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 209

ACG-CSB 052521209

Reference Number ACG-CSB 052521209

UNDERSTANDING THE RISK OF FLEECEWARE

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

Fleeceware scams promise free subscription trials but deliver costly charges to victims. Researchers have discovered a total of 204 fleeceware applications with over a billion downloads and over $400 million in revenue on the Apple App Store and Google Play Store. The purpose of these applications is to draw users into a free trial to "test" the app, after which they overcharge them through subscriptions which sometimes run as high as $3,432 per year. These applications generally have no unique functionality and are merely conduits for fleeceware scams. Avast has reported the fleeceware applications to both Apple and Google for review. The fleeceware applications discovered consist predominantly of musical instrument apps, palm readers, image editors, camera filters, fortune tellers, QR code and PDF readers, and 'slime simulators'. While the applications generally fulfil their intended purpose, it is unlikely that a user would knowingly want to pay such a significant recurring fee for these applications, especially when there are cheaper or even free alternatives on the market.

It appears that part of the fleeceware strategy is to target younger audiences through playful themes and catchy advertisements on popular social networks with promises of 'free installation' or 'free to download'. By the time parents notice the weekly payments, the fleeceware may have already extracted significant amounts of money.

Fleeceware is a recently coined term that refers to a mobile application that comes with excessive subscription fees. Most applications include a short free trial to draw the user in. The application takes advantage of users who are not familiar with how subscriptions work on mobile devices, meaning that users can be charged even after they've deleted the offending application.

A majority of the applications has discovered lure users in with a promise of a free three-day trial, attaching a subscription that commences at the end of the trial. Once the trial is over, the user is charged a recurring high subscription fee, generating

substantial revenue for the developers. Importantly, uninstalling the application doesn't cancel the subscription — as a result, the user is likely to be charged further until they cancel the subscription within their device's app market settings. There's also the possibility that users forget to cancel the free trial, resulting in expensive fees. Either way, these scams make use of deceptive behavior that relies on the user not being informed about how subscriptions work and draws them into the scheme through a free trial.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the risk of **FLEECEWARE**:

- Be careful with free trials of less than a week. Applications that offer free three-day trials should be handled with caution;
- Familiarize yourself with the conditions of what you're subscribing to, even if it's a free trial. A closer look will likely reveal the true price of the app;
- Be sure to check app reviews carefully;
- Secure your payments. Ensure that your payment methods are locked behind a password or biometric check. This can prevent accidental subscriptions by children as well;
- Keep track of your subscriptions; and
- Discuss the dangers of fleeceware with your family. Educating children on how to avoid potential scams.

For additional information, please refer to the following websites:

- https://blog.avast.com/fleeceware-apps-on-mobile-app-stores-avast
- https://www.securemac.com/blog/what-is-fleeceware

POINT OF CONTACT

Please contact **PMAJ ROVELITA ROBIÑOS AGLIPAY** Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632)7230401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.