Large Data Breach on an Android Marketplace Exposes Millions of User Names and Passwords

April 21, 2020 - The vast majority of Android users get their apps from Google Play, which is Google's Android marketplace. But there are actually numerous other marketplaces for apps, and some good reasons to use them. One of the largest is Aptoide. And they have apparently just experienced a data breach involving 39 million of its 150 million customers.

If you have never used an alternate source for your Android apps, then you might wonder why anyone else would. The answer is because Google and your phone carrier (which regulates the apps available to you via their version of Google Play) won't allow certain apps to be available for you to use. A good example of this is for tether apps - which allow you to share your phone's connection for data use.

Carriers love to charge monthly fees for tethering; usually around $10 per month. But there are apps you can purchase outright... like Easytether Pro... which allow you to tether your phone without paying any new monthly charges. It's no wonder that you won't find most of these in your carriers Google Play store. They want you to pay these fees.

There are also apps for business that your carrier might not be too happy with. Just one example is an app called BulkSMS. This allows you to take a list of people and send them all individual text messages in rapid succession. If you have a database of customers that have given you permission to text them and an unlimited text plan from your phone carrier, it provides a very inexpensive way to maintain regular contact with them. Again, you are very unlikely to find this app on Google Play.

With these examples in mind, it's easy to see why millions of users look for alternate sources for phone apps. The chances are that if there is something you want to accomplish with your phone, there is already an app for it, but you may have to search to find it.

In the case of Aptoide, the platform was apparently hacked and the records of 39 million customers were taken. To make matters worse, the hackers involved have not published a list of 20 million of these records which includes user login emails and passwords. Aptoide users are advised to change their passwords immediately.

A word of caution here. Downloading apps you arenâ€™t familiar with from third party app stores like Aptoide can be dangerous. Even Google Play has had issues with apps that have turned out to include malware in them, but at least they check their apps regularly. Not all third party sites do. If you are considering using an app from one of these sites, do some research first and make sure it is legitimate. Not doing so could allow a malicious hacker to gain access to anything else on your phone, including bank and credit card data, your pictures and pretty much anything else you have stored there. It can be very dangerous even for experienced users, so proceed with extreme caution.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS