User-data security design guidelines

User data security is the practice of keeping user data protected from corruption and unauthorized access. Thus helping to ensure privacy. Applications should give high priority to user data and should not modify, delete or broadcast it.

A checklist for user data security

- Users data like images, videos, messages, contacts should not be altered without their permission.
- Access point information should not be modified without informing user.
- For using GPRS, user confirmation should be taken.
- Sending background SMS should be discouraged.
- Secure information like Password should be encrypted.
- Users should be given permission to delete their private data.
- Users should be encouraged to take backup of their private data.
- Application's sensitive data should be created in the private folder of the application, so that it is not accessible to other applications.
- While sending data to the web, it would be pertinent to notify the user of the vulnerability of the data in case there exists one.
- While deleting any data through the UI always display a confirmation dialog to the user to avoid inadvertant delete of data.
- Allow some kind of backup/restore mechanism for application which contains lot of sensitive user data.

Some Technical Mechanism To Protect User Data

Encryption

This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only by decoded or decrypted by the party that possesses the associated key.

Strong User Authentication

Authentication is another effective part of data security.The single sign-on scheme is also implemented into strong user authentication systems.

Backup Solutions

Data security wouldn't be complete without a solution to backup user critical information.

(C) Copyright Nokia 2014. All rights reserved.