

Fake AV Goes Mobile



mobilesecurity.com [[Mountain View, CA](#)] Just when we thought it was safe to go back in the water, news comes from UK tech site [ITProportal](#), that the bad guys are adapting their favourite desktop tricks to suit the mobile app markets. A new Trojan, which Symantec has named [Android.FakeLookout](#), is disguised as an update for a well-known mobile security app and has been discovered lurking on Google Play.

Unsuspecting Android users who visited the app store to update their security app (instead of simply updating through the app itself) were unknowingly installing a piece of malicious code that was designed solely to steal their sensitive personal information - including SMS and MMS messages, images and videos.

This app has already been removed from Google Play, but could potentially appear on other app markets and is likely to provide encouragement for cybercriminals to continue finding ways to target our devices and personal information.

Hiding viruses in legitimate-looking apps isn't a new concept – fake antivirus (or Rogue AV) is one of the most prevalent (and profitable) methods used by malware authors to harvest credit card information and gain access to PCs., whether it's mobile security or any other popular, trusted app on Android devices.

Google Play works with the security industry to maintain a safe app market, but it remains possible that cybercriminals will get ahead of the curve on occasion. As we increasingly rely on our smartphones to manage our personal information, communication and online lives, it's ever more apparent that we all need to be vigilant and pay close attention to every app we install. Whether you download your apps from Google Play or any other app market, it doesn't take a minute to check the trustworthiness of a particular app on our [AppView](#) directory.

Mobilesecurity