Data Privacy Concerns

Our project processes sensitive text inputs (emails, messages, potential phishing content. Handling this kind of data responsibly is critical.

1) Issues About Data Privacy

Here are the **main privacy risks** we identified:

1. **Storage of Sensitive Data**
   - Every user analysis (input text + AI result) is stored in the database (analyses table).
   - If a user pastes a real email containing **personal data** (bank info, passwords, IDs), it gets persisted in plain form.
2. **User Authentication Data**
   - User emails and password hashes are stored in the users table.
   - If improperly secured, this could expose login credentials.
3. **Generative AI API Calls**
   - User inputs are sent to the Gemini API for analysis.
   - This raises concerns about whether the data might be used by the provider for training or logging.
4. **Lack of Explicit User Consent**
   - Currently, the app does not ask users for explicit consent before analyzing and storing their data.
5. **Data Retention**
   - No clear policy on how long analysis data is stored.
   - Keeping data indefinitely increases privacy risk.

2) Solutions to Address Privacy Risks

We propose both **technical** and **legal/organizational** measures:

Technical Solutions

- **Hashing & Salting Passwords**
  - We already store password hashes (not plain text).

   - Use **bcrypt/argon2** instead of weaker hashes.
- **Encrypt Sensitive Fields**
   - Encrypt analysis text column at rest with a DB encryption key.
   - Decrypt only when displaying to the user.
- **Data Minimization**
   - Store only necessary metadata for dashboards (judgment + date).
   - Allow users to **delete their analyses** from history.
- **Anonymization for Statistics**
   - For global statistics (charts), aggregate results and strip user identifiers.
- **Secure AI Calls**
   - Ensure API keys are stored securely in environment variables, not code.

Legal & Organizational Solutions

- **Privacy Policy**
   - Publish a clear privacy policy explaining what data is stored, for how long, and how it is used.
- **User Consent**
   - Add a checkbox at signup: *"I consent to my messages being analyzed and stored for phishing detection purposes."*
- **Data Retention Policy**
   - Auto-delete analyses older than **90 days** unless user explicitly keeps them.
- **Right to Erasure**
   - Implement a **"Delete Account"** option that removes user data permanently.

Conclusion for E

- **Issues Identified :** storing sensitive text, API calls, retention, lack of consent.
- **Solutions Proposed :** password hashing, encryption, anonymization, user consent, retention policies.