Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 168

ACG-CSB 072219168

Reference Number ACG-CSB 072219168

Be Wary of an Online Application on Social Media Known as "Face App"

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as "Restricted" pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

FaceApp is a photo-morphing app that uses what it calls artificial intelligence and neural face transformations to make creepy, hilarious, weird, and sometimes fascinating alterations to faces. The app can use photos from persons library or from a photo within the app.

FaceApp allows users to put an age filter on any photo and show how they will look after 40 years. There are millions of people to include the Filipino netizens who are transforming their current photo using the said app and these people are also sharing these photos on social media.

The app can scan photo from the person's library and pull out only the photos that feature faces. It uses server-side technologies to process the said photos and add its creepy-cool filters then uploaded it to the FaceApp's servers.

When FaceApp is downloaded, the person is asked of a piecemeal series of questions, carefully framed to shift responsibility away from corporate actors and onto the user like questions of "Do you consent to having your photo taken?" and "Do you permit access to your device and to your photos?". Privacy policies always frame the terms of service as personal consumer choices.

The choice to download and upload is to the users, but the consequence is far-reaching. Data collected for one purpose can always be used for another. Some of the worst misuses of face data come from one bad actor seizing on thousands of people who, as far as they knew, agreed to take on the responsibility themselves.

Once something is uploaded to the cloud, the sender lost control of it. And with so many breaches, cyber criminals can get information and be able to create a database of people all over the world with information without the consent of the targeted people by the culprit.

FaceApp's terms and conditions states, "You grant FaceApp a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you." By using the services, the users agree that the user content may be used for commercial purposes."

If the FaceApp data falls into the wrong hands, it can be used to sketch an extensive profile of the user's online behavior. The collected photos and the identification code of the phone can be linked to data from, for example, data leaks, to identify the user's interests. Even leaked e-mail addresses, credit cards and passwords can be linked to this profile. Such data can be misused for identity theft or espionage.

RECOMMENDATION

The public are advised to follow these tips in order to avoid the risks of using FaceApp, to wit:

- Download apps from trusted sources. Read the reviews and ratings of the apps as well as the terms and conditions;
- Remove apps that are no longer use in order to prevent Wireless Labs from collecting new data from you;
- Update your operating system's software as soon as updates are made available from the software company. Cybercriminals tend to exploit security holes in outdated software programs;
- Avoid simply clicking "next" during an app installation; and
- Pay attention to the list of permissions of FaceApp apps are requesting.

For additional information, please refer to the following websites:

- https://www.imore.com/faceapp
- https://www.theatlantic.com/technology/archive/2019/07/faceapp-mess/594361/
- http://www.interaksyon.com/trends-spotlights/2019/07/18/152122/faceapp-russia-data-privacy/
- https://www.digitaltrends.com/news/faceapp-photos-privacy-terms-of-service/
- https://businessmirror.com.ph/2019/07/19/kaspersky-detects-fake-faceapp-app-warns-users/

POINT OF CONTACT

Please contact PMAJ ANGELICA STARLIGHT L. RIVERA, Asst. Chief, ARMD thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.