Attacks on Android devices are increasing - Phoenix Software

Malware on mobile phones and even tablets is becoming an even bigger problem than PCs, especially if the mobile device runs the Android operating system. According to Juniper Networks, Android malware samples increased 472% in the period between July and November last year.

"Hackers have declared war on Android devices, and you might get caught in the crossfire," says Simon Campbell-Young, CEO of Phoenix Software. "This is obvious in the increasing number of attacks we have seen, most recently with the fake versions of the Instagram Android app, which sends background SMS messages to premium rate services, earning its creators revenue."

He says that users that have system updates should make sure to install them. Most devices notify the user of a pending over-the-air update, but some manufacturers and carriers prefer to do tethered updates for some phones. By keeping abreast of their software status, users can close many security holes before they are exploited.

Exercise common sense

However, the update route may not always be an option. Campbell-Young points out that there are several different types of security vulnerabilities and attacks that users should be aware of, not all of which can be easily defended against. "At times like this, users should make use of security software such as Kaspersky One or AVG Mobilation. These applications are designed to scan apps as they are installed and detect malware."

More than anything else, he adds, users need to exercise common sense. Virtually all of the apps in the Android market are safe, with a few notable exceptions. Glancing at the reviews and screenshots of an app can be an excellent way to avoid shady apps that might briefly appear in the official market.

Most of the genuine trojans for Android only show up in alternative app stores, and as standalone APK files on forums. "It almost goes without saying that users should only install an app from outside of the market if they are totally confident of the origin. A beta app from a well-known developer is fine. A random APK from a Chinese forum thread is extremely risky. Even a passing understanding of the situation is likely the most useful tool to prevent a phone from being exploited," Campbell-Young concludes.