1. Want to Earn a Few Extra Bucks? A First Look at Money-Making Apps

Yangyu Hu (1); Haoyu Wang (1); Li Li (2); Yao Guo (3); Guoai Xu (1); Ren He (1)

Source: *2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER). Proceedings*, p 332-43, 2019; **ISBN-13:** 978-1-7281-0591-8; **DOI:** 10.1109/SANER.2019.8668035; **Conference:** 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), 24-27 Feb. 2019, Hangzhou, China; **Publisher:** IEEE, Piscataway, NJ, USA

Author affiliation: (1) Beijing University of Posts and Telecommunications, China (2) Monash University, Melbourne, VIC, Australia (3) Peking University, China

Abstract: Have you ever thought of earning profits from the apps that you are using on your mobile device? It is actually achievable thanks to many so-called money-making apps, which pay app users to complete tasks such as installing another app or clicking an advertisement. To the best of our knowledge, no existing studies have investigated the characteristics of moneymaking apps. To this end, we conduct the first exploratory study to understand the features and implications of money-making apps. We first propose a semi-automated approach aiming to harvest money-making apps from Google Play and alternative app markets. Then we create a taxonomy to classify them into five categories and perform an empirical study from different aspects. Our study reveals several interesting observations: (1) moneymaking apps have become the target of malicious developers, as we found many of them expose mobile users to serious privacy and security risks. Roughly 26% of the studied apps are potentially malicious. (2) these apps have attracted millions of users, however, many users complain that they are cheated by these apps. We also revealed that ranking fraud techniques are widely used in these apps to promote the ranking of apps inside app markets. (3) these apps usually spread inappropriate and malicious contents, while unsuspicious users could get infected. Our study demonstrates the emergency for detecting and regulating this kind of apps and protect mobile users. (0 refs)

Inspec controlled terms: data privacy - fraud - invasive software - mobile computing - program diagnostics
Uncontrolled terms: money-making apps - app users - alternative app markets - studied apps
Classification Code: C6130S Data security - C6150G Diagnostic, testing, debugging and evaluating systems - C6190V Mobile, ubiquitous and pervasive computing
IPC Code: G06F9/44 - G06F11/36 - G06F21/00
Treatment: Bibliography (BIB) - Practical (PRA)
Database: Inspec
Data Provider: Engineering Village