# CYFER

## Project Description:

Cyfer is a secure, cross-platform password manager designed to help users store, organize, and protect their credentials with ease. Created to address the growing need for secure digital identity management, Cyfer uses military-grade encryption and a zero-knowledge policy to ensure only the user can access their data. Its clean interface, auto-fill capabilities, password generator, and secure sharing options provide a seamless and safe experience for both individuals and teams.

The intended users of Cyfer are students, professionals, and everyday internet users seeking a reliable and user-friendly way to manage passwords across devices.

## Requirements Summary:

Minimum and recommended system requirements for Cyfer:

| | Minimum Requirements | Recommended Requirements |
|---|---|---|
| Processor Cores | Dual Core | Quad Core |
| OS (Desktop) | Windows 10 / macOS 10.14 | Windows 11 / macOS 12 |
| OS (Mobile) | Android 8.0 / iOS 13 | Android 10+ / iOS 15+ |
| RAM | 2 GB | 4 GB |
| Storage | 100 MB | 200 MB |
| Permissions | Internet, Biometrics, Storage Access | Internet, Biometrics, Notifications, Storage |

## Overview of Evaluation Plan:

To evaluate Cyfer's prototype, the team will conduct a three-part usability study:

1. Usability Testing – Participants complete tasks such as adding, editing, and deleting passwords.
2. Heuristics Evaluation – The prototype is assessed against Nielsen's 10 usability heuristics.
3. Participant Survey and Feedback – Users rate their experience and provide suggestions using a Likert-scale survey and open-ended responses.

## Task Examples for Participants:

- Launch and login/logout of CYFER
- Add a new password entry
- Use the password generator
- Share a credential securely with another user
- Edit or delete a password

## Heuristics Evaluation Highlights:

A summary of the heuristic evaluation for Cyfer:

| Heuristic | Evaluation Summary |
|---|---|
| Visibility of System Status | System gives real-time confirmation (e.g., 'Saved', 'Copied'). |
| Match Between System and Real World | Clear terminology like 'Vault,' 'Password,' and 'Secure Share.' |
| User Control and Freedom | Undo and cancel options available in all forms. |
| Consistency and Standards | Icons and buttons are consistent across platforms. |
| Error Prevention | Strong password rules with tips and validation. |
| Recognition Rather Than Recall | Password categories and icons improve recognition. |
| Flexibility and Efficiency of Use | Quick access features for power users. |
| Aesthetic and Minimalist Design | Clean, dark/light theme toggle, intuitive layout. |
| Help Users Recognize and Recover | Simple messages guide users when errors occur. |
| Help and Documentation | Built-in Help section and onboarding tutorial. |

## Participant Feedback:

| Survey Question | Mean | Interpretation |
|---|---|---|

| | | |
|---|---|---|
| How easy was it to add a new password? | 4.6 | Highly Acceptable |
| How would you rate the overall UI design? | 4.4 | Acceptable |
| How safe did you feel using the app? | 4.8 | Highly Acceptable |
| How easy was it to share a password securely? | 4.2 | Acceptable |
| Was navigating the app intuitive? | 4.5 | Highly Acceptable |

## Design Implications:

- Improvement Area: Some users found the UI for generating password unnecessary.
- Action Taken: Replaced the YES/NO button with a checkbox.

## Critique and Summary:

The evaluation process for Cyfer proved highly beneficial. Online testing allowed rapid collection of user insights, though connectivity issues caused minor delays. Given more time and resources, the team would explore backend integrations for secure password syncing and offline functionality.

Cyfer's core strengths include its strong encryption, ease of use, and minimalistic design. Some areas, such as feature discoverability and icon clarity, have been identified for improvement. Overall, the prototype is deemed successful and ready for further development and refinement.