Cyber Security Advisories
01-12-2018

Security issues of Fake mobile applications

CERT-IN published advisory regarding Security issues of Fake Mobile applications on 16/11/2018. The fake Mobile applications can install malware to steal personal information, lock personal files and demand money and they can even delete all your personal data. Fake apps can harm your device in many possible ways.

Best practices for Users:

- Do not use "Jailbroken" or "Rooted" devices for mobile banking or other financial transactions.
- As per CERT-IN, Do not download and Install application from untrusted sources, Ensure to turn off the "Unknown Source" option in the Security setting page on Android based Mobile Phones.
- Install applications downloaded from reputed application market only, like Google Play Store.
- Install updates and patches as and when available from device vendor/service providers.
- Always run a reputable mobile security app for your device, and keep it up to date regularly. A mobile security app can help to scan the apps you download, malware, spyware and protects you from unsafe websites.
- Be aware about threats associated with fake game apps and pirated video games as they can harm your mobile device by installing embedded malicious program.
- Always do some research on the Developer of the app you plan to install. Search the Developer name and scan through the results. A genuine developer is most likely to have a website and other details on the internet. Apps that have the tags "Editor's Choice" or "Top Developer" are more than likely to be a genuine legitimate app.
- Read all app permissions carefully. When in doubt the best rule of thumb to abide by is to ensure that the permission asked by an app must comply with its functions/features. For example, if a flashlight app is requesting permission to access SMS, Call Logs, Media files, etc., then this is definitely a red flag and not an app you should be downloading.

==