**Security Vulnerabilities in the Google Play Store**

Just like AppStore for iOS devices, Google Play Store is considered a reliable and secure platform for downloading and installing mobile apps on Android devices. When we talk about app market for mobile devices, Play Store is acknowledged as a major worldwide shareholder.

When it comes to security, however, there is no denying that Apple has always been far ahead of Google. But even then, it has always been unimaginable for Android users to think that Google would take the security of its Play Store lightly, as it the primary medium for apps to make their way into Android devices. This is why it comes as a surprise to know that a number of recent research studies have identified some alarming security red flags for some of the apps on Play Store.

As it turns out, the identified apps pose alarming threats to standard Android app security expectations, particularly with reference to their privacy policies. The study conducted by Carnegie Mellon University stated that around nine thousand apps did not have any privacy policy in place out of the total 18 thousand apps studied. As if this is not enough a blow to Android app security, many of these apps also do not inform the user that they will gather personal data while the app is being operated on their device and also fail to mention that the collected information will be shared with other entities.

This news comes as a warning especially to those users who do not look into the conditions an app puts forward while it is being installed. To maintain Android app security, it is important for users concerned about privacy to closely pay attention to the app details before installing it. If an adequate security or privacy policy is nonexistent, it is better not to install the app and look for a better alternative.