**CSC318: The Design of Interactive Computational Media**

**Design Concepts, Low-Fidelity Prototype & Initial Evaluation**

**TA: Ken (Studio D)**

**A REPORT**

**by**

**Team Vulcan**

Aayush Bhan (aayush.bhan@mail.utoronto.ca)

Asma Mohammed (asma.mohammed@mail.utoronto.ca)

Madhav Kanna Thenappan (madhav.thenappan@mail.utoronto.ca)

Mugdha Banthwan (mugdha.banthwan@mail.utoronto.ca)

Sahil Handa (sahil.handa@mail.utoronto.ca)

Stephen Lim (alfonsusstephen.lim@mail.utoronto.ca)

UNIVERSITY OF TORONTO

November 2023

**TABLE OF CONTENTS**

1. Chapter 1: Introduction 3
2. Chapter 2: Design Concepts 4

1. Concept I

2. Concept II

3. Concept III

1. Chapter 3: Storyboards 12

1. Storyboard I

2. Storyboard II

3. Storyboard III

4. Storyboard IV

5. Storyboard V

1. Chapter 4: Low-Fidelity Paper Prototype 22

1. How It Works

2. Design Features

3. Advantages of the Design

4. Disadvantages of the Design

1. Chapter 5: Evaluation of the Low-Fidelity Prototype 27
2. Think Aloud Evaluation

1.1 Study Protocol

1.2 Key Findings

1. 2. Expert Evaluation

2.1 Study Protocol

2.2 Key Findings

1. Chapter 6: Takeaways and Implications for Design 34

1. Takeaways

2. Modifications to the Design

1. Appendices 37

# **CHAPTER 1:**

# **INTRODUCTION**

Over the years, online shopping has become very popular due to the variety of goods, convenience, and different types of delivery options it offers. However, as much as it has eased our lives; it also has certain drawbacks. One of the most important drawbacks is the risk of fraud and scams.

There has been a steady increase in the number of online purchase scams over the years. These commonly take place in the form of phishing emails, impersonation calls, fake deliveries, etc. Not only do scams lead to revenue loss for institutions and customers, but they also affect people’s mental health. Scams often result in financial losses, which can lead to significant financial stress. The worry over repaying debts or regaining financial stability can contribute to mental health problems such as insomnia and overall anxiety.

***Our aim is to find ways to prevent and reduce online purchase scams and their effects on our stakeholders. We also want to find ways to guarantee online privacy for them.***



Figure. Common online scam prevention techniques.

# **CHAPTER 2:**

# **DESIGN CONCEPTS**

1. **CONCEPT I:** Making an accessible method of learning more about recent scam trends (podcasts, articles, etc).

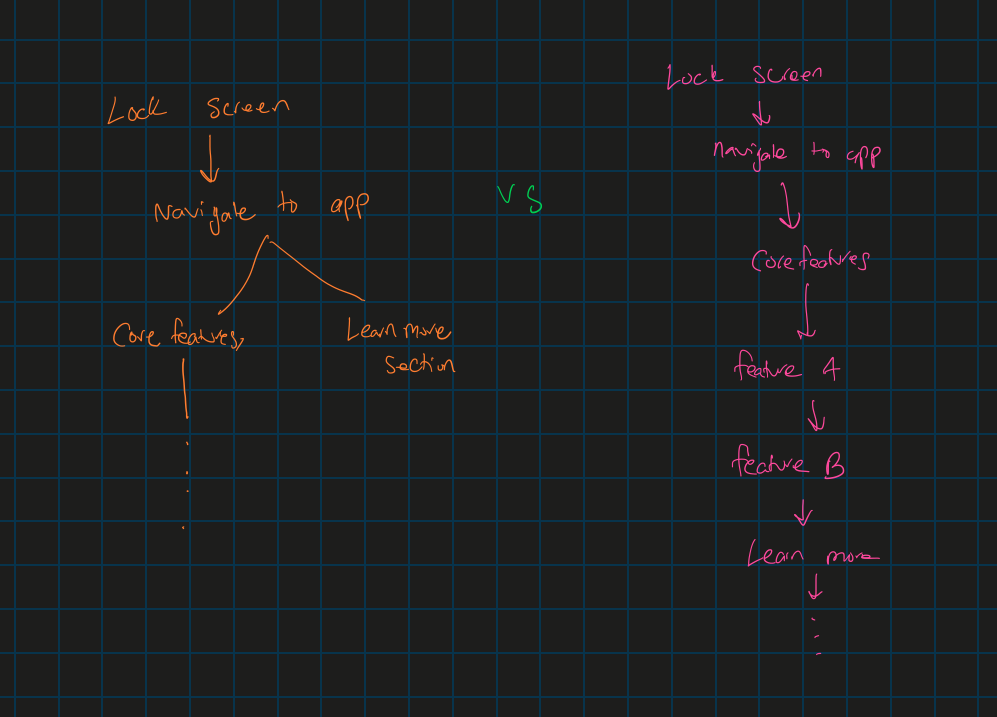


Figure. Sketch 1

* Sketch 1 describes an example of how an application flows. In modern UI, there are methods to access various pages from many avenues. This tree diagram shows a comparison between spreading out different methods of accessing pages vs having everything in more flow.

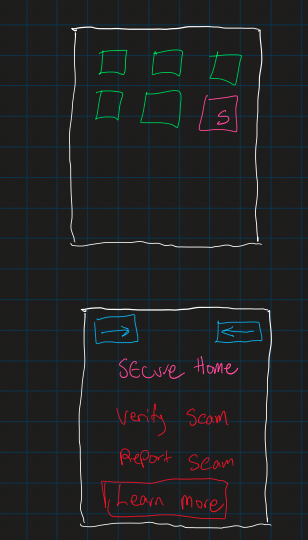


Figure. Sketch 2

* Loading to the front page we can see all options that are accessible. Here we will focus on the Learn More tab as this concept covers context 1.

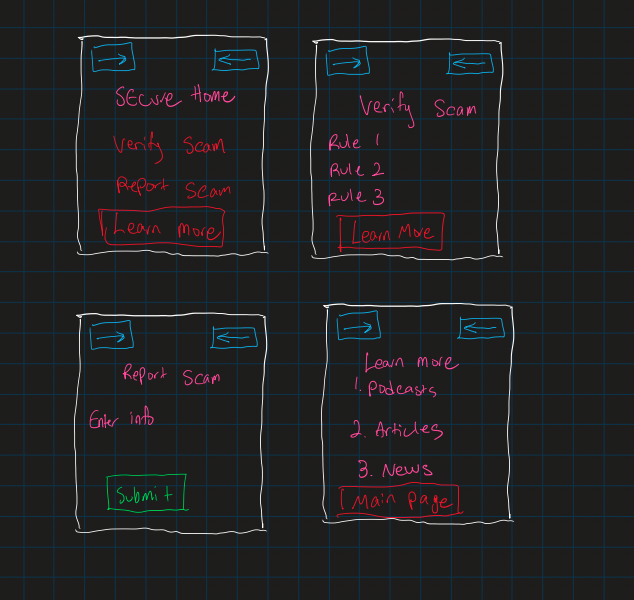


Figure. Sketch 3

* The key concept is that we can navigate to a relevant page right away rather than clicking back (working back up the page tree mentioned at the start) to get to certain pages. The idea is that we want pages accessible for relevant scenarios. Ie) What if the user wants to verify if a call is indeed a scam call, then they may also want to know about new scams, etc.

**Advantages**

1. Easy to access different pages according to current pages
2. Saves time for users, especially in high-stress situations
3. Promotes learning throughout as users may neglect this feature (knowledge is key)
4. Easier to navigate and seamless

**Disadvantages**

1. The page may become too cluttered
2. Might create a weird cycle or loop of pages
3. Navigation may become confusing if the setup is not clear
4. If we extend our program to add more features, then we have trouble deciding what pages should be linked next.
5. **CONCEPT II:** Automating scam detection in text messages and phone calls by automatically handling reporting scams and blocking numbers.

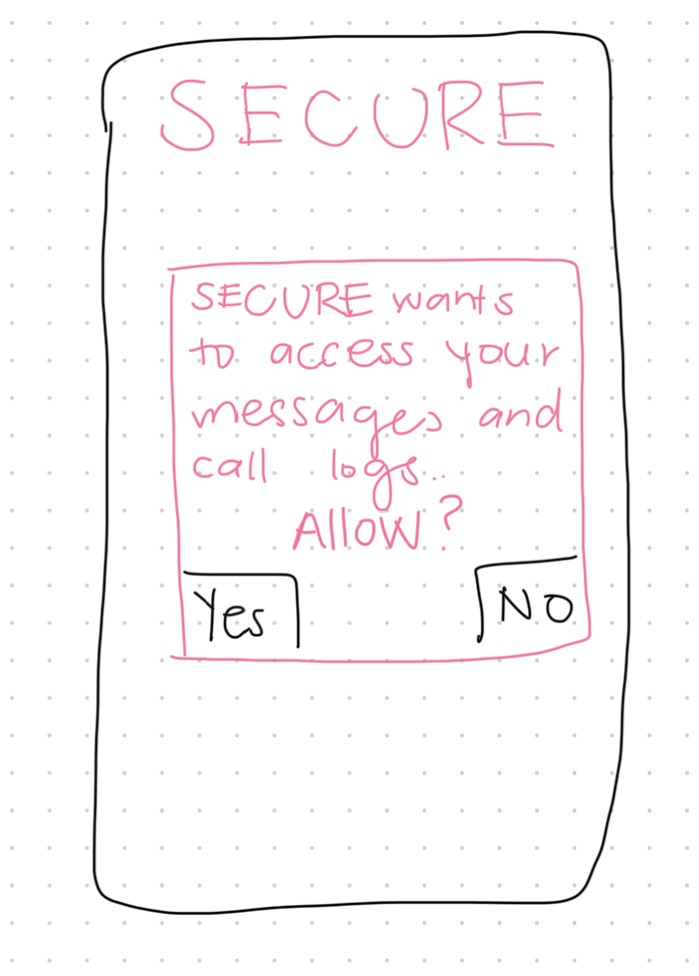


Figure. Sketch 1

* Once users download SECURE and set it up, they are asked to give the app permission to their messages and call logs so that the plug-in is added.

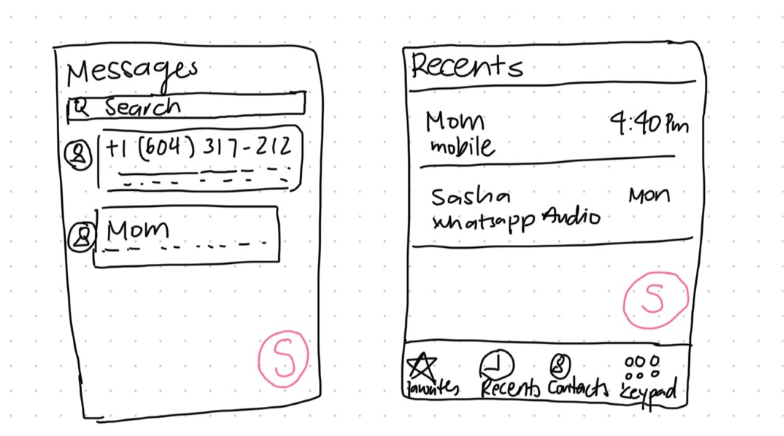


Figure. Sketch 2

* This sketch shows how the plug-in will appear and look after the user accepts SECURE’s permission.

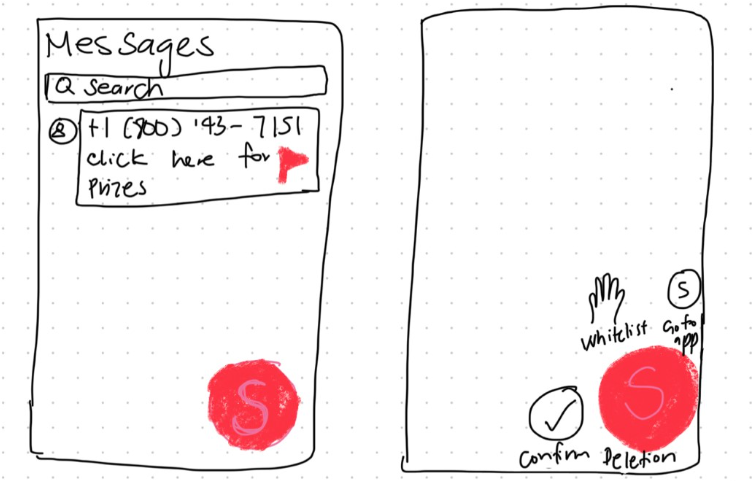


Figure. Sketch 3

* The key concept is that the plug-in will use blacklisted phone numbers in the app’s database and automatically detect scam numbers in real time. The plug-in will also scan texts to detect suspicious words/links and flag them before the user opens them. Users can still retain some control over the plug-in’s activity by confirming a malicious text deletion and number blocking or whitelisting it.

**Advantages**

1. Easy to use
2. Saves users time and hassle by automating scam detection process
3. The plug-in can be moved around the screen or hidden when not in use
4. Provides users with final decision despite automation

**Disadvantages**

1. Automation might require constant refreshing and use up a lot of the phone’s memory space.
2. Poses a privacy concern as to what extent can a user’s texts and phone calls be accessed.
3. Deletion and blocking of scam phone numbers requires user input.

**3. CONCEPT III**:Implementing real-time alerts with clear messages about detected scams or suspicious activities.

* This idea can show us if there is an anomaly in the transactions where detected scams or suspicious activities provide benefits that significantly improve the overall security and user experience of an online platform.
* This quick response capability makes users take immediate action, such as confirming or denying transactions, so it minimizes the risk of financial losses and leaking sensitive information.
* These alerts become a way to educate users about common scam tactics, increasing their awareness and ability to recognize scams in the future.

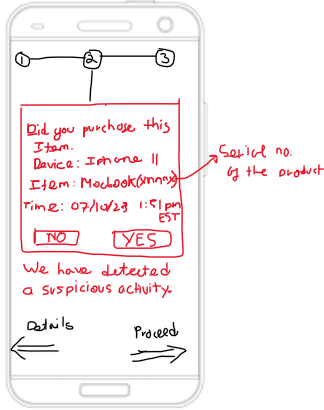
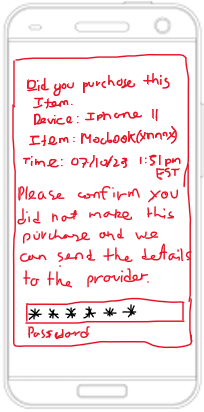


Figure. Sketch 1  Figure. Sketch 2

Sketch 1 shows the platform detecting suspicious activity in the purchases of the user and after the user becomes suspicious of the purchase, they can click yeas and type in the password that they used to register for this account as shown in Figure 2 and then the platform could send that information to the web provider where the transaction can be disputed.

**Advantages**

1. Users are immediately informed of potential scams or suspicious activities as they occur since they would know the device from what they purchased.
2. Users can take immediate steps to secure their accounts, preventing further unauthorized transactions by disputing it with their financial institutions.
3. Increases overall security by quickly identifying and addressing potential threats.

**Disadvantages**

1. Constant alerts may overwhelm users, especially if they lack an understanding of security practices.
2. Users may experience fatigue due to errors if they receive too many notifications.
3. Implementing timely alerts requires constant maintenance from the backend and may take up a lot of processing power of the system.

# 

# **CHAPTER 3:**

# **STORYBOARDS**

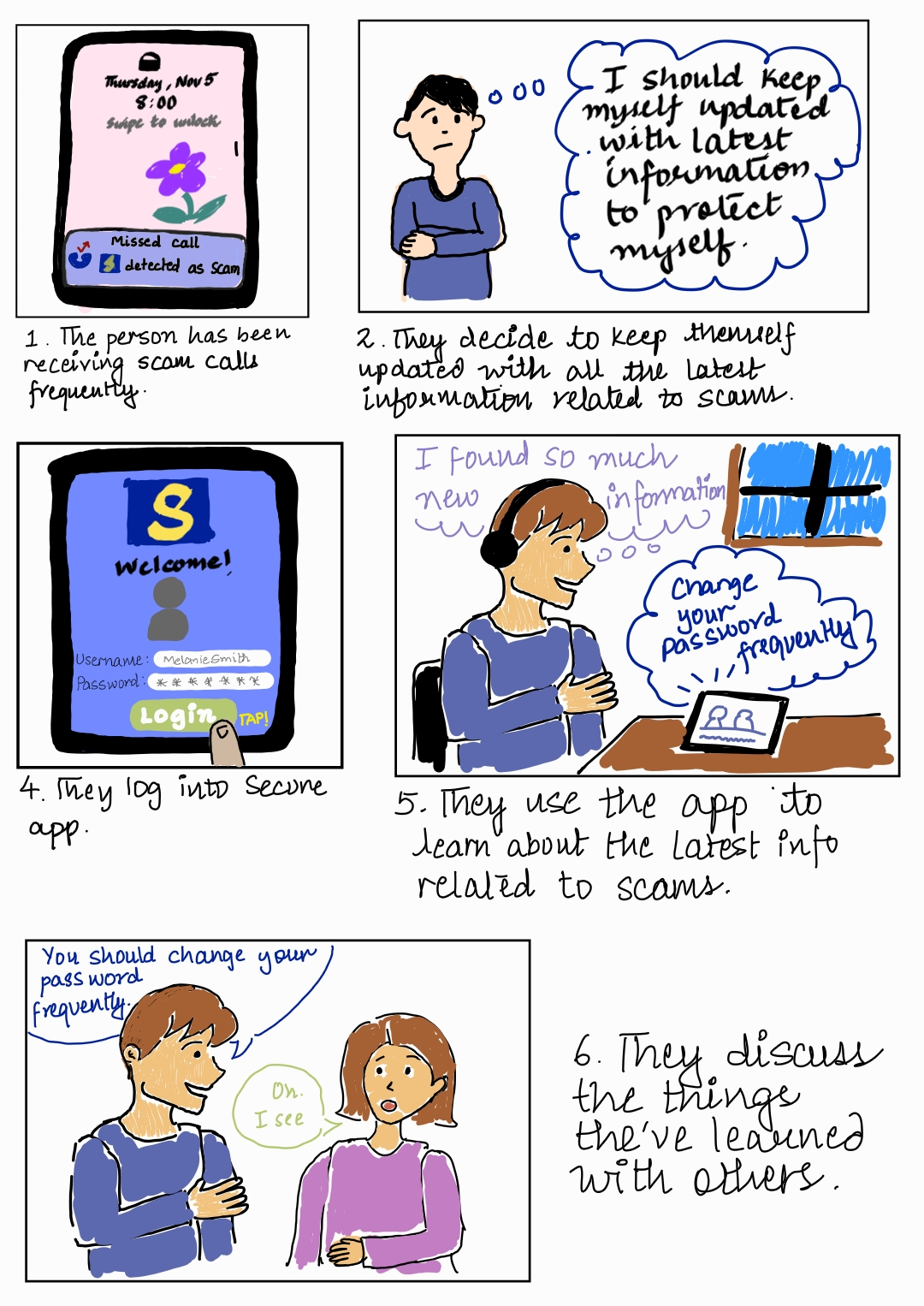
1. **STORYBOARD I (HIGH LEVEL)**

****

**MOTIVATION & PURPOSE:**

We want to help users avoid scam calls and warn them when a scammer tries to contact them. Scammers try to win the victim’s trust by acting familiar (for e.g. providing the victim with their details). In such cases, the victim might feel conflicted about the caller’s identity. The above storyboard describes how our solution would detect scam calls and warn the user. Automatically identifying fraudulent phone numbers makes it easier to avoid scam calls from the very beginning.

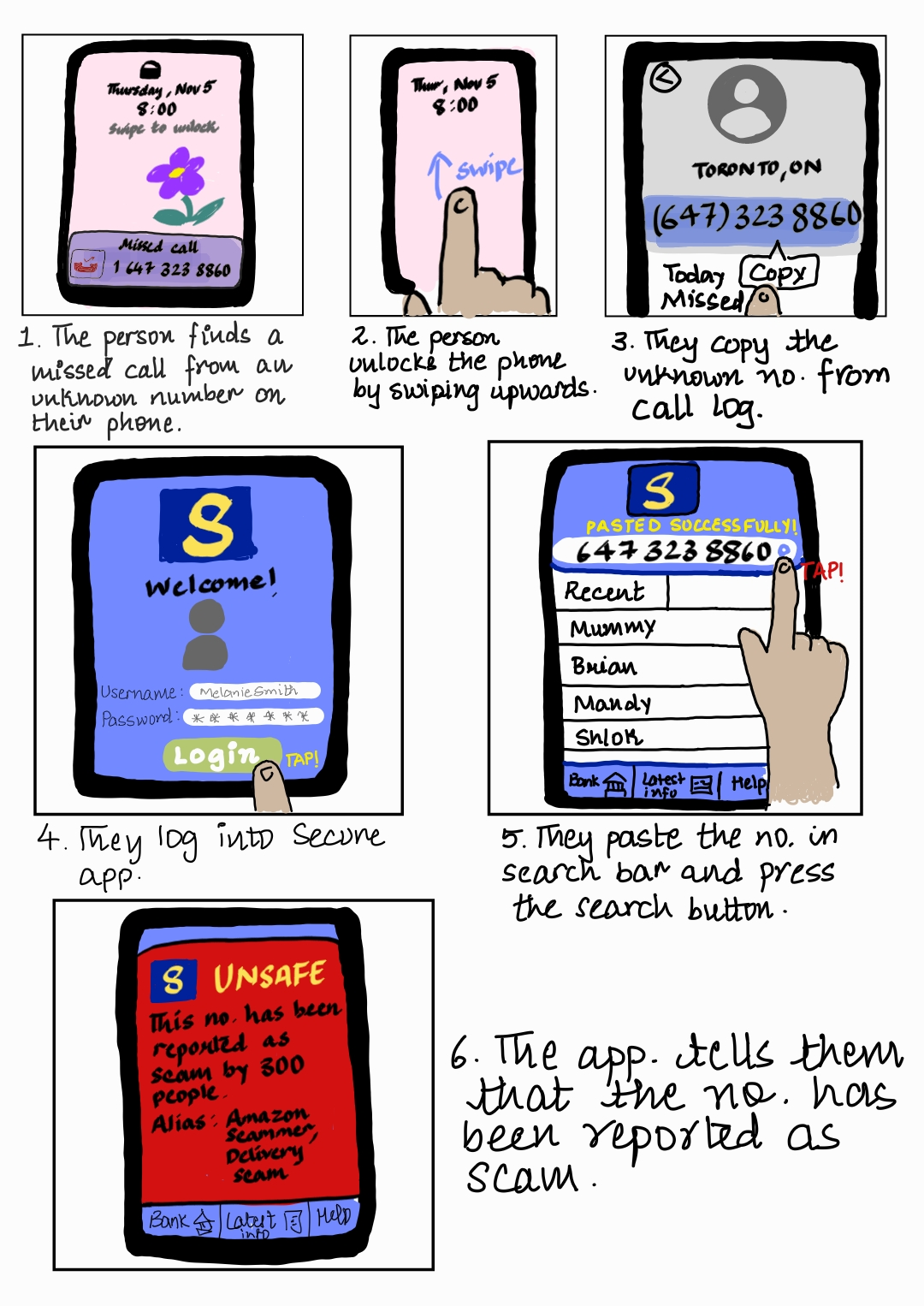
1. **STORYBOARD II (HIGH LEVEL)**

****

**MOTIVATION & PURPOSE:**

We want to make people aware of the latest information in the field of scams and security.It is easier to avoid scams if we are aware of how they occur and the techniques to protect ourselves. Many vulnerable populations such as the elderly and newcomers are the most prone to scams because such information is not easily available to them. The above storyboard describes how our solution can spread and increase awareness through different multimedia means (e.g., videos, and articles) among people.

1. **STORYBOARD III (SCREEN LEVEL)**

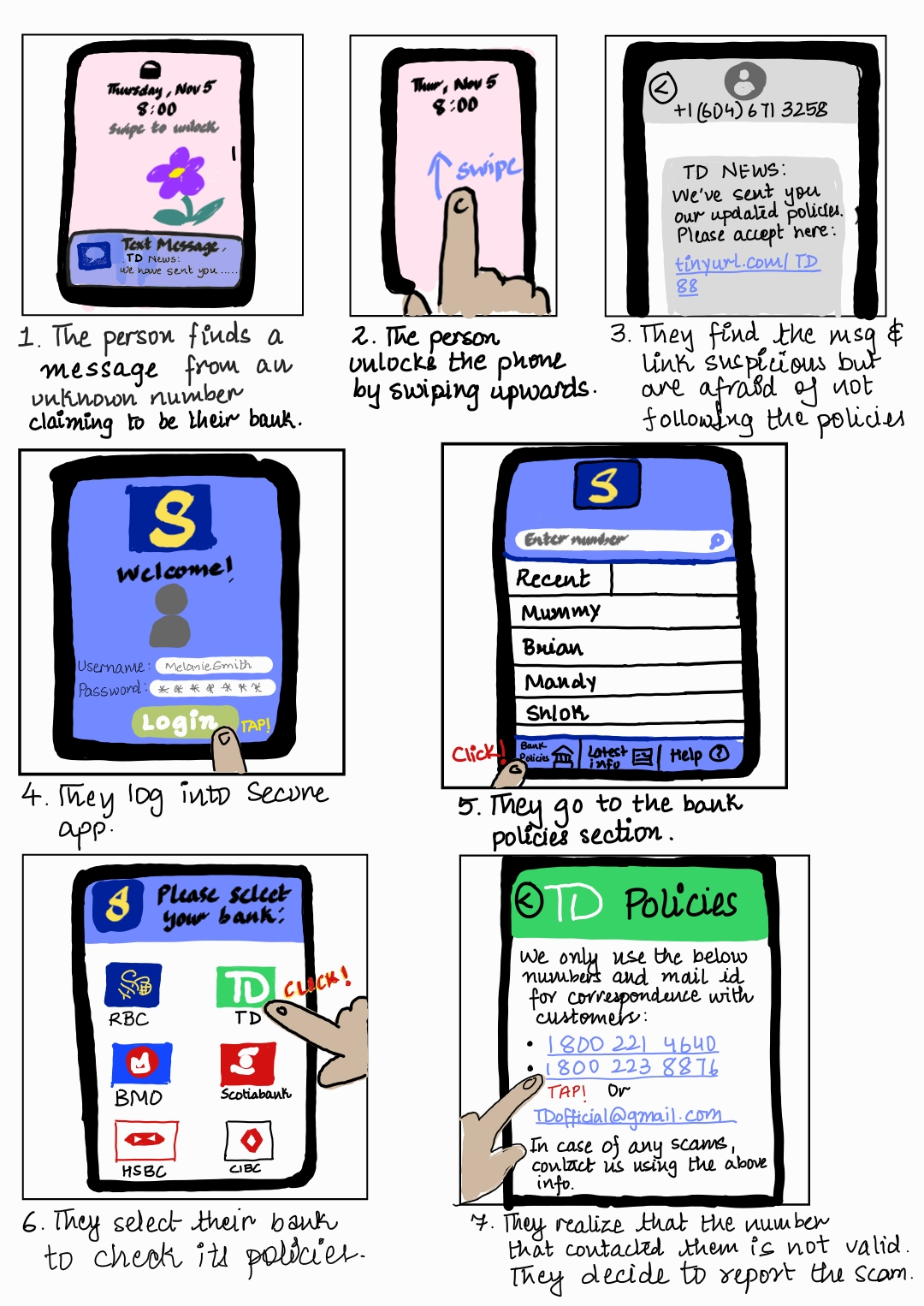
****

**MOTIVATION & PURPOSE:**

We want to help the user distinguish between legitimate and fraudulent phone numbers.

The above storyboard describes how our solution can provide the user with information about an unknown caller. Based on the information they receive, they can then make an informed decision whether to reply/ call back the caller or not. In case the caller is a scammer, the system will warn the user against continuing correspondence.

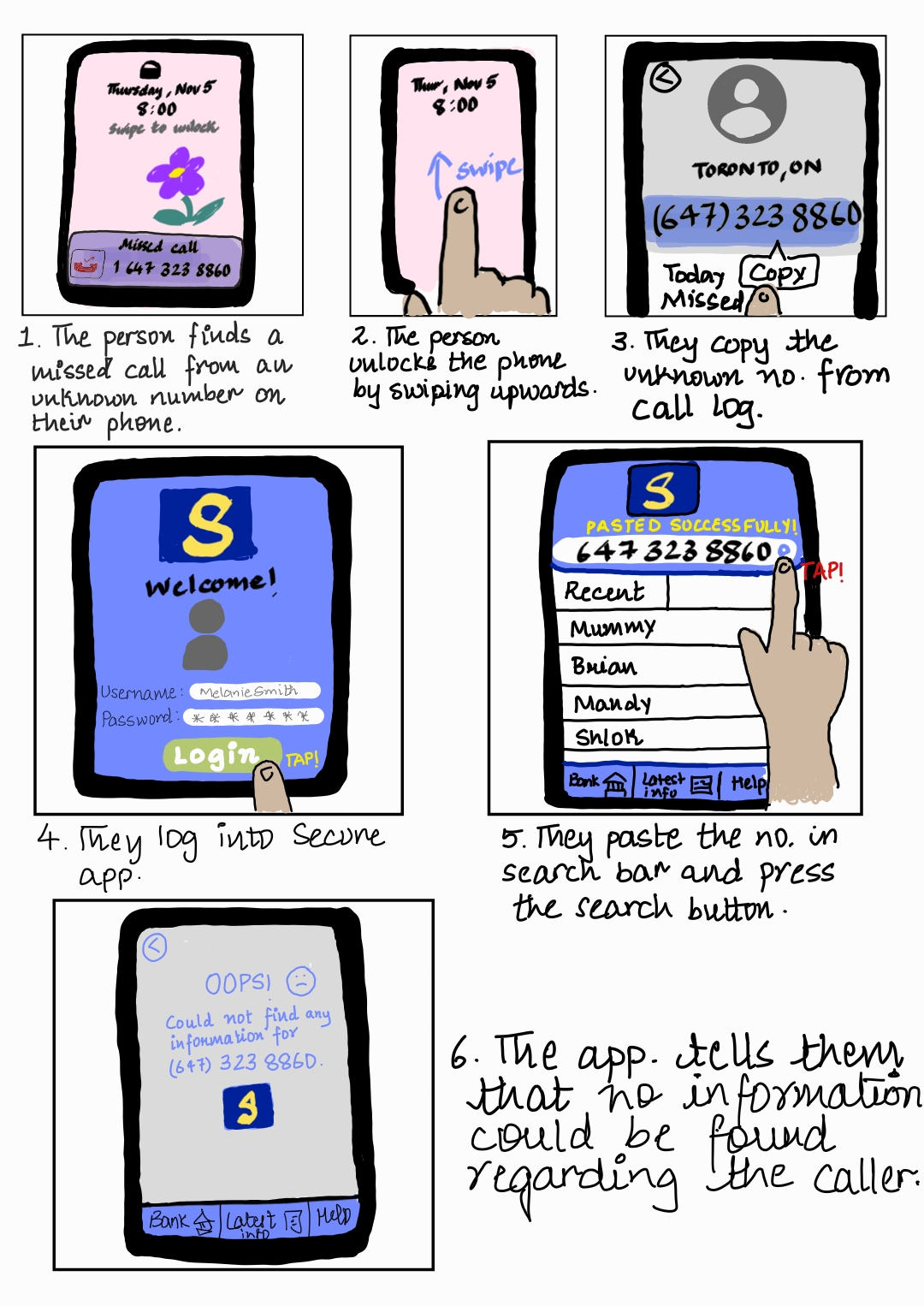
1. **STORYBOARD IV (SCREEN LEVEL)**

****

**MOTIVATION & PURPOSE:**

We want to help secure people’s privacy by keeping them up to date with the policies and help offered by their respective banks. Most people are unaware of their bank’s policies and safeguards available against scams. Victims are often unsure of the appropriate steps to recover their funds and information after the scam. The above storyboard describes how our solution can give users quick access to this information. It includes their bank’s contact information which will ensure that they can contact them and get help as quickly as possible.

1. **STORYBOARD V (SCREEN LEVEL)**

****

**MOTIVATION & PURPOSE:**

We want to help users avoid fraudulent calls. Scammers frequently change their numbers. If you block one, they try to contact you with a new one. The above storyboard describes an edge case for our solution where the caller’s number does not exist/ has not been reported before on our system. In such a case, our solution would inform the user that it could not find any information for the caller.

# **CHAPTER 4:**

# **LOW-FIDELITY PAPER PROTOTYPE**

Link: <https://drive.google.com/file/d/1-XZv7gPxGbifQSvLJkI4ypK6uOiGohQm/view?usp=sharing>

# **HOW IT WORKS:**

The paper prototype has 3 contexts of use - phone calls, messages and the app itself.

1. Phone calls:
   1. A fraudulent caller in the database:

When the user receives a phone call from a number, not in their contacts, and it has previously been reported by users and stored in Secure’s malicious contact database, Secure displays an easily noticeable pop-up alerting the user of the scam call, and how many users this number has been reported by. In case the user chooses to pick up the call, an additional pop-up comes up, asking the user if they really want to proceed. Thus, by clearly alerting the user of the scam contact, we’re able to prevent scams.

* 1. Fraudulent Caller not in the database:

In case the caller’s phone number isn’t stored in the database, the user is able to pick up the call as usual. This prompts the “record call” permission from Secure to pop up, asking for permission to record calls for the intent of intent detection. After the user accepts, they are able to answer the phone, with a status icon on the phone screen saying “Intent Detection - Active”, which can be used to turn off the intent detection feature when the user wants 100% privacy. Now, in case the caller asks for sensitive information, the LLM trained to perform intent detection shows a vibrant red pop-up and plays a sound to alert the user that the caller is trying to scam/phish them. Here, the user is able to choose whether to report the caller or not and end the call or continue talking with them. In case the user wants to continue talking with the person, they are also able to whitelist the caller on their phone.

1. Messages:

In case the user wants to check their messages and has conversations in their messages that contain malicious links or have been determined by the intent detection algorithm to be malicious, then the Secure app marks those conversations as Scam in vibrant red within the messaging app itself. In case the user tries to open the conversation, then they are shown a pop-up alerting the user that this is an unsafe conversation and the reason for it as determined by the large language model. They are only allowed to interact with the conversation if they accept the risk and press proceed. The messaging app remains the same for all other conversations.

1. Secure App:
   1. Contact Alias Search:

In case the user wants to search up a particular number from their caller history or wants to know what aliases other people on the Secure network have given to a contact, they may open up the Secure app. Then, if it’s their first time opening the app, then they will need to give permission for Secure to access their contacts. If no permission is provided, they will not be able to enter the app. On entering the app, they will be able to select a number from their recent call history to search aliases for or type in any number. In case the number they’ve typed in and searched is flagged as malicious, then they are alerted in vibrant red.

* 1. Awareness:

In case the user wants to gain awareness about scams and be better prepared to deal with scams, then they may open the app, and navigate to any of the three sections “Articles & News, Videos, and Podcasts”. The user may swipe left or right from one screen to another to access each of these 3 media types, and the user may see which screen they are in by the highlighted slider at the top of the screen. Once the user clicks any of the listings for video, podcast or news article, they are led to an external link where they may consume the media.

* 1. Support:

In case the user has some questions on how to use the app or any questions in general, they may open the app, and click on the support tab on the navigation pane at the bottom. Then, on the support page, they may click on any of the FAQs(Frequently asked questions) to resolve their concerns. Or, they may make use of the AI chatbot feature to more generally answer their questions relating to the app.

* 1. Bank Policies:

In case the user wants to know about the specific policies of their bank, they may open the app, click the bank policies tab on the navigation pane at the bottom. Then in the bank policies screen, they may choose their specific bank from all the choices. This leads to another page containing all the specific policies of the bank.

1. **DESIGN FEATURES**

| **NO.** | **DESIGN FEATURE** | **RATIONALE** |
| --- | --- | --- |
| 1. | Permission Pop-ups | This feature is added to inform the user that the app accesses their contact's records calls in order to optimally detect and prevent scams. |
| 2. | Ability to engage with the malicious agent after sufficient warning. | In case the user intends to engage with the identified malicious agent, then after sufficient warning, they are allowed to. This is in alignment with the user control and freedom heuristic. |
| 3. | FAQs + AI chatbot assistant | In case the user has any questions regarding how they should use the app, or any miscellaneous questions, they may rely on this. Aligns with the Help and documentation heuristic. |
| 4. | Slider indicating the media page that the user is currently in. Helps in navigating. | This displays the state of the system(which page the user is currently on) and helps with navigation. This aligns with the visibility of system status and flexibility and efficiency of use heuristic. |
| 5. | Navigation bar at bottom of the screen | This makes it really easy for the user to recognize icons and navigate through the app, letting them access a specific page in one click. Aligns with the flexibility and efficiency of use, and recognition rather than recall heuristic. |

1. **ADVANTAGES OF THE DESIGN**

The advantages of the design are:

1. It allows for complete user freedom - the user is able to choose permissions, even if they would like to engage with identifiably malicious agents.
2. The solution to call and message scams is completely passive, and the user doesn’t have to take any action to make Secure monitor their text and voice conversations.
3. **DISADVANTAGES OF THE DESIGN**

The disadvantages of the design are:

1. It requires invasive contact, message and call recording permissions, which would pose a privacy concern to users.
2. The LLM model for intent detection if not trained rigorously enough might produce false positives and negatives.

# **CHAPTER 5:**

# **EVALUATION OF LOW-FIDELITY PROTOTYPE**

## **METHOD I: THINK ALOUD EVALUATION**

**1.1 STUDY PROTOCOL**

Our research aims to uncover how individuals become victims of online scams, guiding the design of interactive media for online shoppers. The design problem revolves around users receiving scam inquiries, resulting in millions falling prey to online scams and substantial financial losses. Our goal is to find a solution and eradicate online scams.

Moreover, the participants that are chosen for the think-aloud evaluation are students who work in the finance industry who have been exposed to online scams or students who have experienced online scams. This is relevant as they will provide useful and relevant feedback for our study on finding a solution to online scams.

Furthermore, the participants are asked to evaluate our paper prototype by giving them a few specific tasks to test features from the app. These tasks include asking the user to test out the contact database feature where they have to search for a specific number and identify the number’s nicknames or reports if available. The users are also asked to test out awareness features such as news/articles, videos, podcasts, existing bank policies and app support which are intended to help users prevent scams or even provide some guidance in the event that the scam has already occurred. Lastly, users were asked to test our call and messages feature which is intended to detect scam/phishing attempts whether by call or text.

**1.2 KEY FINDINGS**

1. Description:

The app prototype received positive feedback from interview participants, where they indicated the prototype’s high level of interactivity and its practical utility in preventing online scams. Furthermore, the Contact Database feature gathers significant attention during discussions. This feature enables users to search any phone number and check if it has been reported for suspicious activities. Participants expressed enthusiasm and amazement for this capability, recognizing its potential to proactively detect and prevent scams before they occur.

Importance:

The Contact Database feature significantly enhances the app's importance by directly addressing a critical aspect of online security. By enabling users to assess the legitimacy of phone numbers and identify potential risks, the app empowers individuals to take preemptive measures against online scams. The positive responses from interview participants highlight the feature's significance, aligning with the growing concern about online security threats. This proactive approach not only boosts user confidence but also positions the app as a valuable tool in the ongoing battle against digital fraud. As online scams continue to evolve, the importance of such a feature becomes increasingly evident, emphasizing the app's contribution to fostering a safer online environment for users.

1. Description:

Interview participants expressed skepticism regarding the app's legitimacy, citing their lack of prior experience with similar applications. A common concern among participants was the hesitancy to share their contacts, driven by a lack of familiarity with the app.

Note: This description feedback is extended to all types of apps in general where users are not comfortable or familiar, this may not be a specific issue to our app

Importance:

The skepticism among participants highlights a crucial aspect that needs attention to enhance the app's importance. Addressing user apprehension about the app's legitimacy is important for building trust. Creating awareness about the app's uniqueness and security measures could alleviate concerns and encourage participants to share contacts confidently. By mitigating these apprehensions, the app has the potential to establish credibility and broaden its user base, emphasizing the importance of fostering trust and familiarity among potential users.

1. Description:

Three out of four participants encountered difficulty locating the button in the search feature after querying a specific number. Additionally, a user emphasized the absence of a crucial blocking feature, expressing the need for a mechanism to block numbers identified as associated with scams or phishing.

Importance:

The identified usability issues, such as the difficulty in locating the search feature button, highlights the importance of optimizing the app's user interface for enhanced user experience. Addressing this issue can lead to increased user satisfaction and engagement. Furthermore, the absence of a blocking feature, as highlighted by a participant, represents a valuable insight into enhancing the app's functionality for better scam prevention. Implementing a blocking feature aligns with user expectations and can significantly contribute to the app's effectiveness in providing a comprehensive solution to online security concerns. These improvements not only enhance user satisfaction but also reinforce the app's role in proactively combating scams and phishing attempts.

## **METHOD II: EXPERT EVALUATION**

**2.1 STUDY PROTOCOL**

The expert evaluation study aims to evaluate the low-fidelity paper prototype against a list of pre-determined heuristics to determine any weak points. The participants of the study are experts who have previous knowledge of the predetermined heuristics. They are instructed to complete tasks using the paper prototype under different contexts, where no help is provided to the expert, and they are instructed to complete the task as they would without the help of the facilitator, even if they get stuck. The members of the research team act as the facilitator, instructing the expert, the computer wizard, emulating the app, and the observer, observing and taking notes. The researchers also switched around their roles to get different perspectives in notes and being computer wizards and facilitators.

The contexts and associated tasks are:

1. You get a call from an unknown number - make sure to cater to any concerns of the caller, while at the same time avoiding providing sensitive information and getting scammed.
2. You want to gain awareness about scams and bank policies - navigate through the app and explore the different methods you gain awareness about scams and bank policies.
3. You want to read the messages in your inbox - make sure to read all emails while being able to identify whether a mail is a scam/phishing email or not.

**2.2 KEY FINDINGS**

1. Description:

All experts found that the homepage of the app was very cluttered, with all the features for searching phone numbers and consuming the different types of media to gain awareness on one page. This made it really hard for them to effectively navigate, find the required information and complete the context’s tasks. Some experts even got stuck at this point, not able to find the item they were looking for on the page.

Importance:

The ability of the users to navigate the app and satisfy their requirements with ease is important as it ensures that all users, regardless of technical ability and attention are able to gain awareness of and avoid getting scammed. Further, a minimalistic user interface is important to prevent user mental and eye fatigue in case the app is being used for a long period. The current design has different pages for each media type, support, and bank policies and is minimalistic, and thus resolves the issue.

1. Description:

All experts noticed that navigation within the app was absent/hard to perform because of a non-obvious/absence of back buttons or a universal navigation bar. This made them not be able to complete tasks by being stuck at a particular screen.

Importance:

Flexible and visible navigation makes the app easy to use, and allows the user to quickly and easily move to the required pages within the app, and more importantly, be able to finish tasks within the app. The current design implements back buttons and the navigation pane, which is always present on every screen of the app, to provide these advantages.

1. Description:

Some of the experts aren’t able to immediately determine what the icons on the homepage of the app for the banks mean as the experts aren’t able to recognize the bank icons in the task where the users want to learn about bank policies. This leads to the users not being able to complete the task.

Importance:

The ability to be able to recognize icons within the app, rather than having to recall them from memory is important because it reduces the mental load during the usage of the app, and is essential for the usability of the app as a large portion of users are able to complete tasks faster. The current design implements this by not only making the bank icons larger but also labelling them.

# 

# 

# 

# 

# 

# 

# **CHAPTER 6:**

# **TAKEAWAYS AND IMPLICATIONS FOR DESIGN**

1. **TAKEAWAYS**
2. The Contact Database feature received very positive feedback from the evaluation participants as it allows them to detect scam/phishing numbers very easily. Unfortunately, a big weakness of this feature is the lack of a blocking feature where users could easily block a number if they deem it necessary.
3. Skepticism on the legitimacy of the app is very high as users have not encountered a similar app in the past where they have to give up their phone contact information. This provides a problem for us as we have to find a way to ensure our users of the security of the app and the purpose of collecting these sensitive data.
4. App features such as the latest information updates, bank policies, and app support also receive positive feedback which helps users to be aware of evolving scams and also provides some guidance in the event that the scam already occurs. However, there are some weaknesses in some specific features such as bank policies where the app only provides the policies for major banks in Canada. Another weakness is the missing feature to report a number after encountering scam/phishing attempts.
5. **MODIFICATION IN THE DESIGN**
6. We have a feature which allows users to search for the policies and contact information of their financial institutions. Currently, our design has only six banks and users don't have an option to search for banks outside the given option.

We will be adding more financial institution's information to our solution. Listing them out and having the users scroll through all of them will be tedious. This will require us to provide users with a search option for bank names.

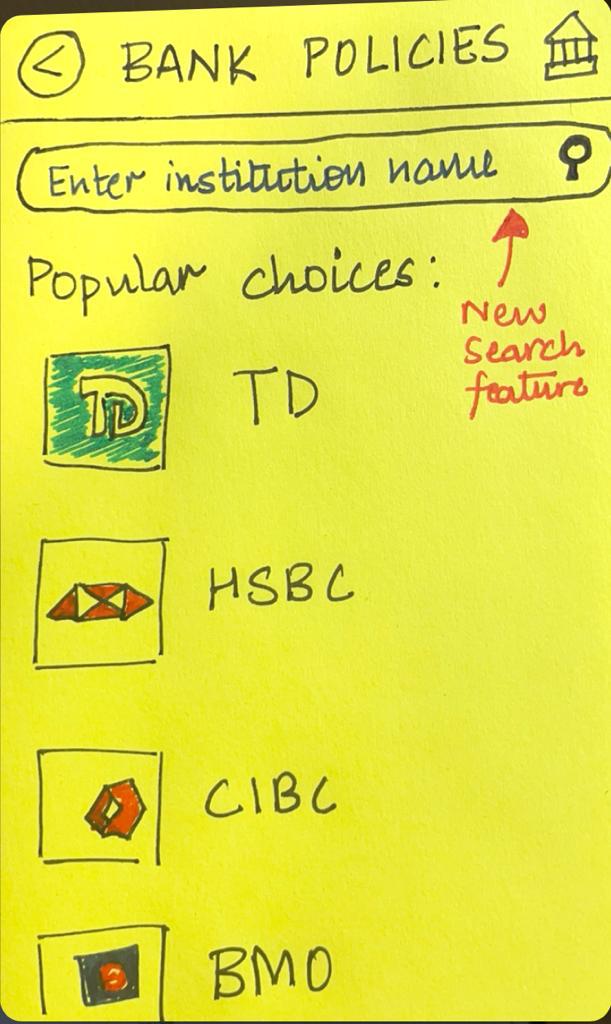


Figure. Envisioned changes for bank policies feature

1. Users do not have the option to voluntarily report a scammer’s information to the database. We intend to implement a feature using which they can report the number and provide some description of the scammer as well, which would further enable scammer contact tracking and scam avoidance.
2. One major issue with the current app is that users do trust the app by using user contact and call recording data properly. To address this, before the user is prompted for permission to access contacts and record call audio, a screen may be displayed assuring the user that the data that we collect is purely local(depending on the implementation of the LLM)/ transmitted and stored with industry-standard encryption, and will only be used for the purpose of assisting the user with scam avoidance.
3. Some users in the think-aloud study didn’t access the full list of aliases as they were unable to identify that the number that pops up on search is clickable and leads to a page containing all aliases. The addition of a button indicating “view all aliases” would resolve this issue.
4. Currently, the Secure app only allows the user to report the malicious contact to the Secure database to be marked as unsafe, but doesn’t integrate blocking the contact number from calling/texting the user. The addition of this feature would make it quicker for the user to block unsafe numbers.

# **APPENDICES**

1. **IDEATION PROCESS**

* CONCEPT I

**Notes (Gather info):**

1. Need tiny UI features that add up to the overall experience
   1. Back buttons
   2. Enter
   3. Submit
   4. Other buttons that we use that we have taken for granted
   5. Improves usability
2. Less Cluttered pages
3. Seamless Flow of one UI to the next

Context one:

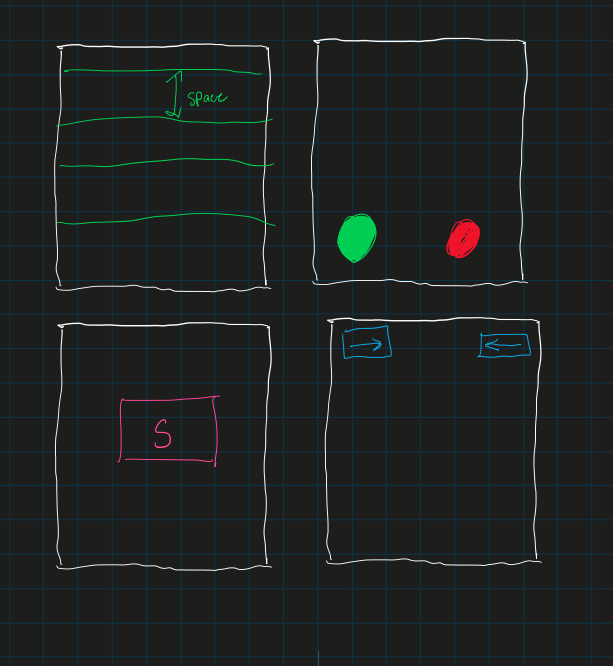
* 1. Idea is to get people more informed about current scams
  2. Want this attribute to be quite accessible and not hard to find
  3. We want to promote this feature even though it is not a core feature
  4. Have this option available ie) don't make this a special branch

Context two:

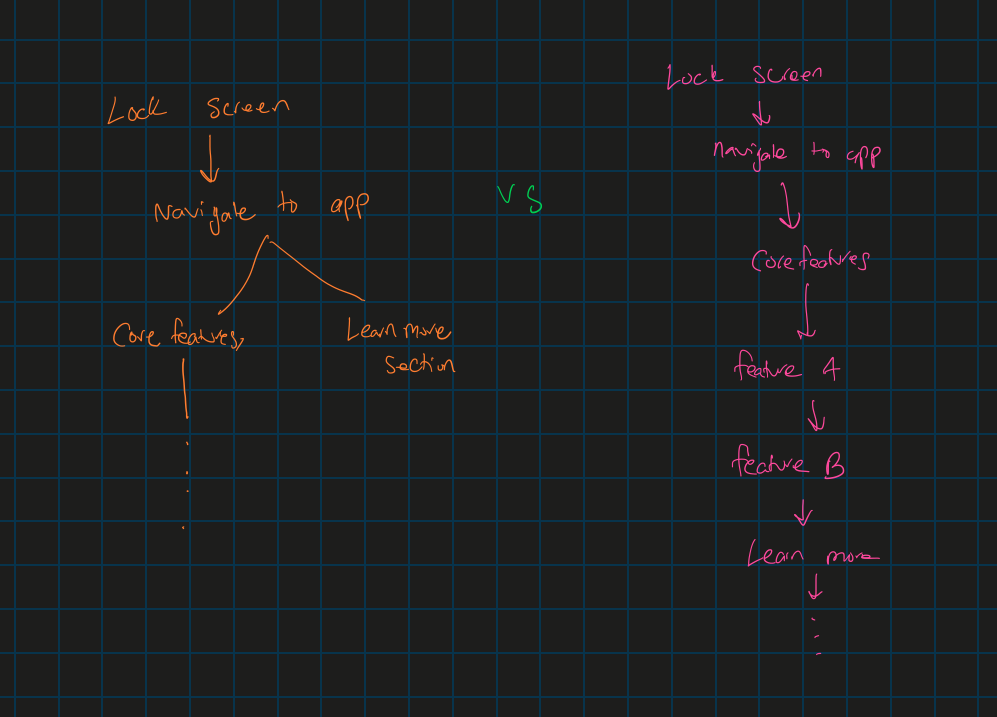
* 1. We want people to determine if a point of contact is safe
  2. Note that a lot of things are happening in the backend but we need to tell the user what's going on at all times
  3. Notify backend processes to the UI for users to see and understand

Automation of scam detection for text messages and phone calls

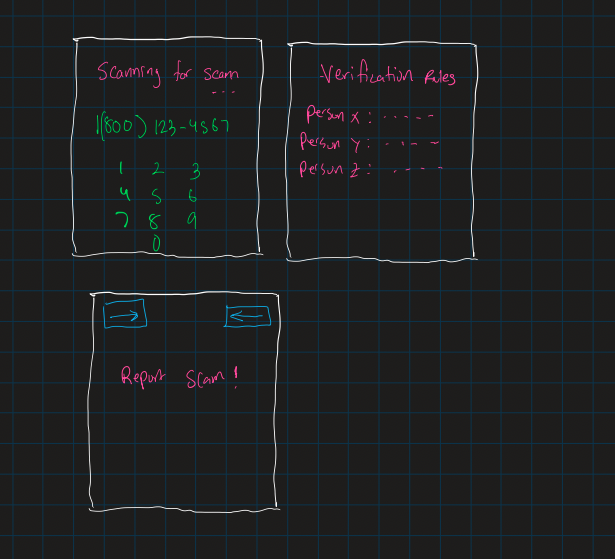
* 1. Includes temporary hiding of scam text/calls and permanent blocking of scam phone numbers.



Context 1 idea branching: We want the option available right away

****

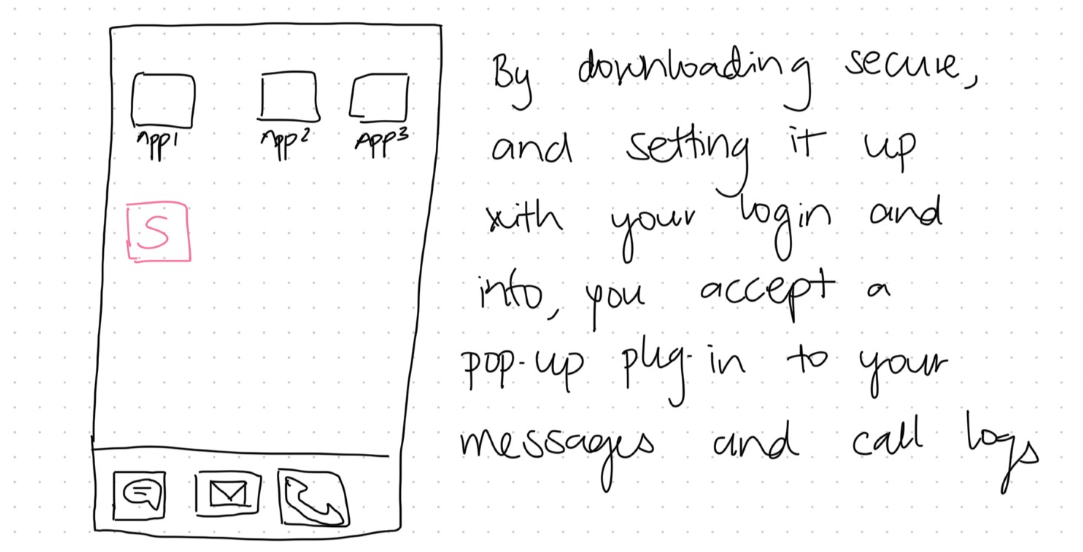
Context 2:

****

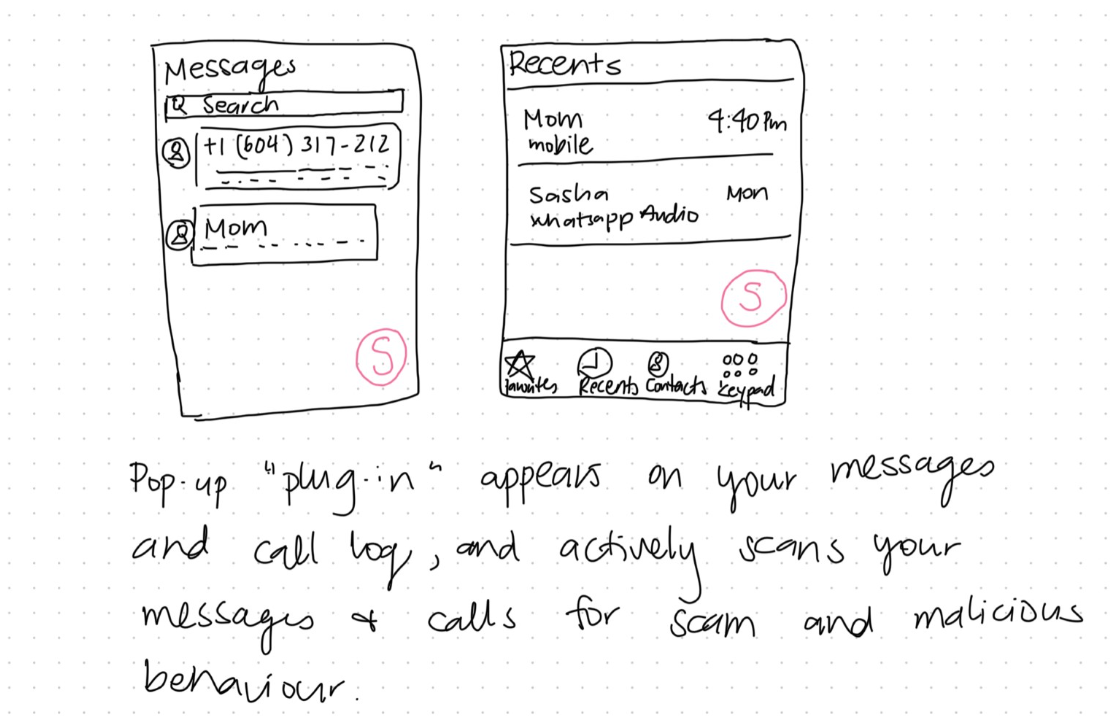
Scanning methods show what happening and indicate that the user may have to execute certain tasks following

CONCEPT II

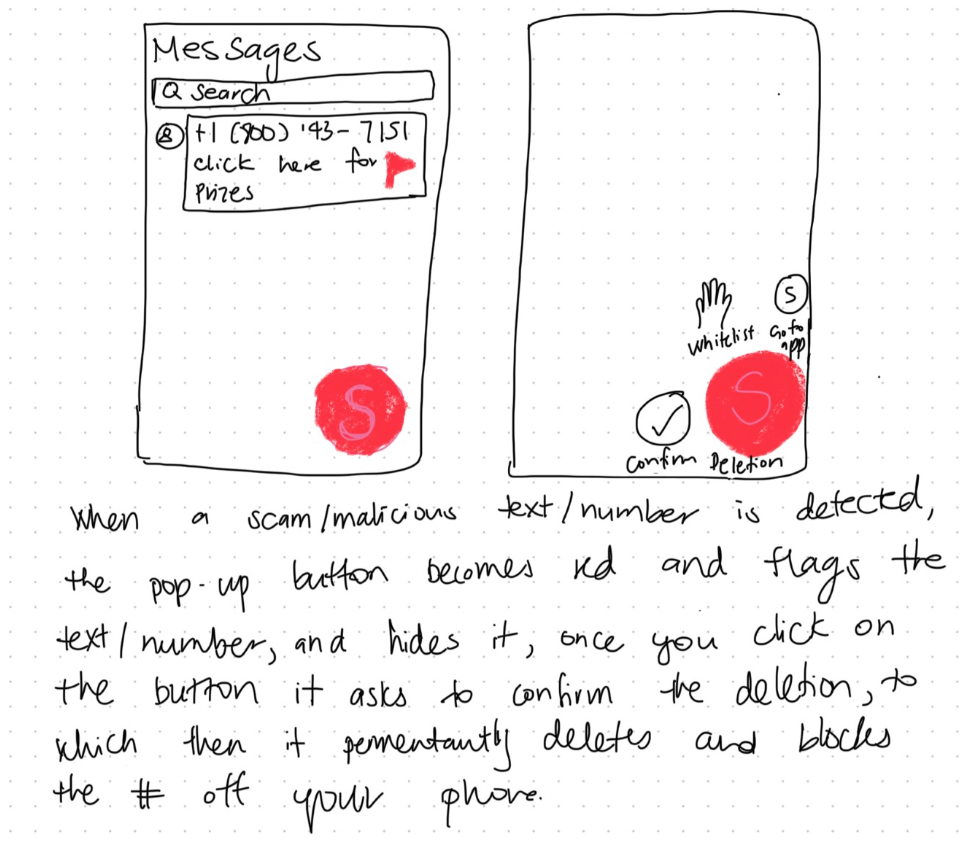
Concept 2: Automation of Scam Detection



1. Users have to accept Secure’s access to their messages and call logs before they can use the feature, this ensures user’s privacy is respected.



1. This is what it looks like after the plug-in is added to messages and call logs.

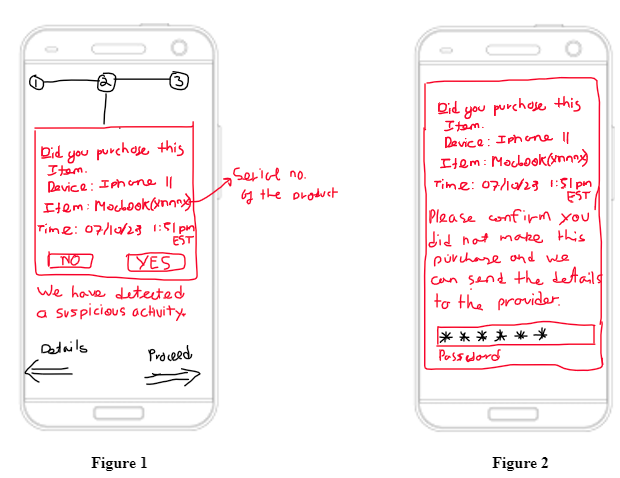


1. Plug-in flags message with a red flag and turn red to indicate real-time scam detection.
2. Gives users the option to confirm deletion to give users control over their messages.

* CONCEPT III

Implementing real-time alerts with clear messages about detected scams or suspicious activities.

* The idea of implementing alerts with clear messages about detected scams or suspicious activities is rooted in the goal of improving online security and user protection. The brainstorming behind this concept involves many factors.



* Users would be aware that systems need to be adaptable and they must be aware timely about any potentially fraudulent activities on their accounts.
* Users must have a platform that allows them to be proactive about combating scams or unwanted transactions from their account, so they can be responsible themselves for monitoring their account as well as the institution they are purchasing from.

1. **THINK ALOUD EVALUATION**

* STUDY PROTOCOL
* Project Title: Securing Privacy and Preventing Scams during Online Purchases
* Investigators: Team Vulcan
* Purpose: The purpose of our research is to understand how individuals fall victim to online scams to help us derive requirements for the design of novel interactive computational media that are intended to be useful to online shoppers. A brief description of our design problem is: Many users are sent scam or fraud inquiries through online sources. Millions fall victim to these online scams and millions of dollars are stolen. We want to find a solution and end online scams.
* Process to be followed: We will brief the participants about the purpose of the study, explain the consent form to them, and ensure that they sign the consent form. We will then engage the participants in a 20-minute (maximum) evaluation session. We will also, with their permission, make observations as follows: The insight provided from the interview will be used to make observations for the development of the app and enhance user-friendliness.
* Participant selection: Participants will be chosen from their experience with dealing with fraud cases. They will be identified via personal network connections and selected according to their years of experience dealing with these types of problems. In general, they will be characterized by their occupation and work experience in any fraud department.
* Relationships: The participants recruited for our study consist of family members, friends and professional connections.
* Risk and benefit: There will be minimal risk to the participants, for example, that they feel that they have wasted their time. The only benefit will be to contribute to the education of the investigators. Participants are free to withdraw before or at any time during the study without the need to give any explanation. The method of interviewing is a low-pressure knowledge transfer in pursuit of a solution to a global problem.
* Consent details: We will brief the participants about the purpose of the study, explain the attached consent form to them, and ensure that they consent to participate and sign the consent form (see section II of Appendices).
* Compensation: Participants will receive no compensation.
* Confidentiality: Information will be kept confidential by the investigators. Names or other identifying or identified information will not be kept with the data. The only other use will be to include excerpts or copies in the assignment submitted, but names and other identifying or identified information will not be submitted.
* INSTRUMENTS

Context 1:

Imagine that you are a young adult aged 18-26, you want to use the SECURE app to see if any of your recent calls/contacts are unsafe. You will start on the lock screen of your phone.

Task 1:

First, navigate through your phone and open the SECURE app. Note that you have to give the app permission to access your contacts, in order to use the app. We already gave you a set username and password to try out the app. Now, I would like you to identify which of your recent call contacts is unsafe and why. Second, I would like you to use the search feature and search 647 231 4166 then tell me what other nicknames Miriam is listed as.

Context 2:

Imagine that your friend who is similar to your age got scammed recently and you want to keep up with the latest updates on scams or ways to prevent scams.

Task 2:

Now, I would like you to show me how you would make use of the application and list what features you can use to raise your awareness of online scams. Feel free to explore the app's interface as you see fit.

Context 3:

Imagine that you are getting a call from an unknown number. You pick up the call and the caller says that they are an official at RBC (you have an account at RBC). They identify you by your name and your profession. You are confused as to whether it is a scam or not and want to verify your identity.

Task 3:

Now I would like you to show me how you would go about verifying the caller’s claim. Feel free to explore the interface as you see fit.

Context 4:

Imagine that you are someone who uses text messages quite often. You’re trying to check your inbox at the start of your workday, and want to address every email and message. You checked a few emails and felt suspicious of the messages. You want to read all emails but don’t want to click on malicious links or share sensitive data.

Task 4:

Now, I would like you to read all new emails and messages in your inbox while ensuring that you are able to avoid being scammed/phished, and identify which of the emails is malicious.

1. **CONSENT FORMS**

**Consent Form: Securing Privacy and Preventing Scams during Online Purchases**

I hereby consent to participate in a research study conducted by Team Vulcan for an assignment in the University of Toronto Computer Science 318, Design of Interactive Computational Media.

I agree to participate in this study, the purpose of which is to evaluate the paper prototype for their solution for preventing online scams and securing online privacy for their stakeholders.

I understand that

* The procedures to be used are think-aloud evaluations. We will give a brief explanation of the goal of the research and the tasks that need to be done. The participants will be asked to express their opinions and feelings about the usefulness and usability of the paper prototype. The whole session will be recorded.
* I will receive no compensation for my participation.
* I am free to withdraw before or at any time during the study without the need to give any explanation.
* All materials and results will be kept confidential, and, in particular, my name and any identifying information will not be associated with the data.

**PARTICIPANT**

**Name (please print)**

**Signature**

**Date**

**INVESTIGATOR(s)**

**Name Signature**

1. **VIDEO RECORDINGS FOR THINK ALOUD SESSIONS**

**Evaluation 1:** <https://drive.google.com/file/d/1-aZanuBHaZNSOs9mEDD8sEdvtvAZsozt/view?usp=drive_link>

**Evaluation 2:**

<https://drive.google.com/file/d/124zZf4DZcQOBf9gdWQ-9swJBJLgw4s13/view?usp=drive_link>

**Evaluation 3:**

<https://drive.google.com/file/d/10OsFhBrL7jLksddf4SuLNQjM2tn6iezW/view?usp=drive_link>

**Evaluation 4:**

<https://drive.google.com/file/d/10MR30Ich3UKPjjWpslHMrZkxipL8S77S/view?usp=drive_link>

1. **EXPERT EVALUATION MATERIALS**

**Script**

Context 1:

Imagine that you are getting a call from an unknown number. You pick up the call and the caller says that they are an official at RBC (you have an account at RBC). They identify you by your name and your profession. You are confused as to whether it is a scam or not and want to verify your identity.

Task 1:

Now I would like you to show me how you would go about verifying the caller’s claim. Feel free to explore the interface as you see fit.

Context 2:

Imagine that you are someone who uses text messages quite often. You’re trying to check your inbox at the start of your workday, and want to address every email and message. You checked a few emails and felt suspicious of the messages. You want to read all emails but don’t want to click on malicious links or share sensitive data.

Task 2:

Now, I would like you to read all new emails and messages in your inbox while ensuring that you are able to avoid being scammed/phished, and identify which of the emails is malicious.

Context 3:

Imagine that your friend who is similar to your age got scammed recently and you want to keep up with the latest updates on scams or ways to prevent scams.

Task 3:

Now, I would like you to show me how you would make use of the application and list what features you can use to raise your awareness of online scams. Feel free to explore the app's interface as you see fit.

**List of heuristics for the expert’s usage**

1. Visibility of system status

2. Match between system and real world

3. Aesthetic and minimalist design

4. User control and freedom

5. Consistency and standards

6. Error prevention

7. Recognition rather than recall

8. Flexibility and efficiency of use

9. Recognition, diagnosis and recovery from error

10. Help and documentation

**Severity Rating Scale**

0 = Not a usability problem

1 = Cosmetic problem (fix if extra time)

2 = Minor usability problem (low priority to fix)

3 = Major usability problem (high priority to fix)

4 = Usability catastrophe (must be fixed before release)

1. **EXPERT EVALUATION FOR OUR PROJECT**

*Rating*

*0: not helpful; 1: helpful; 2: very helpful*

| **Round No.** | **Name of the Expert** | **Name of the Expert’s Team** | **Rating** |
| --- | --- | --- | --- |
| 1 | Kevin | 404 NOT FOUND | 1 |
| 2 | Eric | 404 NOT FOUND | 1 |
| 3 | Dario | Project Team 12 | 2 |
| 4 | Oliver | Team UXperts | 2 |
| 5 | York | Design Disruptors | 1 |
| 6 | Farzana | STACKOVERFLOWERS | 2 |

1. **EXPERT EVALUATION BY OUR TEAM**

*Rating*

*0: not prepared, 1: well prepared, 2: very well prepared*

| **Round No.** | **Name of Team Member** | **Served as Expert for Team** | **Rating** |
| --- | --- | --- | --- |
| 1 | Asma Mohammed | ThankQueue | 2 |
| 2 | Madhav Kanna Thenappan | Gr8 Warriors | 2 |
| 3 | Mugdha Banthwan | Team UXperts | 2 |
| 4 | Sahil Handa | ByteBrilliance | 2 |
| 5 | Stephen Lim | Team UXperts | 2 |
| 6 | Aayush Bhan | *Absent due to sickness* | *-* |

1. **DOCUMENTATION OF DATA ANALYSIS PROCESS**

* The data we collected from our Low-Fidelity Paper Prototype Evaluation was primarily qualitative in nature.
* The data was collected in the form of notes. Our observers jotted them down in separate Google documents for each interview (think-aloud eval) and evaluation round (expert eval).
* After we completed our expert evaluation, we separated the data into two problem categories: Interface/UI and Functional/Features.
* We made changes to our paper prototype based on the expert feedback. We then used the newer version for think-aloud evaluation.
* We used our think-aloud evaluation to ensure that our design was user-friendly.
* We compared the feedback from both kinds of evaluation. We leaned more towards the users’ feedback regarding Interface/UI issues and experts’ feedback for Functional/Feature issues when thinking about modifications to our design.

1. **GROUP MEETING NOTES**

MEETING NOTES

2 November 2023

* Create changes to paper prototype - Madhav and Mugdha
* Set up structure of A2 report - Aayush Bhan
* 3 Design concepts?
* 2 persons for per concept
* Grp 1 - Aayush & Madhav
* Grp 2 - Asma & Stephen
* Grp 3 - Sahil & Mugdha
* Find people for think-aloud eval
* Next meeting: 5 November 2023

MEETING NOTES

5 November 2023

* Done with design concepts
* Done with Paper Prototype
* Begin with interviews
* Stephen found some willing people
* Madhav will be doing chapter 4 (explaining paper prototype)
* Mugdha will be doing storyboards
* Design Concepts writing in the report
* Concept 1 Sahil
* Concept 2 Asma
* Concept 3 Aayush
* Next meeting: 10 November 2023

MEETING NOTES

10 November 2023

* Done with think aloud
* Done with storyboards
* Chapter 5 evaluation of prototype content in report
* Think aloud - stephen
* Expert - madhav
* Rest people work on chapter 6 takeaways and implications
* Next meeting : 11 November 2023

MEETING NOTES

11 November 2023

* Done with chapter 6
* Mugdha and Asma refine report structure
* Aayush and sahil check for grammar
* Madhav n stephen check the appendix
* Next meeting : 12 November 2023

MEETING NOTES

12 November 2023

* Checked everything and seems fine
* Done with the report :)