BioCatch

WHITEPAPER

Lock Cybercriminals Out of Mobile Banking

Behavioral Biometrics for Mobile

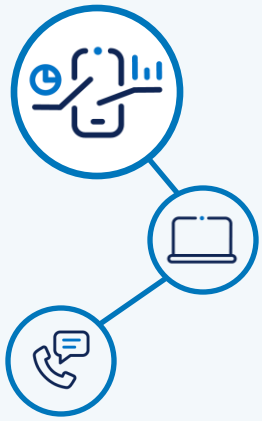
Lock Cybercriminals Out of Mobile Banking

Table of Contents

Today's Mobile Arena

Mobile banking is the customers' preferred choice of engaging with their banks. Over the past five years, mobile banking usage has increased more than 125%, with nearly two billion mobile banking users worldwide today[1].

Going forward, mobile banking will continue to be the main channel through which users transact and interface with their banks - well exceeding internet, branch, and telephone banking. Banks are aware of this trend and continue to offer more functionality in their mobile banking apps; and at the same time, look for ways to ensure their customers are secured and can transfer money safely.



Executive Summary

As mobile devices eclipse computers and laptops as the preferred method for consuming online services, cybercriminals have followed users, porting their modus operandi. While mobile presents new ways for users to communicate and connect without being tied to a desk or a power outlet, it also provides criminals with more opportunities to perpetrate fraud and carry out attacks that bypass traditional detection tools. As a result, companies need to apply new fraud controls to protect mobile users and enable them to carry out banking activities securely. 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 organizations to provide users with a frictionless experience while ensuring top security? How can financial institutions protect their customers from fraud?

The BioCatch Behavioral Biometrics platform provides continuous protection of mobile application and browser sessions and detects account takeover attack methods such as remote access tools, malware, social engineering scams, mobile emulators, and more.

BioCatch delivers behavioral biometrics by continuously analyzing a user's physical and cognitive digital behavior to distinguish between genuine users and cybercriminals. Furthermore, the technology is invisible to users, allowing financial institutions to immediately detect fraudulent activity while providing the kind of experience that users have come to expect in the mobile era.

[1] Source: Jumio Research

How Cybercriminals Attack Mobile Channels

Many mobile banking apps currently provide only a subset of the functionality available. 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.

In fact, across its global customer base, BioCatch has seen mobile fraud make up almost 50% of confirmed fraud cases; and it is very likely that this percentage will continue to rise with mobile banking usage. The tools and tactics have been successfully ported from online banking fraud, including Remote Access Tools (RATs), malware, social engineering scams, and general account opening and account takeover fraud.

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

RAT, short for Remote Access Tool, uses an inherent remote assistance capability that allows remote control of a user's device. This attack leverages protocols that exist in just about any operating system. In this fraud scenario, the fraudster gains full control of the user's device, opens a banking browser or application, logs in with credentials stolen in prior sessions, and then does whatever they please inside the account. The growing popularity of RATs stem from the fact that they are almost impossible to detect using traditional fraud controls. Since the activity comes from the real user endpoint, location and device fingerprint analysis is effectively neutralized; and 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 cybercriminals they do not behave as malware: they don't inject code, overlay the screen, or manipulate the session in any way. They simply allow someone to control the device from afar. For this reason, they cannot be detected by dynamic malware detection tools that would normally catch banking malware.

The year 2019 in particular has seen a rise in the use of RAT technology to perpetrate online banking fraud using financial malware like Cerberus, Dridex and Triada. Cerberus is currently one of the most popular banking Trojans; and as of early 2020, its latest variant provides cybercriminals with complete remote control of a user's device allowing them to steal personally identifiable information (PII) and conduct fraud.

Mobile phones and apps are not immune to RAT attacks. When the popular Pokemon Go app became available to the public, some sneaky cybercriminals launched a similarly named rogue app that included RAT functionality enabling full control of the victim's device. Such malware that include RAT functionality are not uncommon: Monokle, SpyNote, Pegasus, and OmniRAT are RAT malware to watch out for.

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 legitimately for remote assistance. RATs are equally effective in evading detection in mobile apps as they are in browsers, and for the same reasons. Identifying the device or network doesn't really help spot remote access as the victim's genuine device is in use, and malware infection detection is limited to known malicious apps and prone to a 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. So how does it work? See Figure 1 below.

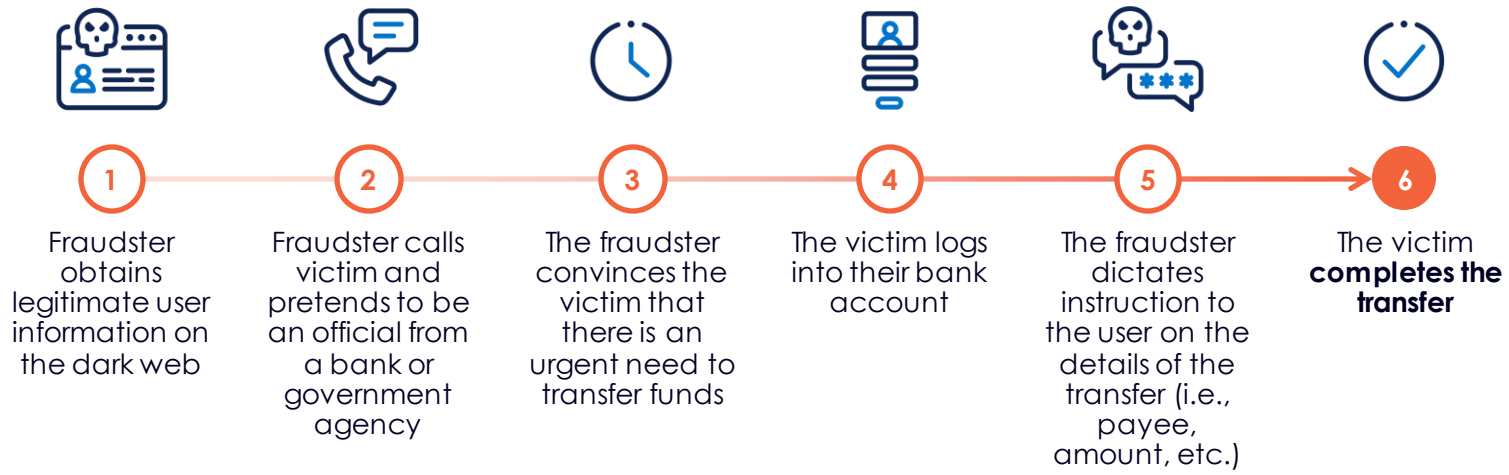


Figure 1 | The Anatomy of a Social Engineering Scam

Social engineering attacks are one of the hardest banking threats to detect as the user and device are trusted and genuine. In this scenario, traditional fraud detection solutions are easily circumvented. Regardless of how strong authentication or device and network profiling are, the legitimate user is conducting a fully authorized transfer under the influence of a cybercriminal.

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, as it adversely impacts user experience and customer retention. Further, once a cybercriminal obtains a user's credentials and personal information, they can then employ other attack methods, such as social engineering, to bypass authentication methods including one-time passwords.

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 scam delivered via email or SMS. 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 username and password as they are typed. The stolen credentials are then used by the attacker to access the account from another device.

Another fraud scenario that might occur is when a device is stolen or lost. Some devices are not password protected, and once the device is in the wrong hands, the fact that it is 'trusted' is no longer relevant.

BioCatch Behavioral Biometrics: A Trusted and Frictionless Mobile Banking Experience

With a dramatic increase in mobile usage over recent years, and despite prevalent use of protections such as device identification, malware detection, and other sophisticated authentication controls, mobile fraud has continued to rise. Further, financial institutions have struggled to provide optimal security and deliver a frictionless customer experience.

BIOCATCH TAKES A DIFFERENT APPROACH TO MOBILE BANKING SECURITY

The BioCatch Platform leverages mobile-specific sensors such as accelerometer, touch, orientation, and gyro to continuously analyze user behavior throughout a mobile banking session.

This data is used to profile and analyze a user's digital behavior **on three levels:**

1. **Behavioral Biometrics:** Profiling a user against their historical profile based on physical traits such as how the user holds their device, swipes, scrolls, and taps, to detect behavioral anomalies, including human versus automated or bot activity.
2. **Cognitive Analysis:** Profiling a user against population-level behavioral patterns based on cognitive choices, such as how the user inputs data or navigates a session, to identify genuine versus criminal behavioral indicators.
3. **Behavioral Insights:** Combines user and population-level profiling to determine user intent and emotional state in context of the activity to detect complex fraud scenarios such as when a user falsely claims their age as part of the account opening process or when a user conducts a transaction under the guidance of a voice scammer.

When deployed to a mobile banking application or website, BioCatch continuously collects physical and cognitive digital behavior to generate an anonymized user profile. These historical insights enable the BioCatch solution to detect instances where a user's behavior shows significant variations from their unique user profile.

By monitoring for behavioral anomalies and criminal indicators, the BioCatch platform detects a broad range of mobile fraud attack methods including malware, remote access tools, social engineering scams, device theft, and mobile emulators.

Unlike traditional fraud controls that heavily rely on device elements, user behavior can never be stolen, spoofed, or replicated. This is the case even if a cybercriminal steals password information and logs into an account from their own device, or remotely logs into the banking app on the user's trusted device.

The following are examples of behavioral data collected by the BioCatch solution:

Tap gestures

The visual in Figure 2 illustrates two users monitored by BioCatch when tapping on the touch screen to submit a transaction on a mobile banking application. The charts in Figure 2 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.

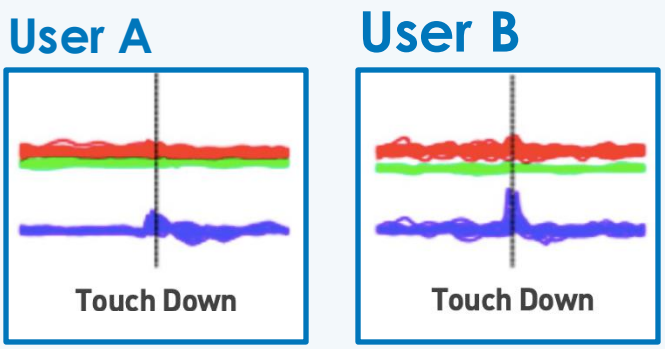


Figure 2 | Device Holding

The **green** and **red** lines represent left-right and backward-forward movements respectively, and the **blue** line represents vertical up and down motion of the device. The data shows that User A has a consistent and unique vertical movement pattern right after they press a button. Further, their hand is quite steady (red and green lines). On the other hand, User B has somewhat of a shaky hand (red 'scribbles') and thumps the device forcefully whenever they hit a button. The combination of a shaky hand and a strong thump is something very consistent and rather distinct.

Scrolling Patterns

Based on touch and scrolling events, BioCatch collects patterns that are unique to each user. The patterns can indicate if the user is using both hands or a single hand while scrolling. In Figure 3 below, we see six different online users using the same page on a mobile application; each have their own unique way of scrolling.

For example, user #1 (top left), uses both thumbs equally when scrolling, while user #2 rarely uses their left thumb.

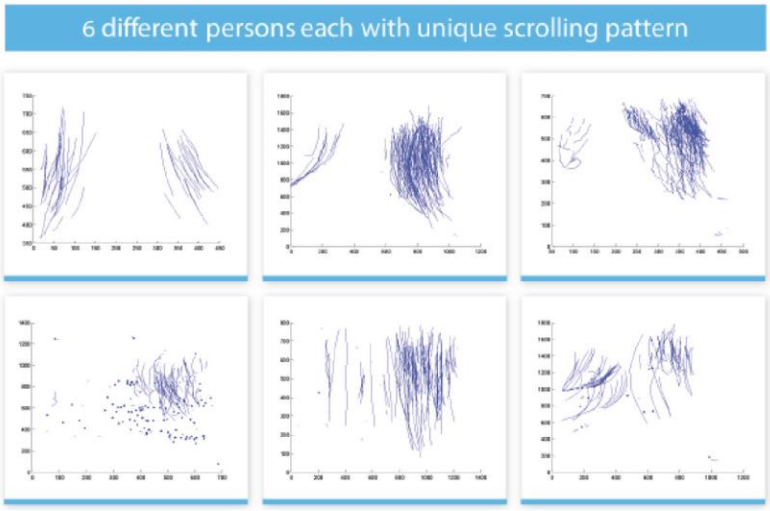


Figure 3 | Scrolling Patterns

Touch & Gyro Events

BioCatch extracts touch and gyro events when a user operates their mobile device. By doing so, the platform considers other unique user characteristics including dominant hand, touch size and pressure as part of the risk assessment process. Features extracted allow the solution to detect subtle behavioral anomalies that can indicate high levels of risk.

Summary

Mobile devices are clearly the future of online banking. Increased user mobility and frequent device changes make it hard to validate user activity based solely on location, platform, and network attributes.

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

1. Looking beyond device and authentication solutions, as these alone cannot ensure continuous protection.
2. Integrating a next-generation behavioral biometrics solution, which ensures financial institutions can protect their customers from fraud and identity theft without adversely impacting customer experience.

Financial institutions often face a difficult challenge in achieving both risk and business objectives. While many traditional fraud prevention solutions compromise user experience, behavioral biometrics allows users to go about their banking activities safely and without friction.