Learn tips to Avoid Malware Infection on Mobile Devices

A recent report compared the risks of using Apple® and Android® devices. **The bottom line? Both have risks to the users.**

Apple Devices

The major differences, a report by Marble Labs stated, is that Apple controls distribution of the apps and for the most part, iOS users with non-jailbroken devices can only download apps from the official store, making it more secure.

There is another way, however, that users can insert risk into their iOS devices, which is through enterprise marketplaces that provide testing apps. This becomes a "secret entrance" into the device. Because iOS allows management configurations on the mobile devices, hackers can also use social engineering tactics to try to lure iOS users to a website and convince them to install a malicious app.

Android Devices

Android is a much more open system and users are allowed to download apps from a variety of sources that are not necessarily secure. In addition, because of the openness of Android, there are many different versions, making it more difficult to secure. Hackers can also use social engineering tactics on users with Android devices.

Tips and Advice

- Always secure mobile devices by locking them when not in use
- Never leave them unlocked and unattended
- Use the automatic lock feature *(if available)*
- Use strong passwords on mobile apps
- Always update devices and apps with the latest security patches
- Be aware of the apps being downloaded to ensure they are safe
- Only download apps from the official app stores!

Get the lastest information from our website. Scan the QR Code to go directly to this page.