The dark side of mobile apps

Mobile device security threats are on the rise and it's not hard to see why.

Source: pixabay.com

In 2019 the number of worldwide mobile phone users is forecast to reach 4.68 billion of which 2.7 billion are smartphone users. So, if you are looking for a target, it certainly makes sense to go where the numbers are.

Think about it, unsecured Wi-Fi connections, network spoofing, phishing attacks, ransomware, spyware and improper session handling – mobile devices make for the perfect easy target. In fact, according to Kaspersky, mobile apps are often the cause of unintentional data leakage.

“Apps pose a real problem for mobile users, who give them sweeping permissions, but don’t always check security,” says Riaan Badenhorst, general manager for Kaspersky in Africa.

“These are typically free apps found in official app stores that perform as advertised, but also send personal - and potentially corporate - data to a remote server, where it is mined by advertisers or even cybercriminals. Data leakage can also happen through hostile enterprise-signed mobile apps. Here, mobile malware uses distribution code native to popular mobile operating systems like iOS and Android to spread valuable data across corporate networks without raising red flags.”

In fact, according to recent reports, six Android apps that were downloaded a staggering 90 million times from the Google Play Store were found to have been loaded with the PreAMo malware, while another recent threat saw 50 malware-filled apps on the Google Play Store infect over 30 million Android devices. Surveillance malware was also loaded onto fake versions of Android apps such as Evernote, Google Play and Skype.

Beware of viral apps

Considering that as of 2019, Android users were able to choose between 2.46 million apps, while Apple users have almost 1.96 million app options to select from, and that the average person has 60-90 apps installed on their phone, using around 30 of them each month and launching nine per day – it's easy to see how viral apps take several social media channels by storm.

"In this age where users jump onto a bandwagon because it's fun or trendy, the Fear of Missing Out (FOMO) can overshadow basic security habits – like being vigilant on granting app permissions," says Bethwel Opil, enterprise sales manager at Kaspersky in Africa.

"In fact, accordingly to a previous Kaspersky study, the majority (63%) of consumers do not read license agreements and 43% just tick all privacy permissions when they are installing new apps on their phone. And this is exactly where the danger lies – as there is certainly 'no harm' in joining online challenges or installing new apps."

Relook at permission settings

However, it is dangerous when users just grant these apps limitless permissions into their contacts, photos, private messages, and more.

"Doing so allows the app makers possible, and even legal, access to what should remain confidential data. When this sensitive data is hacked or misused, a viral app can turn a source into a loophole which hackers can exploit to spread malicious viruses or ransomware," adds Badenhorst.

As such, online users should always have their thinking caps on and be more careful when it comes to the internet and their app habits including:

- Only download apps from trusted sources. Read the reviews and ratings of the apps as well
- Select apps you wish to install on your devices wisely
- Read the license agreement carefully
- Pay attention to the list of permissions your apps are requesting. Only give apps permissions they absolutely insist on, and forgo any programme that asks for more than necessary
- Avoid simply clicking "next" during an app installation
- For an additional security layer, be sure to have a security solution installed on your device

"While the app market shows no signs of slowing down, it is changing. Consumers download the apps they love on their devices which in turn gives them access to content that is relevant and useful. The future of apps will be in real-world attribution, influenced by local content and this type of tailored in-app experience will lead consumers to share their data more willing in a trusted, premium app environment in exchange for more personalised experiences. But until then, proceed with caution," concludes Opil.