Is your personal information safe on apps?

Did you know that research suggests that over 1,000 Android apps collect location data and other information from phone users, even if no permission was given?

Source: pixabay.com

While some app developers will often use information about you with your prior consent, to monetise or improve their in-app service as a unique customer experience, some developers may abuse your trust by stealthily collecting information unrelated to their app's functionality and by selling your data to third-parties.

Consumers must pay more attention to this as well as the very real issue of fake apps, warns Riaan Badenhorst, general manager of Kaspersky in Africa.

"Many of us download applications for various reasons, be it entertainment, education, nutrition, fitness or just to make your day-to-day life a little bit more convenient. However, do you really know what information your apps are collecting on you or if the app you have downloaded is indeed real or fake?" suggests Badenhorst.

We all have been warned against downloading apps from untrusted sources due to the high risk of getting hacked or infecting the device with malicious viruses.

It is always recommended to use official app stores, as all apps in the store go through rigorous multistep checks and

approvals before being published, and as such is usually considered a safer option for downloading software. However, while security measures are always taken, nothing is 100% safe, and from time to time malware distributors manage to sneak their apps into official stores.

“Last year, Kaspersky experts discovered a money-stealing malware called MobOk hiding within seemingly legitimate photo editing apps, available on the Google Play store. At the time of detection, the apps, titled ‘Pink Camera’ and ‘Pink Camera 2’ had been installed around 10,000 times,” adds Badenhorst.

“The apps were designed to collect and steal personal information from victims and use that to sign them up to paid subscription services. Victims only discovered they’d been hit when they saw unexpected costs on their mobile services bill. Of course, since then, the apps have been removed from the Google Play store and are no longer available.”

This is just one of the many incident’s users may find themselves in, even if the source used to download the app on is deemed trustworthy.

Clean up

So, with the start of the New Year, let’s clean up our devices, remove old apps and take further precautions when downloading new apps in 2020.

Here are some tips on how you can do this:

- not download apps to your smartphone straight away. Read user reviews of the app - they can contain valuable information about its behaviour. Look for information about the developer; perhaps past creations were removed from the store, or the app is linked to some dubious stories.

- Install system and application updates as soon as they are available - they patch vulnerabilities and keep devices protected.
- Read user reviews with caution. Keep in mind that some ‘shady’ developers may flood their pages with positive reviews, so look for reviews of a decent length (not simply “Great app!” after “Great app!”) that use natural-seeming language and have a legitimate feel.
- Make it a rule to rid your Android smartphone or tablet of unnecessary programs once every few months. The fewer apps on the device, the easier it is to monitor and control them and the information they can collect.

- Use a reliable security solution - this will provide you with an added layer of protection from malicious apps that the app store moderators may miss.

“While applications have changed the way we live and what we use our devices for, it is still important to remember that your safety and security comes first. Compromising your personal data can lead you into ‘hot waters’ and in some cases, recovery of your data can be a long journey. Therefore, it is important to always be alert and careful when downing apps – ensure the app is legitimate and have an understanding of what the app will use your information for before you just provide the permissions. Following these steps will support a safe online experience,” concludes Badenhorst.