BIOCATCH™
Less Friction · Less Fraud

PREVENTING FRAUD IN A MOBILE ERA -

Addressing Authentication, Malware and Social Engineering

White Paper

TABLE OF CONTENTS

Executive Summary

As mobile devices eclipse computers and laptops as the preferred method of going online, fraudsters have followed users, porting their modus operandi –account takeover, social engineering, and malware based remote control attacks – to the mobile arena. Mobile has opened up many new ways for users to communicate and connect without being tied to a desk or a power outlet – and at the same time, it has presented hackers with many more opportunities to perpetrate fraud and carry out attacks that cannot be detected with traditional tools used to detect attacks in web sites. As a result, companies need to apply new fraud controls to protect mobile users and enable them to carry out transactions, check bank accounts, make purchases, etc. Nevertheless, end user experience cannot be negatively impacted by these security measures: Users want to open and use apps freely, without being required to take additional authentication steps. They also expect to be protected continuously, throughout their entire journey.

As mobile banking becomes more common, is there a way for banks to provide users with a frictionless experience while still ensuring top security? How can banks protect their customers from account takeover, or from being social engineered into giving fraudsters access to their devices?

The BioCatch Behavioral Biometric technology provides continuous, secure authentication on mobile apps and detects threats such as remote access, malware, account takeover and device spoofing. BioCatch's proprietary technology authenticates users based on who they are, rather than what they know (secret question) or what they have (tokens). Furthermore, the technology is invisible to users, but allows banks to immediately detect if a fraudster is attempting to break into an account via purloined authentication data, or through other malicious means.

BioCatch's solution provides that extra layer of security, while ensuring that organizations can provide the kind of experience that users have come to expect in the mobile era.

Today's Mobile Arena

Mobile banking is the customers' preferred choice of engaging with their banks, and has now overtaken branches and phones. Over the past five years, adoption of mobile banking and smartphones has more than doubled, while that of tablets increased roughly 8.5 times. Meanwhile, a study by Wells Fargo shows that 72 percent of millennials use mobile devices for banking. And that by 2020, a research from CACI for the BBA[1] forecasts that customers will use their mobile to manage their current account 2.3 billion times – more than Internet, branch and telephone banking put together.

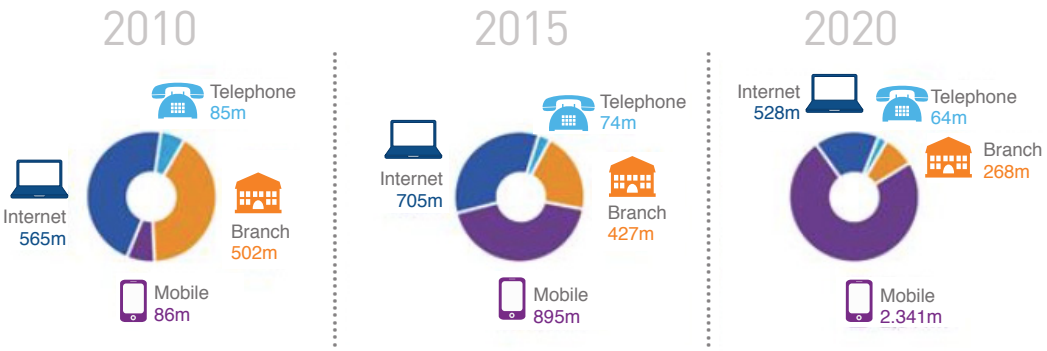


Figure 1 | CACI Research – banking channel usage 2010-2020[2]

Going forward, mobile banking will be the main channel through which users will transact and interface with financial institutions. Banks are well aware of the trend and offer more and more functionality in the mobile banking apps; and at the same time, look for ways to make sure their customers are secured and can transfer money safely.

RAT-Malware, Social Engineering and Account Takeover – From Online to Mobile

Many mobile banking apps currently provide only a subset of the functionality available online (e.g. changing personal details like a phone number or setting up a wire transfer). However, all banks are quickly closing the gap between online and mobile banking, and often introduce additional functionality exclusively on mobile. Naturally, these changes have not escaped the eyes of the fraudster community, driving a shift to mobile banking fraud.

[1] *World of Change* The way we bank report https://www.bba.org.uk/publication/bba-reports/world-of-change-2/

[2] *World of Change* The way we bank report https://www.bba.org.uk/publication/bba-reports/world-of-change-2/

Mobile malware has been growing exponentially in the last few years, but only recently did banks begin to see a significant number of fraud attacks directed at mobile banking users. The tools and tactics have been successfully ported from online banking fraud, and include three main attack vectors: RAT Malware, Social Engineering and general Account Takeover fraud.

There is a RAT in Your Mobile – The Most Alarming Use of Mobile Malware

RAT, short of Remote Administration Tool, uses an inherent remote assistance capability that allows remotely control the user's device; it leverages protocols that exist in just about any operating system. In a RAT attack, the fraudster gains full control of the user device, opens a browser or app, logs in with credentials stolen in prior sessions, and then just do whatever they please inside the account. The growing popularity of RATs stem from that fact that is almost impossible to detect using commonly used fraud controls. Since the activity comes from the real user endpoint, location and device fingerprint analysis is effectively neutralized; the same applies to any device-based defense such as USB connected tokens and PKI.

RATs are included in many banking malware packages, but when used by fraudsters they do not behave as malware: they don't inject code, overlay the screen, or manipulate the session in any way. They just allow someone to control the device from afar. For this reason they cannot be detected by dynamic malware detection tools that would normally catch any banking malware.

The year 2016 in particular has seen a rise in the use of RAT access technology to perpetrate online banking fraud using financial malware like Dyre, Dridex and Neverquest. Dridex is currently the most widespread Trojan that uses RAT; it uses VNC functionality with back-connect server setup (a server that keeps an open-line remote access connection with the victim's device). VNC or RDP remote administration has become the de facto standard for most malware for sale in the underground community.

Mobile phones and apps are not immune from RAT attacks. When the popular Pokemon Go app became available to the public, some sneaky fraudsters launched a similarly named rogue app that included a RAT functionality enabling full control of the victim's device. Such rogue apps that include RAT functionality are not uncommon: Palo Alto reported additional attacks in mid 2016: "SpyNote is similar to OmniRAT and DroidJack, which are RATs (remote administration tools) that allow malware owners to gain remote administrative control of an Android device."

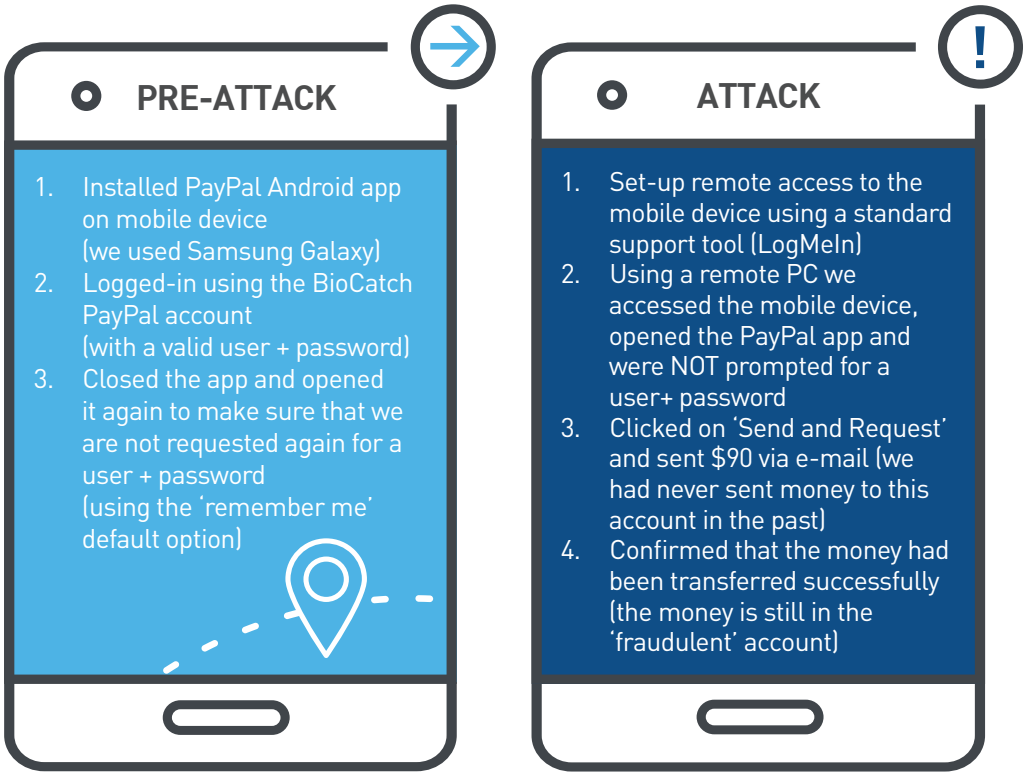
Interestingly, unlike most malware that is sold in the fraud underground, OmniRAT is openly sold to the general public – $25 for an android license. The reason is that like other software tools, OmniRAT can also be used for benign uses such as remote assistance. RAT is equally effective in evading detection in mobile apps as it is in browsers, and for the same reasons. Identifying the device or network doesn't really help in spotting remote access as it is using the victim's genuine device, and malware infection detection is limited to known malicious apps and prone to high number of false positives.

Mobile Social Engineering Attacks

The weakest link in protecting against financial fraud is the end user – and more specifically the ease at which they can be social engineered into doing, well...anything.

The most common online banking social engineering fraud requires nothing but a phone line and a computer with a support tool installed on it. So how does it work? First the user receives a call from the attacker claiming to be a support person working for a trusted source (Bank, Microsoft, telco carrier etc.). Second, the criminal convinces that user to install a remote support tool like Ammyy, LogMeIn, or TeamViewer on his computer. Third, the user is convinced to grant remote access to the computer and access the online banking site to "reproduce and fix the problem". Lastly, the attacker fools the victim to leave the computer as "it will take some time to run checks" and submits a fraudulent transaction.

Can the same social engineering attack happen in a mobile app? To answer this question BioCatch conducted a short lab test to mimic this type of attack on a payment mobile app. Feel free to try to recreate the scenario yourself:



Note: the information above was shared with PayPal; the same attack would work on many other mobile apps.

Social engineering attacks are hard to detect as both authentication at login and the device are genuine. The RAT itself is not malware, and is often a legitimate, commercially available software. No matter how strong the authentication is or how sophisticated the device and network profiling is, the attacker cannot be stopped using regular security controls.

Mobile Account Takeover Attacks

Username and passwords are still the most prevalent form of authentication for mobile banking in the US and other countries. For this reason, credential phishing has remained a simple and effective way to perpetrate mobile banking fraud. Requiring secondary strong authentication is often dismissed by business owners of mobile apps, as it provides for a poor user experience and negatively client retention (i.e. users will move to wherever it is easiest to do business). The only exception is when the user first downloads the app on a new device; in this case the app often requires a one-time code sent via text message or push notification.

Fraudsters typically bypass that protection by doing SIM swaps, changing the user's phone number on record, social engineering the mobile carrier to forward the SMS to another mobile number, or infecting the user's device with malware that automatically forwards text messages to the bad guys.

Mobile malware that overlays the existing app can also serve for account takeover. In this case the user downloads a rogue app, either directly from the app store or because they fell victim to a social engineering message via email, SMS or other instant messaging platforms. The user downloads the rogue app, and it adds a hidden functionality: when the user opens the real mobile banking app, it overlays it with a fake screen – almost like a phishing site – that captures the user's name and password typed by the user. This is then used by the attacker to access the account from another device.

Another scenario that might happen is a lost or stolen device. Some devices are not password protected, and once the device is in the wrong hands, the fact it is 'trusted' is no longer relevant. What if the device has been misplaced or stolen? How can a bank ensure that the genuine user is using the genuine device without negative impacting the user experience? A good way to solve these issues is using Behavioral Biometrics, profiling the regular user's behavior and then seeing if the device is being handled by the regular user.

BioCatch Mobile Behavioral Biometrics – Frictionless Authentication and Threat Detection

The three main vectors of online banking fraud attacks - RATs, Social Engineering and Account Takeover - are finding their way to the mobile space. Online banking fraud is constantly rising despite the prevalent use of device recognition, malware detection tools and sophisticated authentication controls; the situation in mobile banking is just as bad, and at times even worse because of the strong requirements for smooth user experience, which often clashes with security requirements.

BioCatch takes a different view of mobile app security. Instead of relying on trusted devices, passwords, device and network fingerprinting or even two-factor authentication, BioCatch bases its technology on Behavioral Biometrics.

BioCatch tracks the way a user interacts with an app and compares to a genuine user's profile (i.e. authentication) as well as known bad activity (i.e. threat detection). This analysis breaks down the user's interaction into hundreds of features extracted from multitude of sensory data points (accelerometer, gyro, touch, orientation) coupled with application contextual data.

When installed on an app, BioCatch collects over 500 parameters for each user, and uses machine- learning algorithms to generate a unique individual profile. When a session starts, the system begins to continuously and **passively** collects information and in addition uses **active** semi-random pro-active challenges in order to generate a user's identity and invoke a response.

Similarly, BioCatch has profiled multiple bad behaviors such as remote access, malware, bot and mobile emulators. And, in cases were the interaction is consistent with known bad behavior the application is alerted and fraud attempt is prevented.
Because there are so many parameters being used, the likelihood of a hacker being able to "pretend" to be the legitimate user is close to zero – whether they steal password information and log into an account from their own device, or whether they log into the app remotely on the user's trusted device.

The following are examples of behavioral mobile data collected and features extracted:

Tap Gesture Analysis (Passively Collecting Acceleration and Tap data)
Below is an example of two users monitored by BioCatch when tapping on the touch screen to submit a transaction on a mobile banking app: The charts represent accelerometer data at the point of pressing a "submit" button ('touch down'). The dotted Touch Down line marks the action, and the charts show half a second before (left) and after (right) the tap.

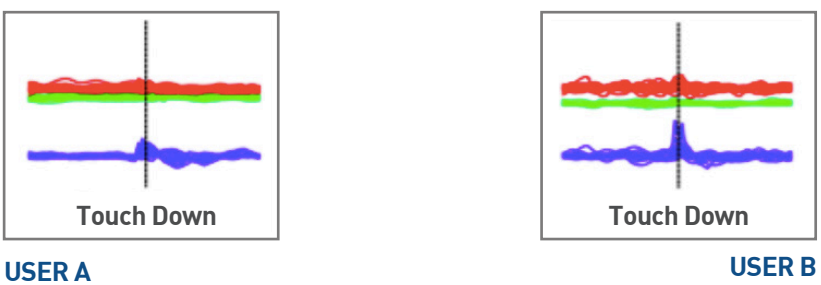


Figure 2 | Device holding

The green and red lines represent left-right and backward-forward movements respectively. It's clear that user B has a somewhat shaky hand (red 'scribbles'). The blue line represents vertical up and down motion of the device; the data shows that user B thumps the device forcefully whenever he hits a button. The combination of a shaky hand and a strong thump is something very consistent and rather distinct. User A, on the other hand, has a consistent and unique vertical movement pattern right after the event of pressing the button. His hand is quite steady.

Scrolling Patterns

Based on touch and scrolling events done on the mobile device, BioCatch collects the patterns that are unique for each user. The patterns can indicate if the user is using both hands for scrolling up and down or is using one hand only. In the image below we see six different real online users, each with very different way of scrolling.

User #1 (top left) for example, uses both thumbs equally when scrolling his device, while user #2 rarely uses his left thumb.

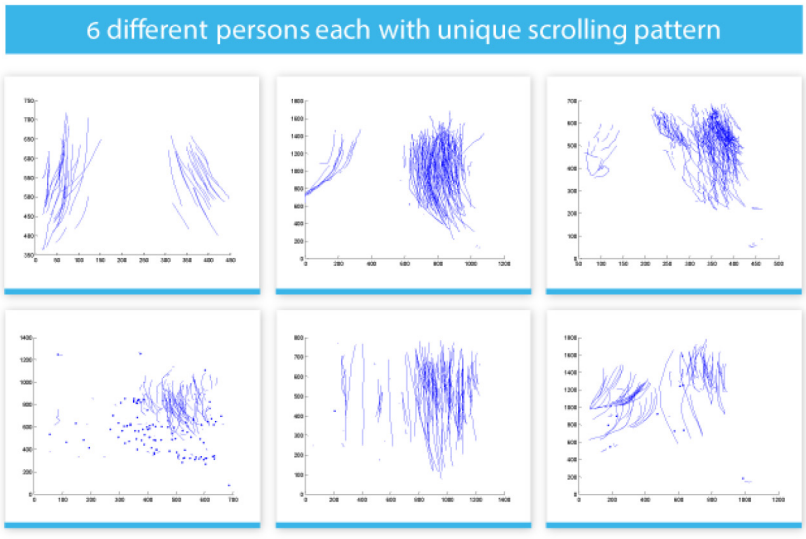


Figure 3 | Scrolling Patterns

Invisible Mobile Challenges

At the heart of BioCatch's technology is the patent-pending approach of subtle behavioral-invisible challenges.

The following exemplifies the use of this technology in mobile apps:

Spinning Wheel

A common user interaction element in mobile apps is the spinning selection wheel for dates, time, numbers, etc. This is often used when entering information such as a new destination account for money transactions.

Figure 4 | The spinning wheel

BioCatch collects passive measures related to spinning the wheel (speed, stopping strategy, corrections towards the end). In addition, subtle fluctuations are introduced into spinning wheel control – rotation speed can be accelerated/ decelerated value selection tolerance can be enhanced or reduced. While users are not aware of this minute "Challenges" they do "Respond" in order to compete their task. And, the way people respond becomes part for their behavioral profile. Moreover, when attack tools are used (malware, remote access, and bots) the reaction to there "Invisible Challenges" is clearly non-human and so they can be spotted easily.

Multiple Users on Same Device (e.g. Husband/Wife Situation)

BioCatch supports multiple users per device by approaching the problem in two ways. First, the system identifies that two users share the same device, then it either builds a separate models for each user or, if suspicious, sends an alert to the bank. Note that detection of multiple users may happen in two cases: during initial training or after the model is built for the main user.

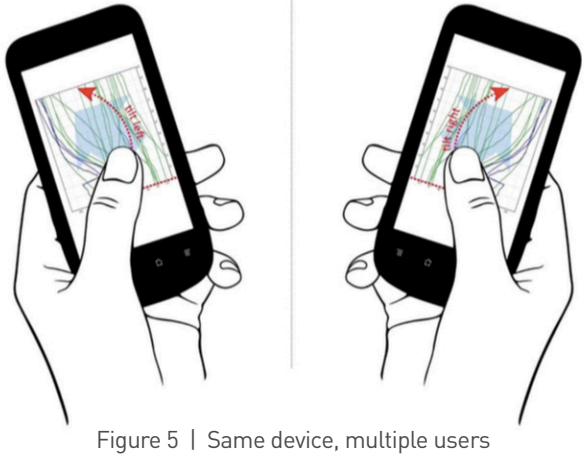


Figure 5 | Same device, multiple users

Analyzing Touch and Gyro Events to Calculate Size

BioCatch extracts touch and gyro events when a user operates the phone. Cross-correlating these two pieces of information - the radius and angles of movement - can be measured, and the size of the hand and finger can be extrapolated. The size of the person's hand and fingers is a unique biometric feature. This feature doesn't change over time or from moving from one device to another.

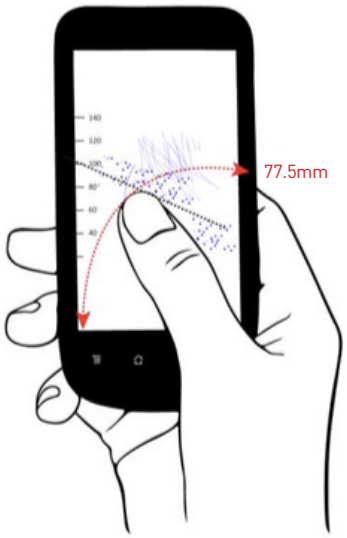


Figure 6 | Measuring the touch and gyro data to extrapolated the size of the hand and fingers

Summary

Mobile devices are clearly the future of on-line communication, commerce, and finance. Increased user mobility and frequent device changes make it hard to validate user identity based solely on location, platform and network attributes. Combined with Social Engineering Attacks, mobile banking has become a serious weapon with fatal consequences.

To effectively reduce fraud, banks need to begin thinking about security in non-traditional ways such as:

1. Looking beyond the device and "regular" strong authentication as these alone cannot ensure end user security
2. Integrating next-generation behavioral biometrics solution, which ensures that organizations know who is connecting with them and identifying RAT, malware, bots and other common threats

Organization are often used to think that when it comes to mobile authentication and threat detection, something generally has to give - either security or usability. BioCatch Behavioral Biometrics offering with its unique and proven authentication and threat detection, enhanced with a top Invisible Challenges technology help organizations offer their mobile customers a full solution that addresses both security as well as frictionless user-experience.