(8) ⇒ Best Practice For Android :-

i) Installing Safe Applications & The easiest and safest way to install new application on android is to use Google's Play Store.

ii) Store encrypted Data :- Whenever you have to store the important or personal data on your android phone then try to store that data in encrypted form or try that data should be password protected.

iii) Recording Password Safely :- You can store most of your passwords in a single, encrypted file on device by installing some apps. These apps allow you to remember a single, strong master password and use it to lookup your passwords. This is the safest method.

iv) Physical Device Security & Always set a strong screen lock code and avoid sharing it with others. Regularly backup important data from phone to computer.

v) Spam applications & If someone sends you a application by a spam email or message then dont try to install that application, that may be virus.

Scanned with CamScanner

⇒ Best Practice For IOS :-

i) Encryption :- You can easily protect the content on your device using encryption. If someone gets physical access to your device they will also need password for decryption.

ii) Safe Applications :- The safest and easiest way to install or download new applications on iOS is to use Apple's Store.

iii) Malicious Applications :- If some random person sends you any link of website or application then dont try to open that link. It might be some malware or virus which will delete your whole data or do something illegal.

iv) Secure Password :- In iOS, there is an application named Minitey Pass which can help you to remember a single, strong master password and use it to lookup your passwords.

v) Scree Lock :- Always set a strong screen lock code and avoid sharing with others. Also try to change passwords after some time.

Scanned with CamScanner