BUGFRAUD MOBILE

ONLINE FRAUD PREVENTION IN THE MOBILE BANKING ERA

With a penetration of 42% and a yearly global growth rate of over 3%*, **Mobile banking has come to stay** and is now the target of fraud attacks.

Mobile banking needs to face all the security risks resulting from User Impersonation (ATO) or Malware attacks against banking Apps like:

- ✓ **SMS Grabber**
- ✓ **Smishing**
- ✓ **App Overlay**
- ✓ **RitM (RAT in the Mobile)**

Because of our unique **user-centric approach** to fighting fraud powered by **Deep learning** technology, **bugFraud Mobile** is able to identify even the most sophisticated cyber attack on mobile banking.

* Source: GlobalData Annual Retail Banking Insight Survey 2018

BENEFITS

CONTINUOUS USER SESSION MONITORING

Our Deep Learning algorithms analyze dozens of sensor parameters collected from the user's behavior, device and environment (finger size, pressure, speed, gestures, typing fluency, gyroscope position, OS, geolocalization, etc.) in order to identify any attack attempt or possible anomaly during their banking transactions.

MALWARE PROTECTION

Prevent targeted attacks resulting from malware in your device or App, such as Screen Overlay, App overlay, Data loss and others, preventing fraud before it happens.

USER EXPERIENCE IMPROVEMENT

Due to its lightweight technology and continuous behavioral monitoring, bugFraud Mobile can help to enhance your user experience by reducing enrollment processes and Multi-Factor authentication challenges.

REAL-TIME VISIBILITY

Know Who, How, When and Where abnormal user events are happening at all times so you can take the proper actions before fraud is committed.

KEY FEATURES

DEVICE FINGERPRINTING

User profiling including a list of common devices used and a risk analysis of each of them

USER BEHAVIORAL BIOMETRIC PROFILING

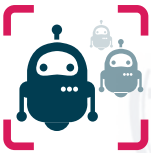
A unique physical and behavioral profile associated with each user that detects any deviation from normal operations.

USER ENVIRONMENT ANALYSIS

User connection pattern analysis: Country, WiFi id, geolocalization, etc.

EMULATOR & MALICIOUS APP DETECTION

Our intelligence is able to detect when the user's mobile is infected by Malicious apps and differentiate real mobile sessions from emulations running in other kinds of devices



BOTS DETECTION

A dedicated anti bot engine differentiates bot activity from legitimate human traffic

FRICTIONLESS UX & EASY-FAST DEPLOYMENT

Our lightweight and super compatible technology is quick and effortless to integrate and does not impact your banking App user experience

HOW DOES BUGFRAUD MOBILE WORK?

bugFraud Mobile technology is concentrated in a **lightweight SDK library** which, once included in your banking App, is able to collect user behavior, mobile device and environment information parameters running in your App in order to, later on, aggregate, correlate and analyze this information in the bugFraud Deep Learning Intelligence cloud.

The result of this operation is a **Risk analysis rate** that will help your bank to take (in real-time) the proper actions while the user session is running.

This entire process is carried out without requiring or collecting **any confidential or private information** from the user and always treating it as **anonymized data**.