Authentication & Profile Security Risks and Mitigation Plan

This document outlines some of the common security risks and issues that can come with the implementation of the login, signup and profile page of our gaming platform, OMG. The following solutions have also been proposed as a countermeasure for improved cybersecurity in order to protect our users and our team.

Passwords are the first line of defense against unauthorized access to user profiles. Exposed or weak passwords can create risk to other services that users may use the same password for. This is why we need to encourage our users to have strong passwords as well as providing adequate password protection from our side. Below are some mechanisms that should be implemented for proper password management and protection:

- Enforce secure password policies such as a minimum length of 12 characters, the password must include a special character (e.g. . , , , ! , ?), or a number and an uppercase letter
- Passwords when stored on the server side's password file must be first hashed with specialized password hashing algorithms like Bcrypt, PBKDF2, or Argon2
- Salt and/or pepper can be added as an extra measure to strengthen weak password before hashing
- Limited login attempts (e.g. 10 tries a day) can be enforced to mitigate brute force attacks
- Generic error messages (e.g. incorrect user or password) to avoid giving the attacker any useful information
- Optional: Use OAuth 2.0 for authentication to avoid the need to store password hashes and expedite the login/signup process

Social engineering and phishing are still problems that can affect our users even with adequate cybersecurity measures server side. Below are some mechanisms that should be implemented to mitigate the effects of social engineering tactics:

- Provide warning messages and tips in the help section to educate our users of common social engineering tactics.

- Multi Factor authentication (MFA) should be implemented with email verification and human authentication (e.g. CAPTCHA)
- Enforce email verification or MFA when changing user data like username, emails, password, location etc.
- Users should be able to control their privacy settings (i.e. public or private) to protect sensitive information
- Either encrypt or mask sensitive data (e.g. jl*****0@gmail.com)

Additional security measures:

- Proper user input sanitization during the login and sign up process to avoid injection attacks
- Refresh session tokens regularly
- Keep logs of activity to monitor suspicious activities (e.g. the last 90 days):
    - Date and time of user activities
    - Login and signup attempts and their respective user inputs
    - Profile updates or privacy settings changes
    - Changes in the friends list
- Firewall implementations to block malicious or excessive traffic

---

By following these security measures, we can reduce the cybersecurity risks and ensure user satisfaction with our service.