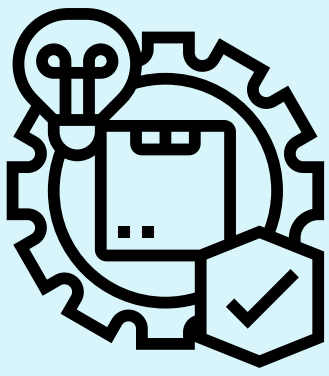
RECOMMENDATIONS
FOR USERS

1. GRANT MINIMAL PERMISSIONS

Only approve permissions that are necessary for the app's functionality.

Be cautious of apps requesting excessive access to your personal data.



2. UNDERSTAND PERMISSION REQUESTS

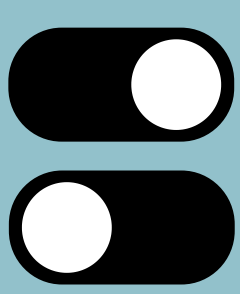
Carefully review the context and explanations provided by the app when it asks for access to your data.

If the reason for access isn't clear, seek further information before granting permission.

3.AUTHORIZE ACCESS INCREMENTALLY

Grant permissions as they are needed rather than all at once.

Avoid giving broad access to features you may never use.



4. VERIFY THE AUTHENTICITY OF LOGIN PAGES AND PROVIDERS

Ensure the login page and SSO provider are legitimate by checking for HTTPS and official domain URLs.

Be wary of phishing attempts that mimic trusted login portals

5.USE MULTI-FACTOR AUTHENTICATION (MFA):

Enable MFA for additional security whenever it is possible.

Prefer apps that offer robust authentication methods such as biometrics or authenticator apps.

6. LOG OUT WHEN NOT NEEDED

Always sign out from SSO sessions on shared or public devices.

Clear cookies and session data when using devices that are not your own.