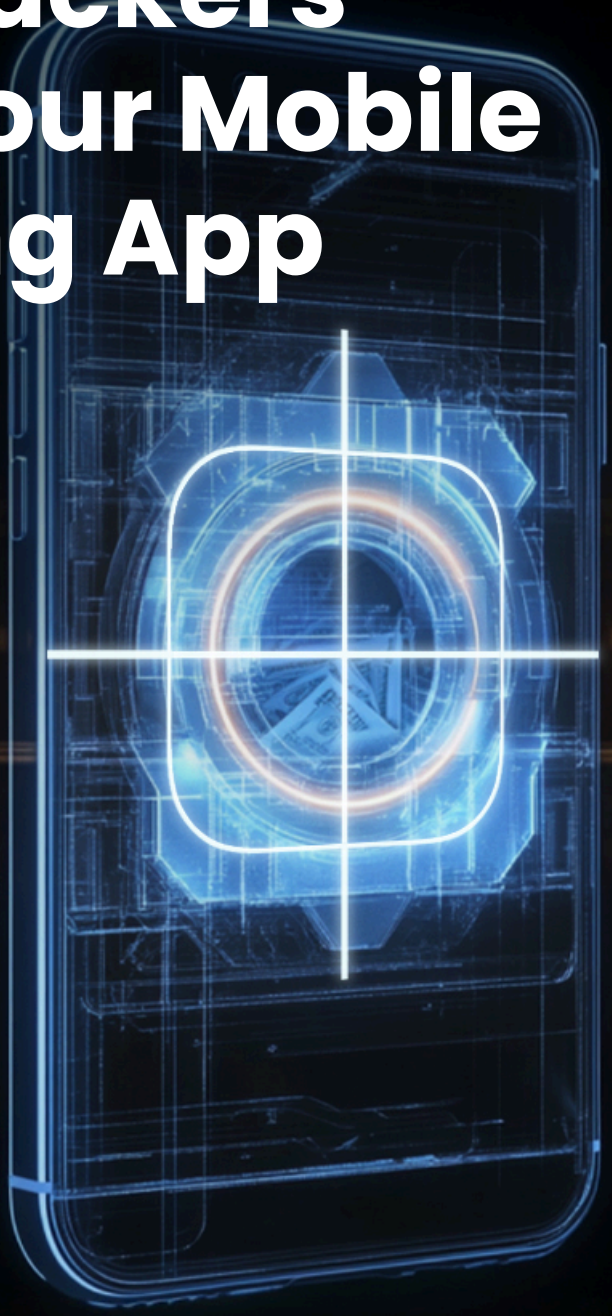
Why Hackers Love Your Mobile Banking App



www.zimperium.com

ZIMPERIUM®

Mobile is changing how we bank.

As of January 2021, there are over 4.32 billion mobile internet users worldwide, representing 59.5 percent of the global population. And by April 2020, over 70 percent of customers from the four largest U.S. banks used mobile banking apps, up from 63 percent a year before. This jump can be attributed to the closure of many bank branches to prevent the spread of the COVID-19 virus.

Today, mobile is the de facto standard. Simply put, if your digital strategy does not take mobile into account, you are missing the mark.

Roughly three in four Americans (**76%**) have used their primary bank's mobile app within the last year for everyday banking tasks like depositing checks or viewing statements and account balances, according to the Ipsos-Forbes Advisor U.S. Weekly Consumer Confidence Survey.

Irrespective of whether it's Retail, Corporate or Commercial banking, your mobile banking app is your new bank!

Mobile banking represents the future due to the undeniable convenience it presents in the post-pandemic era defined by the new low-touch economy. According to RSA Fraud Research, having a mobile app is now one of the **top 3 requirements** for choosing where to bank.

MOBILE BANKING WORKS ACROSS GENERATIONS

97% of millennials indicated that they use mobile banking.

91% of Gen Xers and 79% of baby boomers also reported seeing the benefits of these services.

Source:https://www.businessinsider.com/mobile-banking-market-trends

Unfortunately, the same research indicated that a bank's fraud protection capabilities ranked next to last when making that decision. Consumers will always prioritize convenience over security. But for banking institutions, mobile apps also present a massive digital risk that cannot be ignored.

Mobile banking is a big business.

Banking has been squarely in the center of the mobile evolution. In the post-pandemic era, mobile banking apps have become the defacto standard for banking. Consumers want more self-service features and a personalized user experience within the mobile apps. But this personalized experience requires more and more PII information.

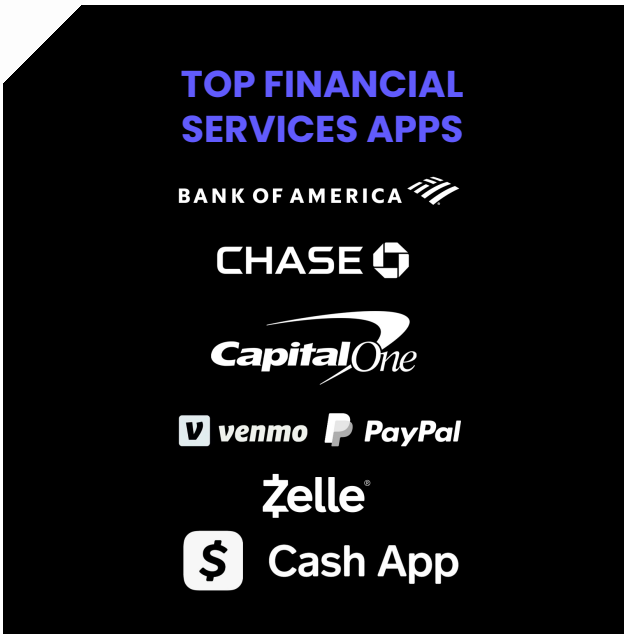
The average smartphone has over 90+ apps, and about 10% of your apps are related to managing your financial health.

Mobile banking is a big target.

Unfortunately, the market's enthusiastic embrace of mobile banking has made the applications and users attractive targets for cybercriminals. Looks at the statistics below:

- Mobile fraud transactions are up 600% in the last five years
- 1 in 20 fraud attacks are due to mobile malware
- 50% increase YOY in banking malware
- 44% of fraud is happening in mobile apps

The sheer volume of mobile transactions has already passed critical mass, where the potential payoff for cybercriminals makes attacks on mobile banking applications a priority. Today smartphone users log into their mobile banking apps an average of 30 times per month.



As the features and capabilities of mobile banking expand, mobile banking activity will continue to increase, and the corresponding surface area that cybercriminals can attack will grow too. But the reality is that mobile banking applications are already facing unprecedented risk.

Mobile banking developers face significant hurdles.

Banks are highly security conscious. How can it be that banking, the security-conscious industry model, would be struggling to deliver mobile application security? The simple fact is that customer demand for mobile banking is far outpacing the industry's ability to provide ironclad security in the fast-changing mobile device ecosystem.

To put it differently, mobile application developers face significant pressure from three different and competing market forces. First, customer demand (and competitive pressure from other banks' mobile apps) is intense. Customers continue to show a considerable appetite for expanding their use of mobile banking. To keep up with customers, developers often focus on features rather than security. Moreover, as deadlines loom, development shortcuts become more appealing, and developers will use unvetted, open-source code for mobile functions. There are over 26 million mobile app developers globally, and most developers are neither oriented nor incentivized towards secure code. They are incentivized to build faster.

Second, mobile platforms compete for market dominance. Developers, therefore, must either work with limited familiarity with the underlying device platforms or become specialists in a narrow, particular platform subset. App development, cloud storage, and other modular development frameworks are constantly evolving and require developers to keep up with the best practices. This fragmentation creates an ideal environment for security missteps.

Third, there is the reality of the way consumers use their mobile devices. Surveys consistently show that mobile banking consumers value security in principle. Even so, consumers do not always prioritize security in practice. We noted in an earlier section, for example, that some consumers do not follow essential security practices such as the use of passwords or updating to the latest operating system. This poor practice exacerbates any vulnerabilities that developers inadvertently allow into their banking applications.

Mobile banking apps run in a zero-trust environment.

Mobile apps today run on devices whose integrity cannot be implicitly trusted. Every mobile device has a unique usage profile and risk posture. Although this is by no means a comprehensive list, consider the following targets for cybercriminals:

- **Compromised and Risky Devices:** Mobile devices themselves can be compromised entirely or risky due to vulnerable operating systems, firmware, and settings.
- **Rogue / Eavesdropping WiFis:** Unsafe networks try to eavesdrop on conversations and transactions to steal confidential information.
- **Malicious Apps:** Other malicious apps that target and exploit banking apps on the device to commit fraud. These apps use a combination of phishing, permission abuse, and screen overlay tactics to exfiltrate information needed for fraudulent activity.

All these threat vectors and techniques are aimed at gaining access to the following:

- **Credentials.** Attackers may seek users' mobile banking credentials to access accounts and commit theft.
- **Personal data.** Cybercriminals focus on potentially high-value customer data such as social security numbers, dates of birth, and other sensitive information.
- **Cardholder data.** Mobile banking attacks can seek to gather card-specific data such as card numbers, expiration date information, and CVV data.

Cybercriminals understand that mobile banking apps are an easy target and present a huge potential. This notion drives hundreds of mobile banking trojans, and more sophisticated variants emerged continuously over the past decade and a half.

Why traditional fraud approaches struggle.

Reliance Transaction Analytics: Most fraud platforms today are primarily focused on transaction analytics for identifying fraudulent transactions. But RSA Fraud Research indicates that the majority of fraud occurs when a new device is involved. Today the average consumer replaces their mobile device every 24 months, making new devices a concern with existing and new account openings. Insight into the risk posture of a mobile device is limited to none.

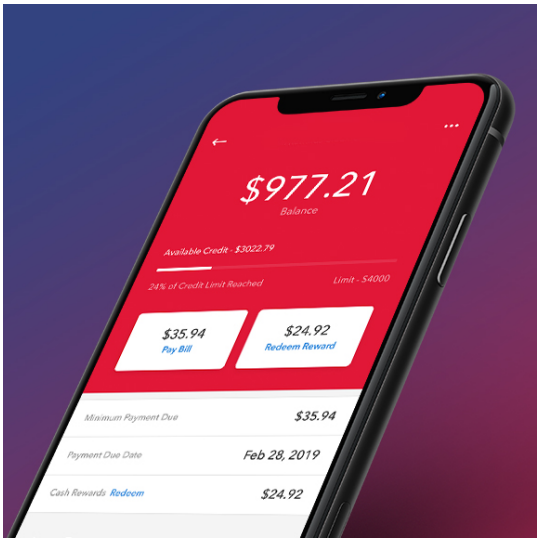
New Interaction Model: Mobile devices and the COVID pandemic have completely changed how consumers interact with banks. Consumers want to do more and more in the mobile app and enjoy a personalized experience as well. But current underlying fraud prevention infrastructure has not yet adjusted and caught up to mobile devices and mobile apps.

Implicit Trust: Most banks implicitly trust customer transactions and focus on efficiencies in executing them. They do not intervene or question the transaction as they worry about poor user experience and the liability associated with those decisions.

Mobile banking has a broad-reaching influence.

Given the incredible momentum propelling mobile banking to market dominance, it is unsurprising that leading banks are also leaders in mobile banking. The importance of the mobile experience pervades the bank's entire organization.

Banks that aim to achieve or maintain a leadership position by harnessing the tremendous potential that mobile banking represents must overcome the barriers to mobile banking security. This has become, in effect, a mandate. Zimperium makes that possible.



Zimperium enhances mobile banking application security for banks and their customers.

Zimperium provides a powerful solution with which allow mobile banking apps to **assess** a mobile device's risk posture and **defend** themselves in real-time. This real-time device attestation capability allows the mobile apps to determine if features need to be disabled or if transactions need further review. The device risk intelligence is a critical piece that's missing from most fraud algorithms today as they rely heavily on transaction analytics. The intelligence from the solution is also made available to Fraud, Risk and Compliance teams to provide visibility to help fine tune their Fraud and Financial Crime strategies for the mobile channel.

This device attestation capability is called zDefend™ and can be easily embedded into any iOS or Android application. The modular nature of the Software Development Kit (SDK) allows developers to quickly and painlessly embed the leading mobile machine learning-based detection engine, Zimperium z9™, directly inside mobile banking applications. z9 empowers the application to determine if the device it's running on is compromised, connected to an unsafe network, and even if there are malicious apps like BankBot are on the device. When a device is under attack, zDefend informs the app to initiate alerts and risk mitigation actions to mitigate the impact. zDefend is entirely configurable by app developers, who can select whatever remedial action should apply, e.g., establishing a VPN, requiring additional authentication, raising fraud scores, or requesting the user to complete their transaction a different way.

The zDefend SDK allows banks to deliver self-protecting iOS and Android apps and implement risk-based workflows within the app. Developers embed the z9 engine within applications using an easy-to-implement SDK that works with native and hybrid development platforms. Developers can spend more time developing without worrying about security.

Key Fraud-Related Benefits

Visibility

The on-device machine learning-based detection engine allows apps to gather known and zero-day attack and threat telemetry and share that with Risk and Fraud teams. The intel spans across Device, Network, Malware, and Phishing vectors. This intel is critical to ensure fraud-related policies and future investments address real risks.

On-Device Real-Time Fraud Prevention

According to RSA's Quarterly Fraud Report, 44% of fraud occurred in mobile apps in Q4 2020. On-device detection allows banking apps to immediately respond to threats on the device when the integrity of a transaction or the app itself is threatened. The advanced z9 engine can detect fake devices, banking malware, advance rooting/jailbreak, and other sophisticated techniques to steal credentials and data. In addition, the SDK allows the app to proactively limit what the user can do based on when the risk crosses a certain threshold due to changes in device, network, or phishing vectors.

Better Customer Screening

The device risk intelligence allows Fraud and Risk teams to build more accurate account holder risk profiles. It will enable banks to develop next-generation watchlists to maximize operational effectiveness. Since banking organizations deal with potentially millions of customers, this telemetry will help prioritize their review activity against those that present the most significant threat.

Continuous Transition Monitoring

Continuous fraud monitoring is the process of constantly monitoring all actions on a bank account – not just the initial login and ensuing financial transactions such as payments and funds transfers. Continuous fraud monitoring looks at all activities and events, whether they are monetary or non-monetary. zDefend provides holistic mobile app protection against mobile cyberattacks. With security safely embedded in mobile banking applications, banks can focus on innovations that will delight customers, increase customer loyalty and unleash the full potential of the mobile banking.

Building Intelligent Self-Defending Apps

Most enterprises have begun their journey of securing their mobile apps. But most stop at basic obfuscation or scanning solutions that are insufficient to counter today's sophisticated exploitation techniques. To better understand how secure your app is, reach out to us and request a FREE risk assessment. We are helping enterprises understand their exposure and secure their mobile apps.

About Zimperium

Zimperium has helped thousands of enterprises and government agencies around the world to successfully employ a mobile-first security strategy—and we're here to help your organization do the same.

Please feel free to **contact us** if we can help your team advance its mobile-first security strategies.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244