GLOBAL MOBILE THREAT REPORT

2025

ZIMPERIUM®

Table of Contents

Executive Summary

The 2025 Global Mobile Threat Report reveals that attackers have adopted a mobile-first attack strategy, making it essential for organizations to understand and mitigate mobile risks. This report offers insights into the evolving mobile threat landscape, helping organizations identify security gaps and align their defenses with relevant real-world risks.

Smishing (SMS phishing) comprises over **two-thirds** of mishing attacks

Key Security Findings on Threats to Your Mobile Devices

Mishing Surge: Mishing (mobile-targeted phishing) represents roughly one-third of threats identified by zLabs. zLabs has observed that smishing (SMS phishing) comprises over two-thirds of mishing attacks. Mobile phishing attacks of vishing and smishing have also risen substantially (by 28% and 22%, respectively), which is not surprising given the widespread rise in the use of AI tools by attackers. Additionally, PDF phishing has emerged as a new and effective attack vector. All of which necessitates a defense response of advanced mobile threat defense coupled with robust user education.

Mobile Vulnerability Management Challenges: A significant percentage (25.3%) of devices are not upgradeable due to the device's age. These older devices present a data compromise risk to the organization if an OS vulnerability is used in an attack.

Sideloaded Mobile App Risk: Sideloaded apps are present on 23.5% of enterprise devices. Sideloaded apps substantially increase the risk of mobile device compromise as they may be repackaged versions of 'legit' apps where additional functionality is offered but potentially malicious code is embedded within the app.

Data Security in Work Apps: Work apps need to be vetted. zLabs found that 23% of apps used on work devices analyzed communicated with risky or embargoed countries. This report emphasizes the need for vetting work apps and for security professionals to understand where the servers of even legitimate work apps are located.

Key Security Findings in Mobile Apps Your Organization Develops

1. App Protection Tooling Reflects Security Posture—And the Gaps Are Alarming

Across Android and iOS, most apps rely on basic tools or have no protection, including in high-risk sectors like Finance. Organizations are either underestimating the sophistication of mobile threats or relying too heavily on platform-level security. The burden of fragmented tooling falls squarely on Android developers, often leading to misconfigurations and friction. On iOS, an over-reliance on the platform results in widespread under-protection. In both cases, the gap between app security investment and real-world risk leaves mobile apps dangerously exposed.

2. The Perfect Supply Chain Attack Is Hiding in Your App

Over **60%** of top Android and iOS third-party components or SDK's are shipped as precompiled binaries, often with partial or missing SBOMs. Even when source code exists, developers commonly test open-source versions but deploy the compiled binaries for speed, leaving what ships and runs unchecked. This allows attackers to **poison the mobile supply chain** with malicious or tampered components, bypassing traditional static and SCA tools. Without runtime introspection, these invisible dependencies become ideal targets for exploitation.

3. Your App Is Only as Secure as the Device It Runs On

At any given point in the year, over **50% of mobile devices are running outdated OS versions,** and a significant number are compromised or infected. This creates untrusted environments where even apps that employ security measures **are susceptible to manipulation**. Without device attestation, apps can't distinguish between safe and hostile execution environments, exposing sensitive data and operations. For AppSec and Dev teams, device attestation isn't a nice-to-have—it's the gatekeeper for enforcing trust, preventing fraud and safeguarding sensitive data at scale.

Recommendations for Leaders:

Rigorous, Continuous App Vetting: Enforce strict processes for analyzing third-party apps on mobile devices to assess the application's composition (e.g. SBOM) and the actual risk it poses, with a deep focus on critical vectors like excessive permissions, insecure data handling, and vulnerable communication channels.

Combat Mishing: To protect against advanced and mobile-targeted social engineering tactics, security teams should implement AI-enabled mobile threat defense and provide regular employee training to raise awareness.

Mobile Vulnerability Management: Define and enforce policy on timely OS and app updates and data access by end-of-life devices to minimize enterprise data and infrastructure risk.

Secure Your Third-Party Code: Require mobile app teams to analyze app binaries early during development, including closed-source components, to uncover hidden vulnerabilities, assess runtime behavior, and prevent malicious code from entering the production pipeline.

Mandate Device Attestation for Your Mobile Apps: Ensure your mobile app development teams implement device attestation to enable apps to detect untrusted environments and respond in real-time on the device to mitigate risk.

Organizations can significantly reduce mobile risk exposure and protect sensitive data by aligning mobile device and application security to real-world threats and risks. For mobile device security, this includes fortifying protections against mishing (mobile phishing) and continuously vetting third-party apps on enterprise connected devices. For mobile app security, organizations must account for today's threat sophistication and move away from fragmented tooling. Organizations should select solutions that simplify the implementation of security measures and foster better collaboration between security and development teams. This allows teams to efficiently build, secure, and release secure mobile apps at scale.

The Expanding Enterprise Mobile Footprint: Scale Meets Risk

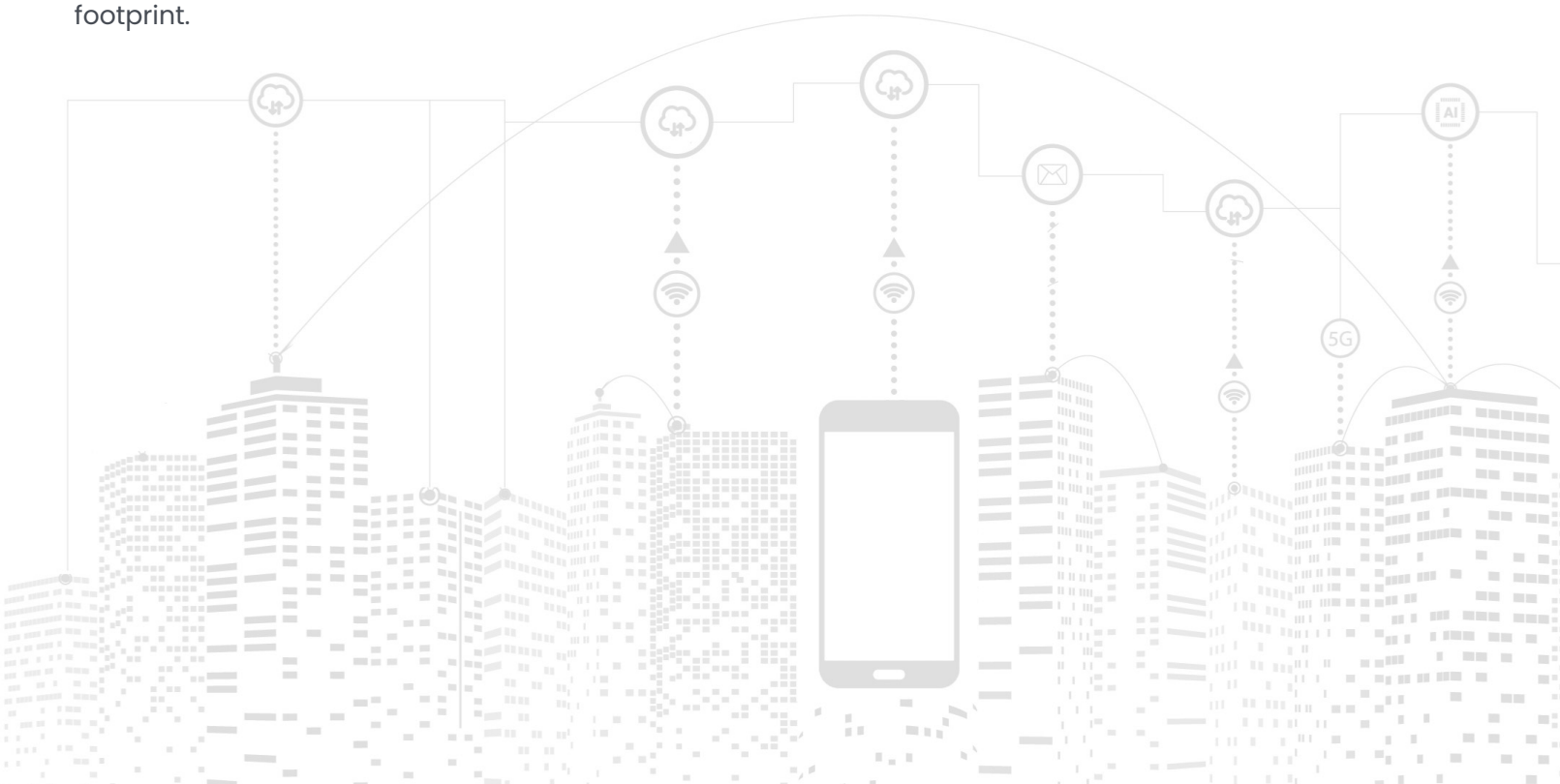
Enterprises are more mobile than ever. As of the end of 2024, there are approximately **7.2 billion smartphone users worldwide**[1] driven by mobile workforces, remote access and enterprise mobility initiatives. Mobile devices now routinely use apps to access sensitive systems, data and workflows once limited to secured desktops—significantly expanding the digital attack surface.

At the same time, the number of work and personal apps has exploded—blurring the lines between enterprise and consumer environments. By the end of 2024, there were around 1.96 million apps on the Apple App Store and 2.87 million on Google Play. A typical user has between 80 and 100 apps installed,[2] yet only 11 are work-related, according to Gartner.[3] Meanwhile, 66% of American employees use their personal smartphones for work,[4] and 70% of organizations support BYOD.[5]

This means the average work-enabled device is dominated by apps outside IT's control, assessment, or development, introducing unmonitored attack surfaces that security teams often can't see, let alone secure. As enterprise mobility scales, so does the risk. The explosion in mobile apps isn't just a usability shift—it's a threat multiplier.

The result is a fragmented, under-secured mobile landscape where apps and devices become potential vectors for data loss, fraud, and enterprise breaches.

A deep dive into today's mobile threat environment based on real-world data reveals where vulnerabilities lie, how attackers take advantage, and what organizations must do to defend their mobile footprint.



Global Threat Landscape

Top Threats and Risks

As mobile devices continue to be prime targets, understanding the specific methods attackers employ to compromise them is critical. Our analysis breaks down the prevalent threats observed across both Android and iOS platforms, highlighting the key attack vectors targeting devices, networks, applications, and users through sophisticated mishing (mobile targeted phishing) and other campaigns.

zLabs has observed and categorized the top Threats by OS platform:

iOS Threats

54% of all iOS threats are mishing based and 39.8% are network threats (man-in-the-middle attacks).

Breaking it down further by Device, Network, Application and Mishing attack vectors:

Device Vulnerabilities

The most critical threats targeting iOS devices involve jailbreaking and system tampering that compromise the integrity of the operating system, compounded by the significant risk posed by failing to apply essential OS updates that address known vulnerabilities. Furthermore, our analysis also revealed disruptive system anomalies, marked by unexpected system and application service crashes observed throughout the year.

Network Risks

The leading iOS network threat originates from connecting to untrusted or insecure Wi-Fi networks, which directly enables attackers the ability to initiate dangerous Man-in-the-Middle (MITM) attacks, on both WiFi and Cellular networks. We also observed critical network anomalies throughout the year, prominently featuring suspicious connections to high-risk countries and excessive outbound data traffic.

Application Risks

Primary app threats surrounding iOS are from applications exhibiting malicious, unexpected and/or risky behavior, exposed from sideloaded app threats, a risk previously more associated with Android but now becoming a notable vector on iOS.

Mishing Attacks

Analysis of our mobile phishing threat data consistently shows that malicious links embedded in mishing content pose a major risk, immediately attempting to direct users to harmful or data-stealing websites upon clicking.

Android Threats

The top Android threats are malicious apps delivered via sideloaded apps and mishing/ social engineering.

Breaking it down further by Device, Network, Application and Mishing attack vectors:

Device Vulnerabilities

The most significant threats to Android devices stem from compromised states such as rooting or privilege escalation, alongside critical risks introduced by failure to patch known OS vulnerabilities or the continued use of devices too old to receive essential security updates.

Network Risks

Connecting to untrusted or insecure Wi-Fi networks remains a primary network threat for Android devices, critically exposing users to Man-in-the-Middle (MITM) attacks where sensitive data can be intercepted. Similarly to iOS, we also observed critical network anomalies throughout the year, prominently featuring suspicious connections to high-risk countries and excessive outbound data traffic.

Application Risks

Sideloaded applications represent the leading application-based threat to Android users, bypassing official app store security checks and frequently containing malicious code or severe security flaws.

Mishing Attacks

Smishing (SMS/text phishing), the dominant mishing threat on Android, involves malicious links designed to immediately redirect users to dangerous phishing or malware-hosting sites.

Based on our analysis across both Android and iOS platforms, Mishing stands out as the top overall mobile threat, aligning with the broader increase in such attacks. While sideloaded applications represent the second biggest threat for Android, a risk historically unique to the platform, network threats are the second most prevalent for iOS. Notably, sideloaded app threats are now emerging as a developing concern for iOS, particularly following the availability of third-party app marketplaces in 2024 due to regulatory changes. A consistent top risk across both operating systems is the presence of devices running vulnerable or outdated OS versions that cannot be upgraded. Mitigating this requires decommissioning non-upgradeable devices and promoting timely OS updates for all users.

KEY TAKEAWAYS

- Mishing, especially via SMS, represents a high risk and requires both threat detection capabilities and user training to combat this threat.
- Time lag between OS upgrade availability and installation by the end user exposes the enterprise to vulnerability risk from outdated/ vulnerable OS.
- Reduce sideloaded app risk by thoroughly vetting every application using a comprehensive application vetting solution to assess security, compliance and overall risk, particularly for apps on devices accessing sensitive enterprise data.

Top Threats in US Public Sector

Based on our analysis across both Android and iOS platforms, the top threats in the US public sector come from mishing, risky wifi network connections that can lead to MITM attacks, and from sideloaded apps on Android. As with the overall analysis, a consistent risk across both operating systems is the presence of devices running vulnerable or outdated OS versions that cannot be upgraded. Mitigating this requires decommissioning non-upgradeable devices and promoting timely OS updates for all users.

KEY TAKEAWAYS FOR PUBLIC SECTOR

- Encourage user upgrades as soon as OS updates are available.
- Discourage users from connecting to unsecured WiFi networks. Implement conditional access policies to avoid sensitive data being accessed or shared over the network when on unsecured networks.
- Reduce sideloaded app risk by thoroughly vetting every application using a comprehensive application vetting solution to assess security, compliance, and overall risk, particularly for apps on devices accessing sensitive data.

Mishing

We discussed the move from phishing to mishing (mobile targeted phishing) in last year's report as attackers adopted a mobile-first attack strategy – attacking via the largely unsecured mobile device instead of the largely secured PC device running Windows or MacOS. This year's data validates that prediction where we observe:

- incidence of Vishing up 28%[6]
- incidence of Smishing up 22%[7]
- the rise of PDF phishing via mobile[8]

In 2024, the United States continues to be the #1 phished region worldwide with zLabs data showing they comprised 44% of mobile phishing targets.

Although mishing can target both consumers and businesses, business compromise via phishing was responsible for $2.9 billion dollars in losses in the U.S. in 2023 according to the FBI's Internet Crime Complaint Center.

In a business phishing attack, a threat actor impersonates an employee, vendor or other trusted party in an email or other messaging communication and attempts to trick the employee into sharing credentials, privileged information, or some other asset. This shows up in the 2024 data:

Vishing incidents in Q3 2024 increased more than 28% over Q2 volumes. And smishing incidents – phishing via SMS and text messages – increased more than 22%.[9]

According to Zimperium's zLabs research team, SMS (smishing) has emerged as the dominant mishing vector, now comprising over two-thirds of observed attack attempts, signifying a critical pivot in threat actor methodology, as presented in Figure 1.

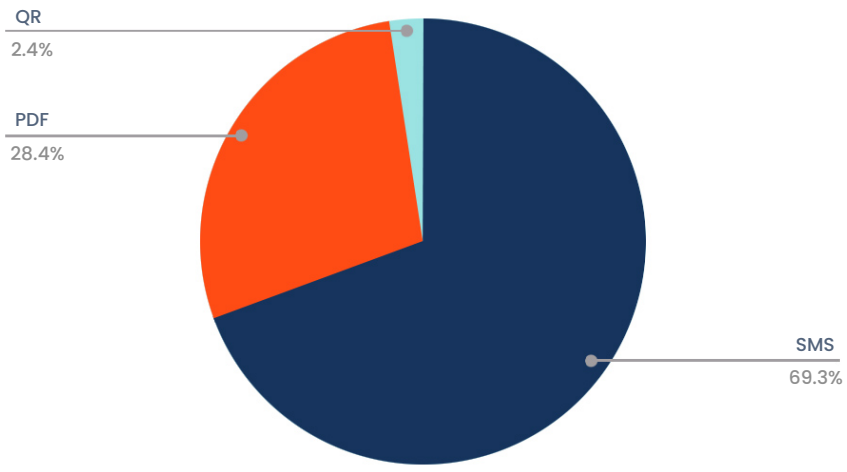


Figure 1: Mishing Attack Vectors (source: zLabs)

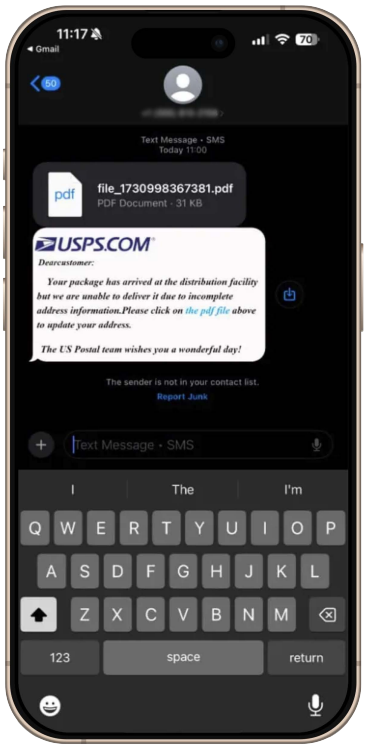


Figure 2: PDF Smishing Attack Example [10]

Attackers are always looking for the next vector. In the past year, Zimperium has observed attackers increasingly leveraging PDF attachments delivered via SMS messages because these files can effectively obfuscate malicious content and evade traditional security scans. This tactic exploits the fact that users have become accustomed to and generally trust PDF documents in their daily interactions, and many defense mechanisms may not thoroughly inspect them for embedded threats. To enhance their deception, attackers frequently leverage well-known brands within these malicious PDFs to manipulate user trust, compelling victims to click through and initiate the attack, as demonstrated in Figure 2. This evolution signifies a sophisticated attempt to bypass established security measures and capitalize on user familiarity and trust.

This example is one of many that attempt to trick a user into downloading a PDF document that executes the attack after download and user activation to “view” the PDF.

A second smishing attack that has surged in volume is one that takes advantage of the widespread prevalence of toll roads in the U. S. This method has received a lot of press attention in recent months.

In this attack the user is told they have an unpaid toll on the widely used EZPass system. This leverages a tool kit that is actively sold via the dark web to enable attackers to easily send text messages to redirect the victim to a phishing site that looks like one for a toll road operator. See Figure 3.

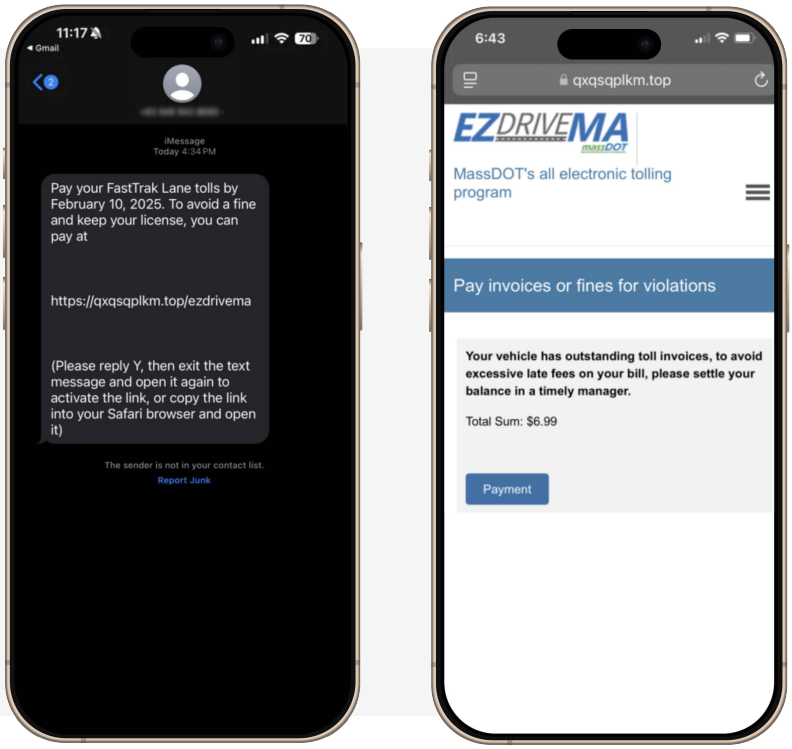


Figure 3: Example of Toll Road Smishing Attack [11]

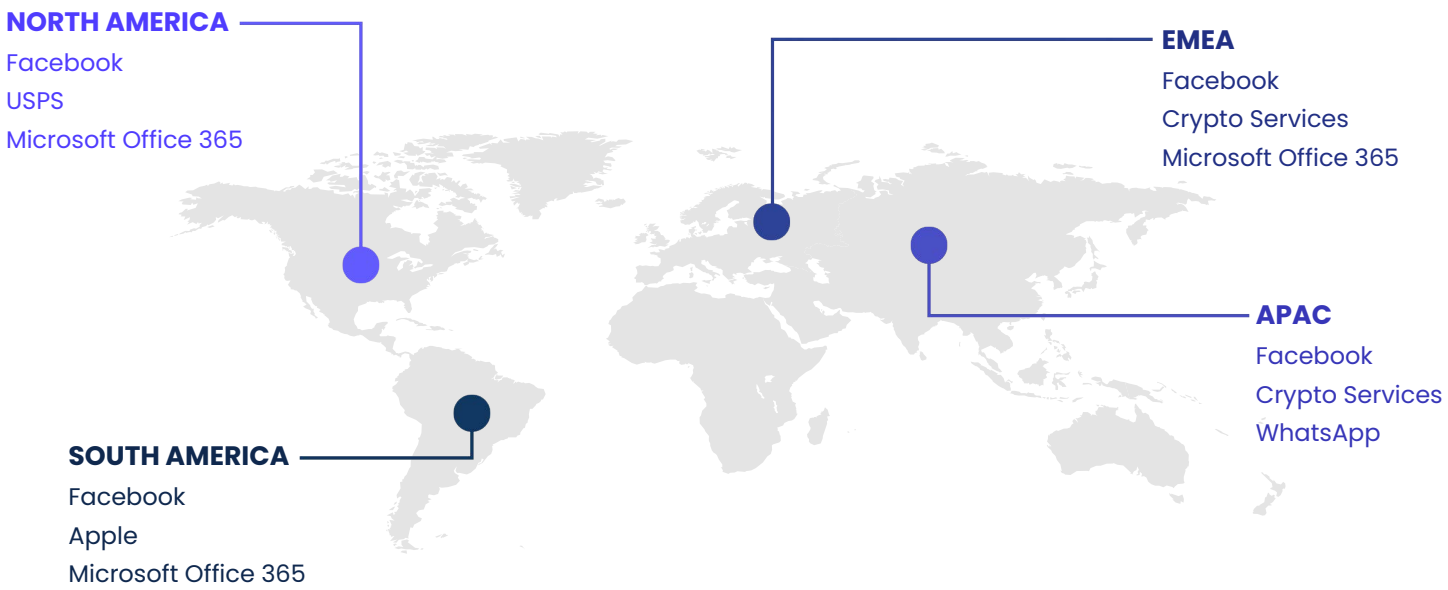
Consumer and Enterprise Brands continue to be exploited as part of Mishing Attacks

Attackers continue to impersonate well-known brands as a means to tricking the user into taking risky actions. Phishing typically impersonates regional consumer and enterprise brands to raise the likelihood of the target responding to the phish attempt. These brands boast enormous user bases and have cultivated significant user trust, making phishing attempts appear highly credible and increasing the likelihood of success. Critically, these services are repositories for vast amounts of valuable personal, financial and business-critical data. By compromising accounts on these platforms, attackers can gain access to everything from sensitive emails and cloud storage to financial details linked to shopping or payment services. Access to one of these accounts, particularly email or social media platforms, can often provide a foothold to compromise numerous other linked services.

Most recently, zLabs researchers analyzed a targeted campaign that leveraged a DocuSign impersonation scheme attempting to harvest corporate credentials from company executives.[12] The analysis of this campaign revealed an interesting attack chain that incorporated advanced evasion techniques, mobile-specific targeted phishing links inside PDF files, and a sophisticated infrastructure designed to circumvent traditional security controls while maintaining a convincing corporate appearance.

The financial incentives are substantial, ranging from direct theft of funds or payment information to leveraging business platforms for larger-scale fraud.

The Top 3 Brands leveraged for mishing by geographic region in 2024 were:



Mobile Malware

Malware remains a primary weapon for both opportunistic cybercriminals and sophisticated advanced persistent threats targeting mobile devices globally. zLabs research confirms the widespread nature of this threat, finding that **18.1% of devices** in our analysis set had mobile malware installed. Figure 4 provides a visual distribution of the prevalent malware types we observed.

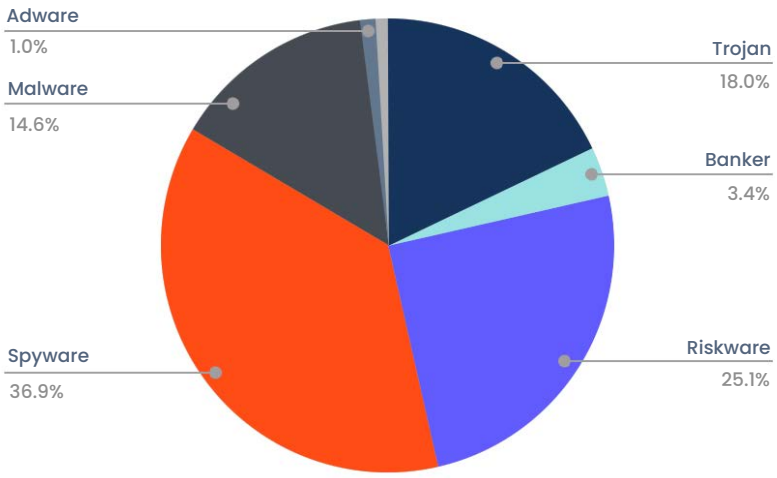


Figure 4: Malware Family Distribution

Malware Trends

Analyzing the malware family distribution reveals that Spyware has emerged as the most prevalent malware family throughout 2024. This is a concerning trend, yet aligns directly with the observed surge in mishing attacks. Spyware is insidious by design; it secretly infiltrates a user's device to stealthily gather a wide range of sensitive data – from personal information to device specifics – and exfiltrates it to attackers without the user's consent. Its hidden data-gathering capability makes it a favored tool in campaigns aiming for covert data theft.

Compounding this picture is a significant escalation in Trojan activity. We have documented a striking **50% increase** in the deployment of Trojans in attacks compared to activity seen in 2023. This surge is further evidenced by zLabs discovery of multiple dangerous new banker trojan families, including Vultur, DroidBot, Errorfather, and BlankBot. The threat posed by these new variants heavily targets the Android ecosystem, as all but the Errorfather family are specifically engineered for Android devices. The dominance of spyware and the alarming rise of sophisticated, Android-focused Trojans collectively underscore the evolving and increasingly data-centric nature of global mobile threats.

Sideloaded Apps

Sideloading is the practice of installing mobile apps on a device that are not from the official app stores. This is typically done on a rooted Android device or a jailbroken iOS device. In 2024, the EU DMA[13] resulted in the availability of sideloaded apps on iOS devices, so we are starting to see their presence on iPhones. With the blurring of personal and professional boundaries, sideloaded apps are increasingly showing up on personal devices used for work.

Sideloading apps can lead to complete mobile device compromise. ***zLabs identified 23.5% of mobile devices having the presence of one or more sideloaded apps***. Sideloaded apps are amongst the top 3 risks for both iOS and Android devices per zLabs.

The Need for Platform Vulnerability Management

zLabs tracks devices having a version that are vulnerable to a known CVE. The CVE data for 2024 is shown in Table.

The **key takeaway** is that users upgrading their device OS as soon as the next release is generally available will reduce organizational risk. IT leaders need to define and enforce policy on timely OS updates and data access by end-of-life devices to minimize enterprise data and infrastructure risk.

		2022	2023	2024
Android	# of CVE	1223	1422	501
	# of high or critical CVSS	494	404	305
	# of zero day CVEs exploited in the wild	41	97	12
iOS	# of CVE	243	269	317
	# of high or critical CVSS	155	120	125
	# of zero day CVEs exploited in the wild	5	20	5

Table 1: CVE data for iOS and Android OS versions[14]

Are Your Work Apps Making it Easy to Steal Data?

Enterprises are becoming more and more reliant on mobile apps to perform basic business operations. They are used for supply chain management, reporting, office functions, expense management and HR to name a few categories. With the ubiquity of apps in an enterprise rising, so does the risk they pose to the enterprise's data.

App vetting is aimed at assessing the risk that an app poses to the organization and to answer a basic question: "Am I comfortable with the potential risk that the app poses to my organization given its functionality, adherence to standards, data handling and communication?"

In this section, we will cover app vetting from the perspective of work apps that are used within the enterprise.

How do work apps handle sensitive data?

In order to fulfill their functions, work related apps require access to data. Sometimes, they require access to private or sensitive data (photos, contact information, text messages, etc. - all of which can expose sensitive information related to the enterprise).

Some permissions an app can ask for are defined by Apple and Google as "dangerous". This usually means that these permissions allow access to data that is sensitive or can put the device itself at risk.

The top 10 permissions requested by work apps[15] fall into a broad category of permissions that provide access to the user's location or personal information stored on the phone. The information these permissions provide access to can potentially be accessed by external parties leveraging app vulnerabilities.

Whether the app actually needs the specific permission in order for it to perform its function or not, those permissions are "there" and most users just grant them without much thought. This fact alone has to be taken into account when an enterprise reviews the specific app in order to decide whether or not to use it.

While apps often ask for permission to access potentially sensitive data, the mobile app stores also encourage the app developers to formally declare what kind of sensitive data they access and what they do with it. The goal is to provide the user with as much information as possible in order for them to make an informed decision whether or not they trust the app to have access to their data, and obviously, for the enterprise to decide if they allow such access.

Our analysis showed that, while not always required, a substantial percentage of apps don't fully declare what sensitive information they access or collect.

Do the apps you use communicate securely?

We have observed a rise in insecure communication of data across numerous work app categories on the Android platform.

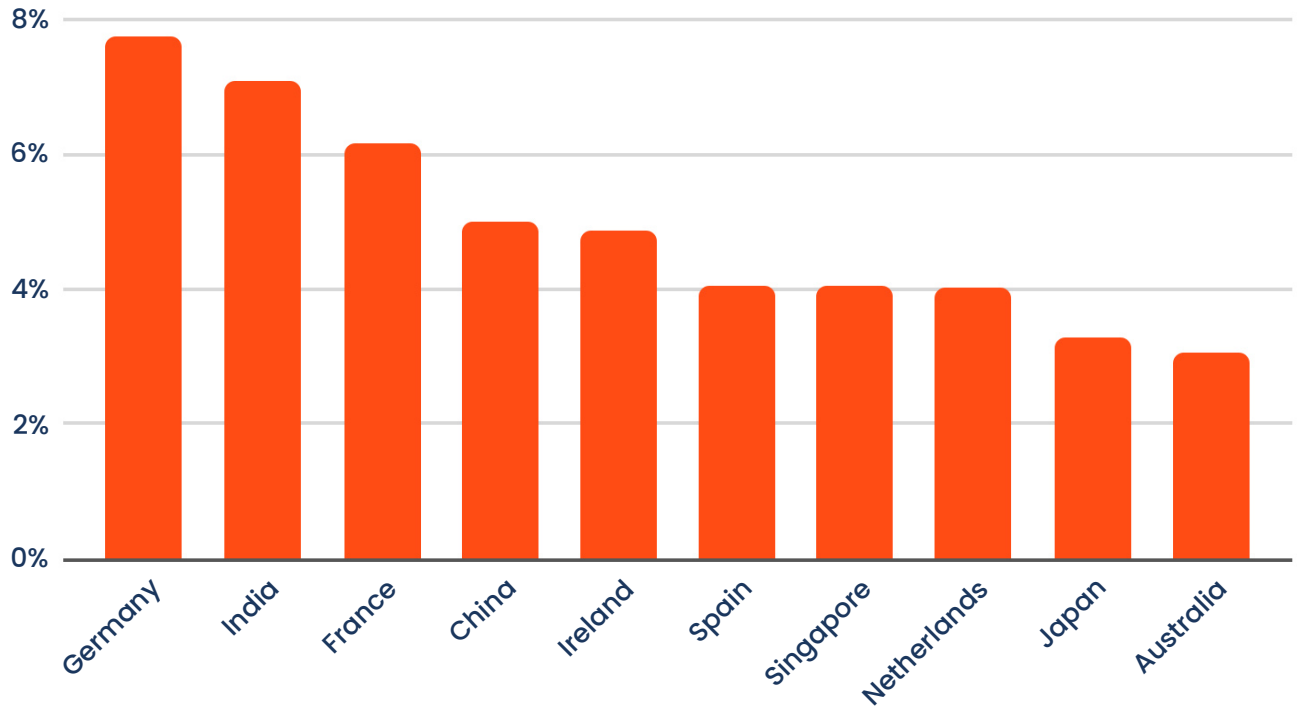
Category	2024
Business	8.37%
Productivity	9.87%
Tools	18.11%
Communication	5.32%
Finance	17.86%

Based on our findings, it is evident that a substantial percentage of work applications engage in insecure communication practices. This often involves critical security failures, such as failing to properly verify the authenticity of the servers they connect to. To illustrate the widespread nature of this vulnerability, we found several apps from the same developer, focused on business management and advertising functionalities with over 100 million combined installs, that do not verify their network communication certificates. Similarly, a widely used international communications and networking app with over 50 million downloads exhibits this same critical lapse in certificate verification. This failure to validate secure connections makes the data exchanged by these apps highly susceptible to interception via Man-in-the-Middle (MITM) attacks, allowing malicious actors to compromise sensitive information without needing to gain direct access to the device itself. ***This direct path to sensitive data helps explain why over 30% of the threats detected by Zimperium originate at the network layer.***

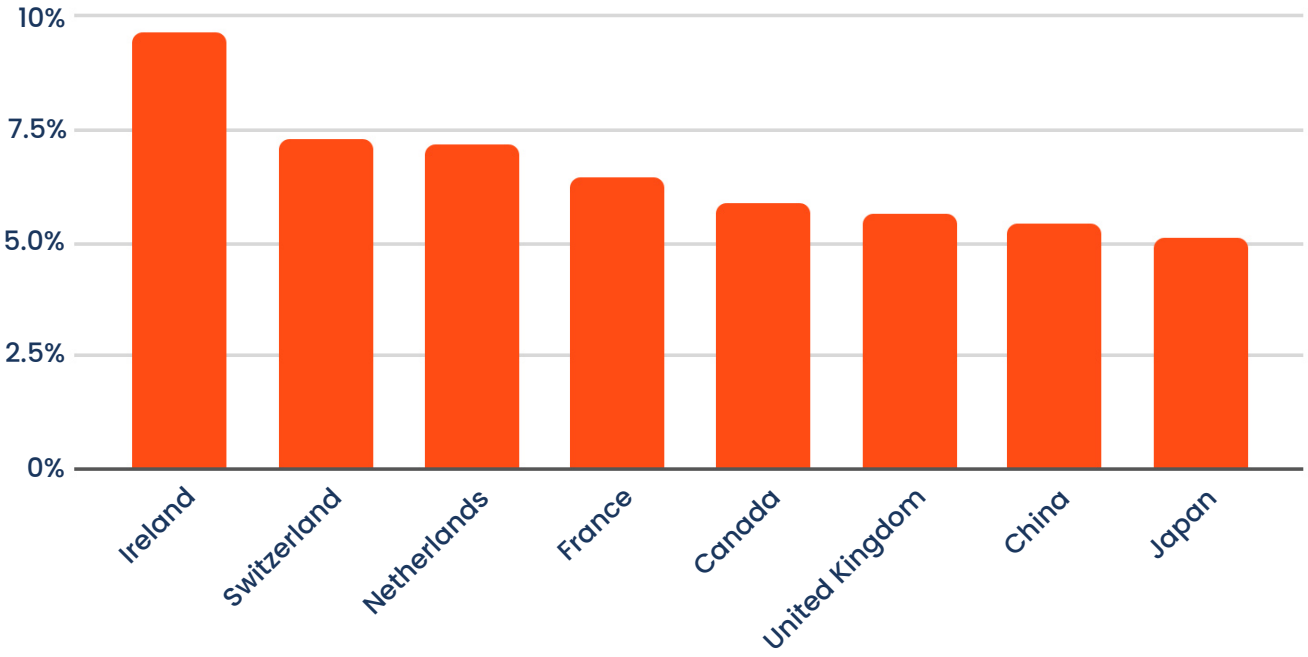
Where's my enterprise data going?

The United States is the country that apps most often communicate with since a large percent of work apps are created by U.S. based companies. The following graphs illustrate the geographic footprint of endpoints and services that apps across key categories – including Business, Finance, and Communication – connect with for both iOS and Android devices. This data highlights the global reach of application communications and underscores the potential risks related to data sovereignty, privacy and compliance as enterprise data traverses international boundaries.

Top 10 non U.S. Countries iOS Work Apps Communicate With

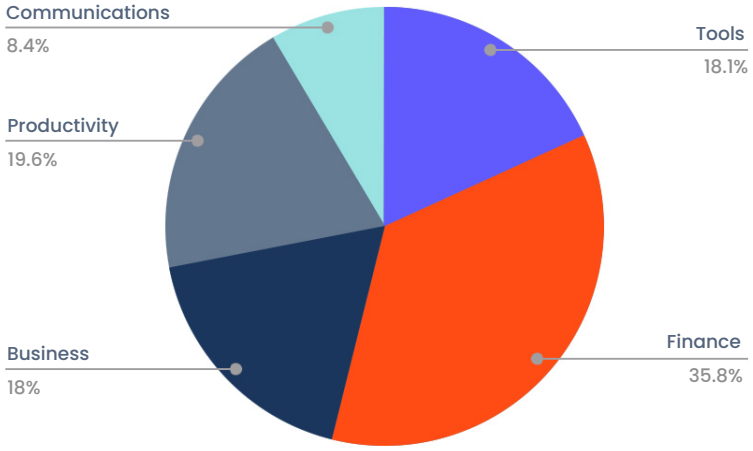


Top 10 non U.S. Countries Android Work Apps Communicate With



App Data Going to Embargoed or High Risk Countries?

zLabs found that **23% of work apps** connect to embargoed or high-risk countries with a third of the apps being financial ones even though that communication might be warranted for the app's function.



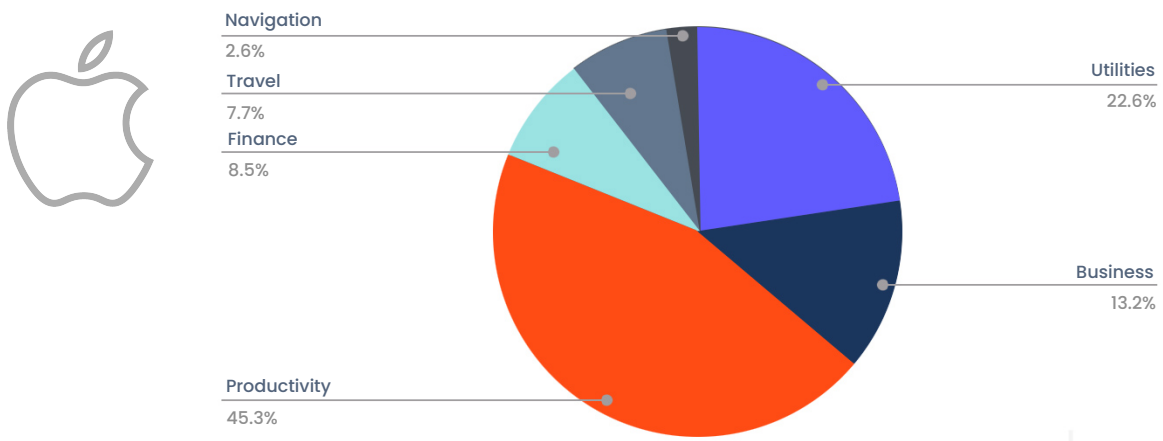
By Market Category

Apps Put the "A" in AI

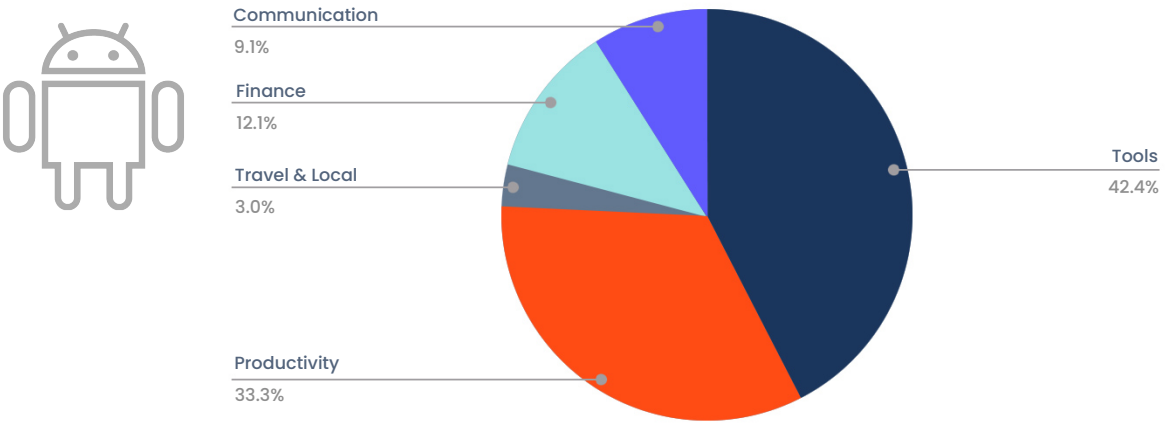
The use of AI has been exploding in apps. Analyzing apps installed on enterprise devices reveals that beyond dedicated AI service applications like ChatGPT or DeepSeek, AI capabilities are increasingly being embedded directly into a wide array of other apps. This trend is accelerating significantly; **we have observed approximately 160% growth in the use of AI services within apps present on employee devices.**

With the huge benefits AI brings to enterprise apps comes significant risk. AI services need data, and lots of it. And apps (and the devices they run on) are the perfect potential source of this data.

Our analysis confirms that AI capabilities are being leveraged across a broad spectrum of application types, extending far beyond typical productivity tools. This includes integration into browsers, travel apps, Customer Relationship Management (CRM) systems, and even financial trading applications. As illustrated in the charts below, this widespread adoption means that the associated data privacy and security risks are now pervasive across the enterprise mobile fleet.



AI Services Usage by App Category (iOS)



AI Services Usage by App Category (Android)

A significant consequence of this development is the use of AI tools in applications where users are unaware of where their data is being transmitted. Popular mobile keyboard apps now use AI to predict text, analyze tone, and autocorrect. However, these apps often fail to disclose where the data is stored and processed. In doing so, they may process everything a user types, including corporate credentials and sensitive data, posing a significant risk of data leakage.

Our analysis also provides insight into the specific AI services most prevalent within these applications, revealing which platforms are potentially handling data from enterprise devices. Unsurprisingly, **OpenAI stands out as the dominant player, integrated into roughly 70% of the AI-powered apps we analyzed.**

Continuous App Vetting is Mandatory

Mobile is a constantly evolving ecosystem and competition among app developers can be fierce. New versions of the operating systems with new capabilities are constantly being introduced. App developers are compelled to take advantage of new features and capabilities that potentially provide more value to their users.

This introduces a significant challenge from a security perspective. The streamlined process of version updates to the formal app stores, and the over-the-air, seamless and transparent version update process requires security professionals to be ever-vigilant to the constant changes being introduced into their app inventory. Hence, apps now need to be vetted continuously to keep up with their rapid updates.

Our analysis of the changes that have been detected in apps installed on enterprise devices yielded several interesting insights. Enterprise security, risk and compliance teams often lack visibility into these risks, especially when relying solely upon release notes or vendor documentation.

Without the insights provided by continuous app vetting, critical changes in privacy, communications, and compliance behavior can go unnoticed. In cases where the risk stems from a third-party supply chain dependency, even the app vendor may be unaware, leaving no mention in documentation or Software Bill of Materials (SBOMs). For example, our analysis of a new version of an iOS business messaging app showed that camera and microphone functionality were added two months after a previous version was released. But the version history in the store only listed the word “improvements.” We also see Finance and Productivity-related Android apps with millions of downloads mistakenly ship with the debug flag enabled in production, leaving them vulnerable to runtime attacks, code inspection, and unauthorized data access.

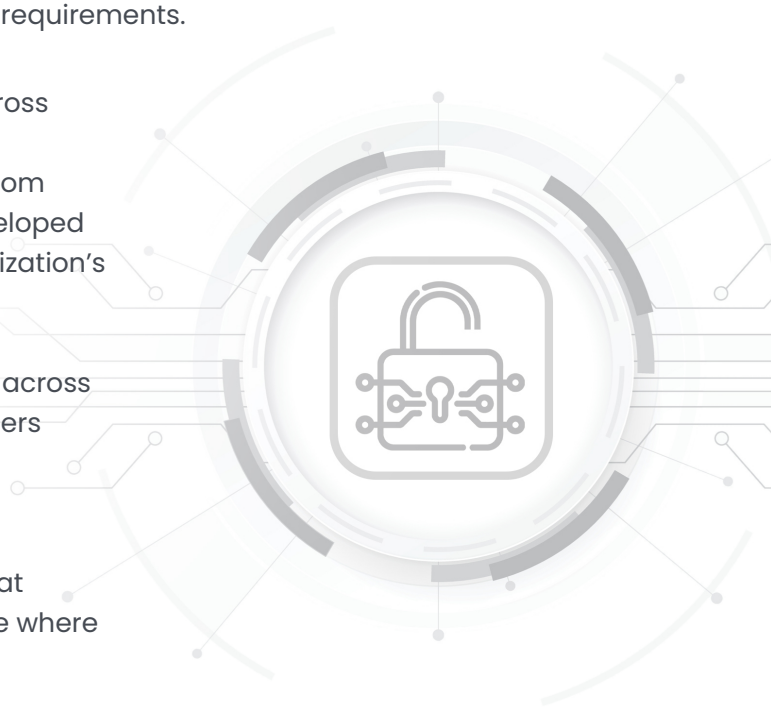
KEY TAKEAWAYS

The story these statistics tell us is about the importance of vetting third-party applications, not just as a precaution but as a **strategic imperative** for enterprises. Without proper security & privacy assessment measures for mobile applications, the risk for sensitive data leakage, whether intentional or accidental, can directly impact organizational integrity, customer trust and regulatory compliance.

Security Gaps in the Mobile Apps You Build

Assessing the third-party applications you use allows you to make informed business decisions. Equally important are the applications that your organization is developing, as they represent your brand, your ability to secure sensitive data, and relevant compliance requirements.

In this section we present our analysis of security risks across 100,000 mobile apps from the Finance, Travel, Lifestyle, Entertainment, and Food & Drink categories, all sourced from official app stores. Our analysis focuses on internally developed apps sold to other businesses (B2B) or used by the organization's end-customers.



We highlight common vulnerabilities and security trends across these categories, offering security and development leaders actionable insights to enhance protection of their mobile applications in customer-facing environments.

The following breakdown highlights the subcategories that comprise each major app category, helping contextualize where different risks originate.

App Category	Key Subcategories			
Finance	Mobile Banking	Payments & SoftPOS	Investing	Insurance
Travel	Airline	Flight & Travel Booking	Ride Sharing	Transportation
Lifestyle	Automotive Connected Apps	Retail	Health & Wellness	Home & Smart Living
Entertainment	Streaming Services	Social Media	Music & Audio	Live TV & Sports Streaming
Food & Drink	Restaurants & POS	Loyalty & Rewards	Food Subscription Services	Nutrition & Meal Planning

What Your Tooling Says About Your Security Posture

Understanding the quality of the app protection tools that app teams implement is vital for assessing security maturity and investment levels. By examining the security tools adopted across app categories, this section uncovers how organizations' choices reflect their true security posture, whether rooted in awareness, assumptions, or oversight.

Breakdown of app code protection tools used in Android apps by category:

Android App Category	Likely Paid Tools	Open Source Tools	No Code Protection
Finance	14.00%	51.20%	34.80%
Travel	20.40%	61.70%	17.90%
Lifestyle	15.80%	64.10%	20.10%
Entertainment	14.90%	68.60%	16.50%
Food & Drink	18.10%	63.00%	18.90%

KEY TAKEAWAYS

- **High "No Code Protection" Rates Signal Risk Across Both Platforms –** A notable percentage of Android apps (**16–34%**) and iOS apps (**60%**) have no code protection at all, leaving them vulnerable to reverse engineering, credential theft, and fraud. While both Apple and Google enforce strong privacy and permission controls, neither platform requires developers to implement critical in-app protections, such as obfuscation, anti-tampering, or runtime integrity checks, leaving the responsibility squarely on mobile app development and security teams.
- **Free Tools Dominate Android - No Enterprise Grade Protection.** Across all categories, most Android apps (**over 60%**) rely on open-source security tools. This suggests that while there is a broad awareness of the need for app protection by security standards such as OWASP, most app teams use minimal or entry-level solutions. Enterprise complexities and constraints may also contribute to this behavior, but the fact remains that these enterprise apps frequently lack strong defenses, including anti-reversing, anti-tampering, and runtime protection.
- **Tool Choice Often Pushes Security Responsibility onto Developers –** Android's open architecture and abundance of free or basic tools put the onus on developers to evaluate, select, and implement protection solutions that fit their technology stack. They must also ensure these tools operate reliably across a highly fragmented device landscape, which adds complexity and risk. To make matters worse, fragmented and poorly integrated protection tools often clash, introducing build errors, runtime instability and more friction than security.

The Data Leaks You Don't See

Data security remains a critical issue for mobile apps across all industries, primarily because these apps routinely collect and handle vast amounts of personally identifiable information (PII). They also request extensive permissions on users' devices, granting them access to sensitive resources, and frequently connect to multiple, potentially unsecured networks. These factors significantly increase the risk of data exposure, misuse and interception, highlighting the importance of robust data protection measures. The tables below illustrate the extent to which these common data security vulnerabilities affect various categories of apps.

Percentage of Android apps with data leakage-related risks:

Android App Category	Use Vulnerable Encryption Algorithms	Hardcode API Keys & Secrets	Vulnerable to Man-in-the-Middle Attacks	Leak Sensitive Data
Finance	18.00%	7.30%	30.90%	27.90%
Travel	23.20%	6.50%	16.00%	38.20%
Lifestyle	28.10%	8.70%	21.60%	39.90%
Entertainment	26.40%	7.40%	17.30%	42.80%
Food & Drink	22.70%	5.90%	17.40%	37.70%

Percentage of iOS apps with data leakage-related risks:

iOS App Category	Use Vulnerable Encryption Algorithms	Hardcode API Keys & Secrets	Vulnerable to Man-in-the-Middle Attacks	Leak Sensitive Data
Finance	2.50%	1.80%	15.40%	57.20%
Travel	1.90%	1.60%	22.80%	59.10%
Lifestyle	3.60%	2.60%	18.80%	60.90%
Entertainment	3.80%	3.60%	13.50%	51.70%
Food & Drink	2.70%	2.20%	19.30%	54.40%

KEY TAKEAWAYS

- **Potential for Data Leakage Is Alarmingly High –** Data leakage typically occurs through logs, consoles, networks, and insecure storage. In apps across all iOS categories, **50–60%** of apps are vulnerable to leaking personally identifiable information (PII), surpassing the Android rate, which peaks at around **43%**. This suggests that iOS app teams may be overly relying on Apple's privacy posture, or developers may not fully understand how background processes, logging or third-party SDKs expose user data.
- **Prone to MITM Attacks Due to Broken SSL Trust –** Many mobile apps remain vulnerable to man-in-the-middle (MITM) attacks due to misconfigured SSL/TLS implementations. This includes accepting self-signed certificates, using insecure socket factories, skipping hostname verification, bypassing certificate errors, and omitting SSL pinning. These flaws collectively allow attackers to intercept, manipulate, or spoof secure communications, undermining even encrypted connections and exposing sensitive data in transit.

Why Most Apps Are Still Failing Industry Best Practice

Compliance standards are vital for protecting user data and maintaining regulatory requirements. This section presents an analysis of compliance violations in both Android and iOS apps, offering a perspective on the regulatory landscape and potential areas of risk.

Top 5 OWASP Mobile Top 10 Categories with Most Violations Across All Apps

For iOS Apps

- **M10** Insufficient Cryptography
- **M8** Security Misconfiguration
- **M5** Insecure Communication
- **M9** Insecure Data Storage
- **M7** Insufficient Binary Protections

For Android Apps

- **M9** Insecure Data Storage
- **M8** Security Misconfiguration
- **M3** Insecure Authentication / Authorization
- **M10** Insufficient Cryptography
- **M7** Insufficient Binary Protections

Top 5 MASVS Control Groups with Most Violations Across All Apps

For iOS Apps

1. CRYPTO
Cryptographic functionality is used to protect sensitive data

2. PLATFORM
Secure interaction with the underlying mobile platform and other installed apps

3. SECURE NETWORK
Secure Communication

4. RESILIENCE
Resilience to reverse engineering and tampering attempts

5. STORAGE
Secure storage of sensitive data on a device (data-at-rest)

For Android Apps

1. PLATFORM
Secure interaction with the underlying mobile platform and other installed apps

2. CRYPTO
Cryptographic functionality is used to protect sensitive data

3. STORAGE
Secure storage of sensitive data on a device (data-at-rest)

4. CODE
Security best practices for data processing and keeping the app up-to-date

5. NETWORK
Secure network communication between the mobile app and remote endpoints

KEY TAKEAWAYS

- **The Industry Basics Are Still Being Missed—At Scale:** Despite increasing awareness and tooling, apps on both platforms continue to fail at foundational security practices, especially around cryptography, secure storage and platform interaction. These aren't advanced edge cases—they're core controls that should be non-negotiable in any secure mobile app.
- **Data Protection and Platform Misuse Are the Most Persistent Risks:** The most frequently violated categories across OWASP and MASVS point to insecure data storage, weak cryptography and improper use of platforms and APIs. This suggests that sensitive data is regularly exposed both at rest and in transit, and that apps may be misusing or underutilizing built-in security features of iOS and Android.
- **Violations Are Not Platform Specific—They Reflect Design Level Gaps:** The overlaps between iOS and Android violations—such as M10 (Insufficient Cryptography) and M7 (Insufficient Binary Protections) suggest that these challenges stem less from platform limitations and more from the need to mature secure development practices. This gap is often driven by limited visibility into how apps are targeted in the real world and the lack of tools to assess the security and compliance of app binaries before release. Strengthening binary-level assessment and integrating real-time threat visibility into the development lifecycle can help teams close these gaps and ship more resilient apps.

The Invisible Risk Inside Your App

Third-party libraries and frameworks are extensively used in mobile app development, and development teams frequently choose proprietary precompiled binaries for critical functionality, such as authentication, payments and encryption, because they offer enterprise-grade support and faster integration. However, these binaries often come with limited source code and dependency visibility, making assessing their behavior or security posture difficult. This lack of transparency introduces silent vulnerabilities that traditional security tools struggle to detect, creating a blind spot in the mobile app supply chain that attackers can exploit.

The tables below give insight into some of the top third-party libraries and framework components and the significance of the internal supply chain visibility gap these represent.

Top 10 Third-Party Frameworks in the 1,000 most popular Android apps in the store

Framework/Library	Category
firebase	Authentication, Realtime DB, Cloud Functions
kotlin	Programming Language
firebase-installations	Manages app instance IDs
firebase-analytics	Tracks user behavior, events, and app performance
okhttp	Handles HTTP requests
gson	Data Serialization
firebase-cloud-messaging	Push Notifications
glide	Media Handling
lottie-by-airbnb	UI/UX Animations
ZXing	Scans barcodes/QR codes using the device camera

Android Insight

62% of the **top 100** widely used Android frameworks are only available as precompiled binaries.

Top 10 Third-Party Frameworks in the 1,000 most popular iOS apps in the store

Framework/Library	Category
firebase	Authentication, Realtime DB, Cloud Functions
firebase-installations	Manages app instance IDs
firebase-analytics	Tracks user behavior, events, and app performance
fabric-crashytics	Crash Analytics
nanopb	Data Serialization
firebase-cloud-messaging	Push Notifications
sdwebimage	Optimizes image loading
firebase-remoteconfig	Deploy OTA changes to app's behavior and appearance
lottie-by-airbnb	UI/UX Animations
react-native	Enables cross-platform development

iOS Insight

46% of the top 100 widely used iOS libraries and frameworks are **only** available as pre-compiled binaries.

KEY TAKEAWAY: The "Pre-Compiled Binary" Blind Spot

Traditional CI/CD workflows often rely on source code scanners and SCA tools, which cannot assess the runtime behavior of third-party libraries, especially when access to the source code is not available. This lack of visibility becomes even more dangerous considering that **90%** of the codebases include components more than **10 versions behind** the latest release.

Most proprietary, closed-source components are responsible for critical functions, such as authentication or payments, so the impact of security failures here can be costly.

Know Your Device - Device Attestation Is Critical

Today, the mobile device itself has become a critical point of vulnerability. As attackers increasingly target the underlying mobile environment to bypass app-level defenses, ensuring that an app is running untampered on a secure, uncompromised device is no longer optional. Outdated operating systems, rooted or jailbroken devices, application toolkits to manipulate applications and malware infections create blind spots that traditional app protection tools cannot mitigate alone. Device attestation is essential for validating device integrity in real time, allowing organizations to block high-risk interactions, protect sensitive data and defend against fraud before it starts.

Risky & Unsafe Devices

The percentages of various device risk factors:

The number of Android devices running an outdated operating system during any given 12-month period.	**61.2%**
The number of iOS devices running an outdated operating system during any given 12-month period.	**49.2%**
Total Vulnerable-Non-Upgradeable Devices	**25.2%**
Android Devices that have encountered malware	**18.1%**
Android Devices with Side-Loaded Apps	**25.3%**

Compromised Devices

1 in 400 Android devices is **ROOTED**

1 in 2,500 iOS devices is **JAILBROKEN**

3 out of every 1,000 mobile devices are **COMPROMISED**

1 out of every 5 Android devices encountered **MALWARE**

How Attackers Leverage These Devices

Rooted Devices	Jailbroken	Compromised
• Bypassing app protections • Inject malicious code into apps or hijack flows • Steal sensitive data directly from app storage or memory	• Hook into secure app functions (e.g., payment, authentication) • Read private app containers to steal keys, tokens, or PII • Tamper with runtime logic to alter transactions or spoof UI	• Create phishing overlays on legitimate apps • Perform device spoofing for fraud or fake check-ins • Harvest app data silently, even in the background

KEY TAKEAWAYS

- **App-level security Is Undermined Without Comprehensive Device Attestation:** Even apps using paid protection tools remain exposed if they run on compromised or outdated devices. The absence of device attestation results in trusted code running on untrusted environments, diluting the value of app-layer defenses.
- **Modern Mobile Fraud Now Starts on the Device –** With malware encountered by **1 in 5** Android devices and many running outdated or compromised OS versions, attackers are shifting their focus to the device itself. By targeting the endpoint, they can bypass in-app protections, manipulate app behavior, steal credentials and execute fraudulent transactions, often without triggering server-side alarms. This shift is reflected in threat trends: Kaspersky reported a 196% surge in Trojan banker attacks on smartphones in 2024 compared to the previous year, underscoring the growing role of compromised devices in mobile fraud.

Conclusion

The findings of this 2025 Global Mobile Threat Report make one thing clear: **mobile is now a primary attack surface, not a secondary concern and should be treated to the same comprehensive protections as traditional desktops.** Despite widespread awareness of mobile threats, security measures across both apps and devices remain fragmented and create security gaps due to misalignment with the realities of today's threat landscape.

Organizations must adopt a risk-based approach to mobile security to counter the mobile-first strategies of attackers who exploit vulnerable devices, poorly protected apps, and blind spots in third-party supply chains to access sensitive data and systems.

This means:

- Treating device-level risks such as mishing (mobile-targeted phishing), outdated operating systems, and side-loaded apps as integral to mobile endpoint security outcomes.
- Continuously vet third-party apps on employee devices to evaluate their actual behavior, beyond stated functionality, with every update, ensuring they don't become hidden threats to the enterprise.
- Analysis of developed applications should be thoroughly assessed **PRIOR** to release to ensure best practices, industry standards and to validate protection against expected benchmarks.
- Embedding security **throughout** the mobile app development lifecycle, not just at the code level, and assessing applications for compliance to these requirements prior to release.
- Shifting from reactive controls to **proactive visibility,** including binary-level analysis, runtime protection, and device attestation.

Mobile security is no longer optional or peripheral. **It is now a strategic pillar of enterprise risk management.**

Want to understand how secure and compliant your apps are? Get a **free 30-day trial** to uncover hidden vulnerabilities, insecure code, and misconfigurations—before attackers do.

Contact Us to learn how we help teams secure mobile apps across the entire development lifecycle.

Sources

1 https://explodingtopics.com/blog/smartphone-stats

2 https://buildfire.com/app-statistics/

3 https://www.gartner.com/en/newsroom/press-releases/2023-05-10-gartner-survey-reveals-47-percent-of-digital-workers-struggle-to-find-the-information-needed-to-effectively-perform-their-jobs#:~:text=According%20to%20the%20survey%2C%20the,or%20more%20applications%20at%20work.

4 https://attotime.com/blog/cell-phones-work-statistics

5 https://jumpcloud.com/blog/byod-statistics#:~:text=to%20the%20report:-,Over%2080%25%20of%20organizations%20use%20BYOD%20today.,it%20will%20increase%20%E2%80%9Cdramatically.%E2%80%9D

6 "Phishing Activity Trends Report, 3rd Quarter 2024," APWG, 4 December 2024.

7 https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf

8 https://www.zimperium.com/blog/hidden-in-plain-sight-pdf-mishing-attack/

9 https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf

10 ibid.

11 https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

12 https://zimperium.com/blog/mobile-spear-phishing-targets-executive-teams

13 https://digital-markets-act.ec.europa.eu/index_en

14 https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=15556&startdate=2024-01-01&enddate=2024-12-31

15 https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis/thankyou.html

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium delivers unparalleled protection for mobile applications and devices. As cybercriminals adopt a mobile-first attack strategy, Zimperium's AI-driven mobile security enables organizations to stay ahead of evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. Learn more at www.zimperium.com.

ZIMPERIUM®

Disclaimer

Zimperium, Inc. makes this report available on an "as-is" basis with no guarantees of completeness, accuracy, usefulness or timeliness. The information contained in this report is general in nature. Opinions and conclusions presented reflect judgment at the time of publication and may change at any time. Zimperium, Inc. assumes no responsibility or liability for errors, omissions or for the results obtained from the use of the information. If you have specific mobile endpoint or application security concerns, please contact Zimperium, Inc. via https://www.zimperium.com/contact-us/.