2024 Global Consumer Expectations of Mobile App Security

Introduction

The Open Worldwide Application Security Project (OWASP) is the world's largest nonprofit foundation and global community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain secure applications that can be trusted.

Thousands of teams around the world build software applications of all types including web, cloud, mobile, IoT and more across a myriad of platforms. The OWASP Mobile App Security (MAS) flagship project provides a proven, community-driven security standard for mobile teams to deliver high quality, secure mobile apps.

In 2024, OWASP is proud to join Appdome to bring the voice of Consumer Expectations of Mobile App Security to the OWASP community and raise awareness among cyber practitioners at software organizations to the cybersecurity and anti-fraud demands of everyday mobile end users. The report provides a powerful voice of consumer expectations about mobile app security and privacy protection.

The report highlights three critical areas relevant to all mobile brands and enterprises:

1. People depend extensively on mobile apps in life and work.
2. People have strong and detailed expectations of security, anti-fraud and data privacy in their mobile applications.
3. People will reward brands and enterprises that protect their mobile use against these threats.

These consumer perspectives on fraud, security, privacy and trust are highly valuable for every organization. Cybersecurity leaders can leverage this consumer and employee feedback into the conversation about proper defense models, requirements and practices. This same voice can be used with business leaders, development teams, and other stakeholders to show the OWASP mobile standard matters to app users more than ever.

The 2024 Appdome Global Consumer Survey confirms that the OWASP mobile standard is more than the best practice guideline for mobile app security. The OWASP mobile standard is the baseline expectation of global consumers. This validation reinforces the critical value of OWASP mobile standard and the importance of implementing comprehensive security, anti-fraud, anti-malware and other defensive measures in mobile applications. Mobile software teams should leverage the OWASP Mobile App Security project and resources as a baseline for their mobile security and privacy programs. Mobile software teams should also leverage the data in the 2024 Global Consumer Survey to deploy the security, anti-fraud, anti-malware and data privacy protections demanded by all users, globally.

Andrew van der Stock

Executive Director, OWASP Foundation

Top Findings: 2024 Global Consumer Expectations of Mobile App Security

The Appdome 2024 Consumer Expectations of Mobile App Security Survey continues to showcase the increasing dominant role of mobile apps in consumers' daily lives to bank, bet, shop, socialize, work and more. The survey, now in its fourth year, gathers data from 120,000 consumer responses across 12 countries, shows the growing clarity and strength of demand consumers have for robust anti-fraud, security, and data privacy protections in mobile apps.

Mobile Fraud Protection Takes Center Stage

In 2024, mobile fraud is a primary consumer concern. With social engineering and AI-based scams growing globally, 58% of consumers declared fraud as the #1 concern, the highest level since we began this survey in 2021. Additionally, consumers are growing increasingly aware and alarmed about the diverse ways mobile fraud manifests itself, including location spoofing, social engineering, and account takeovers. Nearly half of this year's respondents reported first- or second-hand personal experiences with fraud, social engineering scams and other incidents. An overwhelming 98% of consumers expect mobile apps to protect them against fraud, with 84% favoring preemptive anti-fraud measures are a must in mobile apps.

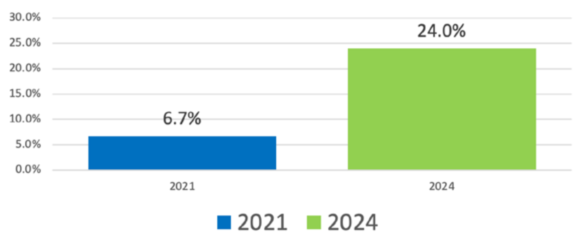
On-Device Data Privacy on the Rise

Consumers are increasingly worried about how their data is used and handled in mobile applications and transactions. Notably, consumers believe mobile app developers do not prioritize security or take mobile app protection seriously, while also saying mobile brands are responsible for secure mobile app experiences. Additionally, 90% of consumers said they seek out information about in-app security and privacy before using new apps. A new "watch out" moment for mobile brands has emerged. Approximately 69% of global mobile consumers have expressed a willingness to cancel accounts and delete mobile apps that do not protect data in mobile apps effectively. For these consumers, protecting PII, particularly identity, credit card and account login information is of paramount importance. These same consumers say brands should be more transparent about security and privacy in mobile apps.

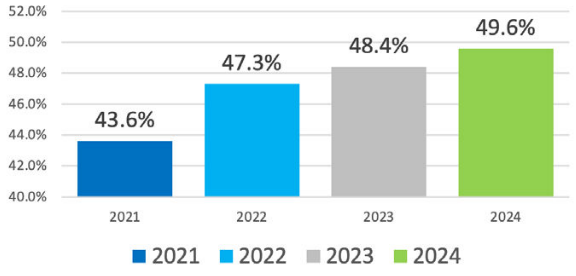
Mobile Brands: Fear and Responsibility at All Time High

This year's survey highlights a critical juncture for mobile brands. As consumers become more familiar with the mobile app threat landscape, more respondents state that "the maker of the mobile app" has primary responsibility for protecting the app experience, which this year was at 57.5%, a 2.4% increase compared to 2023. Consumer skepticism also continues to increase, with 24% of respondents stating that "devs don't care" about securing mobile apps, an increase of 258% compared to our first survey in 2021. Mobile brands must heed these results, using them as a rallying point to act on consumers' concerns and implement comprehensive protections to gain consumer loyalty and trust, increase lifetime value (LTV) and average revenue per user (ARPU), and reduce user churn and customer acquisition costs.

Consumers Who Think Devs Don't Care About Security



Consumers Who Demand the Best Protection



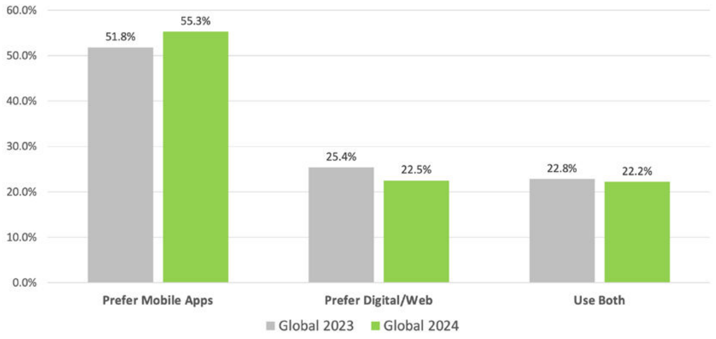
Mobile Apps Continue Ascent to Dominance

In 2024, consumers continued their shift to mobile apps as their primary channel for interacting with brands, conducting work, and completing transactions.

Mobile Extends Leadership Over Web for Purchases

This year marked the 3rd consecutive survey where consumers reported using mobile apps more than web or online sites for purchases and other transactions. The growth gap between mobile and online sites widened at a similar pace as the prior 3 years, making it unquestionable that mobile apps are displacing online sites as the most widely used part of consumers' daily activities. As shown in the chart, mobile apps continue to be the dominant channel for purchases, increasing 6.7% from 2023, taking share away from web channels.

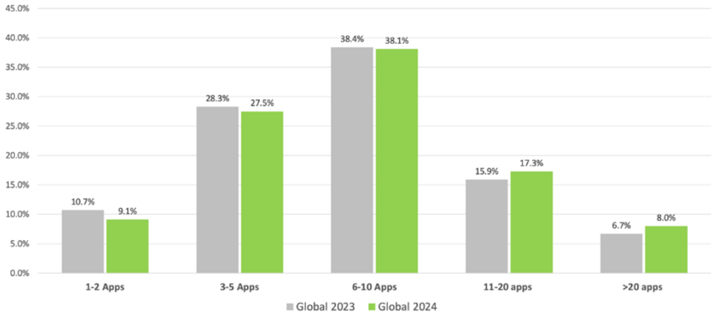
How comfortable are you buying things for yourself, family or friends on mobile apps?



Users Expanding Appetite for More Apps

Consumers continue to increase the number of apps they use every day. Almost 40% of global consumers report using between 6 and 10 mobile apps daily. The number of consumers who use 11-20 apps grew by 8.8%, and those who use 20+ apps leapt 19.4% compared to 2023. The trend toward higher app counts is even more pronounced over the longer term, as the number of consumers using 20+ apps daily has increased 23.1% since 2021. This growth came at the expense of consumers who use 1 or 2 apps daily, which dropped 39.3% since 2021.

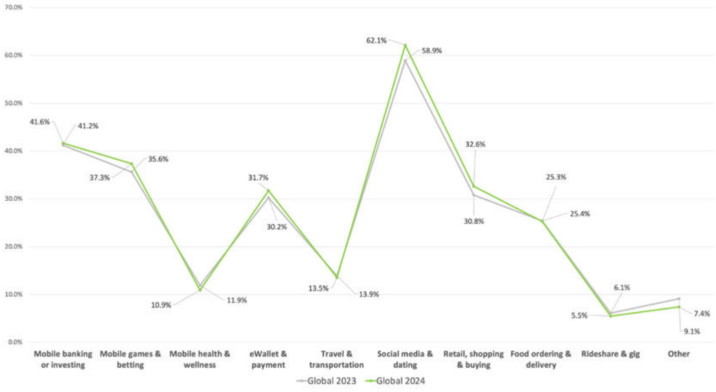
In an average week, how many mobile apps do you use?



More Types of Mobile Apps Dominate the Landscape

Consumers continue to prioritize mobile apps for an expanding array of activities and transactions. The survey underscores a significant reliance on mobile apps for financial transactions, banking, social media/dating, shopping/retail, travel, mobile games, and betting. While in previous years, banking and investment apps dominated the transaction landscape, we now see consumers engaging in transactions across many app types. Notably, use of eWallet apps increased 81.2% since 2021, and consequently, consumers' security expectations for eWallets also grew 38.1% over the same time..

Most Often Used Mobile App Types



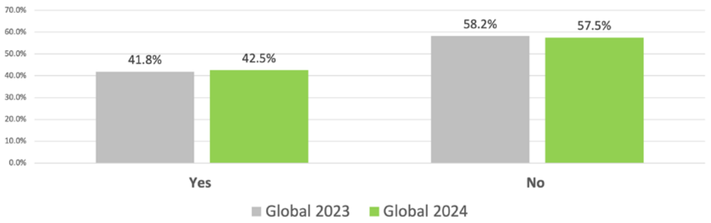
Mobile Fraud Is Top of Mind for the Consumer

Mobile fraud became the top concern for consumers as AI-based attacks grew in both intensity and diversity. Consumers are surprisingly aware of the many ways mobile fraud occurs.

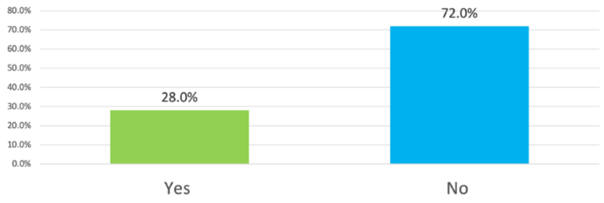
Many Consumers Are Victims

One of the most startling datapoints from the 2024 survey is the significant percentage of consumers who said they have directly experienced mobile fraud and social engineering scams. Of global consumers surveyed, 28% have experienced a social engineering scam, and 42.5% have been the victim of a cyber-attack, mobile malware, or mobile fraud. The actual impact of these attacks is likely to be much higher, as artificial intelligence, deep fakes, voice cloning and the use of other sophisticated techniques make it almost impossible for mobile users to detect attacks until it's too late.

Have you, a family member, or a friend experienced a cyber-attack, malware, or mobile fraud?



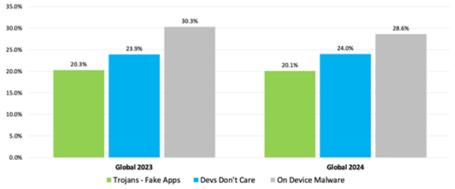
Have you, or anyone you know, experienced a social engineering scam?



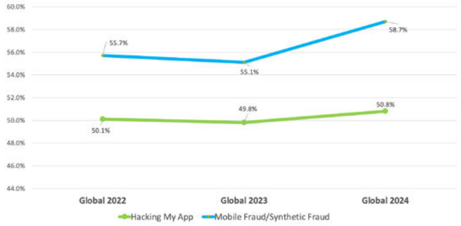
Diversity of Consumer Fears Is Growing

Fraud and hacking top the list of consumer concerns, with 58.7% and 50.8% of respondents, respectively, expressing these vectors as their top concerns. Other top fears expressed by consumers are mobile malware and Trojans, which have increased 121% and 179%, respectively, since 2021. The data also reveals a slight uptick in consumer fears over network-based attacks and data breaches (both up about 4% from 2023), likely influenced by the stream of media headlines of successful attacks and breaches against major brands.

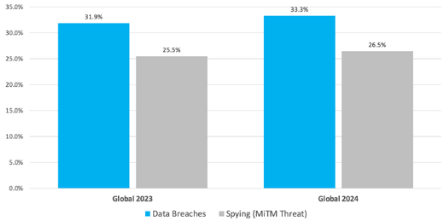
What On-device threats concern you the most as a user of mobile apps?



How have cyber security threats vs fraud evolved over time?



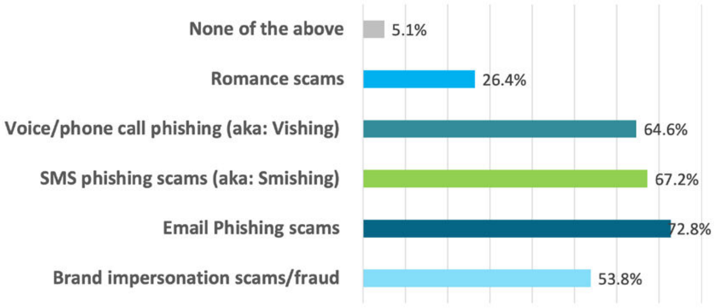
How Important are Network Level Threats such as Data Breaches & MiTM Attacks?



Social Engineering Emerges as a Top Concern

New in 2024, we asked consumers about social engineering attacks. Specifically, 53.8% reported being targeted in brand impersonation scams, and 64.6% were victims of voice phishing, or "vishing." Vishing, where fraudsters use phone calls to trick users into revealing sensitive data, is now a top threat, comparable to email and SMS phishing (smishing). The rise of vishing highlights the evolving threat landscape and the need for robust anti-fraud measures to protect consumers from sophisticated scams.

Which social engineering scams pose the biggest risk?



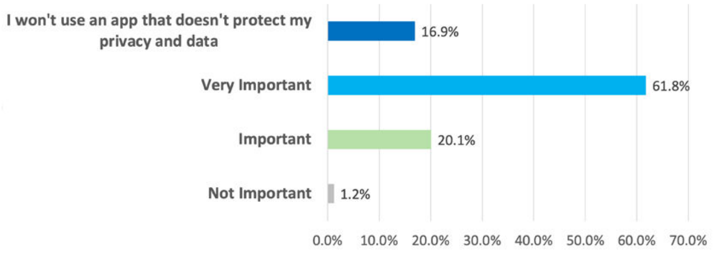
Consumers' Growing Expectations for Security…

Consistent with previous years, mobile app security continues to be a concern for consumers, as more than half of the surveyed consumers

Data Privacy is a Top Expectation

Data Privacy is clearly a top priority for consumers, with 98.8% ranking data privacy as "important" or "critically important." Almost 17% said they would not use a mobile app that didn't protect their data privacy. At the same time, consumers globally are becoming increasingly concerned by the lack of protection of their personal information, and this discomfort fuels increased demands for protection in mobile apps. Consequently, 53.1 % of consumers said that mobile apps that collect, use and share personal data should maintain the highest levels of security and privacy protection, a 3.5% increase from 2023.

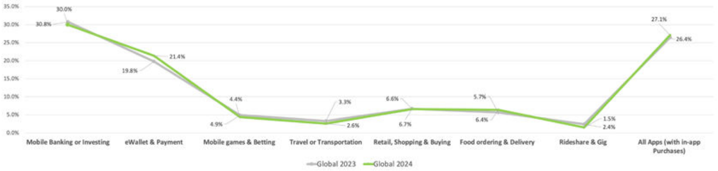
How important is your mobile privacy when using mobile apps?



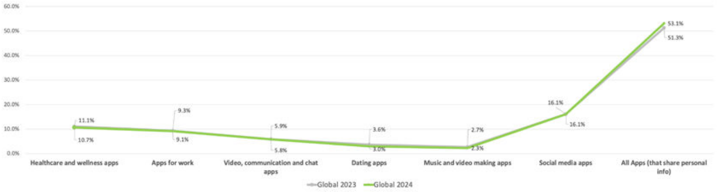
More Selective Security Demands

Consumers continue to refine their expectations for more robust security, prioritizing their security demands based on specific app categories, with e-Wallets, banking apps, retail/shopping apps, and healthcare apps receiving increased demands for better app security. More than half of the consumers surveyed expect robust security and protection of PII from mobile app developers, demonstrating a clear upward trend in consumers' level of concern about fraud year over year. A key takeaway from this data is that global consumers expect the most protection from mobile apps that handle their finances, health, and relationships/connections.

For mobile apps with in-app purchases, which app should have the highest level of security?



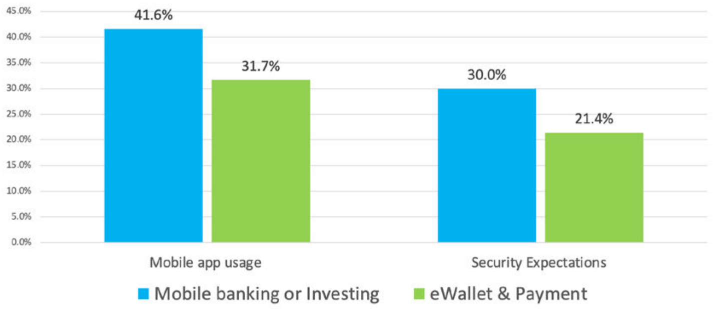
For mobile apps that share personal info, which app should have the highest level of security?



Protection Increase with App Usage

As in previous years, the data suggests a high degree of correlation between mobile app usage and expectations for robust mobile app security, privacy and fraud protections. Generally, consumers have higher expectations for mobile app security and fraud protections for the mobile apps they use the most, with emphasis on apps that handle financial data, transaction-based apps, and apps that handle PII. This is most notable with mobile banking, eWallet and payment apps as shown in the chart below. Yet security expectations have also grown for social media, and dating apps, up 30% and 23.1% respectively since 2021, suggesting a broader trend.

Security Expectations Increase With App Usage



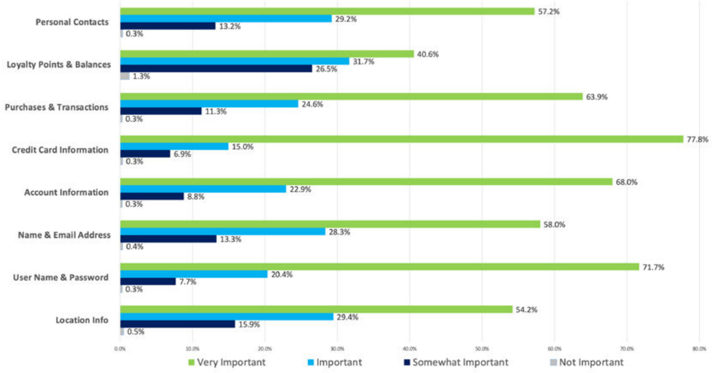
… And Privacy Protections in Mobile Apps

More than 85% of consumers rank mobile app protection as "important or very important," emphasizing secure data storage, robust authentication mechanisms, and PII protection.

PII Protection Is More Important Than You Think

Protecting PII is a top priority for mobile consumers, such as location data, user IDs and passwords, email addresses, contacts, purchase history, and transactions. This year credit card data was top of the list of "very important" to protect at 78%, followed by username/password at 72% and account information at 68%. While loyalty apps did not rank as highly as the others at 41%, we suspect this is based on lower uptake of loyalty programs vs. banking, credit card and other "everyday apps." While financial apps continue to set ambitious standards for security, the data shows that consumers consider other private data types within apps to be equally important.

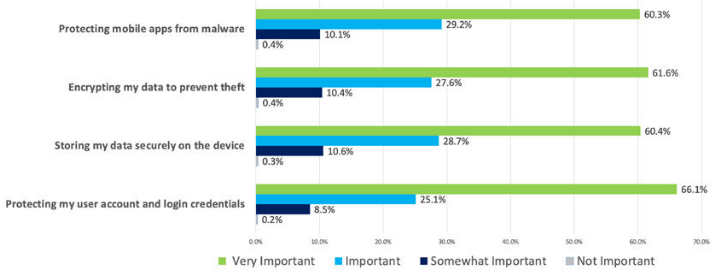
Please assess the importance of security of your personal data for each item



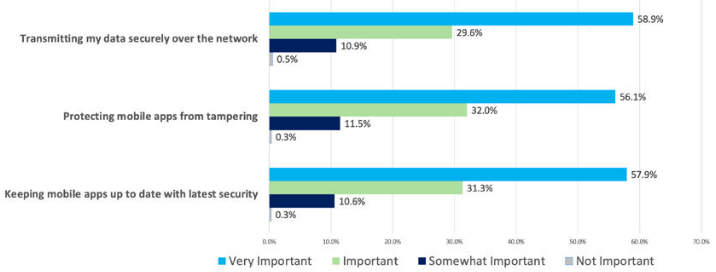
Consumers Demand Comprehensive Protection

Consumers placed the highest importance on protecting their account credentials, preventing malware, encrypting data, and ensuring secure data storage on mobile devices. More than 60% of global consumers ranked each of these aspects as' very important'. The seven controls listed in the charts, which align with the OWASP MASVS standard, signal to developers that each is either very important or important to nearly 90% of consumers in all cases. The data shows that although consumers ranked protection of credentials, malware prevention, encryption, and secure data storage with the highest level of importance, they are not willing to sacrifice one area of protection for another. Instead, mobile consumers demand comprehensive protection across the board when it comes to the MASVS metrics. This highlights a clear consumer expectation for robust security measures throughout the entire mobile application experience. In turn, this underscores the critical need for mobile brands to take a holistic approach to mobile application security, fraud and malware prevention, as well as data and privacy protection, if they expect to meet user demands and ensure their trust.

In the mobile apps you use daily, please assess the importance of each security area listed



In the mobile apps you use daily, please assess the importance of each security area listed



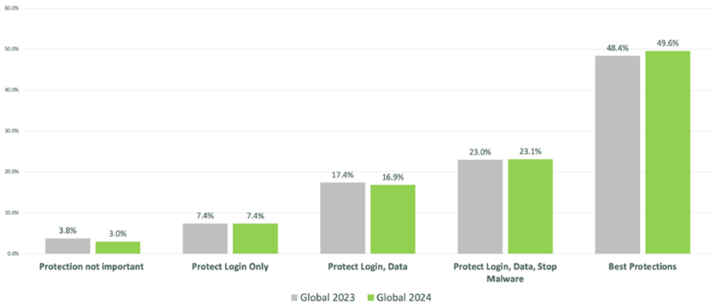
Consumers Reaffirm Developer Responsibility

Despite clear demands, consumers continue to perceive mobile developers are not taking mobile app protection seriously, leading to ongoing concerns about the safety of their data, activities, and transactions.

“We Deserve the Best Protections,” Mobile Consumers

Security and privacy expectations continue to rise. At 49.6%, nearly half of global consumers demand the “best protections,” which include anti-malware and anti-fraud defenses, in the mobile apps they use, up 13.7% since 2021. Similarly, the number of consumers with less demanding security requirements (login and data protection only) continues to decline year over year, and the number of consumers who say protection is not important has declined by 77.5% since 2021. Almost 9 out of 10 consumers now say security and privacy are equal to or more important than features in mobile apps. The data makes it extremely obvious that basic code-level protections alone will not cut it. Advanced protections like anti-malware and anti-fraud represent the "new baseline" for mobile app protection.

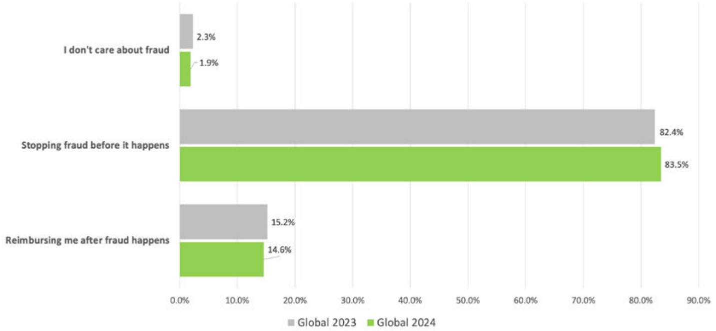
What type of protection do you expect mobile brands to provide you when you use their app?



Preemptive Fraud Prevention Preferred

Consumers' demand for strong anti-fraud measures in mobile apps is unmistakable. Approximately 98% expect mobile apps to protect them against fraud, and 84% prefer preemptive fraud protection/or anti-fraud measures versus reimbursing them after the fraud has occurred. This should serve as a wake-up call for mobile brands using legacy fraud solutions that only reactively respond to fraud. Consumers will prefer brands that provide preemptive fraud prevention inside the mobile experience.

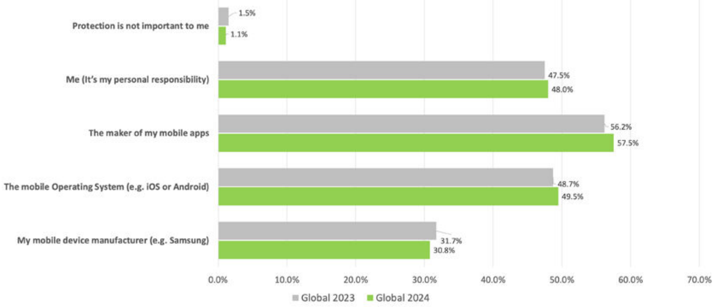
When using mobile apps, what's more important in protecting you against fraud?



Brands Have Higher Responsibilities

More than half of global consumers, or 57.5%, say it’s the mobile brand or developer’s responsibility to protect them from cyber-attacks, malware, fraud and privacy leakage, an increase of 2.4% from 2023. What’s also notable this year is a smaller percentage of consumers say protection lies with the mobile OS or device maker. This shows consumer awareness of mobile brands being in control of their data and transactions and wanting the brands to be held accountable. Consumers do remain skeptical, as 24% of global consumers said they believe “developers don’t care” about protecting them against fraud and security threats, a significant increase from our first year of the study when only 6.7% of consumers said so.

Whose job is it to protect you against mobile fraud, malware and cyber-attacks?



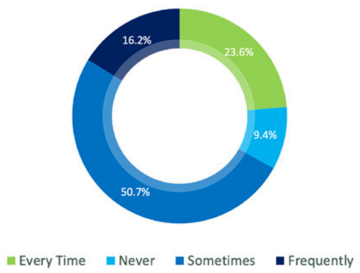
Consumers Take ‘Carrot and Stick’ Approach with Mobile Brands

Secure by design is essential to maintain consumer trust, loyalty, and growth. Will brands heed the call of duty or risk churn & reduced ARPU?

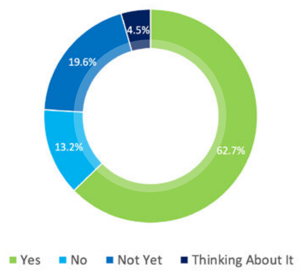
The Double-Edged Sword of App Security and Privacy

Nine out of 10 consumers reported that they seek out information about the security and privacy measures in mobile apps before using them, with 25.6% stating they do this every time. Nearly two-thirds, or 62.7%, said they’ve deleted or stopped using a mobile app because of security or privacy concerns. The data shows the importance of making information about security visible to consumers, via email campaigns or release notes.

Do you seek out information about the security in mobile apps before using them?



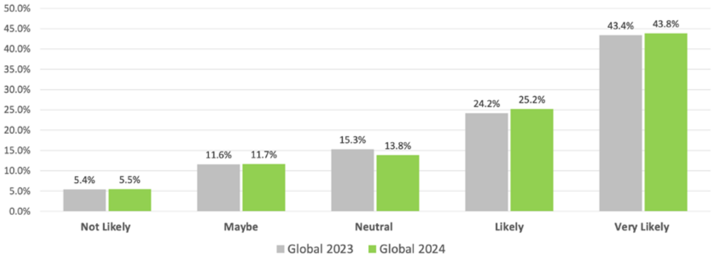
Have you ever stopped using or deleted a mobile app due to privacy or security concerns?



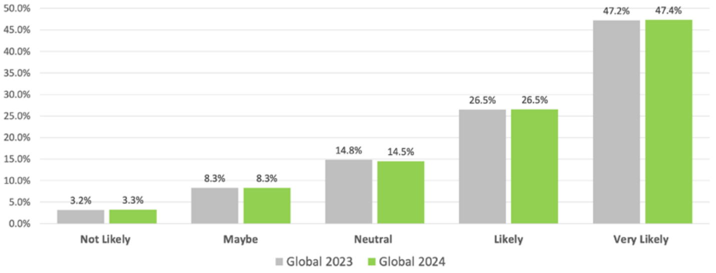
Consumers Churn If Brands Don’t Protect Them…

Global consumers asserted again that they would abandon mobile apps that did not protect them, with 69% stating that they would likely or very likely quit using a mobile app if they discovered that the app did not protect them. Similarly, 73.9% of consumers also stated that they would abandon brands that experienced a breach and encourage their friends to do the same. This data underscores the critical importance of robust security measures for mobile apps, as failing to provide adequate protection leads to immediate customer loss and damages brand reputation through negative word-of-mouth.

If you discovered that your mobile brand didn't protect you, your data, or your use, how likely are you to stop using the app?



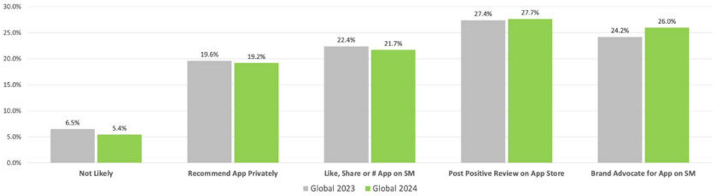
If the mobile app you used actually got breached or hacked, how likely are you to stop using it?



… But Will Reward Brands That Do

When asked if they would promote security-conscious brands, 94.6% of consumers confirmed their willingness. Like in 2023, consumers preferred visible and public forms of advocacy, such as “likes” or hashtags on social media, positive reviews on app stores, and brand advocacy on social media. This trend highlights the importance of robust security and privacy measures both for consumer protection and enhancing brand visibility and reputation, affirming that protecting consumers is good for business.

If your mobile app protected you, your data, or your use, how likely are you to recommend the app to others?



Mobile Dev & CISO Action Plan

Your mobile cyber defense culture should protect the customer first.

Rebalance

CISOs need to rebalance cyber spend and budgets to meet the needs of the mobile business, brand and users. In the past four years, the mobile side of the business has eclipsed web/online channels for brand interactions and transactions. Correspondingly, more mobile consumers care about mobile specific threats like social engineering attacks and other forms of fraud, vishing, and malware. Mobile defense postures often lag online and web defense postures, which leaves mobile brands and their consumers exposed. As a result, CISOs must find ways to enhance mobile app defenses to surpass the sophistication of modern attacks and threats.

Rethink

In light of the consumer voice and data, CISOs also need to rethink the definition of the minimum level of mobile app defense and go beyond Obfuscation and Runtime Application Self Protection (RASP). Mobile consumers are clear in their demand for the best app protections. To meet these expectations, CISOs must go beyond the minimum and add anti-fraud and geo-fraud prevention, anti-malware, and data protections. These additional protections are crucial for maintaining consumer trust and ensuring the security of the mobile brand itself.

Machines

Using an automated platform simplifies the traditionally complex and time-consuming security integration process, enabling faster deployment and enhanced protection against mobile attacks and threats, ultimately ensuring robust and up-to-date security for mobile apps. Leverage platforms that use Machine Learning to ensure rapid, consistent, and comprehensive protections and build in the CI/CD pipeline. Ensure machine-verified implementations to clear releases and verify that every mobile app version has the requisite protections required for that app and that business.

Mobile Data

Mobile app defense telemetry data is crucial to stop fraud and other security attacks, protecting mobile brands' apps and consumers. Using an intelligence framework, mobile fraud, threat and attack data allows apps and SDK services to consume any number of threat signals needed. Telemetry provides real-time insights, enabling early detection, giving mobile brands the knowledge to make data-driven decisions about attacks and threats and improving attack prevention.

Intelligent Defense

Mobile app defense is moving beyond simply closing the app when attacks happen. Modern mobile app defense designs focus on maintaining the consumers' use of the mobile app instead of crashing or closing the app when attacks occur. Instead, mobile brands need to implement frameworks that allow security events to be consumed by the app, allowing mobile brands to limit functionality and provide methods to resolve threats, protecting app brands and consumers themselves.

The Appdome Advantage

Better Mobile App Protection, Faster & Easier than Everything Else.

Easily build, test, and release 300+ Certified Secure™ features like fraud prevention, security and anti-bot defense into Android and iOS apps within the DevOps CI/CD pipeline. Utilize Threat-Events™ for in-app defense and Threat-Aware UX/UI control during attacks and monitor real-time defenses with ThreatScope™ Mobile XDR. Simplify processes, reduce costs, and expedite delivery.

BUILD

Unified Mobile App Defense Platform

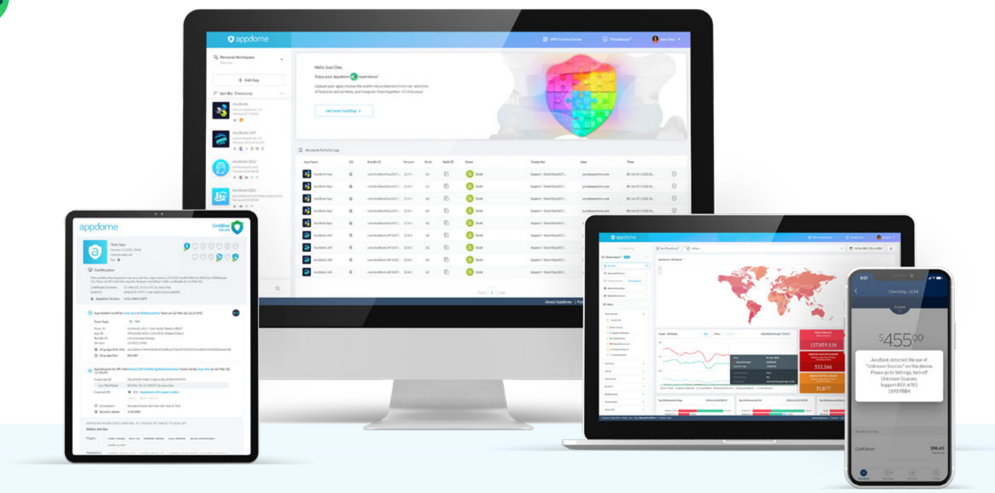
Appdome's platform delivers mobile app security automation with full management and control in a DevOps class tool connected to the mobile CI/CD pipeline. Choose from 300+ protections to protect your apps today.

CERTIFY

Certified Secure™

Appdome's Certified Secure is the sole in-line security certification service ensuring protection for Android & iOS apps within the DevOps pipeline.

Certified secure



PROTECT

Comprehensive Mobile App Protection

Comprehensive protection for any Android or iOS app, including anti-fraud, anti-malware, anti-bot, cheat prevention, geo compliance, social engineering prevention, and more. Start with a single feature and add more as you go. No code, no SDK, no servers, no agents required.

MONITOR & RESPOND

Mobile XDR Threat and Attack Intelligence

Utilize Threat-Events™ for in-app defense and Threat-Aware UX/UI control during attacks and ThreatScope™ Mobile XDR for real-time attack monitoring to validate protection effectiveness, adapt defenses, and make your Android and iOS apps attack-aware.

About Appdome

Appdome is on a mission to protect every mobile app in the world and the people who use mobile apps in their lives and at work. Appdome provides the mobile industry's only Unified Mobile App Defense platform, powered by a patented mobile coding engine, Threat-Events™ Threat-Aware UX/UI Control and ThreatScope™ Mobile XDR. Using Appdome, mobile brands eliminate complexity, ship faster and save money by delivering 300+ Certified Secure™ mobile app security, anti-malware, anti-fraud, anti-social engineering, mobile anti-bot, anti-cheat, geo compliance, MiTM attack prevention, code obfuscation, social engineering and other protections in Android and iOS apps with ease, inside the mobile DevOps and CI/CD pipeline. Leading financial, healthcare, government and m-commerce brands use Appdome to protect Android and iOS apps, mobile customers, and mobile businesses globally. Appdome holds several patents including U.S. Patents 9,934,017 B2, 10,310,870 B2, 10,606,582 B2, 11,243,748 B2 and 11,294,663 B2. Additional patents pending.

2024 Global Consumer Expectations of Mobile App Security

Secure your mobile app today with Appdome - The One-Stop Shop for Mobile App Defense.

To learn more about Appdome, visit **appdome.com**
or sign up for a free trial at **fusion.appdome.com**