jamf

Security 360:
Annual Trends Report
Mobile Devices

Foreword

Across industries and use cases -- from retail workflows to healthcare operations -- business leaders are innovating with mobile to transform the way people work and to optimize organizational outcomes. For many employees across industries, mobile (e.g., smartphones and tablets) are the only devices used at work. And the modern workplace is about empowering employees to connect from anywhere, at any time, and on a device they want to use.

One of the key drivers for mobile work started with the adoption of mobility as a workplace service. They are no longer companion devices, but are increasingly the main point of entry to get work done. While mobility is no stranger to the workplace, its continuous integration into key workflows is more pronounced than ever before. Today's workplace requires not only exceptional digital experiences, but **secure** digital experiences that maximize worker productivity regardless of where they choose to work.

– Josh Stein,
VP of Product Management

Introduction

Jamf's Security 360 is a report that is derived from the analysis of real-world customer incidents, threat research and industry events from the past year. This report is focused on exploring the mobile threat landscape to put a spotlight on the risks that organizations face.

We provide an assessment of the diverse attack vectors that are actively utilized to trick users, compromise mobile devices and infiltrate organizations. These attacks are not limited to device vulnerabilities, so our analysis also includes risky apps, web threats and more.

In addition to analyzing these threat trends, the report includes a perspective from Jamf's CISO to provide the insights security leaders think about when protecting their mobile fleets across the user, device, application and network levels.

Research methodology

To understand and quantify the real-world impact of the security trends identified in this report, we examined a sample group consisting of 1.4 million devices protected by Jamf. Our analysis was carried out in the first quarter of 2025, revisiting the prior 12-month period and spanning globally across 90 countries and multiple platforms – specifically, iOS and iPadOS and Android devices.

To preserve privacy and maintain the highest standards when gathering and handling data, the metadata analyzed in our research comes from aggregated logs that do not contain personal or organization-identifying information.

Purpose of the research

Our intention with this analysis is to enable organizations and users to understand the evolving cybersecurity trends that currently exist, as well as show how organizations and users can take steps to mitigate risks. It also provides overviews of the most impactful research by Jamf Threat Labs, including threats and vulnerabilities they found. By informing our audience about what is out there, we hope to dispel any myths, and show how you can implement safeguards to protect your users and data. Some of the most common best practices organizations can implement:

- Continuous and timely operating system updates
- User education and training
- Application vetting
- Multi-factor authentication
- Zero-trust security frameworks
- Establish and manage compliance baselines
- Implementing acceptable use policies for corporate data

We structure our analysis and report into four categories we found to be the highest priority for organizations around the globe:

I. Mobile Phishing

II. Vulnerability Management

III. Application Risk

IV. Malware & Spyware

This analysis in this report is informed by Jamf's Threat Intelligence, a broad collection of insights that are derived from original threat research, real-world usage metrics, along with news analysis and data feeds. Jamf's Threat Intelligence is made up of human-led research from the Jamf Threat Labs and Data Science teams who monitor devices, app and network traffic for risk, threats and zero-day vulnerabilities.

The stats in this paper are inclusive of **Apple** and **Android** devices.

We also have a Security 360 report focused on **Mac devices** which you can find **here**.

Key trends for mobile

I. Phishing Continues to Challenge Businesses

Phishing continues to be a prevalent attack technique from threat actors and its influence in the threat landscape is as active as ever. In September 2024, **Apple released a blog post** with guidance to iOS users to help "avoid scams and learn what to do if you receive suspicious emails, phone calls, or other messages". No matter how secure a platform or operating system, social engineering techniques – like phishing – are designed to infiltrate business data starting with the least secure part of the device – the user.

II. A single vulnerability can help attackers gain systemwide access

It's a fact: vulnerabilities occur in software (both OS and applications) we use daily. According to **NIST Special Publication 800-124rd**, "In the case of typical software, errors and vulnerabilities exist at an estimated frequency of ~25 errors per 1000 lines of code." Common vulnerabilities and exposures (CVE) published in the National Vulnerability Database (NVD) provides the public with an understanding of the CVEs that are out in the wild. These updates are vital, but that patch needs to be applied before they can be helpful to the organization.

Apple and Google provide important information when a vulnerability is discovered – and what operating system update fixes the vulnerability. For example, earlier this year, Apple released iOS 18.3.2 in response to **CVE-2025-24201** – in which maliciously crafted web content may be able to break out of Web Content sandbox. **Google released the Android Security Bulletin** addressing 43 security vulnerabilities – including two critical zero-day vulnerabilities.

III. Apps Introduce Risk – Even in Secure Platforms

Since it made its debut, Apple's App Store and the Google Play store have protected users and organizations alike. Apple users enjoy safeguards when downloading and using an app from the App Store because Apple "**scans each app for malware and other software that may impact user safety, security, and privacy**". For Android users, the Google Play Store has Google Play Protect. But that does not stop threat actors. **Over the past five years, Apple** prevented over $9 billion in potentially fraudulent transactions. The **European Union's Digital Markets Act** (DMA) allows for alternative app marketplaces to be established and requires 'gatekeepers' to open their walled gardens. Apps distributed through alternative app stores do not go through the same guidelines as Apple's App Store apps – potentially introducing risk to user security, privacy and safety. Social engineering (e.g., phishing), ransomware, consumer spyware and more are documented as risks can be introduced to users downloading apps or using alternative payment systems outside of the Apple App Store.

For Android devices, earlier this year, **Google warned about a new trojan** that was discovered "attacking more than 750 legitimate banking and shopping apps." Now, the two most common app stores were forced allow users to sideload apps in the EU, opening the attack surface for threat actors.

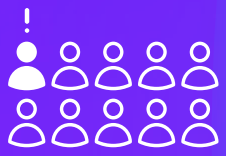
IV. Targeted Attacks put mobile devices at risk

Mobile devices provide the flexibility to work where we want or need; often, high-profile users use mobile devices to conduct business around the globe. **But high-profile users are often the most targeted group of individuals** because of the data their devices hold – intellectual property, financial data and more. Attackers look at well-connected, high-profile individuals at the best return on their blackmail schemes.

Over the past twelve months, we found:

25%

of organizations were impacted by a social engineering attack



1 in 10

users clicked on a malicious phishing link

I. Mobile phishing

Phishing is one of the most common and damaging threats facing organizations today. According to the Cybersecurity & Infrastructure Security Agency, "More than 90% of successful cyber-attacks **start with a phishing email.**"

Phishing comes from a variety of channels on mobile devices. It is no longer only email, but attacks happen via text messages (called smishing), social media or links to phony websites.

But why is phishing so much more successful on mobile devices?

First, it's important to understand that **over 62% of web page views worldwide** come from mobile devices. This means mobile devices make up a larger portion of internet traffic, giving threat actors a bigger pool of potential targets to probe for vulnerabilities.

Conversely, mobile devices are compact devices with smaller screens. It is part of their popularity – their size allows users to take them anywhere. It also allows organizations to implement workflows that involve mobile devices like in:

- Retail (point-of-sale or inventory)
- Healthcare (nursing rounds or patient bedside)
- Manufacturing (operator/machinery instructions)
- Aviation (electronic flight bags or below wing devices)

But these advantages are what make it possible for users to be distracted when it comes to malicious phishing attacks. The perception that mobile devices are inherently secure lives on, but as we have documented, it only takes one link for a device to be compromised.

Top 20 brands used in phishing campaigns

Mobile devices allow organizations to implement new workflows, streamline how to connect with customers and improve the user experience. Using a mobile device is how many of us work today – whether it's a companion device or the main point of entry. Mobile connects us to our life – both at work and at home. Attackers know this fact and use it for their nefarious activities.

In our research, we found that certain popular brands are used as part of social engineering attacks to exploit end users on mobile devices. We broke these brands down into **four categories** that are most used to exploit end user trust:

The myriad of reasons for mobile device use – accessing work emails, ordering a household item, conducting personal banking – has threat actors exploiting these common, often needed, use-cases to gain access to data. In the table below, we show the top twenty brands that were used in social engineering, based on those four categories.

1.	2.	3.	4.
Entertainment	**Business**	**Utilities**	**Personal**
Netflix	Outlook	United States Postal Service	Amazon.com Inc
Bet365	Office365	Gazprom	Telegram
Steam	Allegro	AT&T Inc	Facebook, Inc
	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

Because of their popularity, prestige and influence on both businesses and individuals, these brands are frequently exploited by threat actors in social engineering attacks. Their trusted reputation makes users more likely to engage with malicious content disguised as legitimate communication.

While this list highlights the top 20 brands targeted over the past year, it's far from exhaustive. Attackers constantly adapt, and the brands they mimic can shift at any time. Ultimately, this underscores how attackers use the trust these brands have built over the years to deceive and exploit users.

In the modern world, our personal information is constantly at risk. With more mobile devices being used for personal and work purposes, the attacker's reach continues to expand. Attackers are employing more sophisticated tactics, using realistic interfaces, user experiences and authentic communication styles to lure unsuspecting victims into their trap. But there are safeguards (e.g., continuous employee training and threat prevention tools) organizations can employ to protect their users and data.

Jamf identified approximately **10 million phishing attacks** over the **12-month period** that impacted our sample group of **1.4 million devices**.

Additionally, we found that **1.5-2%** of these attacks were regularly being classified as **zero day**, meaning the attackers were using brand new, never-before-seen destinations to trick users into clicking on malicious links.

Identifying and verifying zero-day phishing attacks helps organizations protect users from falling victim to brand new and undetected phishing sites.

A CISO's Perspective

- **Introduce a robust training program:** This has been integral to our success. We run sophisticated phishing campaigns, run gamified training, offer one off trainings for users that request it and allow users to report phishing emails while seamlessly receiving confirmation and feedback on their submissions all throughout the year. This is not just a once a year and "done" training for us.
- **Keep up with new trends and tactics:** This may seem obvious, but attackers will always capitalize on anything that they can and oftentimes that includes something new, groundbreaking or controversial in the news. You need to adapt your training and blocking tactics to address those situations. This may cause some unease amongst users, but transparency is key. The training is to prepare them for a potential bad actor that will not take their feelings into consideration when causing harm and will often actually look to garner an emotional response to confuse and outwit a victim.
- **Have a layered approach:** There is no one-stop-shop or tool to prevent you from becoming a victim of a targeted phishing campaign. Make sure you are covered from multiple angles. Block malicious domains. Ensure you have MFA in place. Adopt a zero-trust methodology. Have impossible velocity rules enabled. One or two of those things may not be enough, but enforcing multiple layers of security ensures the most viable way to avoid becoming another victim of a phishing attack.

II. Vulnerability management

Vulnerabilities occur when there is a weakness or flaw in a system, application or protocol that can be exploited by attackers to compromise its security, integrity and/or availability. **Apple** and **Google** provide a list of known vulnerabilities which affected their operating systems. What this means, however, is that these vulnerabilities are "out in the world" before Apple or Google provide an update and security patch. From January 1st, 2024 – April 1st, 2025, Apple documented **29 security updates** with CVEs associated for major and minor versions of iOS. And in that same time period, Android documented **39 system vulnerabilities** with an associated CVEs on the Android Security Bulletin.

Apple (via **Rapid Security Responses**) and Google (via **Android Security Patches**) issue standalone security patches between software updates. Why are these patches beneficial? They are timely updates – meaning organizations can automatically apply updates without having to wait for larger updates.

Modern **cyber threats** are creative and complex, and consumers and businesses alike must be vigilant about updating devices. It is not just updating the device but verifying that the **update** is **authentic**.

Jamf Threate Labs recently dove into a specific method used during an attack sequence – maintaining persistence. Their research showed how "adversaries could exploit the iOS settings interface and tamper with the system update settings, complete with prompts and notifications that indicate an available update of iOS."

Let's take a deeper look at some noteworthy vulnerabilities from recent Apple releases: (this report was written in April, 2025)

Apple CVE Fix	Date	Vulnerability scoring	Impact
iOS 18.4.1 and iPadOS 18.4.1	April, 2025	CVE-2025-31200 CVSS – Score: 7.5 | Severity: High	CoreAudio
iOS 18.4 and iPadOS 18.4	April, 2025	CVE-2025-30430 CVSS – Score: 9.8 | Severity: Critical	Authentication Services
iOS 18.3 and iPadOS 18.3	January, 2025	CVE-2025-24085 CVSS – Score: 7.8 | Severity: High	CoreMedia
iOS 18.3 and iPadOS 18.3	January, 2025	CVE-2025-24154 CVSS – Score: 9.1 | Severity: Critical	WebContentFilter

Updated AOSP* versions	Date	Vulnerability scoring	Impact
13, 14, 15	April, 2025	CVE-2025-26416 Severity: Critical	Escalation of Privileges
15	March, 2025	CVE-2025-22403 Severity: Critical	Remote Code Execution
15	February, 2025	CVE-2025-0096 Severity: High	Escalation of Privileges
12, 12L, 13, 14, 15	January, 2025	CVE-2024-43771 Severity: Critical	Remote Code Execution

*Android Open Source Project

The vulnerabilities – all recorded on Apple's and Android website – show us that when building software, vulnerabilities will happen. What is important for security professionals is being able to view and action on those vulnerabilities to keep your data safe.

One of the best ways to do that is with up-to-date operating systems – and the tools to deploy those updates.

Maintain good security posture with up-to-date operating systems

The best way for businesses to mitigate vulnerabilities and to keep their organization compliant is by updating the operating system of their devices. As shown in the previous page, both Apple and Android routinely provide updates to OSes with known vulnerabilities.

A common way for organizations to update the OS (and the business apps their employees use daily) is via a mobile device management (MDM) solution. MDM also provides in-depth inventory reporting for the OS each managed device has installed. But often, organizations have many devices used for diverse use cases, running different apps for different users. It's difficult (and often not feasible – for example, testing apps before deploying) to have every device in a fleet on the most current operating system.

Over the last twelve months:

32%

of organizations operate at least one device with critical (and patchable) vulnerabilities

55.1%

of mobile devices used at work run a vulnerable OS

Organizations were found to run mobile devices without the latest security patches. In our data, we found that **4.8%** of all Android devices with vulnerabilities were used to access company resources.

Mobility lets us work how we want. From taking business calls in the car, to expanding workflows for frontline and customer facing employees, mobile devices unlock what is possible at work. But, like any computing device, the system is vulnerable to threat actors. Organizations can take steps to mitigate threats across their mobile devices through tools that balance usability and security, employee training and understanding the most common threats today.

A CISO's Perspective

- **Ensure visibility into the vulnerabilities across your organization:**
  Gaining as much insight into what vulnerabilities are present on your end user devices, or infrastructure, is a great starting point. You can start with that data to analyze specific app footprint, potential risks, impact radius, etc. This is a great way to start prioritizing your vulnerabilities in a data driven way.
- **Introduce a solid patching program:**
  To bring back the MDM point, having a tool to ensure that you can keep up with the latest or supported N -X versions of software or OS is paramount to keeping a healthy and safe environment. Doing this with little to no impact to end-users just makes it easier to partner and enable the business with.
- **Implement a risk-based entry approach:**
  If you have non-compliant devices attempting to access your companies' resources, you should restrict that access until the end user can correct the situation and bring that device back to compliance with as little effort as possible.

III. App risk

Late November 2024, the Cybersecurity Agency published **a report on the top routinely exploited vulnerabilities in 2023**. (This is the latest version of the report.) The report digs deeper into the top 15 vulnerabilities – including details on what the vulnerability enables attackers to accomplish. The vulnerabilities occur in operating systems across computing platforms, to applications organization's employees and students use daily. As the report mentions, "Malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks in 2023 compared to 2022, allowing them to conduct operations against high priority targets." The Cybersecurity Agency goes on to provide what developers and end user organizations can do to mitigate vulnerabilities. For end user organizations, the report mentions:

- Update software, OS, apps, and firmware *in a timely manner*
- Routinely perform automated asset discovery
- Implement a robust patch management process
- Document secure baseline configurations
- Perform regular secure system backups
- Maintain an updated cybersecurity incident response plan

What makes an app 'risky'? Some of the key attributes of risky apps include:

- Anomalous characteristics
- Malicious code patterns
- Dangerous permissions
- Risky dynamic behavior
- Suspicious developer profile

Gaining visibility into app versions, any leaky apps and more helps organizations stay ahead – ready to investigate and remediate the risk immediately.

It is important for businesses to understand the full health of their applications. Some of the key data points organizations should pay attention to identify and remediate risky apps are:

- Number of users with an outdated app installed
- Number of users with a specific app version
- List of apps with broken encryption implementations, thus causing sensitive data to leak onto unprotected networks
- Apps that request certain permissions to gain access to data on other parts of the device

An in-depth look at a real-world vulnerability
Bypassing Transparency, Consent and Control (TCC)

Across Apple's operating systems, TCC serves as a crucial security framework, prompting users to grant or deny requests from individual apps to access sensitive data such as photos, contacts and location details. A TCC bypass vulnerability occurs when this control fails, allowing an application to access private information without the user's consent or knowledge. What this means is that attackers can get unauthorized access to files and folders, health data, the microphone or camera and more without alerting users.

Jamf Threat Labs uncovered CVE-2024-44131, a TCC bypass vulnerability affecting File Provider on iOS devices. Apple quickly responded to this discovery with a patch in iOS 18.0. CVEs, like CVE-2024-44131, are important reminders of the necessity of keeping organizational devices up to date.

App Store Protections & Fraud Attempts

Mentioned earlier in this report, in the last five years, Apple prevented over $9 billion worth of fraudulent transactions. In 2024 alone, the company blocked more than $2 billion in fraudulent transactions. To go further, in 2024 Apple:

- Terminated more than 146,000 developer accounts over fraud concerns
- Rejected an additional 139,000 developer enrollments
- Rejected over 43,000 app submissions for containing hidden or undocumented features
- Rejected over 320,000 submissions that copied other apps, were found to be spam, or otherwise misled users..
- Detected and blocked over 10,000 illegitimate apps on pirate storefronts

The App Store is generally considered the most secure, user friendly and private way to download apps. The App Store for iOS uses sandboxing, permission requests from the user and only allows signed code to run on the device. But as the data shows, bad actors and potential fraud persists. Apple's commitment to keeping the App Store a safe, trusted place for applications has protected users and developers since its launch in 2008. However, 'sideloaded apps' – apps from third-party app stores, like AltStore – do not enjoy those same protections.

A CISO's Perspective

Effective mobile security requires a layered approach. Using the latest hardware from a trusted vendor and the most current operating system is still not enough to protect your organization and your most sensitive assets from compromise. Good security practices must extend to each layer of your tech stack, and that includes applications as well.

- **Introduce an app vetting program for your organization's sensitive mobile apps:** Start with the most critical apps and routinely check that the latest, secure versions are running across the organization. As you scale the program, vet every application that goes into your enterprise app store.
- **Develop policies that label devices as "out of compliance"** when unwanted applications are installed; prevent these at-risk devices from accessing your SaaS applications, critical data centers, or remote workloads until the risky apps are updated or removed.
- **Introduce mobile app security into training programs** so users can become part of the solution by implementing updates when necessary on devices that stay with them throughout the work day or work week.
- **If your organization does not require alternative app marketplaces**, establish policies to prevent alternative stores from being accessed on work devices. Additionally, prevent sideloaded apps to ensure only those from official sources are used on the device.

The Jamf Threat Labs team published a demonstration of how a sideloaded social media app can monitor photos and upload them to an attacker's server. This application was 'modified, yet perfectly functional'. The team provides some clear safeguards to enhance security, namely:

- Enable and regularly review the App Privacy Report
- Be selective with app permissions
- Avoid storing sensitive information

Only download apps from trusted sources (like the App Store)

Both native applications and cloud-hosted web applications are susceptive to risk. Cloud-hosted applications are more exposed to risks because of the larger attack surface. However, with the right visibility, control, and remediation capabilities, organizations can mitigate risky applications at work.

IV. Targeted attacks and sophisticated spyware

Since 2021, **Apple has sent** threat notifications to users in over 150 countries. These notifications inform and assist users, usually high-profile individuals like journalists, politicians, or diplomats, who are targeted by mercenary spyware attacks. And in late April 2025, Apple, "sent notifications this week to several people who the company believes were targeted with government spyware." But it is not only Apple. These attacks target all types of operating systems and apps. **According to The Citizen Lab,** "spyware had been loaded into WhatsApp, as well as other apps on their [Android] devices."

Malware and spyware, like the ones Apple sends threat notifications about, are some of the most advanced threats organizations and individuals face today. But there are protections to keep all users – at any level of your organization – safe from these advanced threats.

Apple offers guidance for all users on how to protect themselves from malware, many of which we've already covered in this paper. Specifically, Apple advises users to:

- Update devices to the latest software, as that includes the latest security fixes
- Protect devices with a passcode
- Use two-factor authentication and a strong password for your Apple Account
- Install apps from the App Store
- Use strong and unique passwords online
- Don't click on links or attachments from unknown senders

Jamf Threat Labs: Compromising a device without the victim's knowledge

Jamf Threat Labs demonstrated a device – without protective security software – being compromised without the victim's knowledge. The demo showed how an attacker can gain access to email, corporate messaging, two-factor authentication, and more personal data. The team then goes on to show how organizations can protect organizational and personal data:

1. Enforce secure configurations to maintain compliance on both company-owned and BYO devices
2. Enable threat prevention and monitoring with targeting actions, preserving end user privacy
3. Enforce device encryption across all managed devices

A CISO's Perspective

Malware is not as pervasive on mobile as it is on other primary compute devices. However, when it is discovered, it is often found to use very advanced techniques and used to target individuals.

- **Do not become complacent** and assume that mobile malware will never impact your organization. Apple sent notices of spyware compromise to users in approximately 100 countries just last year.
- **At a minimum, appoint a mobile security leader** and task them with providing regular reports on the health of your organization's mobile deployment. Catalog incidents of stolen phones, targeted phishing, performance drops, and anything else that captures irregular behavior. Ideally, establish a telemetry stream from your device management and security tools, and incorporate that data into your security operations center. Treat mobile like every other endpoint.
- **Where possible, gather mobile system data and look for evidence of zero-day attacks.** This will require expertise that could be in-house or contracted. For enterprise organizations with dedicated security analysts, invest in developing a mobile forensics expertise within your teams.

Key takeaways

Mobile phishing is one of the most common way for attackers to gain access to sensitive information. Organizations that can implement a training program, keep up with trends and tactics (including adapting training), and having a layered approach to security provide organizations protection from different angles.

Vulnerabilities occur in software of all types. Establishing proper security hygiene mitigates risks that vulnerabilities can introduce. Regularly updating operating systems and disabling unnecessary controls (e.g., third-party app stores) helps organizations stay compliant with internal baselines and external frameworks.

Improper app management and app use brings risk. It is not always the app itself, but also apps that are making malicious network connections. By establishing an enterprise app store and continually vetting applications (especially for private and custom apps), organizations can better monitor, remediate and patch vulnerable applications.

APTs and spyware attacks are becoming more common. These threats (often originating from nation-states or specialty groups) affect organizations around the globe – often targeting high-profile individuals with sensitive data on their device. By providing a defense-in-depth security strategy, and treating mobile like every other device, organizations can ensure protective measures of their mobile device ecosystem and data devices connect to.

Establish and maintain Acceptable Use Policies for corporate owned devices that require enforceable acceptable use policies, connect to work resources or must comply with organizational policies. On BYO devices, those devices will require additional privacy controls, like the **privacy protections Apple provides** for devices.

jamf

Contact us to learn more about the mobile threat landscape.