KLH
(DEEMED TO BE UNIVERSITY)
BACHUPALLY CAMPUS

AOOP DTI Project

1. Team

Team Name: **Lock & Key**

Team Logo:

Team Members:

1. Surya Teja Kudupudi, **2320030229** (Section-4)
2. Varun Paleru, **2320030233** (Section-4)
3. Vajja Tejesh Venkat Reddy, **2320030246** (Section-4)
4. Balgury Ashrith Rao, **2320030442** (Section-4)

2. Problem/Opportunity Domain

Domain of Interest: **Cybersecurity and Password Management.**

Description of the Domain:

The increasing number of online services has led to a surge in password creation and management needs. Users often struggle with remembering complex passwords, leading to security risks through the use of weak or repeated passwords. The challenge is to provide a solution that not only secures user passwords but also offers ease of use.

Why did you choose this domain?

This domain was chosen due to the rising concerns about cybersecurity and the frequent issues users face with password management. There is a significant market potential for secure, user-friendly solutions, especially given the increasing frequency of data breaches.

3. Problem/Opportunity Statement

Problem Statement: Password forgetfulness can lead to significant disruptions, especially during critical moments.

Problem Description: Users frequently forget their passwords, resulting in lockouts from accounts and increased frustration. This project aims to address this issue by providing a secure platform for storing and managing passwords.

Context (When does the problem occur): The problem often occurs during account logins when users forget their passwords, particularly when accessing critical accounts or during time-sensitive activities.

Alternatives (What does the customer do to fix the problem): Customers may resort to writing passwords down, using simplistic passwords, or relying on browser-saved passwords, which may not be secure.

Customers (Who has the problem most often): The primary group affected includes regular internet users who manage multiple online accounts.

Emotional Impact (How does the customer feel): Customers feel frustrated, anxious, and insecure due to the challenges of remembering complex passwords and the fear of being locked out of accounts.

Quantifiable Impact (What is the measurable impact):

The impact can be measured in terms of time wasted in password retrieval or resets, potential financial losses due to account access issues, and the emotional toll from security concerns.

Alternative Shortcomings (What are the disadvantages of the alternatives): Existing solutions often lack adequate security measures or user-friendliness, leading to increased vulnerability to cyber threats.

Any Video or Images to showcase the problem:

littlefish
Cyber Security Services

Password Security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following UK National Cyber Security Centre advice makes password security easier for your users – improving your system security as a result.

How are passwords cracked

Manual Guessing

Personal information, such as name and date of birth can be used to guess stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Interception

Passwords can be intercepted as they are transmitted over a network.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Shoulder Surfing

Observing someone typing their password.

Searching

IT infrastructure can be searched for electronically.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Key Logging

An installed keylogger intercepts passwords as they are typed.

How to improve your Password Security

Blacklist the most common password choices.

Don't store passwords in plain text format.

Monitor failed login attempts... train users to report suspicious activity.

Change all default vendor supplied passwords before devices or software are deployed.

Prioritise administrator and remote user accounts.

Use account lockout, throttling or monitoring to help prevent brute force attacks.

0344 848 4440 info@littlefish.co.uk www.littlefish.co.uk

4. Addressing SDGs

Relevant Sustainable Development Goals (SDGs):

Goal 16: Peace, Justice, and Strong Institutions (Promoting secure and safe online experiences).

How does your problem/opportunity address these SDGs?:

By providing a secure and user-friendly password manager, the project aims to enhance online security, contributing to a safer digital environment.

5. Stakeholders

Who are the key stakeholders involved in or affected by this project?

- Users (individuals who require password management).
- Cybersecurity experts (to ensure robust security).
- Developers (for implementation and maintenance).

What roles do the stakeholders play in the success of the innovation?

- Users provide feedback on usability and features.
- Cybersecurity experts ensure the solution meets security standards.
- Developers implement the features and maintain the software.

What are the main interests and concerns of each stakeholder?

- Users want security and ease of use.
- Cybersecurity experts are concerned about data protection and vulnerabilities.
- Developers are focused on the technical feasibility and implementation efficiency.

How much influence does each stakeholder have on the outcome of the project?

- Users (High influence, as their feedback shapes the product).
- Cybersecurity experts (High influence on security aspects).
- Developers (High influence on technical execution).

What is the level of engagement or support expected from each stakeholder?

- Users will engage through testing and feedback.
- Cybersecurity experts will provide consultation and audits.
- Developers will collaborate closely throughout the project.

Are there any conflicts of interest between stakeholders? If so, how can they be addressed?

Potential conflicts between usability and security needs. Regular discussions and workshops can help bridge these gaps.

How will you communicate and collaborate with stakeholders throughout the project?

Regular meetings, feedback sessions, and collaborative tools
(e.g., Slack, Trello).

What potential risks do stakeholders bring to the project, and how can these be mitigated?

User resistance to new technology. Address this through comprehensive user training and support.

6. Power Interest Matrix of Stakeholders

- High Power, High Interest: Users, Cybersecurity Experts
- High Power, Low Interest: Developers
- Low Power, High Interest: General public (potential users)
- Low Power, Low Interest: Non-tech-savvy individuals

7. Empathetic Interviews

I need to know (thoughts, feelings, actions)	Questions I will ask (open questions)	Insights I hope to gain
Thoughts	What challenges do you face with password management?	Understand users' concerns and habits.
Feelings	How do you feel when you forget a password?	Gauge the emotional impact of password forgetfulness.
Actions	What do you do when you can't access an account?	Discover current coping strategies.

SKILLED INTERVIEW REPORT

User/Interviewee	Questions Asked	Insights gained (NOT THEIR ANSWERS)
User 1	What challenges do you face with password management?	Users often feel overwhelmed by password complexity.
User 2	How do you feel when you forget a password?	Forgetfulness leads to anxiety about account security.
User 3	What do you do when you can't access an account?	Many users resort to using the "Forgot Password" feature.

Key Insights Gained:

Insight 1: Users desire a simplified approach to password management.
Insight 2: Security concerns heavily influence users' password choices.

8. Empathy Map

a. Who is your Customer?

Description: Regular internet users aged 18-50, who utilize multiple online accounts and seek a secure and user-friendly password management solution.

b. Who are we empathizing with?

Description: Users facing difficulties in remembering complex passwords, often leading to frustration and security anxiety.

c. What do they need to DO?

Users need to securely store, retrieve, and manage their passwords efficiently.

d. What do they SEE?

Users see numerous password prompts and security warnings while managing multiple accounts.

e. What do they SAY?

Users express frustrations about password forgetfulness and the need for a secure solution.

f. What do they DO?

Users write passwords down or use repetitive simple passwords to cope with forgetfulness.

g. What do they HEAR?

Users hear advice about password security but often feel overwhelmed by the complexity.

h. What do they THINK and FEEL?

Users feel anxious about security and frustrated by forgetfulness but desire a more manageable solution.

i. Pains and Gains

Description: Users' main pain points include forgetfulness, insecurity of simple passwords, and frustration with the complexity of managing multiple passwords. Gains include having a reliable, secure, and easy-to-use password management solution.

9. Persona of Stakeholders

Stakeholder Name: Average Internet User

Demographics:

Age: 25-45
Gender: All
Income: Varies
Location: Urban areas

Goals:
To manage passwords securely while ensuring ease of access.

Challenges:
Struggles with remembering complex passwords and fears of data breaches.

Aspiration:
To have a seamless and secure online experience.

Needs:
Secure storage for passwords, ease of access across devices.

Pain Points:
Frustration from forgetting passwords, anxiety about account security.

Storytelling:
As an active online user, they often forget their passwords, leading to stress during critical access moments. A secure and user-friendly password manager can relieve this frustration.

10. Look for Common Themes, Behaviours, Needs, and Pain Points among the Users

Common Themes:

- Security concerns in password management.
- Need for user-friendly interfaces.
- Frequent forgetfulness of passwords.

Common Behaviours:

Users frequently reset passwords or use simple passwords due to forgetfulness.

Common Needs:

A secure and intuitive solution for password management.

Common Pain Points:

Time wasted on password retrieval and resets.

11. Define Needs and Insights of Your Users

User Needs:
Users require a secure, reliable, and easy-to-use password management system that helps them store and retrieve passwords effortlessly.

User Insights:

- Many users prioritize security but are overwhelmed by complexity.
- Users value simplicity and efficiency in password management tools.

12. Ideation Process

Brainstorming Session:

- Conducted a session where all team members contributed ideas.
- Ideas included features like password generation, security alerts, and user training modules.

Methods Used:

- Mind mapping, rapid prototyping, and user scenario creation.
-

Top Ideas:

- A secure password vault with auto-fill capabilities.
- Two-factor authentication for enhanced security.
- A user-friendly interface that simplifies password management.

13. Prototyping and Testing

Prototype Development:
Developed a low-fidelity prototype focusing on key features such as password storage, auto-fill, and security notifications.

User Testing:
Conducted user testing sessions with 10 participants, gathering feedback on usability and design.

Feedback Summary:

Users appreciated the auto-fill feature but suggested enhancements for the user interface.

14. Feedback and Iteration

Feedback Mechanism:

Implemented a feedback form within the prototype for continuous user input.

Key Changes Made Post-Feedback:

- Simplified the navigation based on user suggestions.
- Improved security features per user recommendations.

15. Final Solution

Description of Final Solution:

A secure and user-friendly password manager that provides robust security features, including auto-fill capabilities, two-factor authentication, and an intuitive interface for effortless password management.

Key Features:

- Password Vault: Secure storage for all passwords.
- Auto-Fill: Streamlined access to accounts.
- Two-Factor Authentication: Enhanced security for user accounts.

16. Implementation Plan

Implementation Steps:

- Develop the final product based on the prototype.
- Conduct further testing with a larger user base.
- Launch the product with an accompanying marketing strategy.

17. Conclusion

The Password Manager project aims to address the significant issues users face with password management, emphasizing security and usability. Through the Design Thinking process, insights from users guided the development of a solution tailored to their needs.