Fake Facebook app spies on Android phones

ESET has recently discovered a malicious Android app named iBanking that is able to spy on a user's communications. Telephone calls and SMS's can be intercepted, which means that the hackers can potentially hack into the users online bank accounts. This is an aggressive attempt for hackers to infect Android smartphones.

Image: www.freedigitalphotos.net

The bot attempts to lure users into installing an Android Facebook application. Once the user is logged onto Facebook, the malware injects content onto the webpage which asks for the user's phone number, and thereafter a message is displayed confirming that the user's mobile is running Android.

The message displayed is full of spelling mistake and bad grammar and this should be a warning sign to anyone thinking of continuing any further and entering their telephone number. Another warning sign to users is that you may have to change your Android settings to permit the installation; this is because the app is hosted on a third party site.

"This bot is extremely invasive," says Lee Bristow, security consultant at ESET Southern Africa, "hackers are able to listen to calls been made, intercept SMS messages and even listen to your private conversations. Of course, If they have this much power of your phone, they can most certainly break into any online banking"

iBanking is an application that showcases complex features when compared with other earlier mobile banking malware. It can be used in conjunction with any malware able to inject code into a webpage and is generally used to redirect incoming SMS messages to bypass two-factor authentication.