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

**High-Fidelity Prototype**

**and**

**Usability Testing Report**

**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

December 2023

**TABLE OF CONTENTS**

1. Chapter 1: Introduction 3
2. Chapter 2: High-Fidelity Prototype 4

1. Installing And Launching The Prototype

2. Addressing The Issues Raised In A2

3. Prototype Satisfaction: A1 Job Stories

4. Prototype Satisfaction: A1 Functional Requirements

5. Insights from Pilot Studies and Improvements to Instructions,

Protocol and High-Fidelity Prototype

1. Chapter 3: Evaluation Protocol 11

1. Participant Demographics

2. Data Collection Methods

3. Contexts and Tasks

1. Chapter 4: Study Results 17

1. Key Findings: Successful Aspects

2. Key Findings: Areas for Improvement

1. Chapter 5: Takeaways and Implications for Design 20

1. Takeaways

2. Modifications to the Design

1. Chapter 6: Reflection 23
2. Appendices 25

# **CHAPTER 1:**

# **INTRODUCTION**

Recently, there has been a sharp increase in scams and fraudulent texts and calls targeting people. Scams take place in the form of phishing links, impersonation calls, etc. but are not limited to that. Unfortunately, scammers are usually after money and/or personal information. This usually results in financial losses and data leaks.

***We aim to find ways to prevent and reduce scam calls and texts and their effects on our stakeholders. We also want to find ways to guarantee users' privacy and protection.***

Our stakeholders are:

1. Primary Stakeholders: people who own a phone and are in the working age group (16-60 years)
2. Secondary Stakeholders: financial institutions as our secondary stakeholders.



**Figure 1.** Common online scam prevention techniques.

# **CHAPTER 2:**

# **HIGH-FIDELITY PROTOTYPE**

# 

# **INSTALLING AND LAUNCHING THE PROTOTYPE**

* The prototype is created using **Figma**, found at <https://www.figma.com/file/5yyljWoiKTPNazfR831QcX/Secure-App-High-Fidelity-Prototype?type=design&node-id=0%3A1&mode=design&t=Hge8Wf1iMake9ZDn-1>
* It can be directly launched using the **Figma app** or in the **browser**.

# **ADDRESSING THE ISSUES RAISED IN A2**

* Issue 1: Lack of trust in the App with personal data:

Solution: Addition of a page informing the user why their text, voice call, and contact data and permissions are required, guaranteeing that industry-standard data privacy and protection practices are being followed, as well as ensuring them that all data that is collected and stored, except for contact info, is stored and processed locally.

* Issue 2: Inability to block a contact that has been reported as unsafe from the app.

Solution: Added a block button within the contact search page in the app for unsafe contacts to increase the efficiency of task completion during use.

* Issue 3: Users do not have the option to voluntarily report a scammer’s information to the database.

Solution: Include a button that links directly to the user’s financial institution to report fraud or view policies regarding fraud and scams. Only contacts that have been detected to be malicious by the LLM should be added to the scam contact database to prevent false reporting by users. Users can report this contact when the LLM has flagged a contact as malicious during a text or call.

* Issue 4: Users are unable to find their banks in the list of banks listed on the bank policy page.

Solution: Added all major banks functioning in Canada to the bank policy page of the prototype, and added a search feature in the high-fidelity prototype to help users find their banks.

* Issue 5: Users are unaware that they can check the safety and nicknames of a contact in their call history by clicking on the contact card.

Solution: Added a “right arrow” icon in the card to symbolize that it will lead to a new page when clicking on it. All users were successfully able to click this card and check the safety of the contact.

1. **PROTOTYPE SATISFACTION: A1 JOB STORIES**

* Job Story 1: When I receive a call/message from an unknown number, I want to be able to identify the caller/sender, so I can avoid impostors.

Explanation: The prototype includes a feature that hosts the number in a database as well as an LLM that fact-checks the caller. In this method, as the database grows, users will be able to fact-check the call/message

* Job Story 2: When a scam occurs in/around my region, I want to be updated with the relevant information, so I can protect myself from similar attempts.

Explanation: The prototype requests the user's location and caters to scam info accordingly. The user can access the Awareness feature on the Secure app and receive updates. Furthermore, the user has more resources to use to increase protection.

* Job Story 3: When I experience a bank details scam, I want to contact my bank easily and swiftly, so I can protect my account details and finances.

Explanation: The user can access the Bank Details feature which allows the user to choose their bank and provides them with contact details (phone no. & email ID). There is also some general information about how a bank contacts its customers.

* Job Story 4: When I am curious or want to learn more about privacy/scam-related matters, I want to be able to ask questions and ease my concerns, so that I can make informed decisions.

Explanation: There are many resources available to answer questions. Accessing customer support through the Chatbot and finding relevant links to each bank is a method. Furthermore, the scam info page may have common questions answered.

* Job Story 5: When I experience a scam attempt, I want to be able to report the caller/messenger, so that others and I can avoid the same person in the future.

Explanation: The app has a built-in notification that prompts the user to report the number. For messaging, the app flags dangerous senders and prompts the user to report the sender.

# **PROTOTYPE SATISFACTION: A1 FUNCTIONAL REQUIREMENTS**

* Functional Requirement 1: Identify secure and legitimate contacts and flag those that are fraudulent.

Explanation:

* 1. Contact Search feature in the app helps the user search for any contact by number or just from the call history and learn about the different names that the contact goes by, and whether the contact is unsafe.
  2. Unsafe text conversations flagged within the app based on detection from Secure’s prior conversation screening.
  3. When receiving a call from a number that has been reported as unsafe, the user is alerted before picking up the call.
  4. When an unsafe voice conversation is identified through real-time detection, the user is alerted through a loud tone that the caller is unsafe.
* Functional Requirement 2: Keep people updated with the latest information about e-commerce policies and any widespread scams that they should look out for.

Explanation:

1. Satisfied by the **‘Awareness’ page**, containing curated **videos** and **articles** about e-commerce and bank policies, and **scams prevalent in the user’s location**, based on the users’ demographic.

* Functional Requirement 3: Provide a platform for people to ask questions regarding scam detection, privacy-related content and any questions the user may have.

Explanation:

1. Satisfied by the support page in the app, which contains **FAQs** regarding how Secure ensures personal data security and how it detects malicious intent and scams. This page also contains a **chatbot**  as well as a **customer support number** to address any user queries.

* Functional Requirement 4: Provide people with swift access to their financial institution’s contact information and policies.

Explanation:

1. Users can access their specific financial institution’s policy page and contact information within the app in just 3 clicks from the home screen. Their bank’s actual page is also linked directly.

* Functional Requirement 5: Minimize users’ data that is accessible to Secure to better ensure data security and privacy.

Explanation:

1. The implementation of the app would be such that **all processing** of the users’ voice calls, text messages, and contact information is **done locally** on the user’s phone. We thus **minimize the data** that needs to be **collected** for the app to function for any user.
2. We only **collect data that the user authorizes us to**, to help improve the LLM. The user can choose to opt in for this feature, thus allowing the user to completely control their data privacy.
3. We inform the user that we **follow industry-standard data encryption** and **storage protocols** to protect the data that we collect.

# **INSIGHTS FROM PILOT STUDIES AND IMPROVEMENTS TO INSTRUCTIONS, PROTOCOL, AND HIGH-FIDELITY PROTOTYPE**

1. Instructions to the participant didn’t cover the support and bank policy information features offered by the app. Added appropriate tasks and contexts to increase testing coverage to all functionalities offered by the app.
2. One Pilot study participant wasn’t able to complete the task of searching for a contact’s different nick-names as they mistook the search button for the call button and thus were stuck trying to search for the contact. The high-fidelity prototype was improved by putting the search button in the middle of the screen, right below the number for the search functionality. All later participants were able to complete this task after the modification.
3. Participants found bugs in the app, which helped improve the prototype:
   1. The block button on the contact search feature was unclickable and wasn’t updating. Improvement: fixed block button on the contact page to block contact and update to show that contact was blocked.
   2. The call and message flow leads to a dead-end screen, from which the user can’t navigate. Fixed the flow of pages to direct the user to the correct page, and removed the dead end.
   3. Testers would like the “Secure” logo on top to lead to the homepage of the app. Implemented this fix.

# **CHAPTER 3:**

# **EVALUATION PROTOCOL**

# **PARTICIPANT DEMOGRAPHICS**

* Participants and their backgrounds can give insights into their experience with our usability testing.
* The participants can be categorized by the following:
* Group 1: People who have been scammed

We selected these participants from our primary stakeholders through the inner network and the high traction we received from the questionnaires.

* Group 2: Individuals with basic knowledge of the app’s UI

We found these participants from our family and friends.

* We took an iterative approach, where every stakeholder was provided the following scenarios and tasks. The key reason why every participant had the same context and tasks since we want to contrast what components of our application work well for which demographic

# **DATA COLLECTION METHODS:**

**Method I: Interview**

* We conducted a ***Pre-testing Interview*** for the usability studies for the following purposes:

1. Understand the user and their background
2. Gauge their experience and interest in the solution the app is providing
3. Collect important information to compare their previous experience to the post usability experience

* Key insights:

1. Users are familiar with scam attempts
2. Users are passionate about finding a solution
3. Users are willing to learn how to use the app and utilize its benefits

**Method II: Natural Observation**

* We utilized Zoom meetings to collect various data points and ques to gain an understanding of the user’s experience.
* Utilized recording functions to document certain observations
* Jotted key points revealed by the testing to incorporate for future solutions
* Analyzed facial expressions and hesitations as a general rule of thumb to identify observations
* Significance: Natural observations allow our team to understand the experience of a user during the testing and use intimate insights we can observe to make observations. This data collection method is effective as it allows us to make more in-depth and detailed observations of a user’s experience since we can see the app through their eyes.

**Method III: Questionnaire**

* We conducted a ***Post-testing Questionnaire*** for the usability studies:
* Utilized Google survey to document and collect observations of the user’s experience on a scale of the following:

1. Scale on user return to the app
2. The complexity of the app
3. The learning curve of the app

* Significance: Able to identify metrics for the system usability scale (SUS).

The above-mentioned methods were used to collect information that encompasses the following required categories:

| QUANTITATIVE | | | |
| --- | --- | --- | --- |
| Subjective | | Objective | |
| SUS | | No. of mouse clicks for tasks  (efficiency) | |
| Likert Scale | | Count of tasks completed successfully  (effectiveness) | |
|  | | Time spent per completed task  (efficiency) | |

| QUALITATIVE | | | |
| --- | --- | --- | --- |
| Subjective | | Objective | |
| General feedback  On satisfaction and efficiency | | Observed sequence of steps participants took | |
| Participants comments related to completing a given task | |  | |
| A description of observed behavior by participant | |  | |

# **CONTEXT AND TASKS**

# Frame of reference: A 25-year-old working adult Bob

* Represents a sample user who is active on the internet:
* Utilizing online resources such as banking
* Distribution of phone numbers
* Online shopping
* Social media messaging
* Represents the general demographic who fall victim to digital scams
* This type of user is more likely to use our app
* Comfortable with technology and applications and requirements of data/privacy
* Context 1:
* Tests the users ability to identify if a caller is safe or unsafe and how to proceed forward
* Quantitative insights for data collection:

1. Time taken to identify next steps

2. Number of clicks to utilize app functionality

3. Number of correct steps made vs incorrect steps

* Qualitative insights for data collection
* Pain points or instances where the user is stuck:

1. Confidence the user felt when executing certain tasks
2. Utilize natural observations to see mood and or discomfort (what is good vs needs more work)

* Context 2:
* Utilize the app’s media component to be informed about recent scams
* Quantitative insights for data collection:

1. The time required to navigate to the info section of the app
2. Amount of resources explored before the user concluded their task
3. Time spent on individual resources

* Qualitative insights for data collection:

1. Pain points regarding the reading material:

Was it too much?

Too boring?

Hard to read?

Motivation to visit the info page

Did the user find the info section significant

* Context 3:
* Utilize the app to identify if a user is a fraud or legit authority
* Quantitative insights for data collection

1. Amount of time taken to identify if the call was detected by the LLM
2. How many unnecessary steps were made
3. The logic for this context has a lot of functionalities in the backend
4. Able to identify if the number should be reported or not

* Qualitative insights for data collection:

1. Comfortable with call recording
2. Able to understand the warning messages
3. Willing to report the number and contribute to the database
4. Pain points or uncertain elements

# **CHAPTER 4:**

# **STUDY RESULTS**

**1. KEY FINDINGS: SUCCESSFUL ASPECTS**

1. Description: Most participants are satisfied with the user-friendliness of the app as it is easy to locate where all the buttons and features are. This is proven by their recorded mouse clicks and time needed for tasks where most participants finished rather quickly with no issues. From our System Usability Scale survey, we also found out that participants think that our app is simple and easy to use.
2. Description: Participants are comfortable giving access to their data if they can guarantee its security and the credibility of the company. This is confirmed by the participants after they see the terms of service and the FAQ feature.

Video Links: <https://drive.google.com/file/d/1bY3l66ELF1sBhw3QIitqF4NRUAroH02t/view?usp=drive_link>

1. Description: From our System Usability Scale survey, we found out that most participants want to use our app frequently thus proving that our app meets the needs and wants of our stakeholders. This relates to the benefits of addressing our problem where we design the app to prevent scams and provide some guidance if a scam already occurred.
2. Description: Participants are also satisfied with our key features such as (call, message, and contact search feature) as well as our awareness feature. This finding is supported by our SUS survey where participants found the various functions in this system were well integrated.
3. Description: Participants prioritized the usefulness and ease of use of the app. This finding is supported by our results from the pre-interview questions. Most participants said they would put more time into learning an app if they thought that the app would benefit them. Furthermore, our app has also achieved this requirement and this is supported by the SUS survey where most participants said that the app was very easy to use as well as our high-fidelity prototype interview where participants are also satisfied with the app’s features.

Video Link: <https://drive.google.com/file/d/1FQGXPZMCkBjyplMTGFlyrGTXOB0EDz0C/view?usp=drive_link>

1. Description: The **SUS questionnaire conducted** after the usability study resulted in a **score of 88**, which is good, and indicates that our system scores high in usability.

**2. KEY FINDINGS: AREAS FOR IMPROVEMENT**

1. Description:

Participants found a heuristic problem regarding Secure’s user freedom where users cannot access the app if they didn’t give the app permissions (for location, calls, contacts, text, etc). Currently, our app will redirect the user back to their phone home screen if they don’t approve our app permissions.

Video Link: <https://drive.google.com/file/d/1WS91HOxDhjSqRJFdhV-9ubss65aTfeKg/view?usp=drive_link>

1. Description:

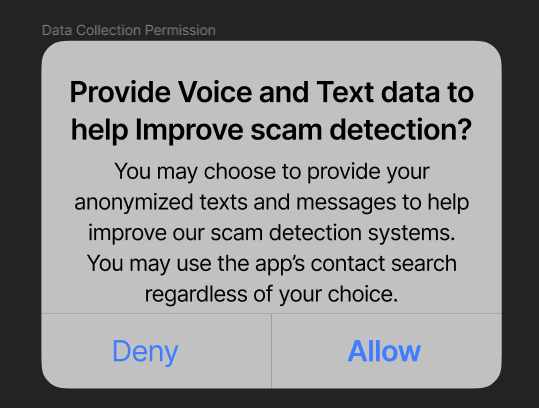
Participants find it time-consuming trying to find which of their recent call history is malicious/flagged as a scam. As of now, our app does not have that feature as callers are flagged inside the app database and not on the user's local phone.

Video Link: <https://drive.google.com/file/d/1okfGDKIwmgdAipwkcfktUvA8ZsH2fa8l/view?usp=drive_link>

# **CHAPTER 5:**

# **TAKEAWAYS AND IMPLICATIONS FOR DESIGN**

1. **TAKEAWAYS**
2. Users are more likely to **trust** the app if they are **informed of how their data is being used,** are **given a choice** of whether they want their data to be collected or not, and the **rigorous data protection and storage policies being** followed to ensure data security and privacy.
3. Users indicated interest in having a **toggle button**, say in Control Center on iOS, where they **can globally turn on or off Secure**. This would be useful in case, for any reason, the user wants complete privacy and peace of mind.
4. During the final presentation, there were suggestions to **improve the reading experience in the app** within the recent scams and awareness page and to make the **headings** to the article and video pages **well-spaced and less dense** to read.
5. Users were confused when there was a **lack of state** within the app. For example, after the user blocked a contact, they would still be able to go back to the messages screen and see that they could block the unsafe user again.
6. Users suggested **visual cues,** a flag, that a particular **caller** is **unsafe** in the recent call history in the contact search feature in the app to allow easy identification of the unsafe contacts, similar to that in the messages app.
7. **MODIFICATION TO THE DESIGN**
8. Allows the user to **access our app’s search feature** (without their call logs) and awareness section **without having to provide permissions**. Users can still change their app permissions in their phone settings if they deem it necessary.



**Figure 2**. Permissions to allow user data sharing

1. We will provide the user with an **option for globally turning on and off Secure’s features**. If it's turned on, all Secure’s features will still run in the background with a notification on their phone. Users will know that Secure is running by a small icon appearing in the upper right part of their screens.



**Figure 3**. Control Center Toggle Button

1. We will choose a reader-friendly font, spacing, and illustrations, and include dark mode to lighten the reading strain on the user.
2. We will maintain “state” during the complete build of the app, in which the app will track which numbers are blocked and which aren’t and update the UI in sync.

# **CHAPTER 6:**

# **REFLECTION**

Our usability testing method comes with several advantages that have significantly contributed to refining and enhancing our app. One key strength lies in **the effectiveness of our interview process**, where insights from just 10 participants have enabled us to **identify over 80 percent** of the app's problems. This targeted approach ensures that we capture valuable feedback from a diverse user base, allowing us to address potential issues comprehensively. Furthermore, our use of the **Figma prototype** has proven advantageous in **showcasing key features**, aligning closely with the wants and needs of our stakeholders. This visual helps in conveying the app's functionality and serves as a valuable tool for satisfying user's expectations.

We have implemented the **System Usability Scale Questionnaire and pre-testing interview questions**. These tools provide a way to measure participants' experiences and expectations during the app evaluation process. By incorporating these metrics, we gain valuable insights into how users perceive and interact with our app solution, allowing us to make informed adjustments for optimal usability. Thinking back on our usability testing, there are a few things we would do differently if we had another go. First off, we will **get more participants to try and evaluate our app**. The more diverse the group, the better chance we have of finding all the advantages and weaknesses of our app. We would also **add a simple keyword questionnaire** where users can choose a few words to describe our app. This would help us understand how users see our app and find some weaknesses in it.

Another idea is to **take the advice from our first users and make changes to our app** based on their feedback. This was implemented during the usability study, but we would want to try to implement some major changes into the design and redo the tests with new users. This way, we can see if the changes we made work and improve the app. For the interviews, we would make sure to do them in **a sound-proof studio with good microphones**. This makes it easier for us to understand what users are saying and helps us get better information. If we had more time and money, we would try to **turn our Figma design into a real app**. Figma is a great start, but it can't completely mimic a real app. Building a real app would help us see how people use all the features more realistically.

# **APPENDICES**

1. **ORIGINAL JOB STORIES**

* Job Story 1: When I am making an online purchase, I want to ensure that my credit card information is encrypted and secure, so I can feel safe putting in my information

Rationale Behind Revision: Credit card encryption is a large space that has many competitive solutions. Furthermore, to encrypt and secure credit cards in itself is a very large process. The revision was to remove such a large task and focus on stories that align with our pivoted problem space

* Job Story 2: When I am buying products online, I want to authenticate the seller, so I can buy genuine and good quality products.

Rationale Behind Revision: Similar to other stories, we want to involve features that can be localized to our app and control. Having a feature that authenticates users on an external platform may prove difficult as there are a lot of regulatory steps we may have to take. Furthermore, users will need to build rapport with our app to populate users regarding authentication.

* Job Story 4: When I am using multiple e-commerce platforms, I want to create strong and unique passwords for each, so I can reduce the risk of having my accounts hacked into.

Rationale Behind Revision: This story no longer makes sense in the scope of our new app change. Once again, the key point is that we want to build something that is localized and does not depend on the cooperation of other platforms.

* Job Story 5: When I find a great deal (in the form of advertisements) on product prices, I want to inquire about the deal with the e-commerce company, so I can be sure that it is a safe investment.

Rationale Behind Revision:

The key change in our revision is reflected by our problem space pivoting more in the direction of personal security.

Problem 1: The job stories in A1 targeted various broad use cases. Hence many functionalities were counteracting each other and reducing the cohesion of the features.

Problem 2: Individual job stories were focused on platform features rather than our app. For example, relying on e-commerce websites to involve security practices proved too difficult to demonstrate in the scope of this app.

Problem 3: Through research, we found our current job stories are more effective since we are incorporating security from the root source (the user).

1. **ORIGINAL FUNCTIONAL REQUIREMENTS**

* Functional Requirement 3: Provide a psychological helpline for people who have been scammed and suffered big losses

Rationale Behind Revision: A psychological helpline for people who have been scammed and suffered big losses won’t be of great help as the scam has already occurred. Thus, we opted for an awareness aspect where we dedicated a section in our app that includes educational content regarding how to prevent scams (this includes articles and videos)

Functional Requirement 4: Automatically detects a transaction scam and blocks it by alerting your banking institution

Rationale Behind Revision: We have shifted our focus to preventing scams received via calls and texts because they usually occur before a transaction takes place. This allows us to intervene early before financial losses occur.

* Functional Requirement 5: Verifies whether an e-commerce website is safe and legitimate to use or not by scanning for any fraudulent activity and user reviews

Rationale Behind Revision: We narrowed down our focus to scam calls and texts to make our app more specific and manageable. Hence, we decided not to focus on the safety of e-commerce websites.

1. **USABILITY STUDY PROTOCOL**

* Project Title: Raising Awareness and Preventing Scams
* Investigators: Team Vulcan
* Purpose: The purpose of our research is to understand how individuals fall victim to scam calls and texts to help us derive requirements for the design of novel interactive computational media that are intended to prevent and reduce scam calls and texts. A brief description of our design problem is: Many people received scams and fraudulent texts and calls. Millions fall victim to these scams which can bring about financial losses and data leaks. We want to find a solution and prevent these 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

first conduct a pre-testing interview where we ask participants 5 questions to get an idea of their needs and goals regarding our app design. We will then conduct the Usability testing by providing participants with a user identity to take up and various contexts and tasks to do. We will observe the participants as they take part in the Usability testing and record the quantitative and qualitative data we are looking for. Finally, we will administer a Post-Testing Questionnaire. 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.
* 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.

1. **CONSENT FORMS**

**Consent Form: Raising Awareness 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. **RESEARCH INSTRUMENTS**

**Pre-Testing Interview Questions**

<https://docs.google.com/document/d/1zFd4PSwwxy6fP2TuKbY2BCu5U0oTSJTVG23l9XROZok/edit?usp=sharing>

**Usability study**

* Context 1: You want to use the SECURE app to check the credibility of a caller who has recently contacted you and make sure that the person is safe to contact, and also see what aliases or nicknames the contact has. You will start on the home screen of your phone.
* Task 1: I would like you to Now, I would like you to identify which of your recent call contacts is unsafe and why.
* Task 2: Second, I would like you to check the credibility of the caller at 1 (234) 567-8900 and tell me what other nicknames or aliases the contact is listed as.
* Context 2: You see that there have been a lot of novel scams going around lately. To protect yourself from the new types of scams, you want to learn about how to avoid them and the specific types of scams going on in your area.
* Task 3: Use the app to explore different ways, using different types of media, you can gain awareness. Also, find out what scams are going around in your region.
* Task 4: Now assume that you are concerned about getting scammed and want to learn about your bank's fraud and scam policies, and you'd like to learn how to report a scam. Use the app to figure out how you'd do this.
* Task 5: Lastly, You have some questions about how the app functions or any general questions. How would you resolve these?
* 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 6: Ensure that you can detect if this is a scam or not, why, and if you should provide information to this person. Block and report this person if necessary.
* Context 4:You use texts to communicate with the people in your life, but you also find that some texts from unknown numbers sometimes contain links that look suspicious. You are confused whether the links are legitimate or not because in the past, you have confused legitimate links(such as for manual e-transfer through text) for scam links.
* Task 7: Now, I would like you to try to read all the texts in your messages app and ensure you can detect if a conversation is safe or not, and block the conversations that are not safe.

**System Usability Scale Questionnaire**

<https://docs.google.com/forms/d/e/1FAIpQLSdBiabOq6doHh97htG5qPI04ya5gLq7IQIS3eZkD8MajCIOMA/viewform?usp=sf_link>

1. **RAW DATA FROM USABILITY STUDIES**

* Participant List and Quantitative Data Recorded:

<https://docs.google.com/spreadsheets/d/1AothEHragRmooPxztxThREy01Sx98LQQfvU2lY3LVjY/edit?usp=sharing>

* System Usability Scale Questionnaire Result:

<https://docs.google.com/spreadsheets/d/1tNg9Uy16i9ADZoSVNP9mgUe5VrAKu5jH8r2PvW-ocLM/edit?usp=sharing>

* Compiled Qualitative Data Notes:  
  <https://docs.google.com/document/d/1aM1Mjcml54Ov4nmXdD4Bp1DtEbz5rYHqLQjSC_DCbxA/edit?usp=sharing>

1. **DOCUMENTATION OF DATA ANALYSIS PROCESS**

* Conducted pre-testing interviews to gauge user expectations for an anti-scam app.
* Notes were taken to collect the data, where observers used Google Forms for this data collection process.
* Conducted SUS post-testing questionnaire using Google Forms to get feedback for the high-fidelity prototype.
* The data collected was split apart into two components:
  + The interface -> UI
  + Functional Features
* We made changes to our high-fidelity prototype based on the first round of usability testing. We then used the newer version for the second round.
* We found out that the design was user-friendly and received positive results such as our system was easy to use, not complex and would frequently use it.

1. **GROUP MEETING NOTES**

Nov 26th Meeting:

* We will be sticking with 10 people for the usability testing, and we need to properly document and justify each of our choices.
* We had a lot of text on our slides and the TA wanted us to refine and make it short and crisp.

Changes that need to be made to the prototype:

* App - Madhav
  + Fill in the content for the app
  + Ask the user for the region
  + Alert user of ongoing scams by content
  + Tailor content to users by region
* Messages - Sahil - implement the messages feature

Make sure that everyone covers the usability testing part for tomorrow’s meeting so we can

Final slides delegation:

* Problem space - Asma and Ayush
* Studies - Sahil and Stephen
* Deliverables - Mugdha and Madhav

Nov 27th Meeting:

* Decided that we should do the usability testing online over Zoom. If it has to be in person, we will conduct it in person
* Decide to have a pre-test interview, test, and post-test SUS questionnaire. We will only be doing an interview pre-test.
* Discuss what needs to be done concerning questions for the usability testing questions - subjective, objective,

Dec 1st Meeting:

* Update on usability testing
* Discussed improvements to tests obtained from pilot tests
* Review progress on High Fidelity prototype
  + Finalize bank policy page info for each bank, add more banks
  + Modify number search page to make finding search page easier

Dec 4th Meeting:

* Start A3
* Chapter 1 - Sahil
* Chapter 2 - Madhav
* Chapter 3 - Stephen and Asma
* Chapter 4 - Mugdha
* Chapter 5 - All
* Chapter 6 - Aayush
* Appendice - All