Scams emerge following FaceApp hype

The latest hype around the FaceApp application has attracted scammers who want to make some quick profits, ESET research has shown.

A YouTube video claiming to offer a link for downloading the installation package (APK) for a "FaceApp Pro" application for Android

Scammers have been using a fake "Pro" version of the application as bait and have made an effort to spread the word about this fictitious version of the viral app. One form of the scam uses a fake website that claims to offer a premium version of FaceApp. The second type of scam includes YouTube videos promoting download links for a "Pro" version. One of the fraudulent YouTube videos had over 150,000 views at the time of writing this research.

The legitimate FaceApp application offers various face-modifying filters and is available for both Android and iOS. While the app itself is free, some features marked as "PRO", are paid. Along with the viral potential of its popular filters, FaceApp has of late, generated a huge wave of media attention amid concerns about online privacy.

In one of the scams that have emerged see attackers use a fake website that claims to offer a premium version of FaceApp. In reality, the scammers trick their victims to click through countless offers for installing other paid apps and subscriptions, ads, surveys and so on. The victim also receives requests from various websites to allow the display of notifications. When enabled, these notifications lead to further fraudulent offers. The YouTube videos contain download links that point to apps whose only functionality is to make users install various additional apps. The shortened links could lead to users installing malware as well.

“There were well over 200-thousand stories online [...] about the fake and fictitious FaceApp Pro. Only one of the YouTube videos we found had more than 150,000 views, however, its malicious links were clicked over 90,000 times,” says ESET Researcher, Lukáš Štefanko.

“Legitimate businesses don’t even dream of such high click-through rates as these cybercriminals have been able to achieve,” he states.

Before joining the hype, users should remember to stick with basic security principles. Regardless of how exciting the ‘opportunity’ seems, avoid downloading apps from sources other than official app stores, and examine available information about the app (developer, rating, reviews, etc.). As insurance in cases where the user falls victim to a scam, having a reputable security app installed on a mobile device can help prevent some negative consequences.