# BIOCATCH™

USING BEHAVIOURAL BIOMETRICS TO COMBAT SOCIAL ENGINEERING VOICE SCAMS AND APP FRAUD

HOW BIOCATCH DETECTS A SOCIAL ENGINEERING SCAM

- Detects behaviours that suggest the person is taking instruction to conduct a transaction
- Analyses the prevalence of known risky behaviours in confirmed fraudulent sessions versus how legitimate transactions are handled
- Generates a VoiceScam indicator in real-time
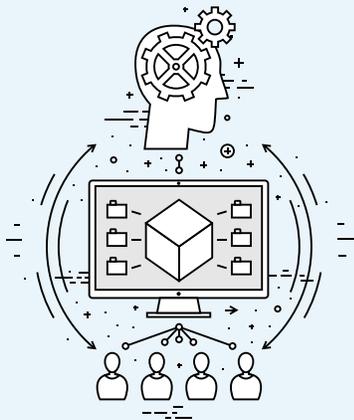
According to a recent report by the UK Finance organization, in 2019 UK Finance members reported 168,376 incidents of Authorised Push Payment (APP) scams over web and mobile channels with gross losses of £379.1 million. This is a 19% increase for web and a 261% increase for mobile from 2018.

The problem is most acute in the UK but is not limited to that country. These types of scams are on the rise everywhere. The European Commission has revealed that it is looking into ways to address this vexing challenge. In the U.S., the Federal Trade Commission has reported that 77% of its fraud complaints involve contacts by telephone, of which social engineering scams is a subset. Most recently, the Australian Taxation Office has issued a warning on the rise of this threat.

Social Engineering Voice Scams: How They Work

Using this tactic, criminals manipulate people into transferring money by posing as a representative from a legitimate organisation such as a bank, the police, a utility company or government official. To persuade people to act, the criminal often claims that there has been suspicious activity on an account and that the customer must take immediate action. The criminal's goal is then to coerce people into moving money into the criminal's account by claiming that the money needs to be transferred to a 'safe account'.

ANATOMY OF A SOCIAL ENGINEERING SCAM

1 Fraudster obtains legitimate user information on the dark web

2 Fraudster calls victim and pretends to be an official from a bank or government agency

3 The fraudster convinces the victim that there is an urgent need to transfer funds

4 The victim logs into their bank account

5 The fraudster dictates instruction to the user on the details of the transfer (i.e., payee, amount, etc.)
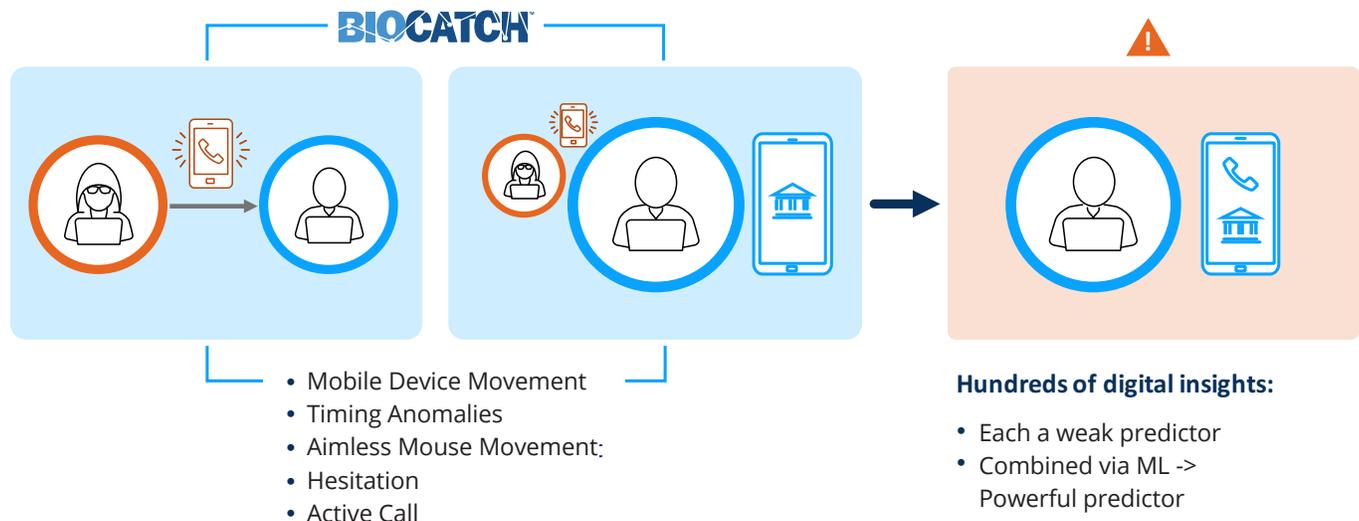
6 The victim completes the transfer

Why is it hard to detect a social engineering scam?

Social engineering voice scams are one of the hardest scams to detect because it essentially involves a person defrauding him or herself while under the influence of a con artist. Traditional fraud detection measures do not work in this instance – the legitimate person is logging in from their own device at the correct location conducting a fully authorised transfer. In addition, if asked for additional authentication credentials, the legitimate user will be able to provide them. So how can this fraud type be detected?

Leveraging advanced behavioural insights to detect a social engineering scam

BioCatch collects physical and cognitive user behaviours that are turned into powerful insights to identify fraud and identity theft. Analysis is done by profiling users based on physical traits such as typing, mouse movement, swiping and press, comparing current sessions to historical profiles to continuously authenticate users. In addition, BioCatch identifies legitimate usage patterns Vs those of cyber criminals, including human versus automated or bot activity. When session behaviors highly correlate with the known, legitimate user, but some behaviors in the session are abnormal, powerful indicators suggest a person is conducting a transaction under the influence of a fraudster. BioCatch's advanced behavioral Insights combine user and population level profiling to determine user intent and emotional state in context of the activity to detect complex situations indicating high levels of risk. When a user operates in an online account under the guidance of a voice scammer signs of duress and distraction are presented. By flagging these high risk activities in real-time, financial institutions can prevent significant losses and better protect their clients and assets.
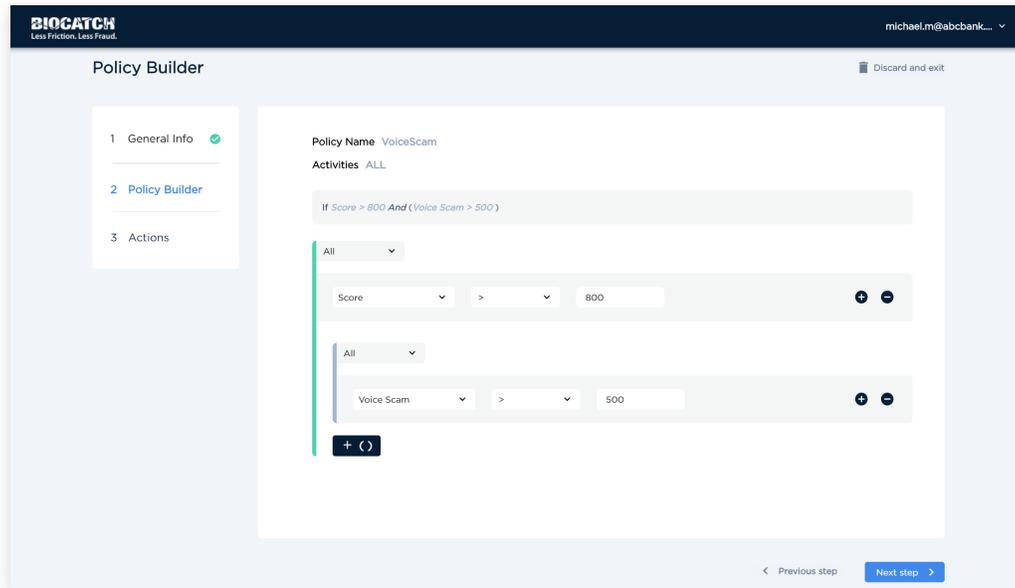
DETECTING VOICE SCAMS

- Mobile Device Movement
- Timing Anomalies
- Aimless Mouse Movement:
- Hesitation
- Active Call

Hundreds of digital insights:

- Each a weak predictor
- Combined via ML -> Powerful predictor

From detection to taking the appropriate action

Customers can use the BioCatch platform tools to investigate activities and determine the appropriate course of action for social engineering voice scams. Using the BioCatch Policy Manager, fraud analysts can set action policies that will decline or defer high risk transactions, rather than asking for additional authentication that the legitimate user is able to pass. Policies can also determine when cases should be created for fraud operators to review.

Finally, the BioCatch Analyst Station provides fraud analysts with visibility into the specific indicators that triggered and a running view of all sessions and their risk scores, and provides a powerful, visual picture of session activity, including all types of behavioural anomalies which are indicative of fraud.

BIOCATCH™

www.biocatch.com   info@biocatch.com   @biocatch   www.linkedin.com/company/biocatch

Tel Aviv | New York | Boston | London | São Paolo | Santiago | Mexico City | Melbourne | Mumbai