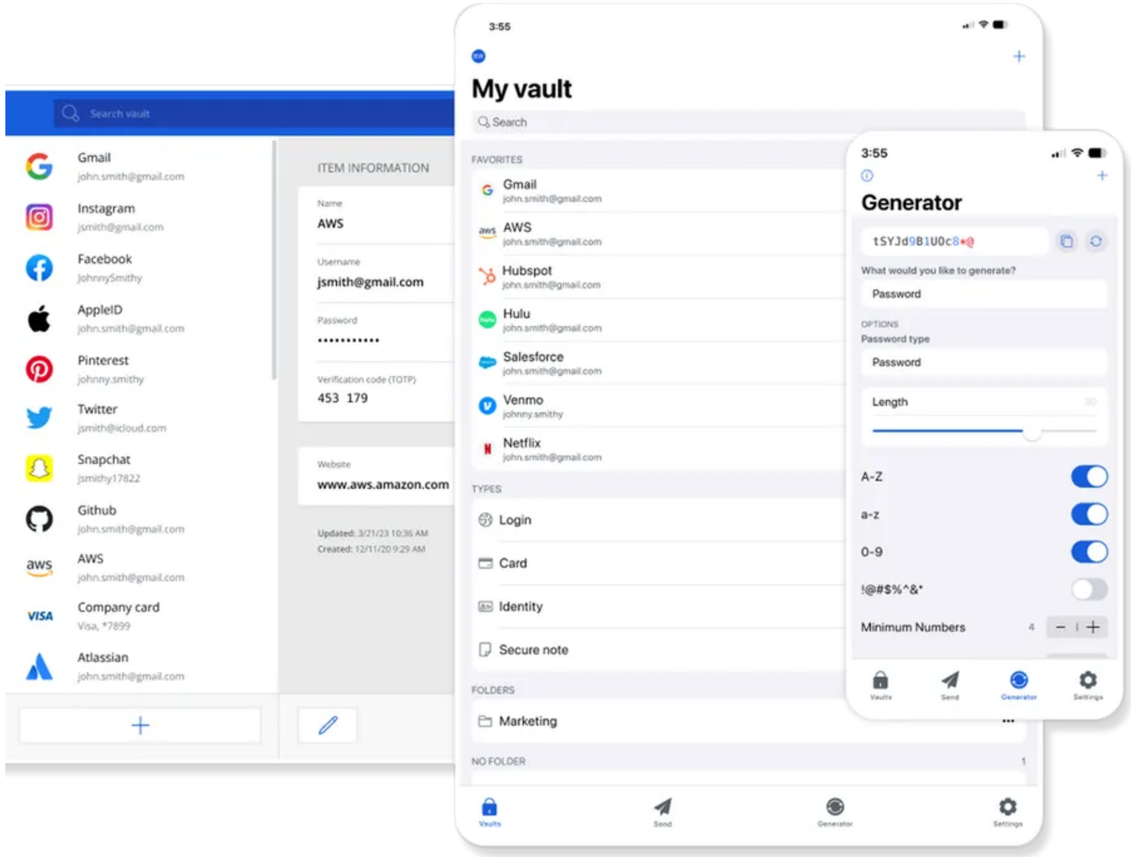
RECIPE
Recentering The Civic Internet Through Partner Engagement

Use this guide to help you build your personal digital security plan. This practical guide provides comprehensive recommendations, for securing your digital presence, devices, accounts, and data.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Personal Digital Environment

To prepare your personal digital security plan, you must start by listing your personal digital environment: the online accounts, devices, and applications you use daily. This inventory is important to build a comprehensive and sustainable security plan that protects all aspects of your digital life.



RECIPE
Recentering The Civic Internet Through Partner Engagement

Key Recommendations

- Make sure to create digital accounts only when needed
- Make sure to use multiple methods for account recovery and access
- Use secured recovery methods, such as phone numbers and secure email addresses
- Make sure to delete digital accounts when you no longer need them

RECIPE
Recentering The Civic Internet Through Partner Engagement

Secure Accounts

A password that is hard to guess and not reused across more than one website or account is the rst line of defense for your digital presence and digital infrastructure. Protect all your accounts with strong .and unique passwords.

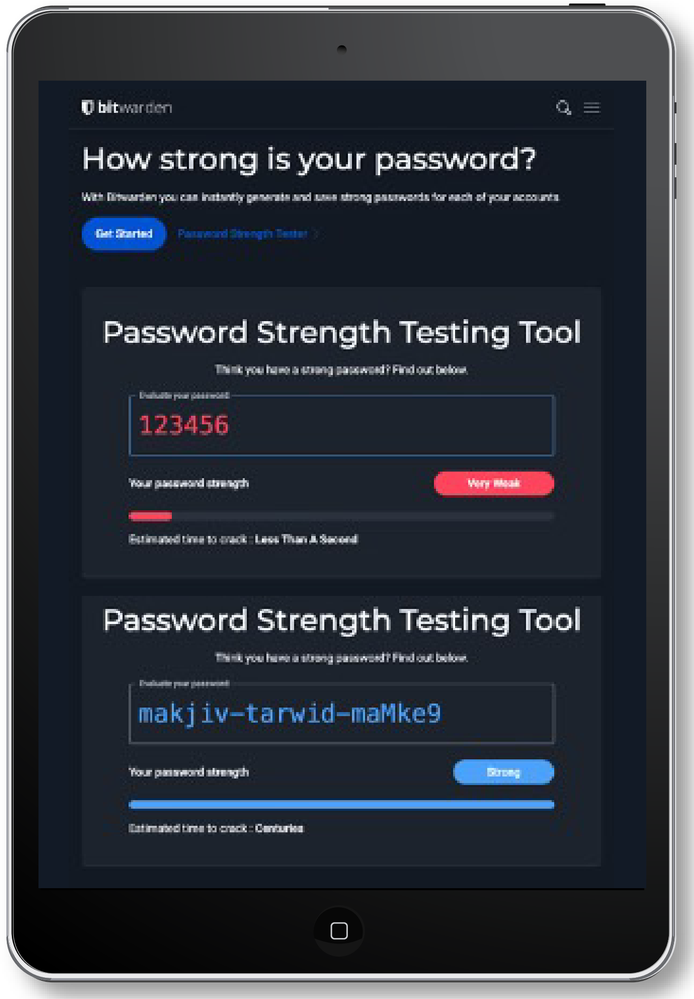
RECIPE
Recentering The Civic Internet Through Partner Engagement

Testing Password Strength

Bitwarden password strength

This is a secure tool that allows you to test the passwords you use and ensure their strength. It also helps you choose strong passwords.

https://bitwarden.com/password-strength/



RECIPE
Recentering The Civic Internet Through Partner Engagement

Password Storage

Do not store passwords in an unsafe place or somewhere that is easy to access.

Using password manager tools is highly recommended.

You can use password manager applications in the browser or on your phone as a single, safe place to store all passwords.

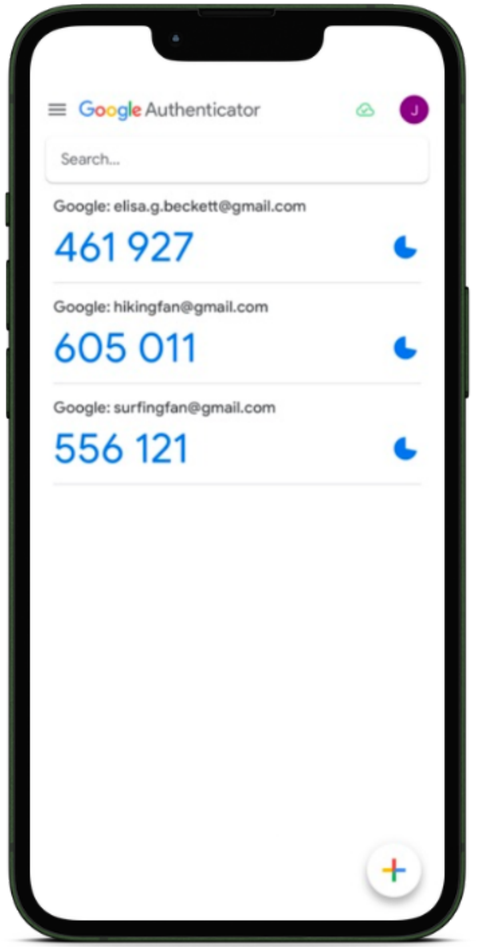
RECIPE
Recentering The Civic Internet Through Partner Engagement

Additional Protection for Accounts: MFA Authentication

An additional layer of protection that allows you to secure access to digital accounts through a changing security code managed by an application on your phone.

https://bitwarden.com/download/#bitwarden-authenticator-mobile

Trusted Alternatives: Authy, Google Authenticator



RECIPE
Recentering The Civic Internet Through Partner Engagement

Secure Systems

- Make sure to use original and properly licensed software and systems
- Make sure to regularly update all essential systems andsoftware
- Use safe and trusted software, and avoid downloading applications from unoffcial websites or stores
- Use free and open-source software or systems as secure and sustainable alternative

RECIPE
Recentering The Civic Internet Through Partner Engagement

Updating Systems andApplications

Make sure to enable automatic or periodic updates for critical systems and applications, such as: Operating systems on computers and phones, Internet browsers Antivirus programs, other applications used daily.

- Enable security and antivirus applications, such as antivirus software or built-in protection tools like **Windows Defender**.

- Ensure the proper use of security applications and periodically check the integrity of systems against malware. It is also recommended to take advantage from advanced features provided by antivirus software, such as: Device protection in case of theft, Device tracking capabilities, Real-time threat monitoring.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Securing Networks and Connections

- Use secure, encrypted Wi-Fi networks and avoid open public networks as much as possible.
- Use a VPN when connectingto untrusted networks or while traveling.
- Make sure to regularly update router settings and network passwords.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Secure Data

- The least costly method to protect data is not to collect it in the first place, or to periodically dispose of unnecessary data.
- A sustainable data protection plan requires classifying data based on importance and sensitivity, so that a dedicated protection plan can be prepared for each category.
- Make sure yourdata protection plan includes: A policy for periodically updating long-term stored data, comprehensive backup strategies, regular reviews to ensure the protection plan remains sustainable.
- Continuous alignment with changes in work methods or environment.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Suggested Data Classification

Basic Data

Important and used daily losing access affects work flow but leakage poses low risk.

Use cloud services with real-time updates and collaboration features.

Strategic Data

Not directly important for daily work, such as long term archives; leakage poses moderate risk.

Use multiple backups on external drives or cloud services; store drives in safe locations.

Sensitive Data

Subject to legal and ethical obligations; restricted access; leakage poses very high risk.

Use encrypted backups exclusively on external drives; store in secure locations.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Secure Devices

- Make sure to keep devices in secure places and avoid carrying them around unless necessary.
- Lock devices with strong passwords and avoid using weak lock methods.
- Avoid storing sensitive data on devices especially mobile phones.
- Use tracking and remote-wipe features to erase data in case of theft or loss.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Secure Phone Lock

It is obvious that all devices must be locked, when needed. It is also recommended to use more secure lock options for phones:

- Use strong passwords instead of easily guessable numeric codes.
- Avoid relying solely on biometric locks such as fingerprints or facial recognition.

RECIPE
Recentering The Civic Internet Through Partner Engagement

For Enhanced Privacy

- Make sure to request deletion of your data when deleting digital account.
- Continuously educate yourself about the digital footprint you leave when using websitesand applications.
- Review private settings on digital platforms and various online services.
- Regularly check the permissions you grant to applications and websites and revoke them when necessary.
- Use browser extensions that reduce and track who collects data about you while browsing.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Handling suspicious emails and attachments

- Do not open emails or attachments from untrusted sources.
- Verify links before clicking on them using URL-checking tool.
- If in doubt, forward the message to the technical support team or open it in a secure environment for analysis.

RECIPE
Recentering The Civic Internet Through Partner Engagement

Building Your Personal Digital Security Plan

Continuous Review

Regularly assess and update your security practices.

Continuous Education

Stay up to date on technological developments, new risks in your digital environment, and look for the latest protection methods and trusted tools.

Working as a Group

Share knowledge and protection tools with colleagues and family to build a safe environment around you.

Seeking Support

If there is a risk or suspicion of risky behavior, contact a trusted technical support entity.


RECIPE
Recentering The Civic Internet
Through Partner Engagement

Stay safe!