

1. Dating with Scambots: Understanding the Ecosystem of Fraudulent Dating Applications

Yangyu Hu (1); Haoyu Wang (1); Yajin Zhou (2); Yao Guo (3); Li Li (4); Bingxuan Luo (1); Fangren Xu (5)

Source: *IEEE Transactions on Dependable and Secure Computing*, v 18, n 3, p 1033-50, 2021; **ISSN:** 1545-5971;

DOI: 10.1109/TDSC.2019.2908939; **Publisher:** IEEE Computer Society, USA

Author affiliation: (1) Beijing University of Posts and Telecommunications, China (2) Zhejiang University, China (3) Peking University, China (4) Monash University, Clayton, VIC 3800, Australia (5) Rivermont Collegiate, Bettendorf, IA 52722, United States

Abstract: In this work, we are focusing on a new and yet uncovered way for malicious apps to gain profit. They claim to be dating apps. However, their sole purpose is to lure users into purchasing premium/VIP services to start conversations with other (likely fake female) accounts in the app. We call these apps as fraudulent dating apps. This paper performs a systematic study to understand the whole ecosystem of fraudulent dating apps. Specifically, we have proposed a three-phase method to detect them and subsequently comprehend their characteristics via analyzing the existing account profiles. Our observation reveals that most of the accounts are not managed by real persons, but by chatbots based on predefined conversation templates. We also analyze the business model of these apps and reveal that multiple parties are actually involved in the ecosystem, including producers who develop apps, publishers who publish apps to gain profit, and the distribution network that is responsible for distributing apps to end users. Finally, we analyze the impact of them to users (i.e., victims) and estimate the overall revenue. Our work is the first systematic study on fraudulent dating apps, and the results demonstrate the urge for a solution to protect users. (0 refs)

Inspec controlled terms: chatbots - computer crime - data privacy - fraud - Internet - mobile computing - software agents

Uncontrolled terms: user protection - distribution network - predefined conversation templates - chatbots - account profiles - three-phase method - systematic study - scambots - ecosystem - malicious apps - fraudulent dating applications

Classification Code: C6130S Data security - C7210N Information networks - C6190V Mobile, ubiquitous and pervasive computing

IPC Code: G06F9/44 - G06F21/00 - G06N20/00

Treatment: Practical (PRA)

Database: Inspec

Data Provider: Engineering Village

Copyright 2021, The Institution of Engineering and Technology