BIOCATCH
Less Friction. Less Fraud.

THE INSUFFICIENCY OF TWO-FACTOR AUTHENTICATION

Making the Case for Continuous Authentication

A BioCatch White Paper | January 2017

White Paper

TABLE OF CONTENTS

Copyright

Introduction

Most organizations that enable users to perform online transactions have implemented security measures to address fraud. Using these controls, organizations can identify a significant percentage of high-risk activities that require mitigation. Currently, one of the most common safeguards used in a wide array of products/services is two-factor authentication (2FA).

In recent years, 2FA has become a common security feature, employed by global tech leaders like Google, Skype, LinkedIn, PayPal, Apple, Facebook and many more. However, recent studies on data breaches during 2016, including analysis from the National Institute of Standards and Technology (NIST) indicate that this method is not secure enough to combat online fraud and malicious cyber-activity.

This report will elaborate on the promise of behavioral biometrics/continuous authentication in thwarting online fraud. Using actual fraud cases, cost and transactional figures, organizations can use this document as a reference for creating their own case for employing continuous authentication for preventing online fraud.

Understanding How Fraud Affects Your Business

In preparing a business case to introduce behavioral biometrics, it is essential to understand the business guidelines that govern organizations and the impact of online fraud.

Business Drivers

Organizations look at the following business drivers when evaluating how an investment in fraud prevention solutions will affect the bottom-line: increased revenue and reduced cost

Increased Revenue

Businesses increase revenue by adding more customers and retaining existing ones. Ease-of-use and lower prices are driving many users to digital channels, which in turn is driving demand for online services. However, digital channels are highly competitive, with significant offerings and no switching costs.

Thus, organizations must provide an ever-improving online experience to drive revenue. Driving revenue is not only related to the number of users visiting a website, but also to the revenue each of them generates during the visit.

A fraud prevention solution that can reduce the friction associated with authentication will increase end-user satisfaction and drive customer base growth, retention, and high conversion rates. Moreover, through better risk analysis, fewer transactions are declined, ultimately generating new revenue streams.

Reduced Cost

In order to maintain a profitable balance sheet, it is essential to contain direct and indirect costs associated with fraud and various prevention solutions.

Cost of Fraud

In most cases, banks and eCommerce sites are liable for fraud perpetrated in their digital channels, and ultimately unrecoverable funds become expenses. Successful fraud also incurs other costs including legal fees, fines, higher interchange rates and reputational damage.

The Problem: Why 2FA Just Isn't 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.

According to the Breach Level Index, 554 million data records were lost or stolen in the first half of 2016, marking a 31% increase from the second half of 2015. Moreover, many other breaches are not even detected or reported.

This statistic means that:

- 4 million records are compromised every day.
- 126,936 records are compromised every hour.
- 2,116 records are compromised every minute.
- 35 records are compromised every second.

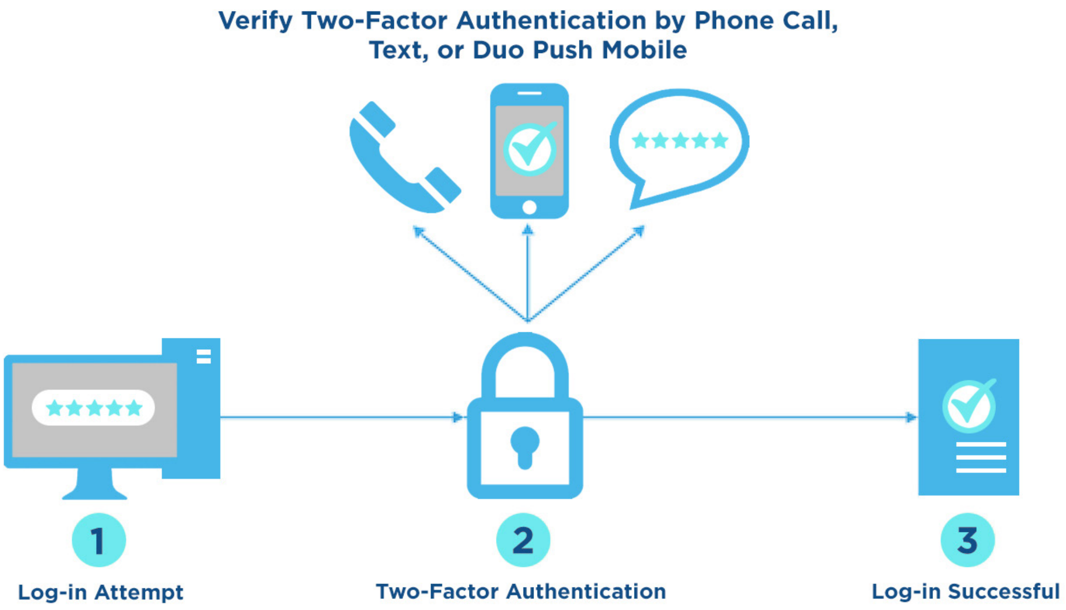
Identity theft accounts for 64% of all known data breaches. Yet, while a second layer of security does make it harder for attackers to access accounts and systems; it's just not enough.

About 2FA

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; it assumes a tiered approach. As a first step, it requires users to enter their user credentials to access a system or personal account. Once accepted, a second prompt is activated, requiring users to enter another set of credentials that only the user is expected to have – a unique code provided via a hardware token, SMS message sent to the user's mobile phone, or a biometric like a fingerprint.

Only today's fraudsters are much more sophisticated and dangerous. They have shown time and time again how easily they can leverage the vulnerabilities of two-factor authentication.

With social engineering, phishing/spear-phishing, harvesting social media, erecting fake cell towers and other innovative attacks, cybercriminals are gaining access to the full spectrum of personally identifiable information and are able to pass through both security steps. Without analyzing other, more dynamic factors during the session, the fraudsters are able to takeover profiles, compromise systems and empty bank accounts.


Verify Two-Factor Authentication by Phone Call, Text, or Duo Push Mobile
1
Log-in Attempt
2
Two-Factor Authentication
3
Log-in Successful

Bypassing 2FA

In recent years, 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.

Social Engineering

Social engineering includes various forms of psychological manipulation to trick users into providing confidential information like user names, passwords, bank data, credit card numbers and other personal information. These techniques include:

- ***Phishing:*** A technique in which the attacker sends fake e-mails or SMS messages, using a legitimate "cover story" to fraudulently extract information from the target. For instance, a fraudster pretending to be a service provider who needs the customer's credentials to access his account and repair false "technical malfunctions".

- ***Spear-Phishing:*** Same as above, except the fraudster targets a handful of high-level individuals and sends them highly customized emails with the aim of extracting sensitive information. For instance, fake e-mails sent to executives, which use real information about the targeted company to seem legitimate and to trick the victims into performing certain tasks or extracting valuable information.

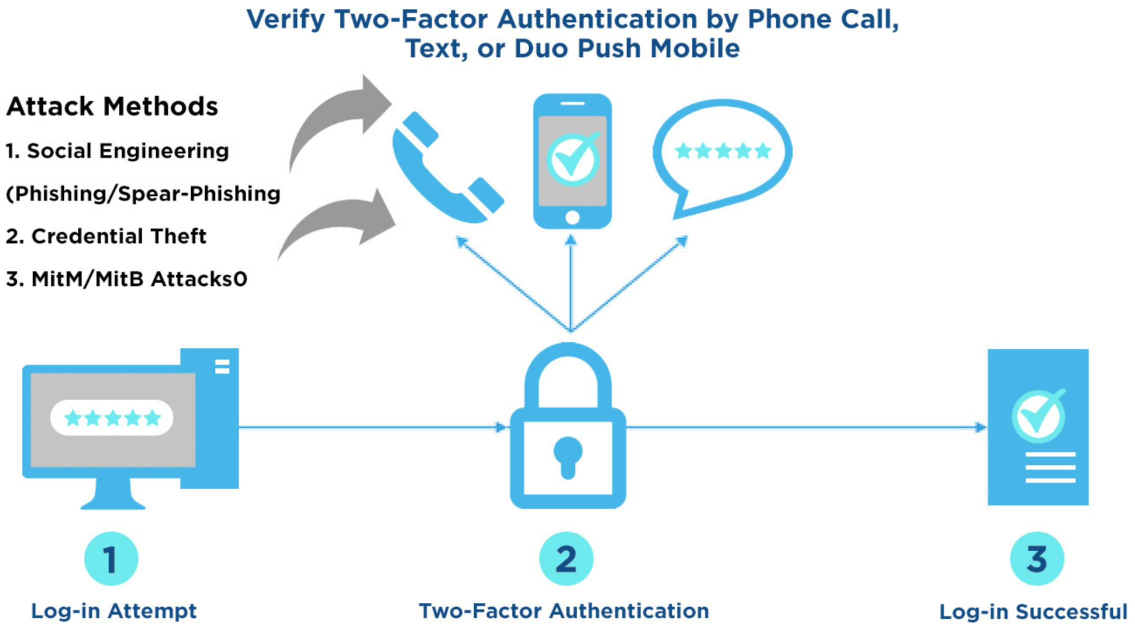
- ***Interactive Voice Response/Phone Phishing:*** A method in which the attacker imitates a legitimate IVR system in order to trick the target over the phone. The attacker may also call the target directly, use a fake identity, present his cover story and prompt the victim into performing a requested task.

Man-in-the-Middle (MitM) Attacks

An attack in which the fraudster modifies the communication between two systems to intercept information. For example, a fraudster can create a fake bank login page and trick the victim into logging into the web page. Once the victim enters his credentials, the attacker intercepts them and later uses the stolen credentials to access the victim's real bank account.

Man-in-the-Browser (MitB) Attacks

MitB threats use Trojan Horses to exploit security vulnerabilities and to infect web browsers. Once the browser is infected, the attacker is able to intercept sensitive information and extract it in clandestine fashion.



Introducing Behavioral Biometrics

Behavioral biometrics is a breakthrough technology that identifies people by who they are, rather than by what they know (e.g. secret question, password) or what they have (e.g. token, SMS one-time code). It analyzes over 500 different behavioral parameters including

- Cognitive traits 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.

One of the major strengths of behavioral biometrics is its ability to continuously authenticate users, passively and transparently. Behavioral biometrics works throughout a session, not just as a one-time verification measure, to recognize anomalies between the legitimate user's normal behavior and what is occurring in real-time. By analyzing user behaviors, behavioral biometrics can provide real-time alerts on the existence of malware or other MitM, MitB attacks, as well as to detect if stolen credentials were used to access an account.

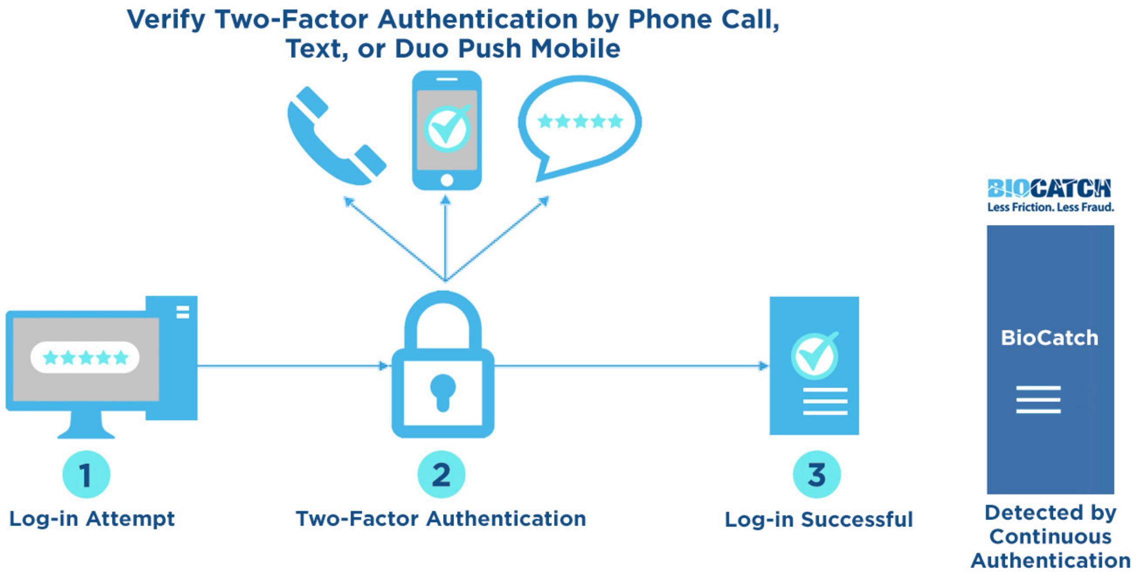
How Behavioral Biometrics Works to Provide Continuous Authentication

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.

As mentioned above, behavioral biometrics is a holistic solution that differentiates between a legitimate user and a human or non-human imposter. For instance, the natural tendencies of an authentic user making their way through an application varies markedly from that of an experienced fraudster. For example, an attacker who has exploited one application multiple times will work through it with a fluency that a new user cannot match.

Or, unlike consumers who manually input personal information from memory, attackers might cut and paste these details into systems. 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.


Verify Two-Factor Authentication by Phone Call, Text, or Duo Push Mobile
BIOCATCH
Less Friction. Less Fraud.
BioCatch
1
Log-in Attempt
2
Two-Factor Authentication
3
Log-in Successful
Detected by Continuous Authentication

Case Study

Social Engineering RAT Attack on Bank Customer Thwarted by BioCatch

The following case was reported by a major UK bank during Q1 2016.

1. The incident began when an individual claiming to be from a well-known internet provider, informed the customer that irregularities were detected on her computer. The caller provided the customer with her account number so the customer presumed the call was genuine. The caller provided the customer with some instructions and was granted remote access to the customer's computer; the customer was told that the procedure was to examine the irregularities.

2. The customer was then advised to login to internet banking and accept an automated call. At this stage, the 2FA failed to stop the fraudster, as he used real credentials and passed the second login step.

3. The fraudster took over the device. On the same day, a new bill payment was setup to another bank payee, and later three payment orders of £2500 were placed. Days later, another payment order for £4000 was placed by the fraudster.

4. Both times, BioCatch's system detected significant behavior changes in the post-login pages and notified the bank in real-time to disallow the transactions. The account was ultimately shutdown.

This case is a good example of why 2FA just isn't enough and demonstrates the effectiveness of continuous authentication, driven by behavioral biometrics.

Key Benefits

Frictionless. Friction can cause a lot of inconvenience to users and drive them away from doing business online. Asking a user to actively authenticate themselves repeatedly during a session is simply not tenable. Behavioral biometrics offers complete transparency while remaining non-intrusive to the end-user, providing a form of identification that cannot be lost, imitated or stolen and that doesn't infringe on user privacy.

Proactive. Using advanced statistical modelling, machine learning and complex behavioral analysis, BioCatch can detect a fake user in real-time. Quickly identifying anomalous behavior which is indicative of fraud, BioCatch sends actionable alerts to the system administrator/operator.

Quantifiable ROI. With highly accurate and targeted, fraud prevention features, low levels of false alarms/flagging and real-time responsiveness, the BioCatch system provides immediate ROI. Using a quantifiable approach, it is possible to convert the use of behavioral biometrics to a specific business value.

Target Industries

- Banking
- Payments
- E-Commerce
- Software Monetization
- E-Learning
- Government and Enterprise

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