**Never Download Android Apps from Third Party Sources Other than Google Play**

In late November, about 1.3 million Android devices were hit by a malware named Gooligan, which collected user data through an ad clicking campaign. The malware was able to infiltrate into Android devices through an app, particularly the one which users could download outside of Google Play Store only.

With this technique, hacking into Android devices and collecting useful information has become a much easier task for cyber criminals. This is where Android app security can be bypassed by cloaking a software as a harmless, authentic app that intends to serve a particular purpose; and then putting it up in a third-party app store where careless users can download them.

The flexible and open-source platform of Android is easy for developers to access, but at the same time it has allowed open opportunities for malicious apps. The key to ensuring android app security is to never download any apps from third-party stores and always download it only from Google Play Store. Google screens out potentially harmful apps from getting place in the Play Store, and even if an app does make its way somehow, it is immediately removed if deemed malicious.

According to Google, in addition to scanning apps before publishing them on Play Store, it has also introduced proactive app review which helps catch such apps early and allows developers and users to flag apps for review. This is something that lacks in third-party app stores where you cannot be sure if the downloaded app is real or if it is actually costing you your money and personal information.

Another problem that confronts android app security is the statistics which show that approximately half of Android users are still using devices running Android 4.4, which was released more than three years ago. Hackers know this and they can exploit Android bugs that have been known for years and even after patches in updates, can be exploited with strategy malware like Gooligan.