

The android platform has revolutionized the technology world and this is very evident from the fact that the android based devices are now the most popular devices today. The sale of mobile devices which utilize the android platform has soared to a point where they will in the near future overtake the PC sales. The expansion of the mobile technology and industry and the astronomic rates of adoption have seen the industry attract hackers and scammers. The continuing rise in popularity of the android devices has seen a reminiscent rise in the numbers of malware identified on android.

This year alone there has been a surge in sales of the android smartphones and this has seen to it that more than 75% of smartphones shipped were android. Hence the android platform has been a favorite for developers since it is an open source platform. This privilege has also been exploited by the hackers in a bid to take advantage on unsuspecting users. Malware has been on a sharp rise and particularly in 2012; malware on android has increased more than six fold. This is according to reports from different security firms and experts. The biggest reason has to do with the ease with which malware writers are able to reach users on the internet in such a big way.

The surge in the number of malware seen on android does not imply that there have been no measures taken to deal with the menace. Google has been tightening the android security screw in a bid to ensure that all apps made available are free from infection. This has been done through the addition of a layer of security to the application store Google Play so as to scan the apps for malicious code and guarantee that apps provided on the store are secure. Away from this app platform, there have been the third party apps and these have been fueling the proliferation of malware on android. The third party apps are either provided free or at a fee and find common use with many different people for a myriad of reasons such as functionality, entertainment and other purposes.

The malware on android has confounded security experts who all report the big percentages in increases for every passing quarter. The malware is intended to achieve different functions for the people behind the development of a particular piece of malware. Many writers of the malware want to make gains from SMS sending from the android smartphones of unsuspecting public, steal data especially personal and sensitive data, make unauthorized payments, malicious and deliberate harm to the smartphone, damage privacy and consequently track activity with and on the smartphone, track web browsing sessions and finally to read and send your location among other form of malicious damage.

Having seen that malware on android is proving to be a real menace and even security experts predicting that 2013 will be the year of malware on android, there are some bits of information which will prove to be very important in protecting the android smartphone or tablet. It is important to know something about the android mobile device before going out and purchasing the device. This will help greatly in the turning off the features of the device which are not an absolute necessity at the moment.

Encrypt data if the technology has been made available to secure the data and ultimately your device. Find a good application to protect you and your device from malware and other threats. Exercise caution when downloading and installing any app and other software into the mobile device. Prevent the android mobile device from connecting to public and unknown wireless networks which may provide access points into the device and by extension to the data stored in it. Web browsing using the device should be done with a lot of caution to avoid falling for the schemes of the hackers and scammers.

Run update to software and firmware to ensure that the risk for attack is greatly brought down. In conclusion, the android mobile device should be treated just as a personal computer is handled with precaution to avoid malware attack.

[telefon dinleme](#)