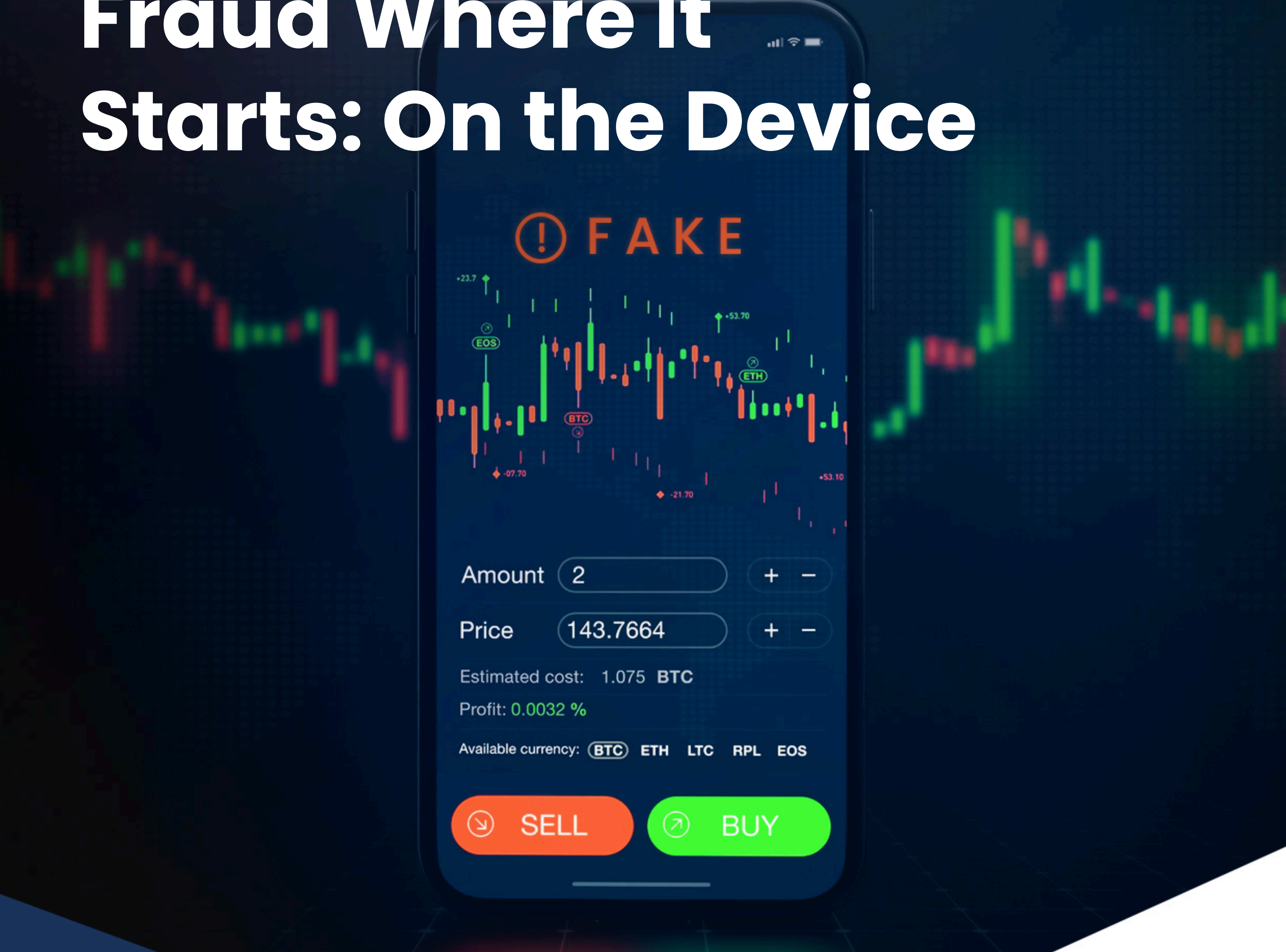
Stop Mobile App Fraud Where It Starts: On the Device



MAPS™

ZIMPERIUM®

The Growing Mobile App Fraud Landscape

The explosive growth of mobile app usage has undeniably revolutionized how we conduct business and interact with services. While organizations have invested heavily in robust online fraud detection (OFD) solutions—many incorporate mobile device intelligence and reputation checks—a critical blind spot remains: the ability to assess and adapt to the **mobile device's real-time device risk** posture. This oversight leaves mobile apps highly susceptible to sophisticated, client-side attacks that bypass traditional security measures and even those OFD systems with some mobile capabilities.

In this paper, we will explore the types of mobile app fraud, how they occur, and how Zimperium can help mitigate them proactively on mobile devices.

Common Fraud Types, Key Characteristics, and Attack Vectors

Fraud Types

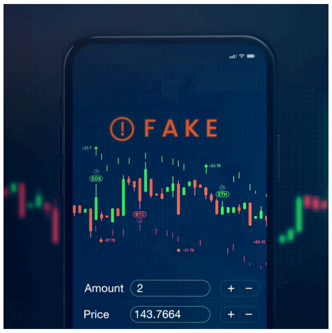
- **Credential Theft:** Attackers deploy malware campaigns to steal login credentials, PINs, or payment information to monetize.
- **Account Takeover (ATO):** Attackers use stolen credentials or brute-force techniques to log into mobile apps and carry out unauthorized transactions.
- **Device Takeover Fraud:** Hijacking a mobile device to exploit its resources.
- **Account Opening Fraud:** Using emulators and synthetic identities to open fraudulent accounts.

Key Characteristics

- **Device-Level Access:** Unauthorized access to the device via malware.
- **Persistence and Stealth:** Designed to remain undetected.
- **Real-Time Manipulation:** Fraud executed by interacting with apps as a legitimate user.

- Between January 2022 and February 2023, mobile finance app fraud was estimated to be over **$2.64 billion globally**.[1]
- In 2023, mobile banking fraud increased from 47% in 2022 to **61%**.[2]
- In 2022, app fraud in Asia-Pacific region about **$1.5 billion and North America was 1.2 billion US dollars**.[3]
- For the first time in 2024, **mobile banking fraud cases have surpassed** those originating from internet banking. This indicates a strategic move by criminals to exploit the growing popularity and convenience of mobile banking apps.[4]
- India has the highest number of mobile malware attacks globally, with a **29% increase in banking malware attacks observed**.[5]

The Growing Mobile App Fraud Landscape



Cloned Fake Applications

Counterfeit apps designed to mimic legitimate ones to gain user trust. These malicious apps are often distributed through unofficial app stores or disguised as popular apps on official stores and distribution platforms.

Below are some real-world examples.

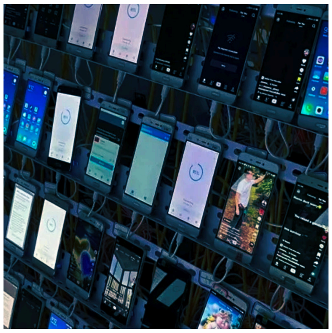
1. Fake trading apps on Google Play and App Store linked to global 'pig butchering' scam | Fortune
2. Government has warned against Union Bank's fake app and these stock trading apps
3. Fake apps posing as LIC now, be careful

Banking Trojans

Banking Trojans often masquerade as benign utility applications, productivity tools, or other seemingly harmless software. Their primary objective is to exploit vulnerabilities and manipulate legitimate banking applications installed on a user's device.

Below are some real-world examples:

1. Mobile Indian Cyber Heist: FatBoyPanel And His Massive Data Breach
2. Android Malware in Donot APT Operations
3. Mobile Banking Heists: The Emerging Threats and How to Respond



Mobile Device Farms

Mobile device farms are networks of real or emulated mobile devices used to automate fraudulent activities at scale. Fraudsters deploy thousands of devices —often running on virtualized environments, emulators, or physical racks of smartphones—to systematically bypass security measures, manipulate app ecosystems, and commit financial fraud. These farms exploit mobile apps, payment platforms, and promotional offers by mass-creating fake accounts, testing stolen credentials (credential stuffing), or executing automated transactions to steal funds, launder money, and exploit referral programs.

Below are some real-world examples:

1. America's DIY Phone Farmers
2. Chinese scammers use 4,600 phones
3. Chinese media exposes criminal smartphone farms | The Register

The Blind Spot: Security Gaps Enabling Fraud

Most organizations have basic security measures, such as source code scanning, code obfuscation, API security, etc. However, according to Zimpeirum's research, these are the most common security gaps in mobile apps that allow fraudsters to abuse and exploit the mobile app.

Most Prevalent Mobile App Security Gaps

Security Gap	Why it Matters for Fraud
Relying solely on signature-based detections 1. For Malware 2. For Rooting/Jailbreak 3. For Emulator 4. For Tampering	1. Attackers use zero-day malware variants that don't match existing signatures, bypassing security checks. 2. Attackers use dynamic hooking techniques to hide root status from security checks. 3. Attackers use runtime hooking, overlay attacks, and repackaging techniques to modify apps without triggering signature-based alerts.
Lack of continuous monitoring and security visibility across the app install base	1. **Blind Spots Enable Attacks** – Without continuous monitoring, malware, tampering, and device threats go undetected, increasing fraud risk. 2. **Delayed Threat Response** – Lack of real-time security insights means fraud teams react too late, leading to higher financial losses and reputational damage. 3. **Regulatory Non-Compliance** – PCI DSS, PSD2, and other regulations require ongoing security visibility, not just point-in-time assessments.
Over-the-air updates are not possible for in-app detections and mitigation actions	1. **Security Gaps Persist** – Without OTA updates, apps remain vulnerable until the next release cycle. 2. **Operational Bottlenecks** – Constantly rebuilding and resubmitting apps slows response time and burdens development teams. 3. **Regulatory & Fraud Risk** – Delayed patches increase exposure to attacks, leading to compliance violations and financial losses.

It's critical to note that these are**device-level** security gaps that are being exploited. They exist at the device level. This means the security gaps are present on the mobile device itself, not just the network or the app's server-side infrastructure. Exploiting these vulnerabilities allows attackers to gain unauthorized access to the device. This security blind spot enables attackers to bypass app protection, steal sensitive data, and carry out fraud unnoticed.

The Remedy: Real-time Mobile Trust Signal

A Real-time Mobile Trust Signal allows an app to instantly assess the risk associated with the device it's running on and adjust its behavior to prevent potential fraud proactively. This real-time assessment enables the app to adapt its behavior by identifying a compromised device or suspicious activity and taking preventative measures such as blocking transactions, limiting access to sensitive data, or triggering additional authentication steps. This real-time response significantly reduces the window of opportunity for fraudsters to exploit vulnerabilities and carry out their schemes.

Zimperium’s Role in Stopping Fraud

Zimperium’s **Mobile Trust SDK** enables a proactive approach to mobile app fraud prevention by empowering apps to assess the **device's risk posture and take preventive action, if necessary,** before allowing any high-risk transactions and events.

The SDK is automatically injected into the application during development via a console, delivering multiple layers of fraud detection and on-device protections without compromising the customer experience (CX). Once embedded, apps can instantly detect threats on the device. Threat responses are selected on a policy page on the central console and pushed over-the-air to all running instances of the app.

Empowered with a **Mobile Trust Signal,** the app can **establish trust before** allowing sensitive activities or transactions. If a device fails these trust checks, it can take action and dynamically limit logins and risky features to protects itself and the user, minimizing fraud exposure.

As fraud techniques and campaigns evolve, the SDK's detection capabilities and threat response capabilities are **updated over-the-air.** Zimperium automatically sends the SDK news detections. Through the central console, app teams can update and deploy threat responses in real-time. Over-the-air security updates allow cybersecurity, compliance, and fraud teams to continuously adapt to fraud-driven attacks and techniques without publishing new versions of apps, saving time and money.

Once Zimperium-protected apps are published, risks, threats, and attacks across the install base are reported in real time to a **central console,** allowing for continuous monitoring across the app footprint, effective incident response, and fraud rule enhancements. Rich APIs allow security and forensics data from this central console to be exported into broader Fraud Management and Orchestration systems.

Detections & Preventions

A Zimperium-protected app can detect and respond to threats on the device in real-time, even without a network connection. Below is a list of detection and actions enabled within the application.

On-Device Detections	In-App Response Actions
App Reversing Attempts App Tampering Attempts App Cloning/Repackaging SSL Unpinning / Network Attacks Key Logger Detection Screen Overlay Detection Devices without PIN Codes Emulators Device Rooted/JailBroken Compromised Devices Device Instrumented with Hacking Tools Devices Running Vulnerable OS Sideloaded Malware Accessibility Permission Active Screen Sharing Active	Alert the Admin Disable Login Disable Feature Crash The App Step-Up Authentication Webpage Redirect Call Custom Function Other

Fraud Prevented Through These Capabilities

Fraud Type	What is the protected app's defense?
Prevent App Cloning & Tampering	Blocks unauthorized execution, reverse engineering, and app modifications using hacking tools like Frida and Magisk.
Stop New Account Opening Fraud	Detects emulators, device farms, and bots, preventing fraudulent account creation.
Prevent Account Takeovers	Blocks credential and key theft via malware, stopping fraudsters from hijacking user accounts and executing unauthorized transactions.
Enhance Account & User Risk Scoring	Leverage the on-device AI engine to generate real-time security telemetry, enabling organizations to identify high-risk users and fraudulent account links proactively.

Conclusion

Zimperium's Mobile Trust Signal is an essential part of an enterprise's holistic online fraud prevention strategy. Integrating Zimperium with existing service-side and device intelligence solutions provides organizations with a complete strategy. As mobile app adoption grows, the need for mobile trust signals will become increasingly critical in safeguarding user trust, sensitive data, and financial transactions.

Take Action Now

Contact Zimperium to schedule a demo and explore our mobile security solutions.

Contact Us

Sources

1 https://www.statista.com/statistics/1380417/app-fraud-value-by-category/#:~:text=Mobile%20app%20fraud%20estimated%20global%20value%202022%2D2023%2C%20by%20category&text=Between%20January%202022%20and%20February,fraudulent%20or%20fake%20app%20installs.

2 https://www.securitymagazine.com/articles/100194-mobile-payment-fraud-increased-in-2023#:~:text=According%20to%20a%20recent%20report,Read%20the%20full%20report%20here.

3 https://www.statista.com/statistics/1380426/app-fraud-value-by-region/#:~:text=Between%20January%202022%20and%20February,around%201.2%20billion%20U.S.%20dollars.

4 https://www.biocatch.com/blog/annual-uk-finance-fraud-report-shows-fraud-still-top-crime-in-uk

5 https://www.newindianexpress.com/business/2024/Dec/03/india-tops-global-list-for-mobile-malware-attacks-banking-systems-particularly-vulnerable

Author: Krishna Vishnubhotla

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank.

www.zimperium.com

ZIMPERIUM®

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