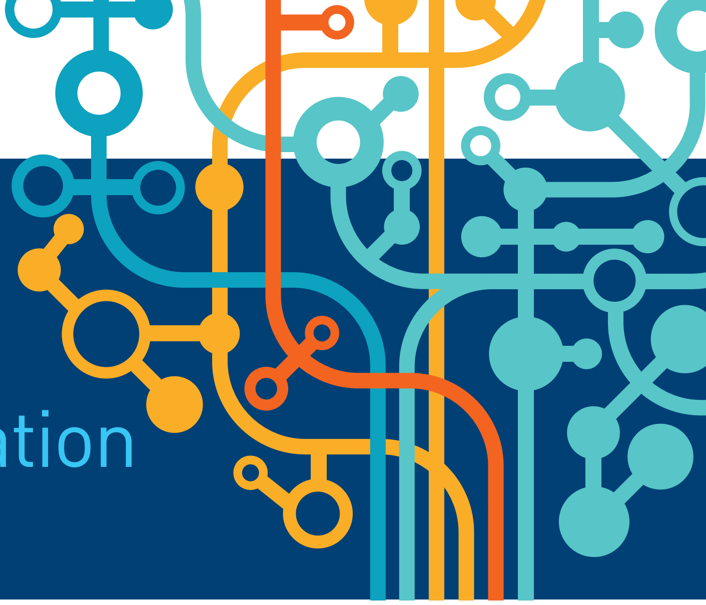
Less Friction. Less Fraud.



Real-Time Fraud Detection Through Continuous Authentication

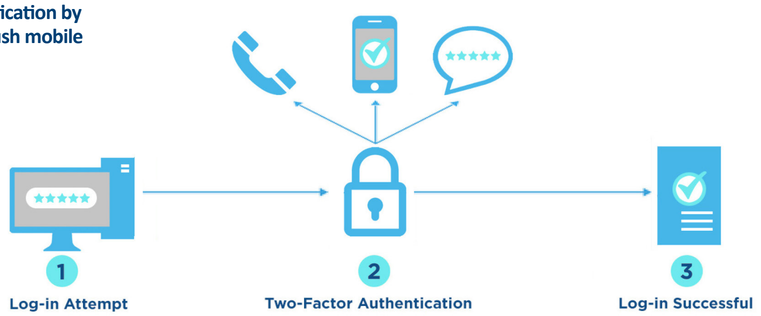
Solution Brief

When Two-Factor Authentication is Not Enough

In recent years, global powerhouses like Google, Skype, and LinkedIn along with a growing number of organizations have employed two-factor authentication (2FA) as a primary safeguard mechanism. They all share the notion that requiring a second security layer will be instrumental in reducing data breaches and cyber identity theft.

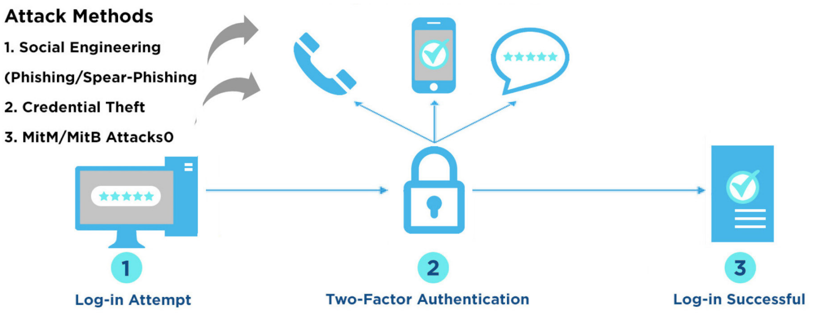
Two-factor authentication is based on the fundamental assumption that at least two out of three authentication factors are used in the process ("something you know, something you have, something you are"). 2FA is not a new security measure, nevertheless, it is in extensive use and considered by many as an effective, tiered approach.

Verify Two-factor Authentication by phone call, text, or duo push mobile



Bypassing 2FA

Recently, hackers and cyber-criminals have used various attack methods to bypass 2FA safeguards and commit fraud. Unfortunately, these attacks have increased every year, resulting in astronomical financial losses. Fraudsters use numerous methods and techniques to bypass 2FA defenses, namely: social engineering, credential theft and MitM/MitB attacks.



Post-Login Fraudulent Activity – Quick Facts

- The average fraudulent transaction amount on a normal day is around $130 for mobile transactions and about $115 for tablets.
- 55% of consumers use the same passwords for online banking, emails and social media accounts. This makes it easier for fraudsters to guess the user's credentials, bypass authentication steps and other login defenses.
- Stolen login credentials (e.g, through social engineering), can be sold on the black market/darknet to the highest bidder. Prices range from $1 to more than $1000, depending on the account balance.

Continuous Authentication via Behavioral Biometrics

With cyber attackers becoming much more sophisticated, security measures must get smarter too. The key is to implement security measures that continuously monitor and test the authenticity of users in ways that are difficult to replicate.

Mapping and monitoring these behavioral patterns, throughout the users' time within the application, continuous authentication can indicate fraudulent behavior that occurs after the login, that is, after the two-factor authentication has been validated.

This method also reduces the risk of false alarms, as opposed to traditional device ID or IP address validation, and identifies threats immediately. This means stopping fraud in real-time and protecting consumers against the range of cyber threats.

How Does the Authentication Mechanism Work?

Our system authenticates users by who they are, rather than by what they know (e.g, passwords, security questions). Employing cutting-edge behavioral biometric technology, the system analyzes more than 500 different behavioral patterns during a session (post-login) to determine whether the user is in fact the genuine user and not a human/non-human imposter. These parameters include:

- **Cognitive factors** such as eye-hand coordination, applicative behavior patterns, usage preferences, device interaction patterns and responses to Invisible Challenges™.
- **Physiological factors** such as left/right handedness, press-size, hand tremors, arm size and muscle usage.
- **Contextual factors** such as, transaction, navigation, device and network patterns.

After comparing the session data to the genuine user's profile, BioCatch provides a risk score in real-time that can be used as a standalone indicator, or combined with other threat detection systems. Our solution reduces friction associated with authentication, increases end-user satisfaction, retention, and drives high conversion rates. Moreover, through better risk analysis, fewer transactions are declined, ultimately generating new revenue streams.

CORE STRENGTHS:

Frictionless | Proactive | Quantifiable ROI | Operational Efficiency

About BioCatch™

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. Banks and other enterprises use BioCatch to significantly reduce online fraud and protect against a variety of cyber threats, without compromising the user experience. With an unparalleled patent portfolio and deployments at major banks around the world that cover tens of millions of users to date, BioCatch has established itself as the industry leader.

The company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks and e-Commerce websites across North America, Latin America, and Europe. For more information, please visit www.biocatch.com

Less Friction. Less Fraud.

Contact Us

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