BioCatch

SOLUTION BRIEF

Advanced Behavioral Biometrics with Biocatch

BioCatch by the Numbers

2B+
Billion
Sessions analyzed each month

200+
Million
Global users protected

50+
Global patents granted

10x
Average ROI reported by customers based on fraud losses prevented

Solutions

BioCatch provides continuous protection across user sessions and visibility into risk for multiple use cases including:

Account Opening Protection

Detect the use of stolen or synthetic identities in filling out online applications to stop fraud at the source and detect positive behaviors to identify legitimate applications.

Account Takeover Protection

Distinguish between genuine users and criminals, whether human or automated such as bots, malware, or Remote Access Tools (RAT).

Advanced Social Engineering

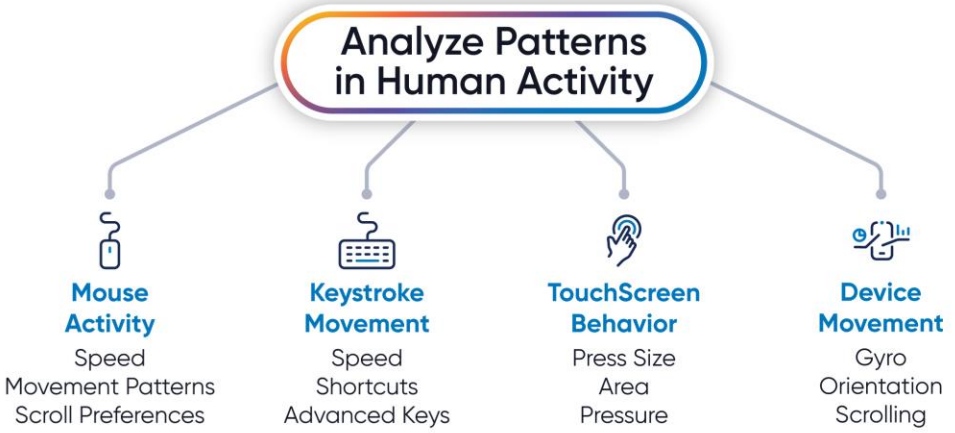
Identify real-time social engineering scams designed to coerce users into transferring money to fraudulent accounts while under duress by a criminal.

Overview

Customer experience is the hallmark of growing revenue in digital channels. However, that revenue can be threatened by losses sustained from new account fraud, account takeover and other cyber threats. As the volume of digital transactions surges, fraud and risk management leaders are tasked with building trust across a broad range of use cases, managing risk across digital channels, and limiting financial losses from cybercrime. BioCatch helps financial institutions and digital businesses to deliver a comprehensive fraud management strategy and build an online environment where customers feel safe to interact.

Behavioral biometrics analyzes a user's physical and cognitive digital behavior to distinguish between genuine users and criminals in order to detect fraud and identity theft and to improve customer experience. This is accomplished by profiling user behaviors such as mouse movements, typing cadence, swipe patterns or device orientation. The activity is then compared against the historical user profile for the individual account to provide a passive authentication layer and against population level patterns to identify statistically observed norms for "good" and "bad" behavior.

For example, cybercriminals input data differently from genuine users.



With over a decade of experience analyzing user interaction data, BioCatch offers out-of-the-box risk models that customers can leverage to gain actionable insights into fraudulent activity, realizing immediate value upon deployment.

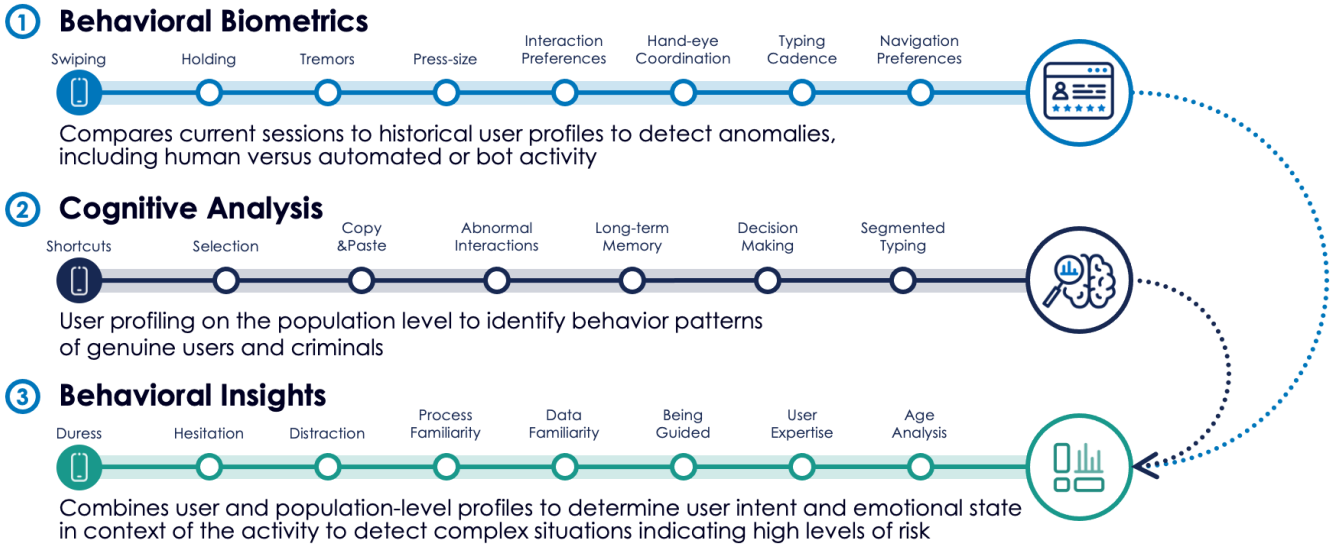
How Does It Work?

Frictionless Experience

Current fraud controls often treat customers like criminals, introducing additional friction into the user experience. This is especially true in the online account opening process where applications are deferred for manual review which can incur high operational costs. Behavioral biometrics delivers better detection of account opening fraud and ATO by understanding behavioral intent to identify illegitimate activity versus that of a legitimate applicant. False declines of applications and transactions are reduced by monitoring user digital behaviors to assess the risk of an activity and driving the appropriate action. The BioCatch solution is designed with customer experience in mind. It is invisible to the end user, allowing consumers to go about their banking activities while also being guaranteed maximum security. With the right tools in place, you can ensure that customer experience is prioritized, and the balance between trust and risk is properly calculated and aligned to business priorities.

Continuous Protection

Providing continuous protection is not only about reducing fraud losses but building trust in digital interactions. Unlike other fraud solutions, BioCatch provides truly continuous protection by collecting and analyzing data throughout the session, so even the most subtle changes within the session do not go undetected. The BioCatch Risk Engine is powered by machine learning algorithms that analyze physical and cognitive digital behavior of users across web and mobile channels. The model takes into consideration real-time physical interactions such as keystrokes, mouse movements, swipes, and taps. This data is used to profile and analyze a user's digital behavior **on three levels:**



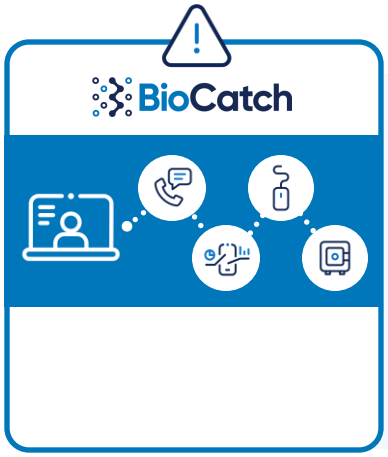
BioCatch analyzes each user session and delivers a risk score based on this deep user behavioral profiling. Depending on the risk score, organizations can initiate additional actions such as requiring step-up authentication or manual review. BioCatch also provides organizations with the top threat indicators to allow further visibility into risk. Confirmed fraud feedback is incorporated to continually enhance the accuracy of the model and adapt to new and emerging attacks. With over a decade of experience analyzing user interaction data, BioCatch offers out-of-the-box risk models that customers can leverage to gain actionable insights into fraudulent activity and realize immediate value upon deployment.

Actionable Intelligence

BioCatch delivers actionable intelligence and built-in tools to empower customers to align action with risk and minimize disruption to genuine users. In addition to the visibility provided through the risk score and top threat indicators, the BioCatch platform enhances investigation and decision making by analysts and business managers with the following tools:

- **Analyst Station** is used by analysts to gain deep visibility into the sessions to determine trends and attack vectors.
- **Case Manager** is used by case operators to determine whether activities were legitimate or fraudulent and provide feedback.
- **Policy Manager** tool enables the creation of configurable rules to automate actions based on risk scores and indicators.

BioCatch allows organizations to leverage the built-in platform tools or integrate BioCatch behavioral data into existing fraud management tools or case management systems through a robust set of APIs, so customers can manage fraud their way.



Building Customer Trust with Advanced Behavioral Biometrics

Advanced social engineering scams, such as authorized push payment scams, have become a growing concern among financial institutions. These scams cost UK banks more than £450 in 2019. Often, consumers are left with little or no recourse except an empty account. These attacks are difficult to detect because it is the legitimate user taking action or unknowingly providing access to a criminal. Traditional fraud prevention tools that use device-based or activity-based controls are unable to detect such attacks. Behavioral biometrics looks at hundreds of risk indicators that signal latency, hesitation, distraction and other user behaviors that indicate a customer may be acting under the direction of a criminal.

BioCatch

BioCatch is the leader in Behavioral Biometrics which analyzes an online user's physical and cognitive digital behavior to protect individuals and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of analyzing data, over 60 patents and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch