BioCatch

Case Study

Top LATAM Bank Reduces Social Engineering Fraud Targeting Mobile Users by 67% with Behavioral Biometrics

Reward Customers with a Trusted & Seamless Mobile Banking Experience

Problem

A Top LATAM bank found their mobile banking customers increasingly targeted and victimized by social engineering scams. Despite increased efforts and technologies, social engineering continued to be the bank's top threat. The bank required a solution that would enable them to deliver a seamless and secure mobile banking experience.

Solution

The bank sought a solution that would help them tackle their number one pain - social engineering attacks. However, with over 80% of their consumer banking activities conducted on mobile devices, the bank required a robust mobile fraud detection solution that could protect their customers against a wide array of attack methods including social engineering scams, mobile emulators, malware, RATs, and more.

Results

>80%

Of social engineering fraud detected immediately following implementation

99.97%

Of mobile sessions remained completely frictionless

67%

Decline in social engineering fraud just months after deployment

A top LATAM bank experienced an increase in fraud threats targeting mobile users. Following more granular investigation, they found that social engineering was the criminal's preferred attack method, consistently making up 60-80% of the bank's global fraud.

With a large majority of user sessions conducted on mobile devices, the bank had previously implemented numerous preventative solutions to protect their web and mobile experiences alike, including an Anti-Money Laundering transaction monitoring solution and an OTP authentication solution.

However, the bank continued to see fraud go undetected at a much higher rate than their acceptable risk threshold. Even more important was the impact these fraud cases would have on the mobile banking experience. The bank had invested significantly in the mobile channel which was suffering due to the number of genuine transactions that required manual intervention.

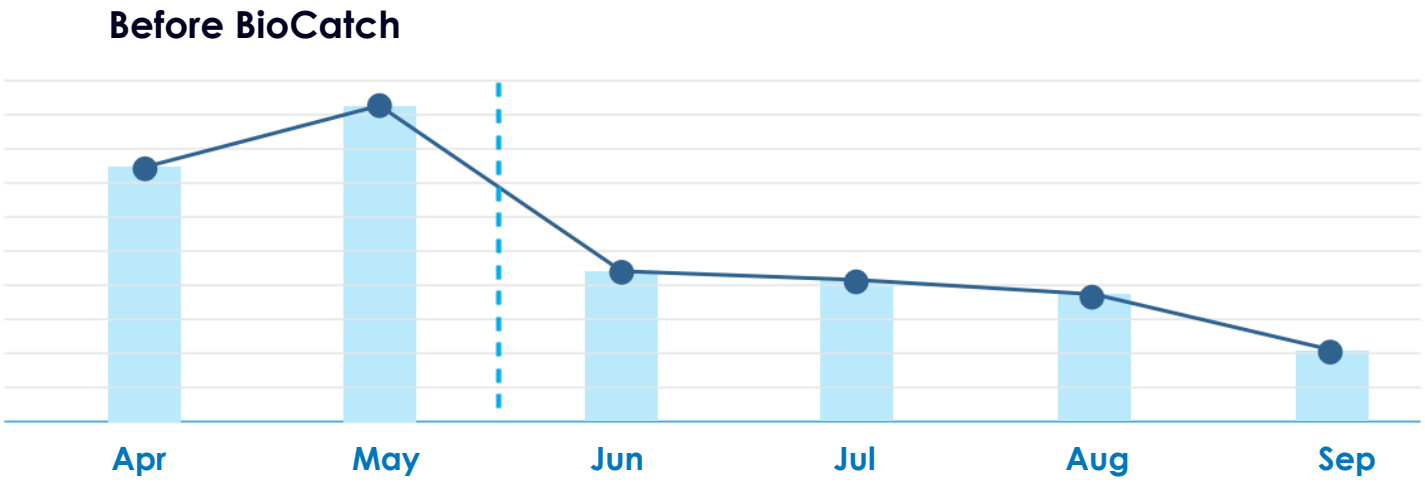
Social engineering threats come in many forms; in this case, cybercriminals obtained user banking credentials including other personal information such as the customer's telephone number and email address, most likely through purchase on the dark web. Since the bank required a one-time password for login, the cybercriminal would then employ social engineering to obtain the user's OTP. For example, a cybercriminal would call the user or send an SMS message reporting a mobile banking synchronization issue, prompting the user to provide their one-time password in order to initiate a resynchronize. With the user's credentials and one-time password in hand, cybercriminals could successfully conduct fraudulent transfers.

Protection that never sleeps

While the bank's transaction monitoring solution provided visibility into transaction-specific anomalies such as abnormal payment amounts, they lacked continuous session visibility. This significantly limited the bank's ability to achieve optimal fraud protection. Visualizing a user session as a timeline, the bank only had approximately a 60-second window that represents the transaction flow to determine if the session was genuine or not.

By deploying BioCatch behavioral biometrics to protect their mobile banking experience, the bank gained visibility beyond just the transaction stage. With continuous insight into user session activity and advanced profiling capabilities, the bank was able to better identify social engineering fraud by observing subtle behavioral anomalies and criminal indicators. After implementing BioCatch alongside the bank's pre-existing tools, the bank detected more than 80% of social engineering fraud. Further, over time the bank saw a steady decline in social engineering fraud and in just months following deployment, the bank achieved a 67% decline in social engineering fraud.

Social Engineering Fraud Count



67% Decrease in Social Engineering Fraud after Deploying BioCatch

Staying Ahead of Cybercrime

With cybercriminals seeing less success in their attempts to socially engineer their way into a user's bank account, they shifted to other attack methods. However, because the BioCatch platform analyzes user behavior against the user's historical profile as well as population profiles, the criminal mode of operation itself becomes less significant. By strongly relying on behavior, the bank succeeded in detecting many other types of fraudulent activity including malware, RATs, and mobile emulators, while maintaining an extremely low false positive rate between 0.15-0.21%.

Enabling a Frictionless Customer Experience

Due to the previous pains the bank experienced as a result of high false positive rates prior to deploying BioCatch including adverse impacts to customer experience, the bank required a solution that would enable their genuine customer base to go about their mobile banking activities without disruption. Further, to achieve this, the bank would not accept the idea of removing pre-existing mobile banking features, such as allowing mobile transfers.

Without making a single change to their mobile banking user experience, the bank leveraged BioCatch risk scores to drive an internal process where they only intervened at the highest risk level. For example, when BioCatch flagged a session at risk level 1000, the bank required the transaction to be done in-branch or using a different device. By limiting this high-friction process to extremely risky sessions, the bank only impacted approximately .03% of user sessions, meaning 99.97% of mobile banking sessions remained completely frictionless. These results were far greater than they had ever achieved before.