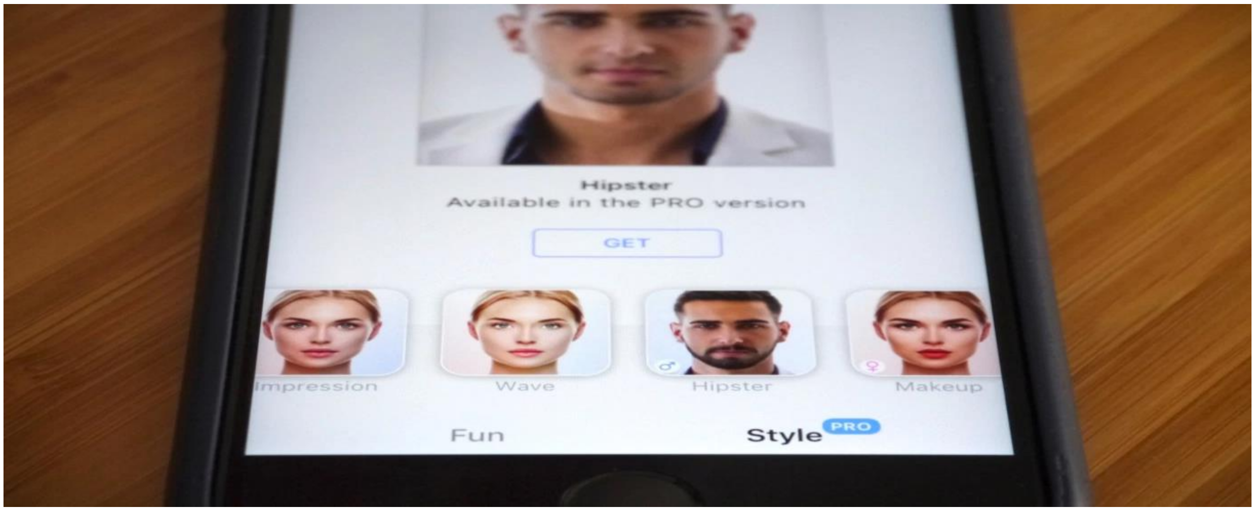
FaceApp trends todays Community Quarantine, is this safe?



FaceApp is a photo and video editing application for iOS and Android developed by Wireless Lab, a company based in Russia. The app generates highly realistic transformations of human faces in photographs by using neural networks based on artificial intelligence. The app can transform a face to make it smile, look younger, look older, or change gender.

All netizens who are already addicted to the use of Faceapp due to the annoyance of the Quarantine Community. Faceapp users who have been developing from abroad, not to put personal information on social media accessible to other users and used in any cybercrime activities.

This week, the keyword “FaceApp” trended again on local Twitter with more than 30,000 tweets after online users including personalities and government officials used the app and shared their edited photos on social media. The app’s gender-swapping features became the new highlight as users shared what they look like should they alter their sexual orientations. Local officials who participated in the trend include Manila Mayor **Isko Moreno**, Kabataan Rep. **Sarah Elago** and Cabinet Secretary **Karlo Nograles**.

However, some Filipinos warned against the consequences of exposing their data to a mobile program.

One Facebook user noted that it was only weeks ago when the sudden emergence of clone or dummy accounts on the social media giant caused public alarm.

“We leaped from Facebook fake accounts scare to giving our data to FaceApp…in less than two weeks,” Facebook user Justine Balane said.

Election lawyer Emil Marañon III also reminded his followers that photos are also personal data that they shouldn't give away easily.

"Dear friends, don't forget that your facial features are DATA. Just like passwords or addresses, you don't just submit them to a random app even if in exchange for something really really cool," he said.

As such, the Face App can access all user personal data such as e-mail accounts, credit cards and passwords of certain social media accounts. This would also provide a hacker with information that can be used to create fake accounts and cybercrime. In addition, the user's personal information may be retrieved and only upon installation is there a security risk.

When downloading applications, we recommend that users take the following precautions:

* Make sure the app is reliable and is downloaded from official websites

* Read the privacy terms to understand what information is being requested

* Treat facial recognition like a password - don't use it everywhere

* Always check the permissions being requested, such as the login associated with an existing account in a certain social network.

References:

- https://www.interaksyon.com/trends-spotlights/2020/06/19/171127/what-happens-when-you-share-photos-on-editing-apps-like-faceapp/
- http://www.ndbcnews.com.ph/news/faceapp-tiktok-delikado-may-security-risk-ayon-sa-pnp-12-cyber-crime-unit-chief
- http://techandlifestylejournal.com/faceapp-possible-security-issues/
- https://manilastandard.net/tech/tech-news/326498/new-faceapp-no-malicious-elements-but-users-must-be-careful.html