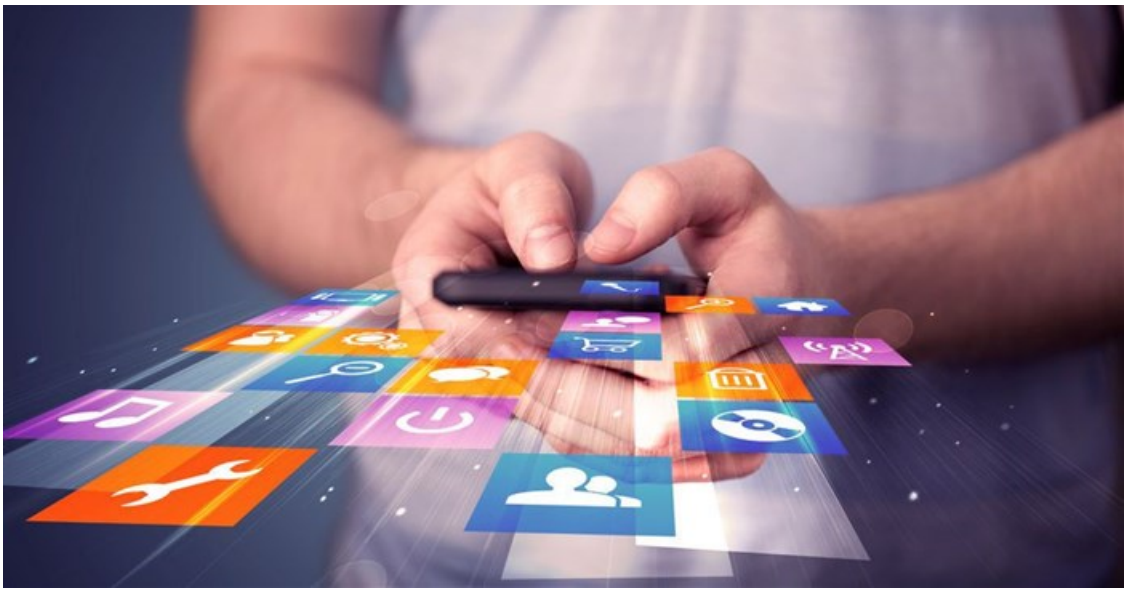
Attention Android users! Be wary of malicious apps

According to South Africa's Wireless Application Service Providers' Association (Waspa), the ongoing shift to mobile and Android's open source appeal has seen increasing attacks on mobile users through malware and ransomware inadvertently downloaded at app stores.



© Rancz Andrei via 123RF

Waspa has urged the country's 35 million plus mobile users to be on the look-out for malicious apps designed for use on the Android mobile operating system.

> ***Worldwide, almost 75% of smartphone users have downloaded the various versions of this popular open source operating system. In South Africa, Android's share of the mobile market is rapidly approaching the 80% mark.***
>
> "The ability to spy on consumers' handset usage, using adware to force a consumer's handset to generate ad clicks and the defrauding of the mobile user through ransomware are outcomes that we are working hard to avoid," says Waspa chairperson, Anthony Ekerold.

If the future in Africa is mobile, identity verification is paramount

Sherry Zameer 25 Apr 2018

The organisation has spent the better part of two decades building trust in the local mobile content and applications industry and championing the cause of responsible self-regulation while educating the South African mobile consumer about ways to protect themselves from various online and mobile threats.

"We are ramping up our consumer education and industry engagement mission in an effort to mitigate the potential threat from malicious, Android-based apps largely developed overseas," Ekerold says.

What can users do?

He explains that local mobile consumers should always ensure they are **downloading apps from reputable vendors** like

the Google Play Store and to ensure they have anti-virus and anti-malware apps installed on their phones.

While not foolproof, only downloading apps from reputable vendors like the official Google Play Store, mean Android users can avoid the overwhelming majority of malicious apps out there. The Google Play Store, for example, has built-in mechanisms to screen every app for malware, ransomware and other suspect software. According to Google in 2016, for users who downloaded apps exclusively from the Play Store, there were 'potentially-harmful apps' on a mere 0.05 percent of devices.

Because potentially-harmful apps do exist in small, but statistically-significant numbers on the official Play Store, another useful tip is for users to be aware of certain device behaviours that may indicate the presence of malware. For example, users should be concerned if they notice an increase in ad pop-ups or unusual notifications on their Android devices. This would suggest they immediately install anti-malware apps while running scans using free available software to clean up their devices.

Booby-trapped messaging apps used for spying

22 Jan 2018

They should also **analyse the permissions** an app requires in order to understand the expected user experience and be aware of any issues before installation.

Reading **installation reviews** is highly recommended. In light of recent news reports regarding data-harvesting, it's crucial for Android users to understand that apps can harvest sensitive user data from such common and universal phone elements as cameras, calendars, and contacts, among other things.

In addition, users should **keep abreast of the latest malware and ransomware** designed to target mobile users worldwide so they become more aware of how their phones behave when infected.

Finally, Android users should **regularly review their operating systems** to ensure they have the latest version complete with the latest and most up-to-date security features.

Serious Wi-Fi flaw found in WPA2 protocol

Ilse van den Berg 18 Oct 2017

"When discovering a potentially harmful app, users should treat it with extreme caution and immediately delete it," advises Ekerold. Users can also anonymously report potentially harmful services and applications to Waspa.

Waspa also regularly publishes its ‘application block list’ which helps inform South Africa’s mobile network operators and its members of any domains where mobile content and application fraud is potentially occurring, although malicious apps often hide identifying details. Waspa members are required to enforce this block list on all services and in so doing, protect consumers from malicious applications that attempt to defraud them.