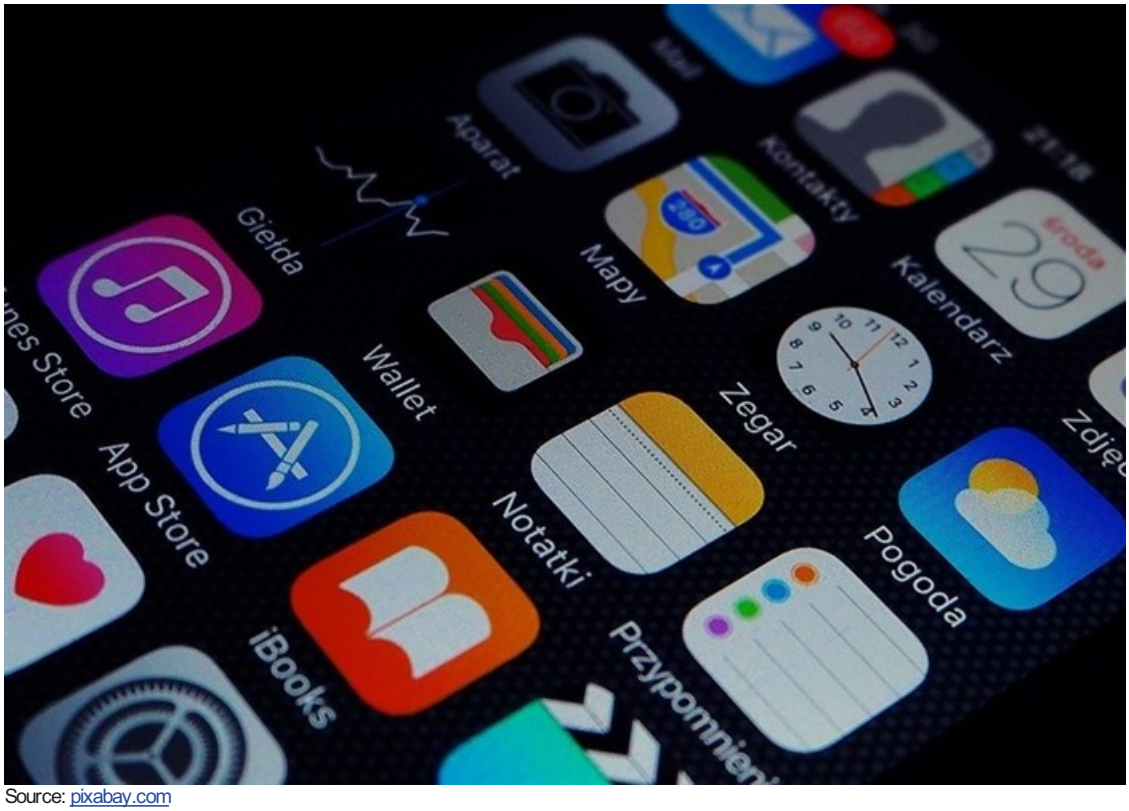
BIZCOMMUNITY

App permissions can be used to exploit your data

By Simon Campbell-Young

26 Oct 2018

Every time an application is installed on a device, the user is asked to allow that app certain permissions.



Source: pixabay.com

These range from being able to view your contacts, to using your camera and microphone, tracking your location, and many, many more. While some of these permissions are necessary in order for the application to function, others are not necessary in the slightest and are only there to gather and exploit the user's sensitive information.

Irrespective of the platform, applications offer great insight into the user, and this data is of great interest to marketers and businesses, but also cybercriminals.

However, on both Android and OS, users are required to give permission to any access, which is why he says carefully reading the list of permissions the apps request is crucial.

> *"Ask yourself if there is a legitimate reason an application might need camera access, for example, or why it would need to track your location. If it isn't necessary, be suspicious. In addition, some apps give the user the option of signing in through a social media platform such as Google, Twitter or Facebook. Here too, check the fine print to make sure you fully understand what information you are handing over."*

Certain apps are fairly cunning with their permissions, asking for those that although do not seem strictly necessary, could have a legitimate need.

If in doubt, ask the developers. Certain apps will also have an explanation of permissions requested in the developer notes, others don't. A good way to suss out the app and see if there have been major issues or privacy violations is to check out the reviews written by users. If too many are bad, then err on the side of caution and don't install the app.

Review your app permissions

It's also wise to review your application permissions on a regular basis.

This is done through the application settings, and is fairly straight forward. Clear out any unused applications too, but remember that removing an application from your device isn't always enough. If you have opted to connect via a social media service, you need to recheck your permissions even after you have uninstalled the app in question.

Then there's the question of people finding ways to bypass certain application functionalities. Take Snapchat for example. Snapchat is one of the most popular and highly rated apps available on both iOS and Android platforms, and has captured the information of today's youth, with its combination of timed photos and videos, and the access it gives to famous and interesting people.

One of the reasons it has become so popular is because messages sent between users self-destruct after a short time, making it the ideal platform to send salacious selfies.

However, there are ways around this - it is possible to take a screenshot of the message. When this happens the sender is notified, but not much else. Moreover, there are several apps available that have been designed to evade this alert, which is giving rise to a slew of security and privacy issues.

So even the most diligent of users can still be in danger. Also, applications have bugs and issues from time to time. No one is accusing them of malice here, but technological issues can see information being exposed or handled in an insecure manner. We do see permission issues boil down to honest mistakes too.

But not always. There have been several cases where apps have been caught selling users' location data, even after the user has specifically opted out of sharing their location with the app. There are many other cases of malicious apps slipping through the security cracks on legitimate play stores and marketplaces. Ultimately it is up to the user to be as vigilant as possible. Check and check those permissions again, and review them regularly.

ABOUT SIMON CAMPBELL-YOUNG

Having started his career as a startup partner for FSA Distribution in 1990, Simon Campbell-Young went on to start his own company called Memtek Distribution in 1995. This was sold to a public company called Siltek Holdings between 1998 to 2000. Shortly thereafter, he took his experience in the technology sector, garnered over more than 23 years, to form specialist distribution company Phoenix Distribution in 2000.

- Adding threat intelligence to the security mix - 26 Nov 2018
- Digital forensics is crucial to the security chain - 6 Nov 2018
- App permissions can be used to exploit your data - 26 Oct 2018
- 57 million riders, drivers affected by Uber breach - 13 Dec 2017
- Prevention through awareness - 12 May 2014

View my profile and articles...