**Primary Stakeholder:** Person that has been scammed

**Background Information:**

1. Can you briefly describe the online scam incident you encountered, without revealing any sensitive information?
2. What type of online platform were you using during the incident (e.g., online marketplace, social media, banking website)?
3. What methods did the scammer use to contact you?

**Experience during the Online Transaction:**

1. Can you walk me through the steps of the online transaction/activity you were attempting to perform?
2. Were there any specific difficulties or confusion you encountered during the process?
3. Did you notice any unusual or unexpected behavior on the website or app you were using?

**Trust and Credibility:**

1. What factors influenced your trust in the website or seller involved in the transaction?

**Emotional Aspect:**

1. How did they capture your interest to make a transaction?
2. How did the incident make you feel emotionally (e.g., angry, embarrassed, anxious)?

**Suggestions for Improvement:**

1. In your opinion, what could the online platform or website have done differently to prevent this scam?

**Secondary Stakeholder: Person working in the FinTech Industry.**

1. Through your work, what goes into ensuring a transaction is safe and credible?
2. What is the fintech industry doing to tackle scammers who are increasing by the day?
3. What advice do you have for people who receive fraudulent links and text messages?
4. How are you ensuring that people’s personal information is protected?
5. Why is it hard to tackle scammers despite all the security measures set up by the industry?
6. Please walk me through what it takes for someone to regain their money after a scam
7. What type of information is most prone to theft and how can one protect themselves from it?
8. Elderly people happen to be the most prone to scams and frauds, how can they protect themselves?
9. Are there any regulations that make it hard to tackle this issue?
10. How can regulating bodies help tackle this issue?
11. As someone who works in the industry, what measures are you taking to protect yourself?

**Secondary Stakeholder: Person working in banking.**

1. Through your work, what goes into ensuring a transaction is safe and credible?
2. What is the banking industry doing to tackle scammers who are increasing by the day?
3. What advice do you have for people who receive fraudulent links and text messages?
4. How are you ensuring that people’s personal information is protected?
5. Why is it hard to tackle scammers despite all the security measures set up by the industry?
6. Is there a way to reverse the effects of a scam?
7. Are there patterns when it comes to the method of scamming?
8. Please walk me through what it takes for someone to regain their money after a scam
9. What type of information is most prone to theft and how can one protect themselves from it?
10. As someone who works in the industry, what measures are you taking to protect yourself?

**Responses (banker)**

In our investigation into online scams, we employed a combination of questionnaires and interviews as data-gathering methods. These methods were chosen to provide a comprehensive view of the online scam landscape, enabling us to understand the processes and impact of scams on both victims and those tasked with rectifying them.

Incomplete POV statements:

1. (WHO) When reading emails, it is difficult to ensure that the email is safe to open
2. Elders common receive (what) type of emails because they may not be very tech-savvy
3. People face online scams because of (which) online activity
4. Scammers are able to contact victims through online methods because of some (insight) indicator
5. The victims was influenced for fell victim to the scam because of (insight)

Study Protocol:

* Our interviewee was a banker in the fraud department who specializes in rectifying scam requests. This individual was selected due to their expertise in dealing with scam cases, providing us with valuable insights into the resolution process and trends in scam requests.
* They were asked a series of questions about their experience dealing with these type of requests
* Who fell victim to the type of scam and what was the scam
* What was the emotional impact (significance) of rectifying these cases
* What improvement would you make to solve this problem

Key finding (Banker Interview)

* **Scam Waves:** Through interviews with our expert in the fraud department, we uncovered a significant trend in online scams. Scams tend to come in waves, wherein a large number of people are targeted by similar types of scams, albeit with varying methods of execution. For instance, during one period, a wave of scams may focus on impersonating online retailers, while another wave may involve phishing attacks. This cyclical pattern of scamming can confuse individuals who are not up to date with the latest scamming practices.
* *Significance:* The discovery of scam waves and the constant evolution of scam tactics is significant for several reasons. First and foremost, it sheds light on why people continue to fall victim to online scams. Scammers adapt their strategies to take advantage of vulnerabilities in people's awareness and understanding of current scam tactics. The cyclical nature of scams creates a state of perpetual vulnerability, making it essential to understand the ever-changing landscape to effectively combat the issue.
* **Confusion and Targeting:** The iterative nature of scam plans initiates mass confusion among victims, especially among frequent online shoppers. As online scams continue to evolve, they take on new forms and disguise themselves under different guises. These ever-changing tactics lead to a lack of awareness and preparedness among potential victims.
* ***Significance:*** The confusion experienced by individuals due to the iterative and constantly evolving scam tactics is significant because it highlights the psychological aspects of online scams. Scammers use tactics that prey on people's lack of awareness about current scams, leading to misplaced trust and ultimately victimization. Understanding this psychological component is crucial for devising effective prevention and awareness strategies.  
  *Design Implications:* This finding underscores the need for user-friendly interfaces, educational resources, and awareness campaigns that are continuously updated to reflect the latest scam tactics. Designing user interfaces
* **The Perspective of a Banker:** Interviews with the banker revealed the complexity of the situation from the side of those tasked with rectifying scam requests. The constantly shifting landscape of scam tactics challenges these professionals to adapt and remain vigilant. Understanding their perspective is vital for improving prevention and response strategies