The Mobile Shopping Report

From Carts to Credentials: Inside the Holiday Surge of Mobile Threats

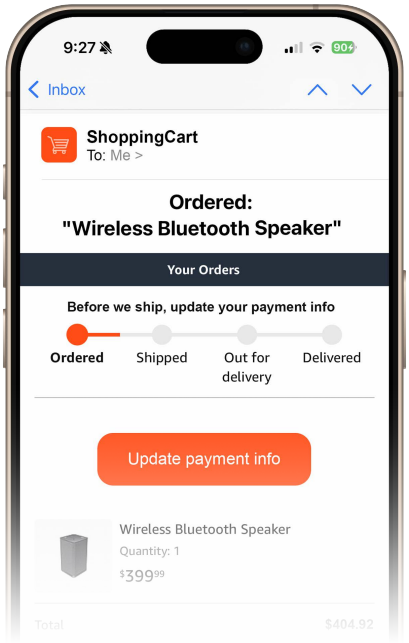
www.zimperium.com

ZIMPERIUM®

Executive Summary

The annual surge of retail sales—from Black Friday through the holiday season—is a lucrative period for both shoppers and cybercriminals. As consumers flock to e-commerce apps, digital wallets, and delivery platforms, threat actors intensify their activity across three major attack vectors: **mishing (mobile phishing), malware,** and **apps.**

Mishing remains the most immediate and scalable threat. Historically, **smishing** (phishing via SMS/text messages) and malicious link campaigns surge in November and December, taking advantage of the flood of holiday-related messages and shipping notifications. We have seen this seasonal mishing surge be as high as 4x in our data. Attackers leverage trusted brand names and create urgency to deceive users into clicking, logging in, or downloading malicious "updates".



Additionally, **malware** continues to evolve, with banking trojans and remote access tools now targeting shopping and payment apps in addition to traditional financial institutions. There are a plethora of malware families that exploit accessibility features, screen overlays, and permissions to steal credentials, capture credit card information, and intercept one-time passwords (OTPs). Even outdated trojans resurface during peak seasons, rebranded or rebuilt to blend in with legitimate traffic.

Finally, **apps** represent a quieter but equally significant exposure vector. Legitimate apps can unintentionally introduce vulnerabilities through use of insecure SDKs, misconfigurations, or granting excessive device data and feature permissions. As retailers rush to roll out seasonal features or marketing updates, these risks increase, creating potential pathways for data exposure, privilege escalation, or tampering by third-party code.

For enterprises, these same threats have far-reaching implications. Compromised consumer devices, malicious apps, or phishing campaigns that impersonate corporate brands can quickly evolve into large-scale fraud, data leakage, or reputational damage. Employees using personal devices for work (BYOD) or interacting with third-party mobile services further expand the attack surface, blurring the line between consumer and enterprise exposure. As mobile commerce and corporate mobility continue to converge, securing this ecosystem becomes a core business and compliance imperative.

Together, these three threat categories define the mobile threat landscape of the holiday season. The following sections examine real-world examples of phishing spikes, malware targeting patterns, and app-level vulnerabilities uncovered during zLabs' ongoing monitoring and analysis.

Mishing: One Click Away

Mishing remains the most active and successful mobile threat vector during the holidays. Smishing campaigns spike around shipping deadlines and retail events such as Black Friday or Cyber Monday. Messages often impersonate logistics providers or e-commerce brands ("Your package is delayed — click here"). Shopping via Mobile apps and devices is becoming more the norm, and cybercriminals are looking to exploit and secure big returns.

As mobile apps and devices become the primary channel for holiday shopping, cybercriminals are exploiting this shift for bigger returns. zLabs' telemetry over the 2024 shopping season observed a 4x increase in mishing sites during sale season compared with monthly averages. We also noted a two fold increase in the number of targeted shopping sites during the Christmas shopping season and a four fold increase during early January. Attackers are also migrating to encrypted mobile messaging platforms, making detection increasingly difficult.

Figure 1 shows weekly active phishing sites that impersonated Amazon during the extended 2024 holiday shopping season. Even though the majority of the phishing attempts reported took place during Christmas and New Year, some notable detection spikes occurred around Amazon's Fall Prime Event and Black Friday, reflecting how attackers continuously adapt to mobile-driven retail events.

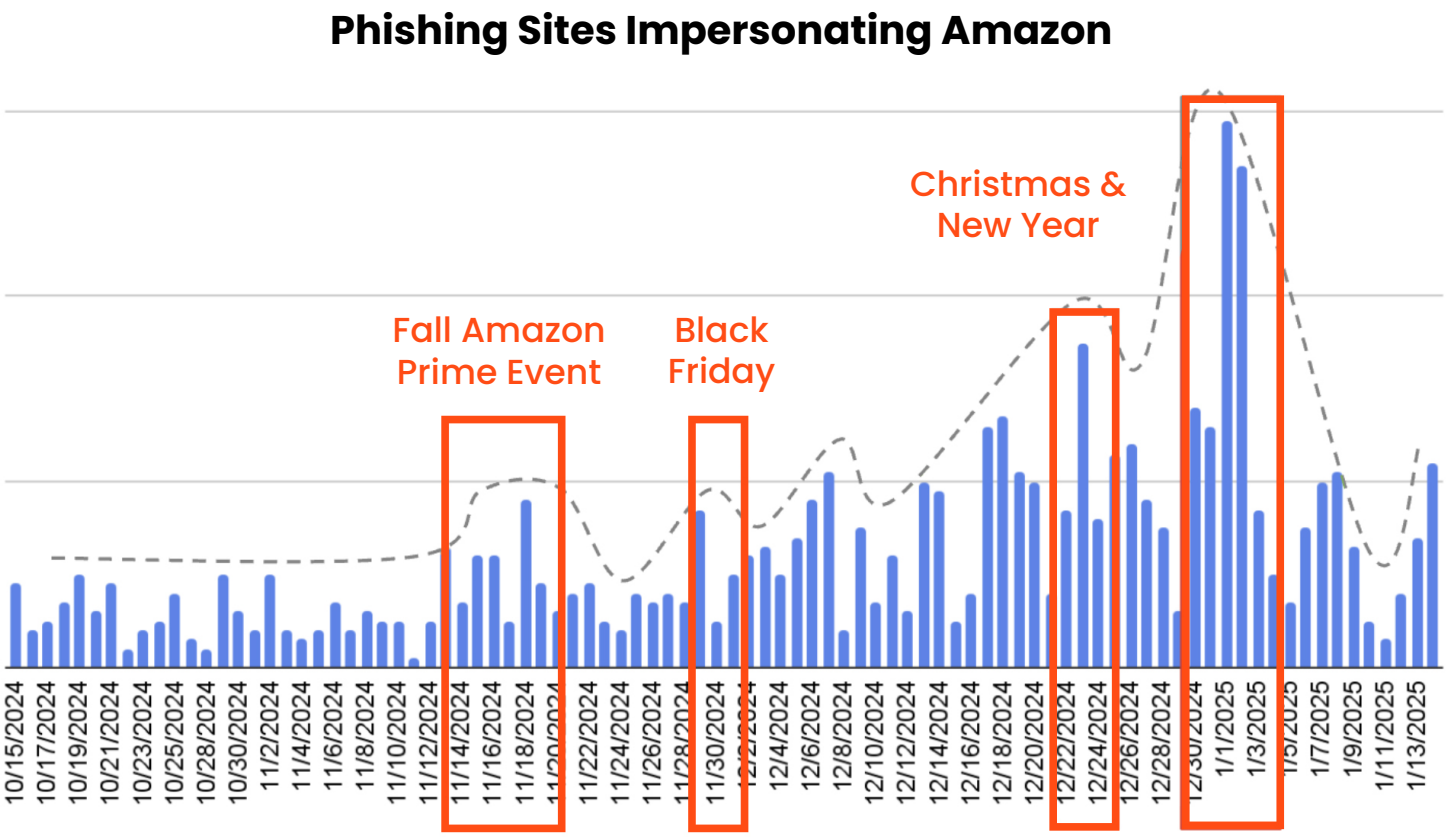


Figure 1: Increase in phishing sites targeting Amazon. The trend shows how the attacks increase during typical sales seasons.

We observe a similar dynamic for all shopping sites. In **Figure 2**, the aggregate trend for all major shopping sites is shown. The red line shows the average number of events detected. We can see how there are multiple periods of time where the number of detections targeting these sites rise well above the average four periods of time across the holiday shopping season:

- **Period 1:** Black Friday in the US.
- **Period 2:** Cyber Monday
- **Period 3:** Christmas buying season. This longer, wider spike captures the full run-up to Christmas, highlighting varied consumer habits from early November shopping to last-minute purchases in late December.
- **Period 4:** This final spike extends into the new year, often reflecting specific regional shopping traditions, such as gift-giving tied to Epiphany morning (January 6th).

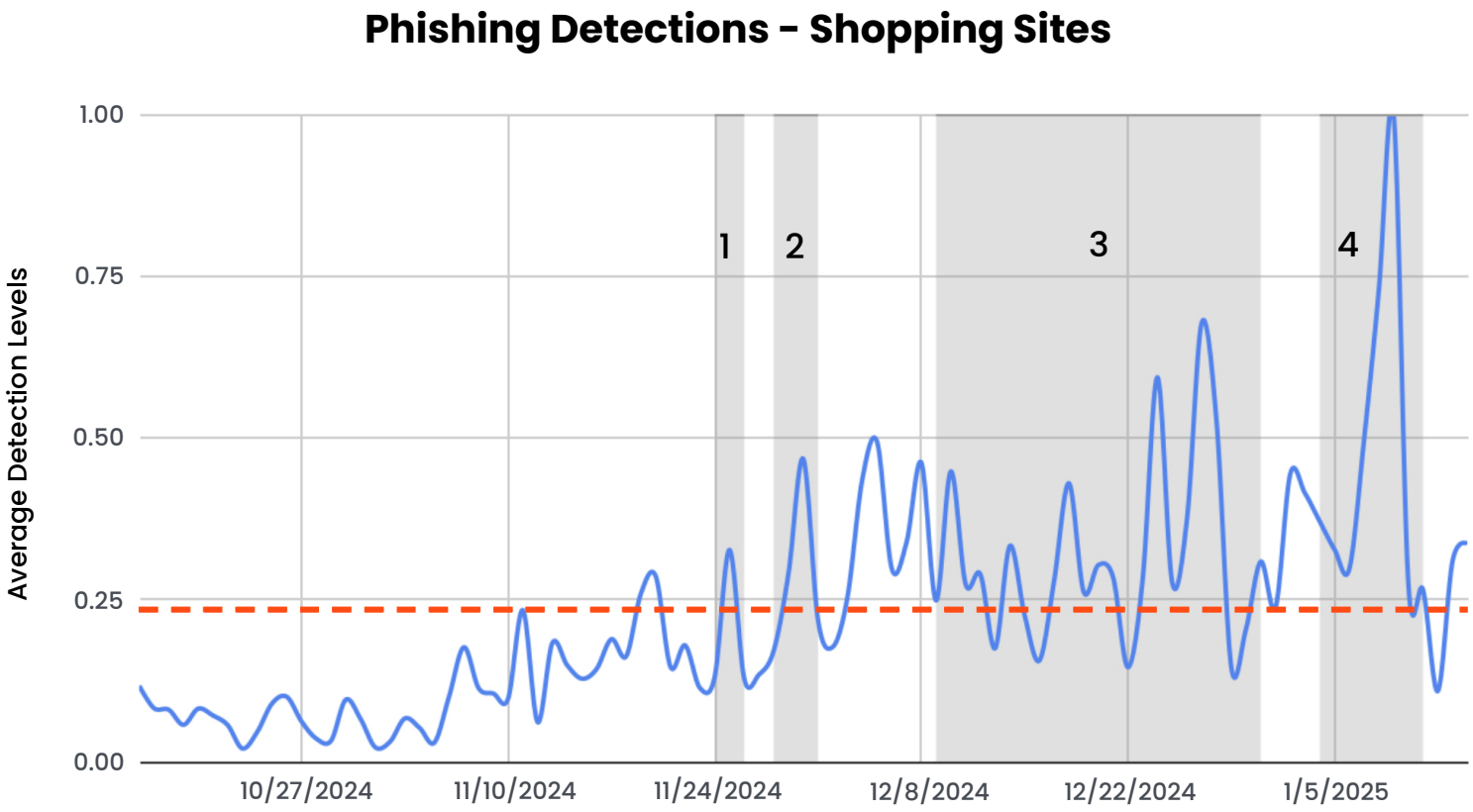


Figure 2: Combined trend for all major shopping sites. We can see how similar dynamic is observed. In this case, there is a bigger dispersion due to different shopping season in different regions.

After analyzing the world's most prominent shopping brands, our zLabs research team identified the top 5 most-targeted organizations **(Figure 3)**. These brands collectively serve billions of people across all geographies, which naturally makes them a highly appealing and concentrated target base for malicious actors.

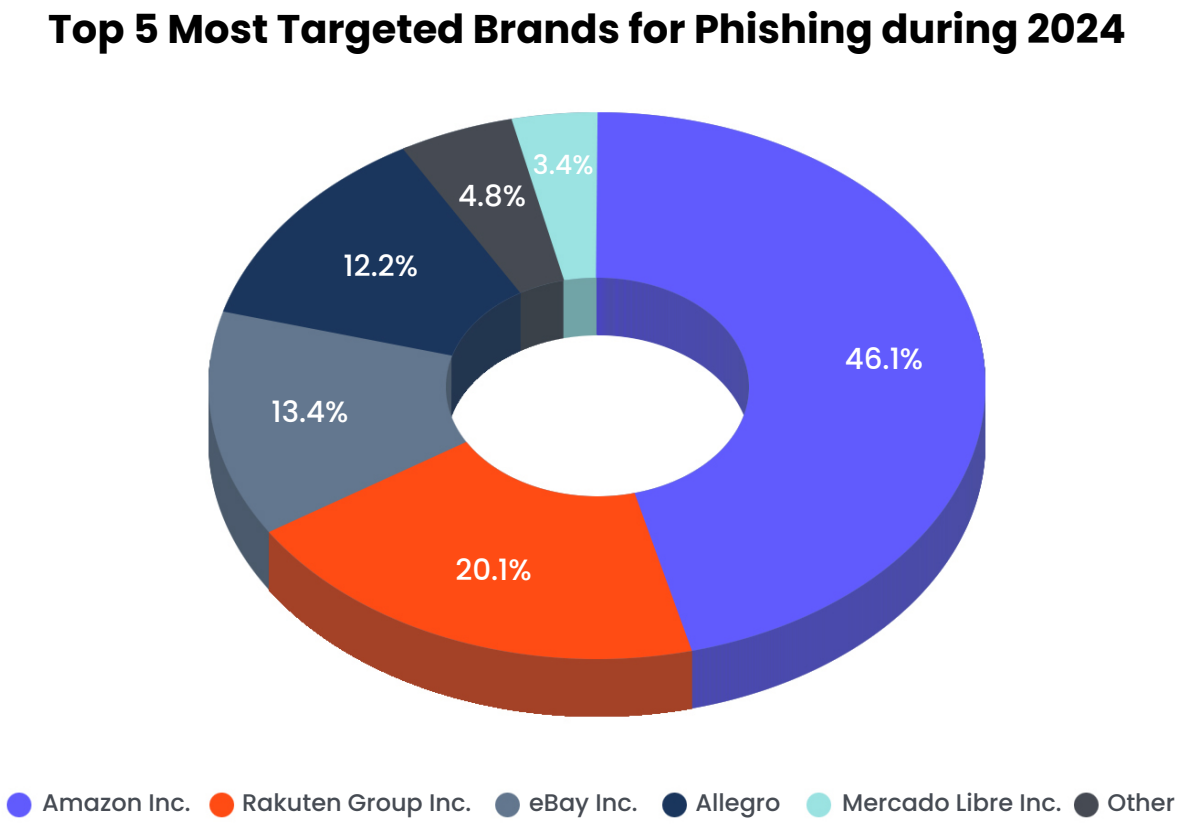


Figure 3: Top 5 targeted brands worldwide in 2024.

Phishing campaigns during the holiday season don't just target online stores — they systematically exploit the entire consumer supply chain. Attackers broaden their focus beyond retail brands to include payment processors, digital wallets, and shipping services, creating a seamless illusion of legitimacy that follows users from purchase to delivery. By impersonating trusted intermediaries such as payment gateways or logistics providers, adversaries can intercept credentials, payment information, or delivery confirmations at multiple points in the transaction flow. This multi-stage approach makes detection by users more difficult and significantly increases success rates, as users expect and trust messages from these services during peak shopping months.

This extended threat surface is clearly illustrated in **Figure 4**, which displays combined fraudulent events targeting popular payment platforms, using data collected by zLabs from third-party feeds. Mirroring the e-commerce trend, the number of detected events substantially exceeds the average during critical timeframes. Notably, two distinct periods are most prominent:

- **Period 1:** Coinciding with Halloween
- **Period 2:** Coinciding with the Christmas shopping seasons

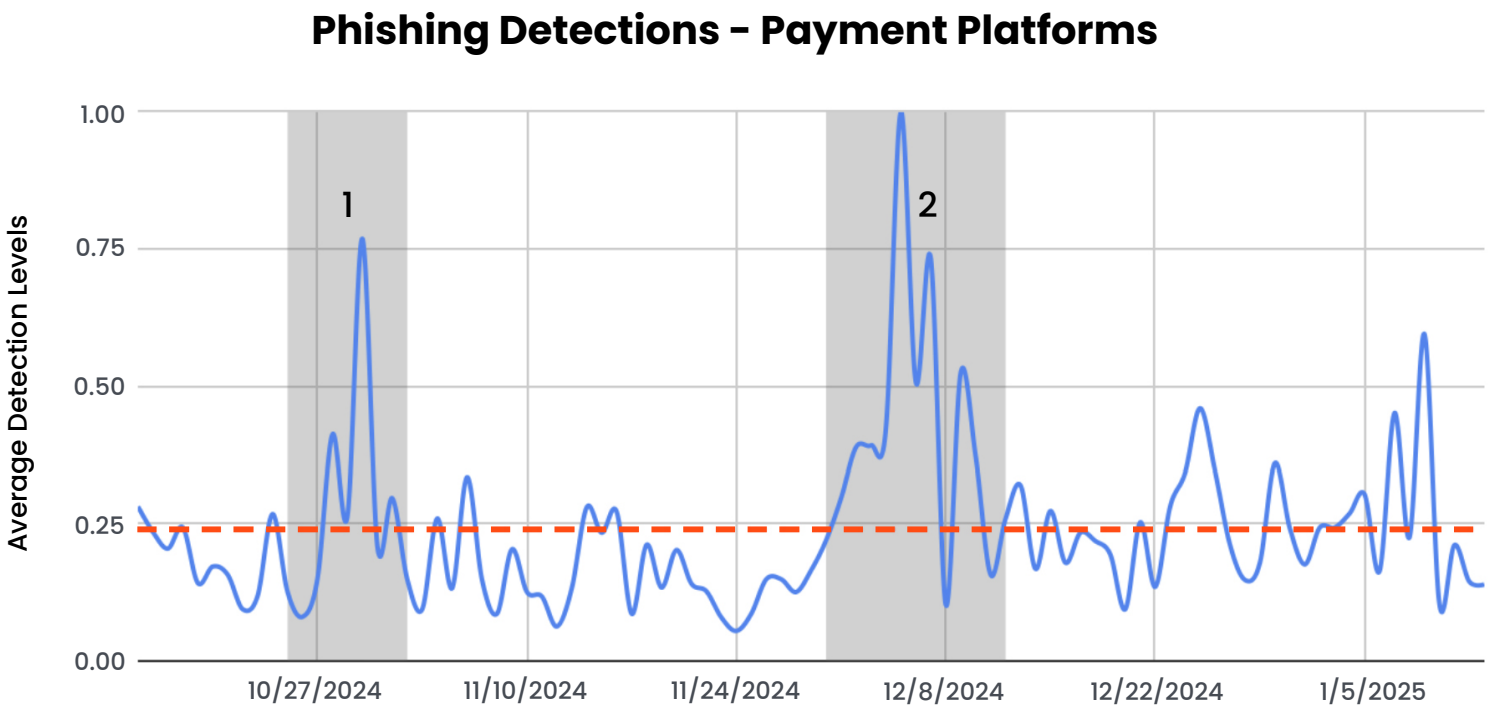


Figure 4: Phishing detections on most popular payment platforms. Similar as before, the red line shows the average number of events. We can see that there are periods of time where the actual detections exceed the average greatly.

Figure 5 illustrates a similar trend but from the point of view of phishing attacks targeting delivery services and couriers. Much like the shopping websites, we can clearly identify 4 peaks of activity:

- **Period 1:** Black Friday and CyberMonday's deliveries
- **Period 2:** Early Christmas shoppers' deliveries
- **Period 3:** Late Christmas shoppers' deliveries
- **Period 4:** Deliveries for people celebrating Epiphany instead of Christmas

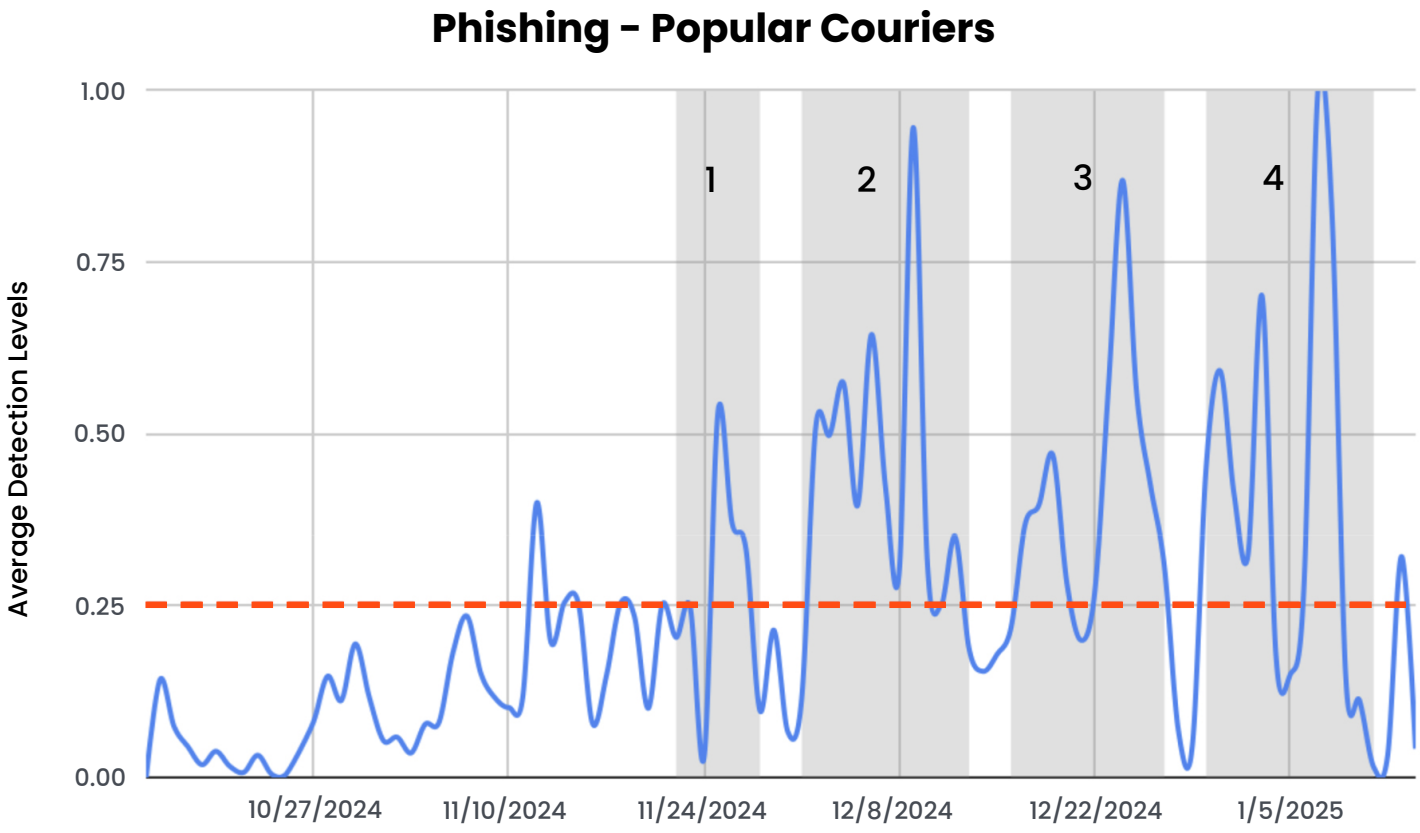


Figure 5: Phishing detections targeting most popular couriers.

For enterprises, these same phishing and smishing campaigns often double as initial access points into corporate systems. Employees receiving brand-related or shipment messages on BYOD or COPE (corporate-owned, personally-enabled) devices can inadvertently expose single sign-on credentials or install mobile malware that bridge personal and corporate environments. These mobile threats extend beyond individual compromise, they create direct pathways into enterprise networks. Logistics and vendor impersonation phishing can also be weaponized to compromise mobile-based supply chain communications, leading to financial fraud or data exfiltration.

Malware Targeting Shopping Apps

The holiday season is prime time for counterfeit retail apps. Threat actors take advantage of the chaos and high consumer activity to publish look-alike mobile retail apps mimicking major e-commerce brands to harvest credentials and payment data. These apps are often distributed through third-party stores, mishing links, or fake update prompts.

Recent industry research identified over 120,000 fake mobile apps in 2025, with 65% impersonating retail or financial brands. At the same time, a Federal Trade Commission's report noted that retail and e-commerce were the most targeted verticals, coinciding with a 25% increase in mobile fraud losses during 2024.
Another source of risk is malicious apps targeting legitimate applications. These are typically trojans and are designed to compromise user data (such as credentials, OTPs and credit card information) by performing **overlay** or more sophisticated attacks.

Figure 6 illustrates the scope of this type of threat, displaying known trojan families and the popular shopping apps they target. While some of these families may be outdated and pose little current risk, their existence highlights well-known shopping applications are a consistent target for malicious threat actors during the holiday season.

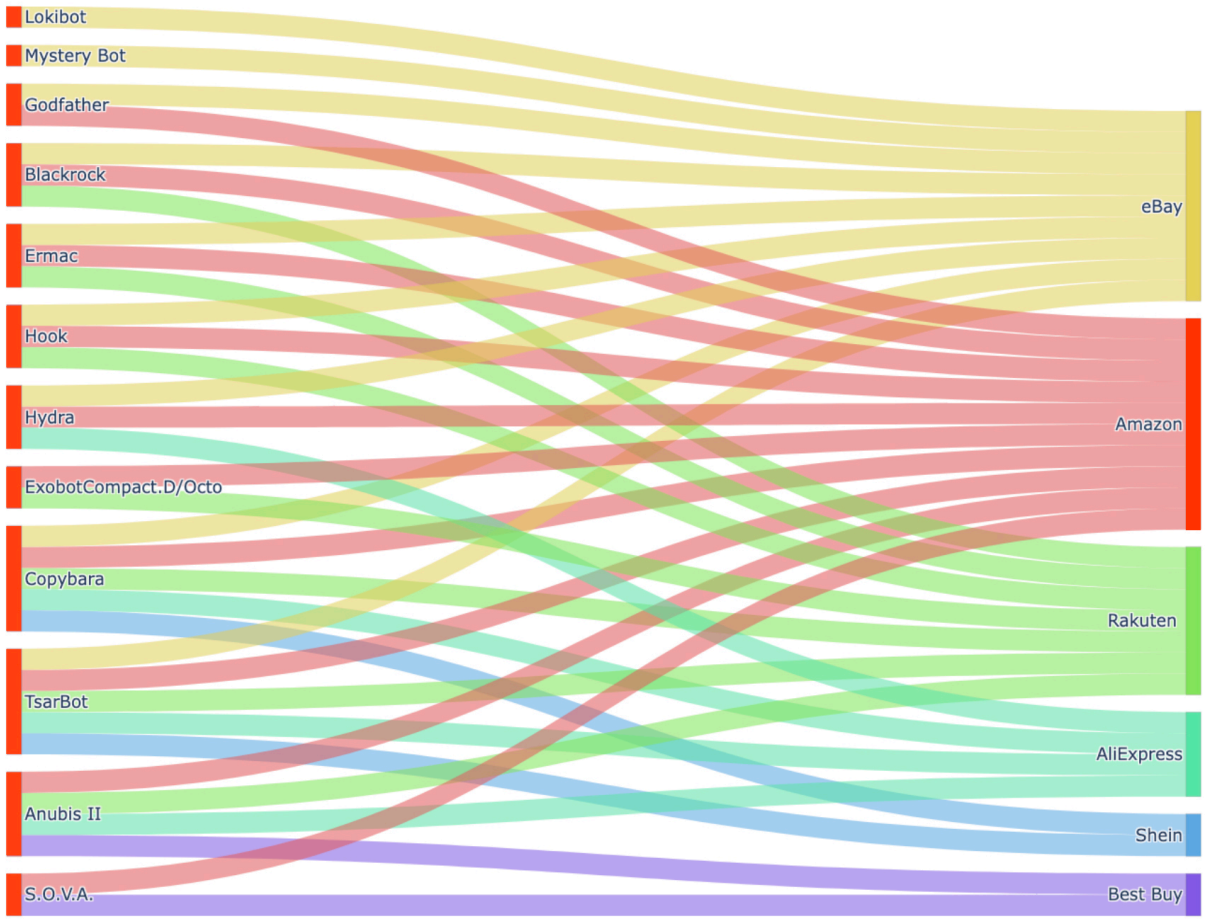


Figure 6: Malware families targeting popular shopping apps. Each malware family is represented in the left of the chart while shopping apps are on the right. A link between a malware family and a shopping app means that the app is a target of that family. As an example, Shein is targeted by Copybara and TsarBot.

During the holiday season, digital wallets and contactless payments see massive use during the holidays, and cybercriminals are quick to take advantage. Banking trojans and overlay malware are increasingly targeting wallet apps and mobile banking clients, stealing credentials and intercepting one-time passwords. These types of threats pose a significant challenge for financial institutions working to protect customers and customer transactions. **Figure 7** shows how malware trojans target the most used and popular wallets and payment apps.

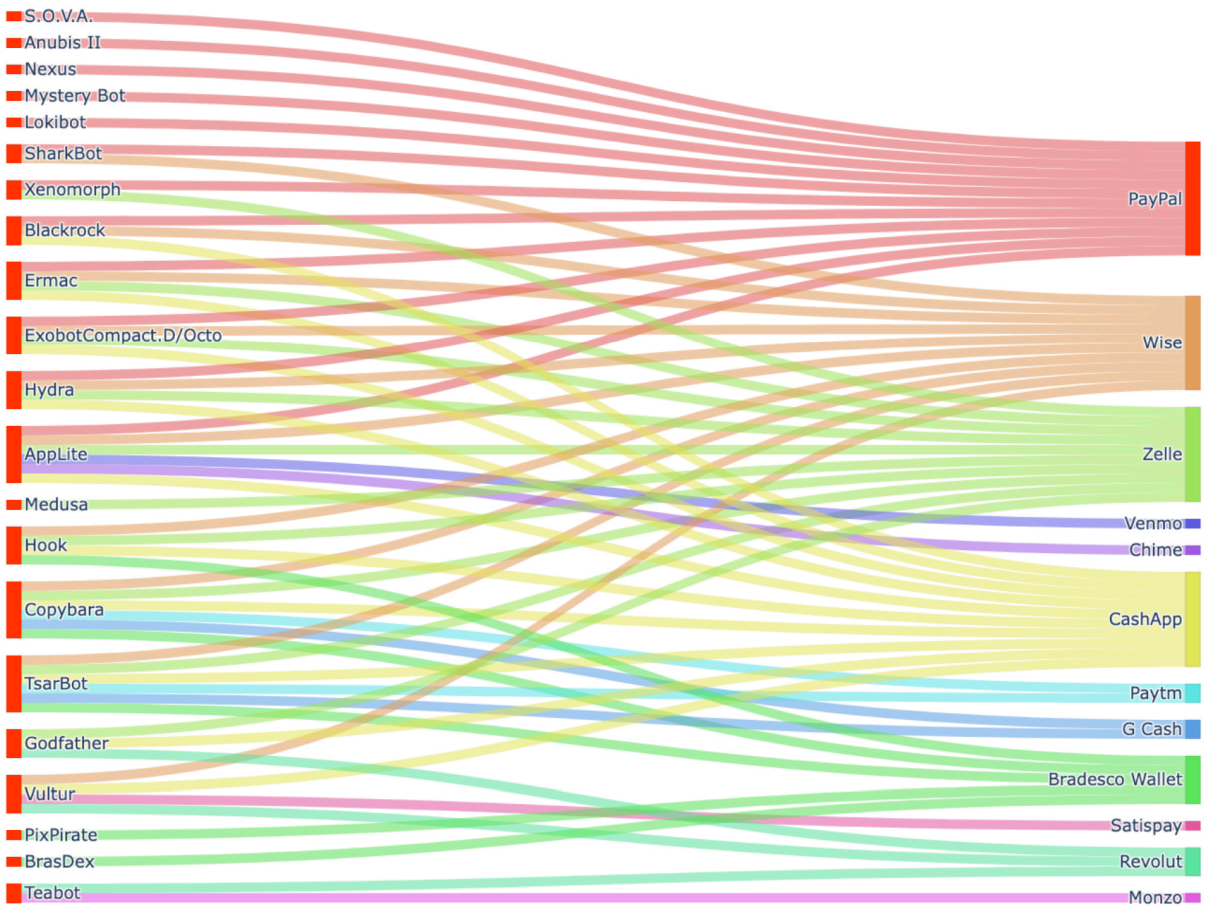


Figure 7: Malware families targeting payment apps. As in the previous figure, malware families are shown on the left and payment apps on the right. Each link indicates a targeted app—for example, Teabot targets Monzo.

These attacks aren't caused by anything the app developer does — aside from the app's popularity making it a target. However, they highlight the importance of implementing mobile runtime protection to limit the impact of trojans and other malicious activity.

For organizations, the presence of such malware within customer ecosystems can erode trust, inflate fraud-related costs, and create compliance liabilities. If corporate or partner devices are compromised, these trojans can harvest business-critical credentials, gain lateral movement into enterprise accounts, or compromise transaction integrity within official retail or banking apps.

App Vulnerability Exploits *(Behind the Checkout Button)*

While phishing and malware dominate the headlines, some of the most overlooked risks originate within the apps themselves. Using Zimperium's zScan and zLabs' mobile application security assessments, we analyzed several top-ranked shopping apps across different geographies to identify privacy, security, and compliance gaps that could be exploited by malicious actors.

From a corporate perspective, these issues extend far beyond end-user privacy concerns. Enterprises that integrate or whitelist vulnerable third-party apps — whether for marketing, logistics, or internal productivity — inherit these same weaknesses into their environments. Likewise, brands whose official apps are distributed alongside compromised third-party cloned versions face direct reputational and regulatory exposure. These findings don't necessarily indicate intentional abuse; rather they often result from common development oversights or risky third-party integrations. However, under the right circumstances, these weaknesses could be weaponized by attackers to harvest sensitive user data, distribute malicious code, or undermine runtime protections.

The following examples highlight real-world examples of highly popular retail and e-commerce apps—each ranking within the top 100 of its category—that contain potential vulnerabilities. Each story illustrates how seemingly minor misconfigurations, such as insecure WebViews, exported components, hardcoded keys, or weak SSL validation, can quickly become exploitable attack vectors when combined with social engineering or trojan-based campaigns.

Story 1

OS: Android

Risk type: Third-party SDK/ Supply-chain

Impact level: Critical

Weaponization potential: Remote payload execution and mass data exfiltration

One of the most concerning findings came from a popular shopping app with over 1M installs used globally. The app integrates a third-party SDK previously reported for secretly collecting and transmitting sensitive user information — including GPS location, call logs, and device identifiers — to servers hosted in China. Beyond privacy implications, this SDK also supports encrypted runtime payload delivery, allowing new code to be downloaded and executed remotely without requiring an app-store update. In effect, the app could be repurposed into a malware dropper at any time without the developer's knowledge or user consent.

From an app-vetting and ecosystem-risk perspective, this is a clear example of how trusted apps can become part of a broader **supply chain compromise.** The silent data exfiltration exposes the brands and partners associated with the app — to regulatory and reputational damage, while the remote code-loading capability elevates the risk from passive surveillance to active compromise of users and their confidential data. Because the SDK is reused across multiple applications, a single malicious update or server command could simultaneously weaponize hundreds of legitimate apps, magnifying the potential for fraud, espionage, and consumer data abuse at scale. For enterprises, this could be extremely risky since the SDK's remote payload delivery could be exploited to distribute malicious code within enterprise-approved apps, creating a stealthy supply chain breach.

Story 2

OS: Android

Risk type: Cloud Misconfiguration/ Data Exposure

Impact level: High

Weaponization potential: Unauthorized access to stored assets and reconnaissance for further exploitation

In another case, we identified a shopping app installed on over 10M devices and extensively used in Eastern Europe. This app contained hardcoded references to **cloud storage locations with world-viewable file and directory listings**. These storage endpoints were publicly accessible and allowed unauthenticated users to browse file structures and contents, a direct path for potential **data exposure** or **unintended disclosure of personally identifiable information (PII).**

From an app-vetting perspective, this represents a **serious security misconfiguration** with potential privacy, compliance, and reputational implications. Publicly accessible cloud directories can be easily discovered through automated scans or search indexing, exposing sensitive or proprietary data to unauthorized access. Even seemingly harmless files (such as metadata, temporary uploads, or logs) can reveal information about users, internal infrastructure, or API endpoints that could be leveraged by attackers for reconnaissance, social engineering, or further compromise. For companies, these weaknesses can escalate to regulatory noncompliance if personal data is ever stored, cached or inadvertently exposed in these locations.

Story 3

OS: Android

Risk type: Hardcoded private key/improper key protection

Impact level: High

Weaponization potential: API Impersonation, Signature Forgery, Decryption of Protected Assets, Credential Compromise

Across three different top 100 shopping applications with over 150M combined installs and a global user base, we identified the same critical issue: the presence of **unprotected private keys** embedded within the app packages. These keys were stored in clear text or other easily extractable formats, without encryption or any platform-level protection. Because private keys are intended to secure sensitive operations — such as authenticating with APIs, signing requests, or encrypting local data — their exposure completely undermines the confidentiality and integrity those mechanisms are meant to guarantee.

From an app-vetting standpoint, this type of finding represents a **systemic and recurring security flaw** rather than an isolated mistake. When private keys are distributed inside production binaries, any attacker or researcher who downloads the APK can extract and reuse them. This allows threat actors to **impersonate legitimate app instances, forge authenticated requests to backend systems**, or **decrypt protected information** if the same key material is used elsewhere. If the same key is shared across multiple apps or reused across versions, the exposure becomes a persistent risk—enabling long-term impersonation and fraud that is difficult to detect or revoke. Moreover, exposed keys can allow attackers to impersonate corporate apps or APIs, potentially signing malicious payloads or distributing counterfeit apps under a trusted brand identity.

Story 4

OS: iOS

Risk type: Embedded jailbreak/tooling artifacts

Impact level: High to Critical

Weaponization potential: Privilege Escalation, Bypass of Platform Protections, or Persistence Facilitation

One iOS shopping app with more than 1M ratings and primarily used in the USA with a global user base contained **tools typically bundled with jailbreak utilities**, including binaries and frameworks known to interact with restricted iOS components. While their presence does not necessarily indicate active exploitation, such artifacts are highly unusual in production apps and can pose significant security concerns.

From an app-vetting perspective, these components could be leveraged to **bypass iOS security controls** or **escalate privileges** if triggered, whether intentionally or through a malicious payload. Their inclusion expands the app's attack surface, undermines user trust, and introduces potential compliance and store-policy violations. Even if dormant, these tools could be reactivated in future versions or exploited as a ready-made vector for privilege escalation.

Story 5

OS: iOS

Risk type: Unauthorized use of private APIs

Impact level: Medium

Weaponization potential: Privilege Escalation, Data Exposure, or Policy & Compliance Violation

Five top 100 iOS shopping apps with worldwide reach were found to be **using undocumented or private Apple APIs**, which are explicitly prohibited for publicly distributed apps distributed through the App Store. Private APIs provide access to internal iOS functions not available to standard developers and can alter system behavior, access protected data, or interact with restricted device components.

From an app-vetting perspective, this creates both **security and compliance risks.** The use of private APIs can lead to **unintended privilege escalation**, system instability, or exposure of protected, and may enable the app to perform actions that violate Apple's sandboxing model. Beyond potential App Store rejection, these calls *expand the app's attack surface and could be exploited by threat actors if flaws exist in the underlying APIs or if sensitive data is mishandled.*

Story 6

OS: iOS

Risk type: Vulnerable third-party/native library (CVE-2023-4863)

Impact level: High

Weaponization potential: Crafted-image exploitation; RCE; downstream payload delivery

Among eight of the shopping apps reviewed, Zimperium's zLabs team identified the same risky dependency: an embedded version of the **libwebp** library version known to be vulnerable to **CVE-2023-4863** (a critical remote code-execution flaw). The vulnerable library is packaged inside each app, meaning that simply opening or rendering a specially crafted WebP image within the app context could trigger the flaw. The presence of this component creates a clear avenue for attack by adversaries able to supply malicious image content — for example, *via user-generated uploads, in-app ad networks, or untrusted WebView content.*

From an app-vetting perspective, this represents a classic supply-chain or third-party component risk that demands immediate remediation. Vulnerable native libraries can enable memory-corruption exploits that lead to crashes, data leakage, or in the worst case, arbitrary code execution on the device—turning otherwise safe functionality (like image rendering) into an active attack surface. Because the same library is reused across multiple apps, a single exploit technique could be leveraged repeatedly across large user populations and regions, amplifying its potential impact.

Broader Risk Trends Across the Ecosystem

Beyond individual case studies, aggregated results from Zimperium's zLabs' assessments of both Android and iOS shopping apps reveal recurring structural and compliance weaknesses that expand the overall attack surface of the mobile commerce ecosystem.

Android applications, in particular, continue to show a high prevalence of dynamic-code and component-exposure risks. **Figure 8** shows the most common problems found in the top 100 shopping apps.

Approximately **24%** of analyzed apps include functionality that can **retrieve Java classes or DEX files from remote locations**, effectively allowing the codebase to change at runtime. While often intended for modular updates or feature delivery, this capability can also be exploited to inject unverified or malicious code without user knowledge or consent.

Around **19%** of apps expose at least one **unprotected exported Service**, which could let any other app on the device start or bind to it—potentially leading to data leakage or unauthorized operations.

An additional **14%** suffer from **implicit activity vulnerabilities** that may let attackers access arbitrary files stored in /data/data/ paths, including user-generated content or credentials. Finally, **11%** of Android apps were found to be **signed with weak APK Signature Schemes**, undermining package integrity and enabling tampering or repackaging attacks.

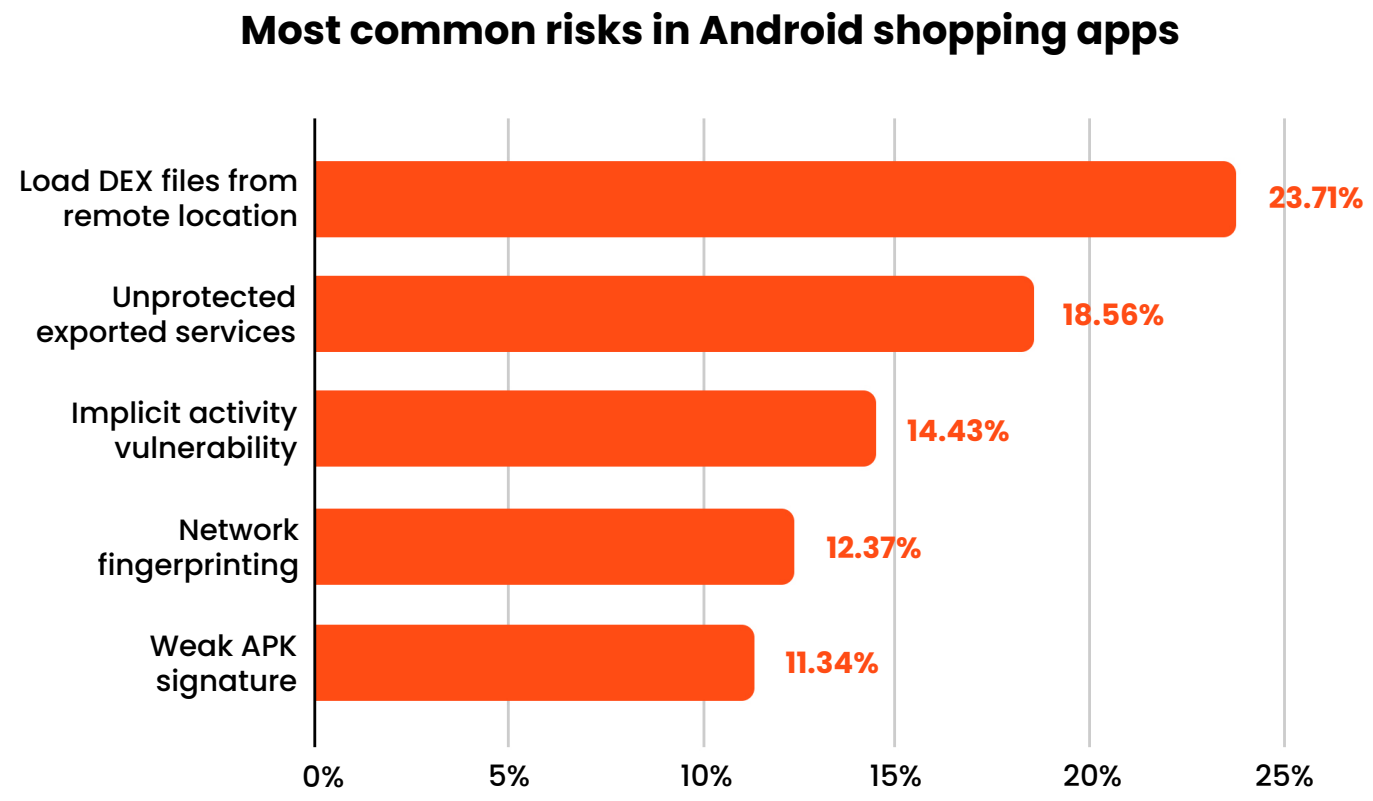


Figure 8: Most common risks found in top Android shopping apps.

iOS applications reveal a different and distinct set of weaknesses—centered more around transparency shortcomings rather than direct code-execution flaws. The most common issue identified across iOS apps involves inaccurate or noncompliant App Store "privacy nutrition labels," which often misrepresent how user data is collected, shared, or tracked ***(see Figure 9)***.

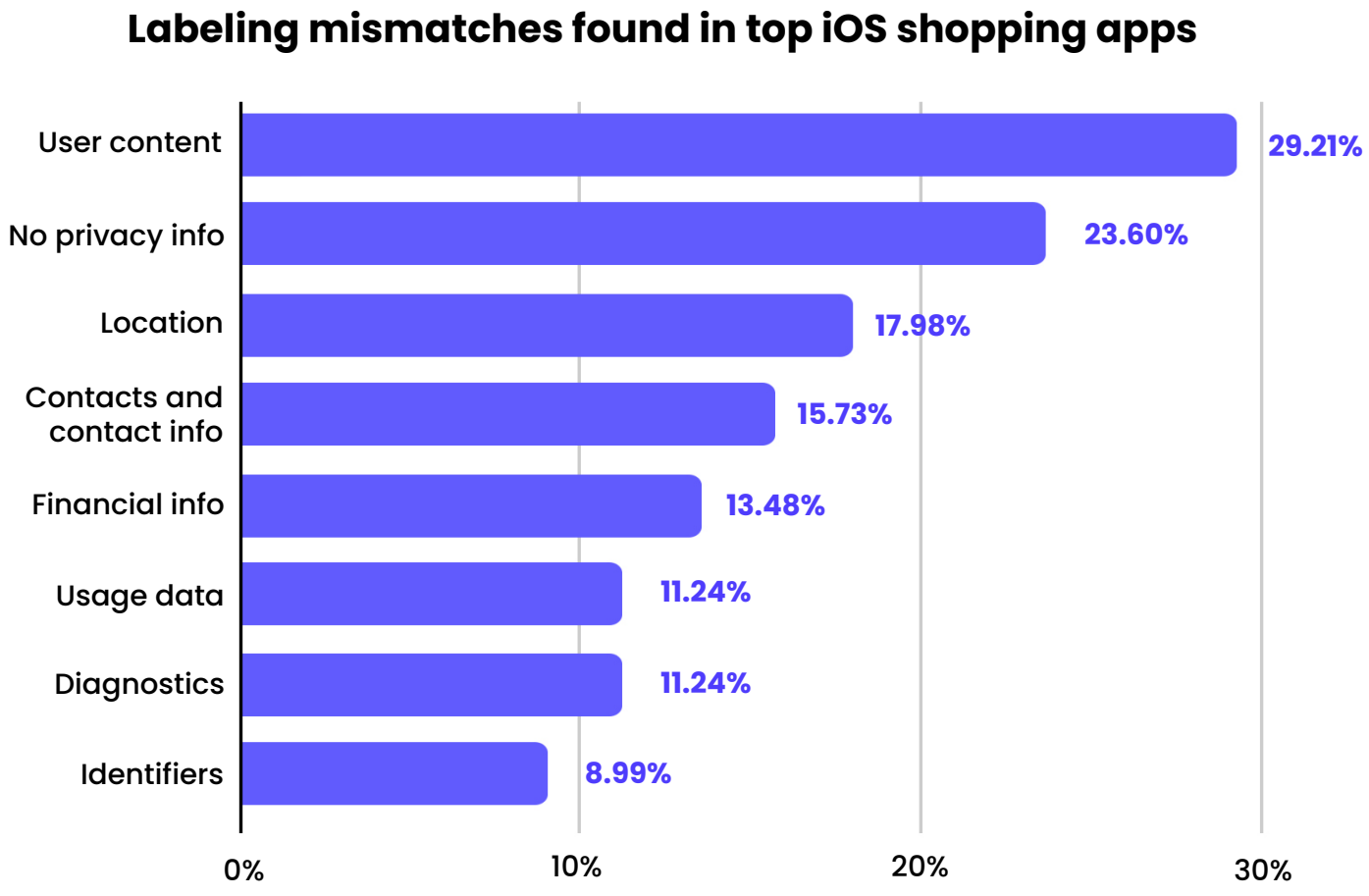


Figure 9: Most common types of labeling mismatches found on top iOS shopping apps.

Roughly **29%** of reviewed iOS apps **access user data without declaring it in their App Store Privacy Overview**, effectively failing Apple's "nutrition label" disclosure.

Another **24%** lacked a **valid Privacy Manifest**, obscuring how data is collected, shared, or which restricted APIs are used.

Specific categories of undisclosed data access were also common: **18%** accessed location data, **16%** accessed contacts, and **13%** accessed financial information without proper declaration. These omissions represent not only potential **App Store guideline violations** but also signal weak internal privacy governance and an increased risk of hidden data collection practices.

Taken together, these findings underscore a persistent dual challenge for mobile ecosystems: **technical exposure** within Android apps stemming from dynamic behavior and insecure components, and **transparency and compliance gaps** within iOS apps. Both vectors ultimately translate into increased regulatory, reputational, and user-trust risk—particularly during peak shopping seasons when app usage surges.

For corporations managing mobile fleets or consumer apps, these statistics represent more than isolated technical flaws — they expose systemic weaknesses across the mobile supply chain. Insecure SDKs, weak signing, and undeclared data collection can lead to brand damage, compliance violations, financial penalties, and user attrition. A single compromised component can propagate through thousands of business-critical apps, emphasizing the need for continuous third-party app vetting and runtime protection at scale.

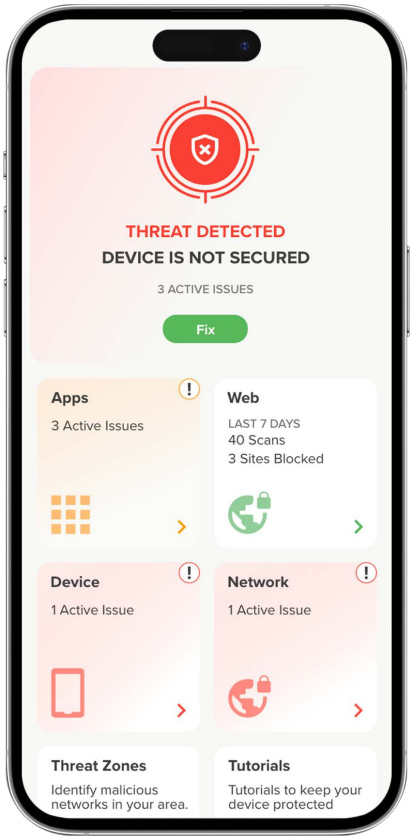
How Zimperium Can Help

The holiday surge in mobile threats highlights not only consumer risk but also **enterprise exposure** across customer channels, employee devices, and third-party ecosystems. Zimperium's mobile security platform delivers the visibility and control organizations need to protect both their workforce and their customers across every stage of the mobile threat lifecycle.

MTD (Mobile Threat Defense): Leverages AI to provide continuous, on-device detection to stop attacks like mishing (mobile phishing), malicious apps, and unsafe network activity, protecting the device even when offline.

zLabs Threat Intelligence: Delivers global visibility into emerging malware families, brand impersonation campaigns, and evolving distribution channels, ensuring Zimperium's detections remain accurate and zero-day-ready.

App Vetting and **zShield:** Enable the discovery and assessment of third-party apps used across marketplaces and organizations. Through static and dynamic analysis, Zimperium can identify privacy violations, insecure SDKs, embedded secrets, or outdated libraries — the same risks surfaced in this report — and evaluate their potential to be weaponized in supply chain or credential-theft scenarios. Enterprises can leverage Zimperium's vetting capabilities to audit partner or third-party apps before deployment in managed environments, ensuring that vulnerable SDKs or misconfigured components do not introduce supply chain exposure into corporate systems.



zDefend (Mobile Runtime Protection): Provides powerful in-app runtime protection for organizations that build or operate their own mobile services. It actively prevents tampering, overlay attacks, and detecting malicious applications that could target the app.

Together, these capabilities provide **end-to-end assurance** from detecting phishing and malware to evaluating and mitigating risk across the third-party apps and SDKs they depend on. By combining continuous threat monitoring with ecosystem-level visibility, Zimperium helps ensure that consumers, enterprises, and app developers remain protected throughout the entire mobile commerce chain — not just during the holiday season, but all year-round.

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. Learn more at www.zimperium.com and connect on LinkedIn and X (@Zimperium).

www.zimperium.com

1 The families tracked are: Anubis II, AppLite, Blackrock, BrasDex, Copybara, Ermac, ExobotCompact.D/Octo, Godfather, Hook, Hydra, Lokibot, Medusa, Mystery Bot, Nexus, PixBankBot, PixPirate, SharkBot, S.O.V.A., Teabot, TsarBot, Vultur and Xenomorph.

ZIMPERIUM®

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