केनरा बैंक Canara Bank

Important Notification to Customers

Android Banker Trojan

Dear Customers,

It has been reported that a malicious application targeting various banking and payment apps [including Indian banks] has been circulating. The malicious application pretending as Flash Player is being offered via third party app stores, possibly when the users are being directed from compromised servers or after clicking on ads. The application is instructed to steal banking credentials, intercept SMSs, displaying false screen (to capture details) on top of legitimate apps, and steal sensitive data to attacker controlled servers, among others.

Best Practices to stay safe from this Malware

- Do not download and install applications from untrusted sources [offered via unknown websites/ links on unscrupulous messages]. Install apps downloaded from reputed application market only.
- Prior to downloading / installing apps on android devices (even from Google Play Store):
    - Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.
    - Verify app permissions and grant only those permissions which have relevant context for the app's purpose.
    - Do not check "Untrusted Sources" checkbox to install side loaded apps.
- Exercise caution while visiting trusted/untrusted sites for clicking links.
- Install and maintain updated antivirus solution on android devices. Scan the suspected device with antivirus solutions to detect and clean infections.
- Install Android updates and patches as and when available from Android device vendors.
- Enable 2-factor authentication for your Google/other accounts.
- Users are advised to use device encryption or encrypting external SD card feature available with most of the android OS.
- Avoid using unsecured, unknown Wi-Fi networks. There may be rogue Wi-Fi access points at public places used for distributing malicious applications.