BioCatch

Case Study

Top 5 UK Bank Saves £500K per Month in Fraud Losses by Preventing Social Engineering Voice Scams Using Behavioral Insights

Problem

A top 5 UK bank experienced a growing increase in social engineering voice scams, also known as Authorised Push Payment (APP) fraud, despite heavy investment in both technology and talent. Making up a large portion of their monthly fraud losses, social engineering voice scams were costing the bank hundreds of thousands of pounds per month and damaging customer confidence and trust.

Solution

Although the bank had implemented a comprehensive fraud technology stack including transaction, device, and malware analysis, among other custom solutions, social engineering voice scams and highly sophisticated cybercriminals were successful in bypassing all controls. Seeking a precise solution, the bank worked alongside BioCatch teams to develop a behavioral approach to fight back.

Results

75%

Detection of social engineering voice scams*

£500K

Saved in voice scam fraud losses per month during a peak period

In the case of this top 5 UK bank, cybercriminals took advantage of a massive and public airline data breach to launch a wide-reaching social engineering campaign, leading to a significant increase in voice scam attacks. By spoofing the bank's phone number, the cybercriminals sent an SMS informing customers that their account had been compromised due to the airline breach. Within the SMS, customers were instructed to call "the bank" immediately. Once on the line, posing as a legitimate bank official and using the recent airline data breach as part of their narrative, the cybercriminal would convince the victim to transfer their total funds to a new, "safe" account.

Social engineering voice scams are one of the most difficult scams to detect because the device, location, network, and user are all genuine. In this scenario, because the legitimate user is conducting a fully authorized transaction, the bank's fraud detection tools and authentication methods were rendered futile, and cybercriminals were maximizing on this gap.

*Achievable detection rate at peak performance with the call status feature implemented

Anatomy of a Social Engineering Voice Scam

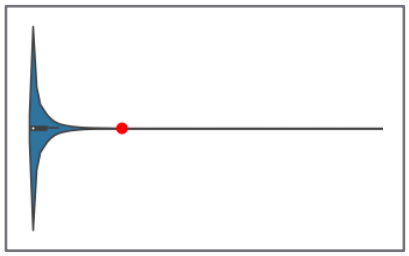
1. Fraudster obtains legitimate user information on the dark web
2. Fraudster calls victim and pretends to be an official from a bank or government agency
3. The fraudster convinces the victim that there is an urgent need to transfer funds
4. The victim logs into their bank account
5. The fraudster dictates instruction to the user on the details of the transfer (i.e., payee, amount, etc.)
6. The victim **completes the transfer**

Working Together to Build Stronger Fraud Protection

Social engineering voice scams quickly became a substantial part of this top 5 UK bank's fraud losses, costing them hundreds of thousands of pounds per month. Seeking relief, the bank looked to BioCatch for a solution. BioCatch teams worked closely with this top 5 UK bank to develop a social engineering voice scam machine learning model to tackle this emerging fraud threat.

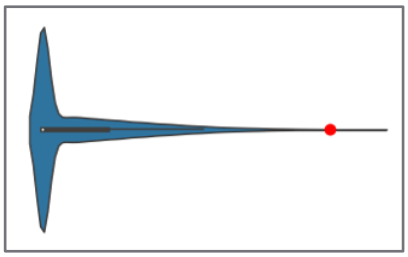
When applying behavioral biometrics to social engineering fraud scenarios where the genuine user is performing the transfer, the user's session behavior will show many consistencies when analyzed against their historical profile; however, because the user is under the guidance of a cybercriminal, their emotional state will have significantly shifted from their norm. For example, when a cybercriminal is speaking with the victim, there is always a sense of urgency conveyed. This can lead to the user feeling overwhelmed, distressed, and distracted which is displayed through behavioral anomalies that can be detected when analyzing how the user moves their mouse, types, and navigates during a voice scam session. When session behaviors highly correlate with the legitimate user, but some behaviors are abnormal, powerful indicators suggest a person is conducting a transaction under the influence of a cybercriminal.

In the following examples, user behavioral anomalies in a voice scam session are evident:



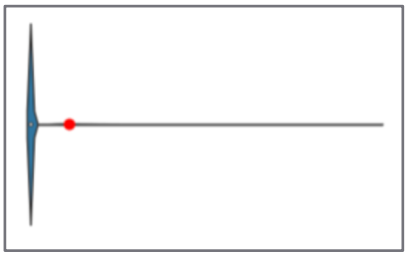
Number of doodle events post log in

The number of mouse doodles present during a voice scam session (**red dot**) is high when compared to the population, indicating distraction.



Amount of dead time post log in

The amount of dead time detected during a voice scam session (**red dot**) is abnormally high, indicating coercion.



Typing speed when adding new payee

The user's typing speed when inputting the payee's details in a voice scam session (**red dot**) is anomalous, indicating hesitation.

Using Behavioral Insights to Prevent Voice Scam Transactions in Real Time

After deploying the BioCatch social engineering voice scam model, the bank detected 60% of voice scams at the model's peak. The bank is now planning to implement the latest voice scam detection capabilities including a call status feature that enables the BioCatch solution to detect if a user is on a call during a mobile banking session. Based on performance results in other customer environments, this is expected to deliver an additional 10-15% detection uplift and bring overall social engineering voice scam detection up to 70-75%.

By incorporating BioCatch behavioral insights including the voice scam risk score and indicators into their fraud protection flow, this top 5 UK bank was able to save between £250K-£500K per month across a four-month period when there was a significant increase in voice scam cases.

BioCatch

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Today, customers around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation and accelerate business growth. With nearly a decade of data, over 50 patents and unparalleled experience analyzing online behavior, BioCatch is the leader in behavioral biometrics. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch