

These Apps Will Steal Your Facebook Password and Cryptocurrency

If you have one of the apps installed below, remove it from your phone right away to protect your Facebook account and cryptocurrencies.

According to the latest report, some apps on Google Play are capable of performing malicious acts such as stealing user credentials and other sensitive data, including private keys. The worrying thing is that the number and popularity of these types of applications is increasing day by day, with some even being downloaded more than 100,000 times.



Some apps you should remove immediately include: Daily Fitness OL, Enjoy Photo Editor, Panorama Camera, Photo Gaming Puzzle, Swarm Photo, Business Meta Manager, Cryptomining Farm Your Own Coin.

They all carry the spyware (spyware) Facestealer, discovered since July 2021. Facestealer steals Facebook information from users through malicious apps on Google Play, then uses it to infiltrate Facebook accounts, serving purposes such as scams, fake posts, advertising bots. Similar to the Joker malware, Facestealer changes its code frequently and has many variations.

Since being denounced until now, they have continuously appeared on Google Play under different guises. TrendMicro's database records more than 200 variations of Facestealer's applications. For example, Daily Fitness OL is ostensibly a fitness app, but its goal is to steal Facebook information. Once the application is launched, it

sends a request to `hxxps://sufen168[.]space/config` to download the encryption configuration. When the user logs into Facebook, the application opens a WebView browser to load the URL from the downloaded profile. Next, a piece of JavaScript code is embedded in the web page to get the login data. After the user is successfully logged into the account, the application collects the cookie, then encrypts all the personally identifiable information (PII) and sends it to the remote server.

The 7 apps were all removed from Google Play by Google shortly after receiving TrendMicro's notification about their real purpose and potential for data theft. However, for those who have installed one of the above applications, what to do now is to quickly change the password of Facebook or other accounts and services.

In addition, TrendMicro also detected more than 40 fake cryptocurrency mining applications, which are variations of previous malicious applications. They trick users into buying paid services or clicking on ads with offers of generous amounts of cryptocurrency.

To avoid encountering malicious applications, users should carefully read reviews from people who have downloaded them before. However, this is also not the optimal solution because many applications will hire highly appreciated services, for example, Photo Gaming Puzzle is rated 4.5 stars, and Enjoy Photo Editor 4.1 stars. Enjoy Photo Editor surpassed 100,000 downloads before being removed.

You finished reading the article "**These Apps Will Steal Your Facebook Password and Cryptocurrency**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.