Focus Group Summary & Analysis

- **Focus Group No:** 01
- **Topic:** AegisSecure App Concept Validation – Performance and Trust among Tech-Savvy Users
- **Date:** September 5, 2025
- **Participant Profile:** 8 participants. DAU Students of different programs. All rated themselves as "very comfortable" with technology.
- **Objective Reached:** Understanding the performance expectations and trust barriers for technically able users.

---

1. Raw Notes & Key Participant Feedback

- A pasted message should have an immediate result with rating, otherwise they'll close it and forget about it. If it takes more than a few seconds.
- A Rating system is more informative. 90% or 60% is better than 'Dangerous.'
- App should not drain the battery. Many have bad battery life, and if the app uses too much, it will be uninstalled.
- As it reads E-mails and SMS, it shouldn't be stored on the server forever and should be privately secured or is risky for installment in the first place.
- It shouldn't use much data, as many people are on limited plans.
- All policies should be clear, any indication of mistrust/misuse would break the deal.

---

2. Inferences & Summary

This technically skilled group focused heavily on performance, accuracy, and privacy. They saw value in the confidence score as a useful data point. Their primary concerns were practical: the app must be fast, light on system resources (especially battery), and transparent about its data handling. The issue of trust, particularly regarding email scanning, was a major barrier. They explicitly stated that a clear privacy policy and assurances about data handling are non-negotiable. They also mentioned the importance of simplicity and clarity which should be acting along the lines with speed.

Observed Requirements:

- **FR:** The system shall provide a confidence score.
- **NFR:** Analysis must be completed in under 3 seconds. The app must have minimal impact on battery life and mobile data consumption.
- **NFR:** The system must not store user message content, and all communication must be encrypted. The app must present a clear and transparent privacy policy.

Focus Group Summary & Analysis

- **Focus Group No:** 02
- **Topic:** AegisSecure Preferences & Common Scam Experiences
- **Date:** September 12, 2025
- **Participant Profile:** 10 participants, aged 17-19, Fresher Students from DAU. All are active smartphone and social media users.
- **Objective Reached:** Understanding preferred User experiences from frequent tech users, and also noting the scams that target them

---

1. Raw Notes & Key Participant Feedback

- ‘Clunky’ designed apps are not visually pleasing, and a more smooth flow of information is preferred. It should look cool and modern as it is cyber security. Font is also important. Ex- Zomato, G-mail, not like Ecampus.
- Should have Dark mode, and be fast. Or the loading screen should be interesting.
- SMS messages with offers on how to ‘Earn ₹5000 daily from home!’. They know they are fake but still people they know have clicked them.
- High amounts of job/internship scams are found. They have clicked and seen a fake website, where they ask for a registration fee. People are desperate so they may fall for it.
- The app itself shouldn’t spam the user with notifications. It should only have a simple one if there is a very dangerous message. Many apps are muted, but that would defeat the purpose of the app itself.
- One Student got a scam saying that they got a scholarship for a laptop, and that it looked very official and professional. It asked for personal details before they got suspicious.
- The app should see what types of scams frequent the user and be more aware against them.
- The app should be high quality and shouldn’t have vulnerabilities or mistakes in itself. It can seem or become a scam itself.

---

2. Inferences & Summary

The younger students showed the face of modern technology, showing both the needed aesthetics to retain users, and also the threats faced by students themselves.

Regarding User Experience: The feedback shows that the look and feel of an application is not a secondary concern; it is a primary driver of trust and adoption. A "clunky" or slow interface

is an immediate deal-breaker. Key takeaways are the demand for a minimalist, modern design aesthetic and a low tolerance for lag or excessive notifications. The quality of the app's own UX is directly linked to its perceived credibility and trust.

Scam Experience: The most frequently cited threats are not generic phishing emails but are highly related to their student life. Part-time job and fake internship scams are incredibly common. Scholarship and prize scams are also common. This provides a critical insight for our AI model .It must be specifically trained to recognize the language, keywords (e.g., "internship," "deposit," "daily earning"), and patterns of these student-focused scams.

This focus group strongly validates and refines the need for:

- **FR:** The model should be adapting to scams occurring to a user.
- **NFR:** The requirement is not just for "simplicity," but for a modern, fast, and aesthetically pleasing UI/UX. A dark mode should be considered a core feature.
- **NFR:** The app must be highly responsive and have a non-intrusive notification strategy.
- **NFR:** The AI model must be specifically optimized to detect job, internship, and scholarship scams. The effectiveness against these specific threats will be a key measure of success for this user group.

Focus Group Summary & Analysis

- **Focus Group No:** 03
- **Topic:** Practical Needs and Trust-Building for Non-Technical Adults
- **Date & Time:** September 14, 2025
- **Participant Profile:** 8 residents from the society, aged 40-60. A mix of working professionals and homemakers with varying levels of comfort with technology.
- **Objective Reached:** Understanding scam encounters prevalent in a residential community and identifying what features would build confidence and provide actionable help for less tech-savvy users.

---

1. Raw Notes & Key Participant Feedback

- Scams regarding payment of bills occur. They look real, and their son had stopped them from going through with it.Users need to be made aware of what action to take after the app detects a message as a scam (block, delete, report?). They are unsure and don't want to do anything wrong. The action can be taken automatically, but the decision should be up to the user, and an explanation should be given.
- They are afraid of not understanding the app, and doing the wrong thing, especially with an app that deals with such a sensitive issue. Clear, simple instructions are needed.
- Scams are usually common for people in a similar area. There should be a simple way to warn other people effectively. Maybe just something they can copy and paste from the app.
- A multi-language experience would be preferred. Both, to manage scams in a different language, and to give explanations in a different language. Mainly Hindi and Gujarati. It will be better at avoiding confusion.
- Clear indications of what to do next and how to achieve a goal once a scam is averted. Clear steps are necessary as this app is focused for people who aren't tech savvy. This includes setting up the app and providing permissions.

---

2. Inferences & Summary

A prominent theme in this group was a general lack of confidence with technology, which manifests as a fear of taking incorrect action. Participants are not just busy; they are often hesitant and worried about making a costly mistake. This fear materializes as a strong demand for post-detection guidance. For these users, simply identifying a threat is insufficient; the app must also provide safe, explicit, step-by-step instructions on what to do next.

This desire for safe action extends to their community. The concept of a feature to share a warning was highly valued,because it empowers less confident users to help their neighbors without the risk of explaining the technical details. Furthermore, the need for multilingual support

(specifically Gujarati) was highlighted as a to prevent misinterpretation and build trust among those less familiar with English tech jargon.

This focus group strongly validates and introduces the need for:

- **FR:** The system shall provide simple, prescriptive next steps after a threat is detected to guide users on the safest course of action, or has preset action settings.
- **FR:** The system shall provide a feature to easily share a warning, empowering users to protect their community.
- **NFR:** The application must support regional languages to ensure clarity and prevent misunderstanding and also catch more scams.
- **NFR:** The user interface must be extremely simple and error-proof, designed to build the confidence of non-technical users and prevent them from feeling overwhelmed.

Focus Group Summary & Analysis

- **Focus Group No:** 04
- **Topic:** Technical Validation, Advanced Features, and Model Efficacy
- **Date:** September 20, 2025
- **Participant Profile:** 6 final-year students. All have completed cyber security/hacking related courses and have a strong understanding of cyber threats.
- **Objective Reached:** To gather expert feedback on the technical implementation, identify potential feature gaps for users, and understand the expectations of a highly technical audience.

---

1. Raw Notes & Key Participant Feedback

- Just ‘AI’ is too vague. More information behind the engine of the app should be given. Is it an NLP transformer or just a keyword-flagging system? There should be more transparency.
- Only flagging URL shorteners isn’t enough. Many people use them. The original URL should be revealed, and even be given a reputation check.
- The model could be wrong. There should be a way to provide feedback on false negatives and false positives. That could also help retain, update and improve the model.
- We should keep an eye out for advanced and evolving attacks. Like smishing of Unicode domains, or QR code phishing attacks. These new ones are more prevalent in e-mails.
- Less tech-savvy people can be satisfied with a simple score and color legend to show a threat, but there should also be an option for ‘Advanced Details’ that other people might want to know. What triggered the alert should also be shown, like the link, the final webpage, the email name, the language, etc. The app shouldn’t be a blackbox. People should also be able to learn from it.
- The app may also benefit from being available as an API. This could broaden its use, and help scale the technology.

---

2. Inferences & Summary

This technically proficient group provided invaluable feedback on the depth and credibility of the application. For them, trust is not derived from simplicity but from technical transparency and verifiable accuracy. They are not content with a simple verdict; they want to see the evidence and understand the logic behind the detection.

The most critical insight is the demand for an expert-level view. A one-size-fits-all interface will fail to satisfy this user segment. They require a deeper layer of information to validate the app's findings. Furthermore, their awareness of the threat landscape is far more advanced. They

highlighted the need for the model to evolve and handle emerging threats beyond simple link-based phishing. Finally, the concept of a **user-driven feedback loop** was seen not just as a feature but as a fundamental requirement for any legitimate machine learning-based system.

This focus group strongly validates and introduces the need for:

- **FR:** The system shall provide an explanation. A detailed view showing the specific threat indicators that were flagged.
- **FR:** The system must allow users to report incorrect classifications (both false positives and false negatives) to help improve the AI model.
- **NFR:** The application should be transparent about the type of analysis being performed, even if the proprietary details are withheld, to build trust with technical users.
- **NFR:** The AI model must be robust enough to identify sophisticated threats, including Unicode-based impersonation and emerging vectors like QR code phishing.