Cyber Crime Information-49

To: All members

From: cyberdost@mha.gov.in

Subject: Cyber Crime Information - 49

Respected Sir/Madam,

Any app from an application store like **Google Play** or **iOS when installed** on a device, requests for access to various information/features in the phone—known as permissions. For example, an app might want permission to access the contacts on device, camera, files, photo gallery or its location etc. Most of the smart phones allow the user to control which permissions an app can access during the app installation or even after the installation is complete on the device. Not giving due attention while giving permissions may allow apps to access personal information on device, which otherwise users may not like to share.

Most of the apps ask for several unnecessary permissions, which are generally not required for performing its basic functionalities. For example, a media player app has no reason to seek permission for access to contacts, camera & microphone etc. Similarly, a chat app may request **'Storage'** permission for access to pictures or media files, so that the user is able to share those with his/her contacts but permission to access location is not an essential requirement unless the user wants to share his/her location on chat. Similarly a gaming app may ask for **'Phone'** permission to keep track of an incoming call, so that it can pause to let the user attend to the call, but requesting **'SMS'** permission to access text messages or **'Location'** permission to know the current location are not required for basic functionality of the gaming App. Thus, it is for the user to decide which optional permissions he/she would like to grant. Any app, which does not function if non-essential permissions are not granted, could be a sign that the app may be misusing the permissions for extracting information from user's device.

Letting apps access more data on a phone than required for its functionality could lead to security risks and expose user's sensitive personal information. Users must periodically check the permissions accessed by an app since these may change over a time period due to multiple reasons e.g. application update or OS upgrade etc.

Suggestions

- When installaing an app, be careful about the permissions sought and avoid giving unnecessary permissions.
- If you feel that a particular permission is not necessary, do not approve it. If that permission is a mandatory permission, then the App will automatically notify when such app is used.
- Periodically review the permissions of installed apps on your device.
- If an app does not work with some of denied permissions, which you feel are not essential, be careful to accept the associated risks in using such app.

Regards
Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23093697