Final Project Proposal

1. **Team Members:**
    - Ryan Romero, Shervin Afrasiabi

2. **Proposed Application**
    a. **Problem Statement**
        - Login passwords have been widely used to secure personal accounts in websites and applications. Over the many years of using string passwords, a problem emerged; many users create and use easy to memorize passwords and hackers have taken advantage of this trend; Many websites and software have resorted to 2-factor authentication to increase security of user accounts. Many users view these extra security protocols as an annoyance, despite it being helpful in securing their account.
        - We have a much simpler solution to discourage hackers. Instead of focusing on trying to create additional security authentication to make user accounts difficult to crack, we believe the better solution is helping users create and memorize better passwords.
        - We will be creating a mobile app that primarily saves user passwords in a database, allowing the app to do all the password memorization for them. The app will also be able to generate long random string passwords that a user may use for new login accounts.

    b. **High-level Description of the Functionalities**
        - **Password Database**: A (preferably local) database will hold every user inputted password they wish to keep saved. The user will be able to manage and filter this list of passwords, allowing the app to memorize and keep track of any and all passwords the user has. This will lift the burden of trying to memorize passwords, allowing users to create even harder passwords. Users will be able to manually add and delete passwords in the database. With every entry to the database, users will have the option of also adding a “hint” that is related to that password. Users can use this section to add any sort of hint as to what they have used “this” password for.

        - **Password Generator**: A small and simple program that is able to generate passwords of random lowercase and uppercase letters, numbers, AND symbols of varying lengths to create difficult passwords. Upon generating a password, the user will be asked if they wish to reroll a new password or save it into the database.

        - **Characteristics of strong passwords:** This will be a simple page of text,in the app, that will detail a concise list of things to consider when creating good passwords. The user can click onto this page/tab at any time to read these general rules for password creating from the homescreen.

3. Implementation

- **Data provider if any**
  - With our current plans for this app, there are no plans of sending/receiving data to a server. The reason being, sending sensitive information such as passwords over a connection poses an unnecessary security risk that we rather avoid. We would prefer that the database is locally saved on the user's device however we are no database experts.

- **Third-party library used if any**
  - N/A