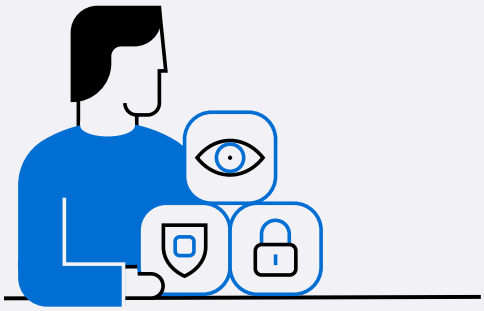


Complying with the Digital Markets Act

Apple's Efforts to Protect User Security and Privacy in the European Union

March 2024

Contents

Apple's Goal Is to Protect Users

At Apple, our highest priority is to make great products that enrich our users' lives around the world. We make products that we want to use ourselves, and that we want our family and closest friends to love as much as we do. We are constantly focused on providing our users with a high-quality and safe experience through the seamless integration of hardware, software, and services. And we know that a big reason why customers choose Apple—and iPhone—is because they believe that we are delivering on that vision.[1]

When Apple introduced iPhone in 2007, it defined the era of mobile computing. And it inspired new products—including nearly two million apps from third-party developers that have become essential to people's daily lives, creating an entirely new app economy responsible for millions of jobs and facilitating trillions of euros in commerce worldwide.[2]

Unfortunately, we also live in a world where security and privacy attacks present evolving and increasingly sophisticated threats to everyone. Bad actors create malicious apps that can alter your data, hold it hostage for ransom, or leak it to the entire web. They can engage in deceptive or fraudulent activity, seek to snoop and spy on you without you knowing it, or compromise the very functionality of your device itself. They can build sham websites designed to trick you into giving away sensitive data, convince you to download dangerous software, or even attack your web browser. They can send phishing emails to convince you to hand over your passwords. Cybercriminals can also attempt to steal your information by accessing your device without your knowledge or consent, using Bluetooth accessories and open network connections—or just getting physical access to your device. Other bad actors can even try to hack your information and messages while they're in digital transit to and from your device. These bad actors have posed, and will continue to pose, threats to everyone no matter where they live.

We built iPhone to protect users against these kinds of risks, combining hardware, software, and services designed to work together for maximum security and a transparent user experience in service of the ultimate goal of keeping personal information safe. This is one important reason why third-party apps have been able to achieve incredible success on iPhone—because, despite all of these well-known and ever-present risks, users trust Apple's commitment to protect them. **These are some of Apple's most important standards:**

SECURITY

Users trust their iPhones with their most sensitive data. We build industry-leading security protections to help prevent anyone but the user from accessing the data on their iPhone. And we believe it's critical for users to have a trusted place where they can safely download and discover software—free from malware, cybercriminals, and scammers.

PRIVACY

At Apple, we believe privacy is a fundamental human right and we design our products and services with innovative technologies and techniques to protect our users' privacy. Users should not be exposed to software or websites that collect, use, or share their information without their informed permission. We build our products and services to give users control over their data and help protect them against the collection, use, or sharing of their information without their permission, and to make sure users know what data of theirs is being shared and how it is used, and that they can exercise control over it.

SAFETY

Users should not be exposed to physical harm through iOS, including through apps that advocate for or cause harm.

These values are fundamental to who we are, to what iPhone users expect from us, and to the integrity of our platform.

We are grateful that users in more than 175 countries and regions around the world have embraced iPhone, and Apple is deeply committed to upholding these core values in every single one of those places. That means finding a way to protect and preserve user security, privacy, and safety while following the law in every country where we do business.

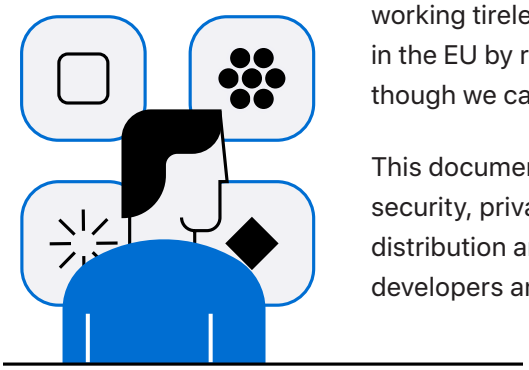
Starting this year, the European Union's new Digital Markets Act (DMA) requires us to take a new approach in our work to serve our EU users.

To comply with the DMA, we have created new options for developers and users—and built **over 600 new APIs and developer tools to enable these changes**. The new options include enabling **sideloading** so that EU users can download apps through app marketplaces other than the App Store, enabling **alternative ways to process payments** on the App Store, and **many other changes**.[3] This required us to change the uniquely successful approach that we've employed to protect users' security and privacy and keep them safe.

Since we launched iPhone in 2007, we have taken the same approach to protecting our users everywhere in the world, encompassing many wide-ranging and industry-leading protections against countless threat vectors. On the App Store specifically, starting with its inception in 2008, we wanted to create a safe and trusted place for users to discover apps and a means of providing a secure and supportive way for developers to develop, test, and distribute apps to users globally—and over the years, we have further empowered developers with more than 40 software development kits (SDKs), 250,000 application programming interfaces (APIs), and many other advanced tools.

By requiring that all apps on iPhone be distributed through a single trusted source, the App Store, we were able to accomplish our goal of protecting users more effectively than any other platform. While our efforts to protect users and developers alike are never complete, iOS has never allowed a widespread consumer malware attack on users—which is exceptional for a 17-year-old, modern computing platform.

The new options we're introducing to comply with the DMA necessarily mean we will not be able to protect users in the same way. To keep offering users the most secure, most privacy-protecting, and safest platform—in line with what users expect from Apple—we've designed and implemented new safeguards that will help to protect and inform them. While the changes the DMA requires will inevitably cause a gap between the protections that Apple users outside of the EU can rely on and the protections available to users in the EU moving forward, we are working tirelessly to make sure iPhone remains the safest of any phones available in the EU by reducing the risks introduced by these necessary changes—even though we cannot entirely eliminate such risks.



This document highlights key steps we're taking on three important fronts—user security, privacy, and safety—to address the changes the DMA requires to app distribution and payments, and what we expect those changes will accomplish for developers and users in the EU.

Apple's Safeguards for App Distribution and Alternative Payments Aim to Protect User Security and Privacy and Keep Users Safe

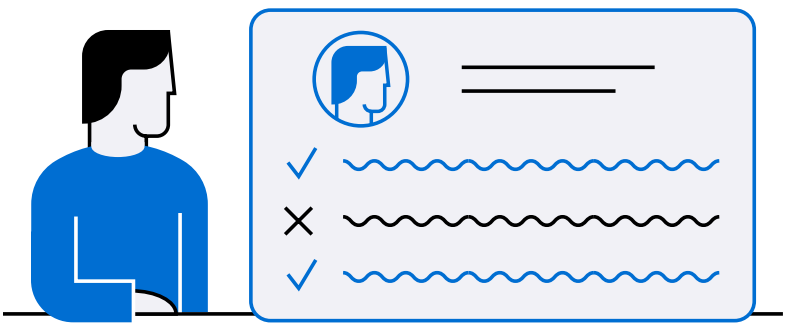
We are introducing and expanding a number of features that will support user security, privacy, and safety while allowing sideloading and alternative ways to process payments on the App Store in the EU. Apple has developed and deployed safeguards aimed at ensuring that we continue to provide the best, most secure experience possible for users in the EU—even if it won't be as secure, privacy-protecting, or safe as in the rest of the world.

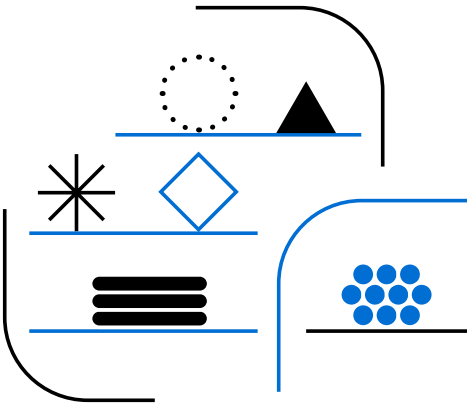
Identifying and Stopping Malicious Apps

To help protect our EU users in the new landscape created by the DMA, **Apple is launching Notarization for iOS—a baseline review of all apps (whether they are distributed through the App Store or an alternative app marketplace) that reflects the new app distribution landscape and is focused on platform integrity and protecting users.**

Apple will electronically sign each app that is distributed on iOS in the EU, no matter how it is distributed—and this signature will be required for any app on iOS. Before signing any app, Apple will analyze each one (using a combination of ***automated tools*** and ***human review***) to check that it is free of known malware and other security threats, generally functions as advertised, and doesn't expose users to egregious fraud. By doing these checks on the front end, we can help prevent cyberattacks and other threats *before* they spread across other users. This process is an extension of Notarization for macOS; for years, Apple has been scanning and signing software distributed on macOS to ensure that it is free of known malware. This has worked well—so we have adapted it for iOS, including new enhancements to meet the unique needs of the most trusted mobile computing platform in the world.

To be sure, Notarization won't cover everything—as discussed further below—like app content, business practices, and other App Store protections for users.





The protections we have put into place begin at the very first step that an app developer must take to distribute an app on iOS in the EU.

App Development

No matter how a developer distributes an app on iPhone, they must sign up for Apple's Developer Program before building an app for iOS (whether in the EU or anywhere else). As part of the enrollment process, Apple requires developers to verify their identity by requiring a legal name, phone number, and address (or, for an organization, other specific identifiers). In some cases, a developer may be asked for their government identification number or to otherwise prove their identity. This initial safeguard is an important anti-fraud measure, allowing developers to be identified and held accountable for what they distribute—Apple prevented nearly 105,000 fraudulent developer accounts from being created in 2022 due to suspected fraudulent activities.[4]

When developers sign up for the Program, **they agree to our Developer Program License Agreement**. This allows Apple to establish basic rules of the road that developers must follow in order to distribute their apps on Apple's devices. Developers agree not to engage in fraud, to abide by applicable laws and regulations, and to refrain from designing or marketing their apps for the purpose of harassing, abusing, spamming, stalking, threatening, or otherwise violating the legal rights of others. If a developer violates the agreement, we can—and do—terminate their agreement. In 2022, Apple terminated more than 400,000 developer accounts for fraud.[5]

In addition, Apple provides **tools to developers** that protect against certain risks that could emerge during the development stage, prior to submission. For example, we have implemented SDK package signing to help developers verify the source of third-party code. This helps to protect developers from inadvertently using code that has been maliciously modified as they build their apps.

Submission

Notarization begins when a developer submits their app binary to Apple. When they do so, the developer will indicate which app marketplaces they plan to distribute the app on, including—if desired—the App Store.

Review

During **Notarization**, Apple conducts both ***automated*** and ***human review*** in an effort to prevent apps that threaten platform integrity—including threats to user security, privacy, and safety—from reaching the user.

The **automated review** uses machine learning, heuristics, and years of accumulated data to help identify problematic apps, scanning the app's binary for instances of known malware or other security threats.

The **human-led review** serves as a critical line of defense to help protect users from bad actors. Our human reviewers analyze each app, and specialists will reject apps that violate the Notarization Guidelines. The team also launches and runs each app on an isolated platform to test whether it works as described and appears to be safe for users. Because automated review relies on past threats, complementing it with human review is essential as we try to detect emerging and novel threats. As cybercriminals become increasingly creative and sophisticated, the human element of our process allows Apple to stay on top of evolving threats. And human review is also essential to our effort to stop apps that pose non-software-based threats, such as egregious frauds, from getting onto iPhone. Human review is particularly important in identifying bad actors attempting to use social engineering techniques to manipulate users into granting them access to their device and information by pretending to be something they are not. Humans can check if a malicious app is attempting to trick a user, such as by posing as a different app or attempting to deceive a user into giving access to their sensitive data, and check for other malicious techniques a machine can't find.

We will apply these same checks to **all app updates**, with the aim of stopping bad actors from sneaking malware or other dangerous features into each app after the initial download.

To be clear: the automated and human-led review processes that together make up Notarization are not App Review. They analyze submissions for compliance with only a subset of the App Store Review Guidelines—and they do ***not*** include many of the most substantial App Store Review Guidelines. Notarization ***will*** encompass checks necessary to protect our users and essential to ***platform integrity***, including those that specifically aim to protect user security, privacy, and safety.

- **Security:** Notarization checks apps for security threats to the device. For example, Notarization works to ensure apps do not contain known malware. We also will not allow apps that attempt to read or write outside their designated

Review

container area, which would allow those apps to manipulate other apps or access unauthorized data from the user's device.

Tricking users into downloading an app under false pretenses—whether because the user thinks it is a different existing app or because the app that is downloaded is different from what the app ***becomes***—is a key method that bad actors use to transmit malware or other viruses onto a device without the user's knowledge, or to threaten device security in other ways. To prevent this, in Notarization, we will also look at whether apps include false information about their features or capabilities; impersonate other apps; or have hidden, dormant, or undocumented features. We will also examine whether apps can download resources that will introduce or alter functionalities post-download.

- **Privacy:** Notarization will seek to prevent threats to user privacy by ensuring that each app properly supports—and does not attempt to circumvent—the privacy features that are built into and essential to the integrity of all Apple devices. To protect user privacy and provide transparency to users into how their data will be used, Apple uses technical measures to prevent apps from accessing users' sensitive information. iOS only allows apps to access this kind of data after they have obtained consent from the user—which the user can revoke at any time. This applies to data and services such as:

  - the microphone
  - the camera
  - Face ID
  - saved passwords
  - location data as provided by Location Services
  - health data
  - the unique device identifier used by advertisers (IDFA)
  - Bluetooth
  - Wallet
  - Contacts
  - Photos
  - Home app data
  - Calendar
  - Game Center friends list
  - Reminders
  - Apple Music library

Notarization will check that apps requesting these permissions are clear and concise as to why the access is needed, so the user can make an informed choice about what permissions to grant—and remain in the driver's seat when it comes to their own data.

Location Services allows apps and websites to use information from cellular, Wi-Fi, GPS, and Bluetooth networks to determine a user's location with a high degree of accuracy and precision.

Under our **App Tracking Transparency** framework, users must consent before a developer can access their unique device identifier used by advertisers (IDFA) to track them across websites or other apps for the purposes of advertising or sharing with data brokers.

Notarization will also evaluate whether apps are handling user data in ways that users expect. For instance, Notarization will seek to ensure that apps obtain user consent for data collection and sharing, and do not attempt to manipulate, trick, or force users to consent to an app's access to their data; it will also examine if apps provide a privacy policy so that users can understand how their data is being collected, used, and sold. Because of the sensitivity of personal health data, we are also requiring that apps do not use or disclose data gathered in the health, fitness, and medical research context for advertising, marketing, or other use-based data mining purposes.

- **Safety:** To pass Notarization, apps should not risk users' physical harm or damage to their devices. For instance, we will prohibit apps that urge customers to participate in activities or use their devices in a way that risk physical harm to others. Notarization will also look for apps that would imperil the functionality of the device, including by rapidly draining an iPhone's battery, generating excessive heat, or unnecessarily straining device resources—all of which could render an iPhone non-functional in an emergency situation.

Notarization Review Guidelines will not include the content and commerce policies in the App Store Review Guidelines, and so will not prohibit or check if apps go against those policies. This means Apple won't be able to prevent apps with content that Apple wouldn't allow on the App Store—like apps that distribute pornography, apps that encourage consumption of tobacco or vape products, illegal drugs, or excessive amounts of alcohol, or apps that contain pirated content (or that otherwise steal ideas or intellectual property from other developers)—from becoming available on alternative app marketplaces. Only apps that opt into being distributed on the App Store will go through the standard App Review process, on top of Notarization, which includes enforcement of these App Store–only policies.

Once an app has passed these reviews, we notarize it—giving the developer the **signature** required for them to distribute that app on iOS. In an effort to ensure that nothing changes between Apple signing the app and the time a user actually installs the app on their iPhone, notarized apps will also undergo a series of basic checks during installation. This will help ensure that the app has not been tampered with since it was notarized and that the installation was initiated through an authorized source.

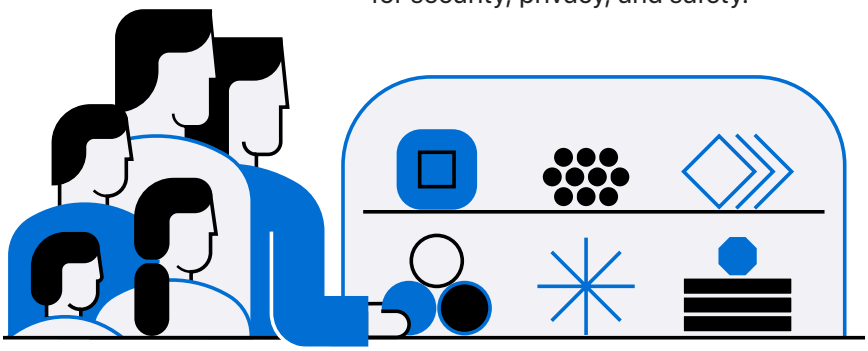
Installation

While we know Notarization will be an important tool in our work to protect users from threats to their security, privacy, and safety—serving as an early line of defense against potential threats and malignant features—we also know that it has limitations. To establish ongoing safeguards for our users even after apps are installed, we have also created **baseline criteria for alternative app marketplaces to help ensure that they have at least the minimum capabilities needed to carry out the important responsibility of protecting users on an *ongoing* basis**. These include:

- ***Committing to ongoing monitoring to detect and remove malicious apps.*** This monitoring is necessary to catch apps that are not blocked during Notarization or that change after Notarization. Our experience has shown us that ongoing monitoring for new threats that can emerge after initial review is imperative to protect users' safety, security, and privacy. We've also found that monitoring requires marketplace-specific signals like user reviews, customer feedback, and analysis of marketplace data; Apple will not have access to these signals outside the App Store. Without each alternative app marketplace conducting ongoing monitoring, user security, privacy, and safety will be seriously compromised.

- ***Guaranteeing alternative app marketplaces have the ability to protect users.*** Operating an app marketplace that facilitates the distribution of third-party apps without significantly endangering security, safety, and privacy is not easy.[6] App marketplaces need resources in order to carry out these important responsibilities, such as the ongoing monitoring for malicious apps. Marketplaces also need to be able to provide ongoing support to users and developers so that developers can run their businesses and users can rely on apps downloaded through alternative app marketplaces to perform as they expect—and get help when they do not. A marketplace that lacks the resources needed to protect users or that leaves users and developers without recourse when a need arises would compromise iPhone.

These requirements are the minimum of what is necessary for an app marketplace to keep users' data secure and private and users safe. They do not encompass the whole of the effort Apple has invested in operating the App Store's high standards for security, privacy, and safety.

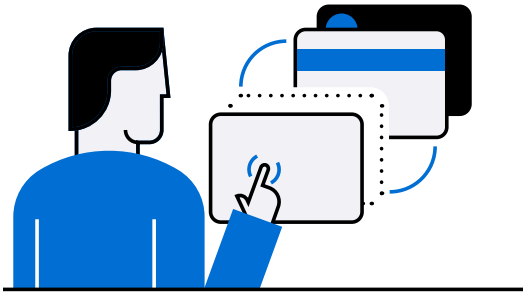


We have also created app installation sheets that empower users to make educated choices about the apps they download. Users choose Apple products in part because of the transparency and control we provide them, which enables them to make educated decisions about what they want on their devices. These new app installation sheets are an essential way that we will continue our commitment to the transparency that users expect from us.

The sheets display information reviewed during Notarization, such as the app name, developer name, app description, screenshots, and system age rating, and identify the marketplace a user is downloading the app from, all in a clear, standardized form. Developers will not be able to change the content of this sheet after their apps are notarized without going through the process again.

To enable all the changes required by the DMA, Apple created over 600 new APIs and developer tools. We built data security and privacy and user safety into these APIs. For example, MarketplaceKit, the framework that allows alternative app marketplaces to operate on iOS, facilitates the *secure* installation of apps distributed from alternative marketplaces: when users download an app through an alternative app marketplace, our API enables the marketplace's web server to directly interface with iOS—providing authentication services, app licenses, and app data to create a secure experience. These APIs are also designed to ensure that app installs from a marketplace occur as the result of the user's interaction with the marketplace—that is, the user affirmatively choosing to download the app—and not through a bug or automated download. And these APIs also enable easy updates to the app, incentivizing developers to keep apps up-to-date.

Apple has also created other new APIs that protect users—like AdAttributionKit, which enables privacy-protective advertising, allowing advertisers and developers to obtain advertising data metrics without tracking individual users or devices across apps owned by other companies. These new tools will help make sure the changes we've made to comply with the DMA work as seamlessly as possible—while keeping users as safe as possible at the same time.



Providing users with a quick-glance summary of this information will let users know what app they are downloading and what the app looked like when it went through Notarization, even if other marketplaces don't have standardized requirements for app disclosures or the app has changed its presentation after Notarization. The disclosures will make it easy for users to choose what apps they want to engage with. A user can also make the choice to turn off the sheets for any marketplace. The sheets will automatically disappear if a user sets the marketplace as their default, as the user has then made the choice to prefer that marketplace.

Letting Users Know About Payments Risks

To support the changes we've announced to comply with the DMA, we are also introducing the ability for developers in the App Store to use alternative payment options to complete transactions for digital goods and services within their apps in the EU. This opens up new options for developers, but it also means users of those apps will not have the same protections and benefits they have come to rely on through Apple's private and secure commerce system, including In-App Purchase (IAP)—such as easy subscription cancellation, a centralized purchase history page, parental controls like Ask to Buy, or protections from predatory tactics like those that aim to trick users into paying a different amount for a digital good than advertised. The burden will fall on users to figure out for themselves, on an app-by-app basis, what benefits and protections might be available to them—and who they should contact for help when transactions go wrong, as AppleCare agents will have limited (if any) ability to assist them.

As always, Apple is guided by the values of transparency and keeping users informed. Therefore, **we are letting users know that Apple's protections will not be available so that the user has the knowledge needed to decide whether to complete the transaction**. Before a user downloads an app, the App Store will display an informational banner on the app's product page to inform the user that the developer is using an alternative payment solution, not Apple's secure commerce system. And before a user makes a transaction outside of Apple's commerce system, they will see an in-app disclosure sheet that lets them know they are no longer transacting with Apple. This information will help ensure users know they should be on alert for developers that employ misleading payment information, predatory pricing, and missing subscription disclosures.

Security, Privacy, and Safety by Design

Importantly, Apple's system architecture and design continues to protect user security, privacy, and safety. Apple designed security into the core of its platforms through its powerful and multi-layered security protection. This design means that even if iPhone in the EU is not as secure as it is in the rest of the world, we believe it remains the most secure option in the EU. At a base level, key security features, such as hardware-based device encryption, cannot be disabled. Apple also provides layers of protection that provide a stable, secure platform for apps. For example, all apps are **sandboxed**, so they are restricted from accessing files stored by other apps or from making changes to the device. System files and resources are also shielded from the user's apps. If an app needs to access information other than its own, it only does so through services explicitly provided by iOS. This means one app generally cannot affect other apps or the iOS system, reducing the risk of malware affecting other parts of the platform. Apple also incorporates **code signing**, which means that all code in third-party apps is linked to the developer whose real-world identity has been verified when they enrolled in the Developer Program. At launch, iOS ensures that the code in the app is what the developer signed when it submitted the app.

Apple has also designed iOS around **privacy**. For instance, iOS requires that users choose whether apps have access to their Location Services data at all—and if they do, whether the app can access the user's precise location or only a general approximation of their location. Apps cannot access iPhone's microphone or camera without a user's permission—and when an app uses a device's microphone or camera, the device displays an indicator to let the user know. For similar reasons, Apple has prohibited apps from accessing the camera if they are running in the background—so that they cannot surreptitiously spy on users.

Of course, Apple also builds in many other protections—including hardware security and biometrics, such as Apple silicon, Secure Enclave, Face ID, and Touch ID; the integrated hardware and software functions that provide for the safe boot, update, and ongoing operation of Apple operating systems; and the networking protocols that provide secure authentication and encryption of data in transmission. Apple devices also include data protection and encryption features to protect devices that have been lost or stolen, and to defend against unauthorized persons attempting to use or modify a device. And, Apple provides framework "kits" for secure and private management of users' homes and health, which third-party apps can also access through APIs, so a user's most sensitive and personal data stays secure and private.

These are just a few examples of Apple's system architecture and privacy-by-design protections that—together with the new changes we are introducing—continue to protect our EU users in this new landscape.

Concerns from Governments and Users

We expect that many will welcome these protections, because we know that there are real concerns about the changes Apple is making to its platform. Since we announced DMA-related changes to iOS, Safari, and the App Store in the EU on January 25, 2024, we have heard concerns from governments—including government agencies of EU member states—and users about the risks of allowing alternative app stores and alternative payment processors on iOS, and asking how and if we plan to put safeguards in place against those risks.

Government agencies, both in the European Union and outside of it, have been quick to recognize the risks created by these new distribution options and the need for protective measures. These agencies—especially those serving essential functions such as defense, banking, and emergency services—have reached out to us about these new changes, seeking assurances that they will have the ability to prevent government employees from sideloading apps onto government-purchased iPhones.

Several have told us that they plan to block sideloading on every device they manage. One EU government agency informed us that it had neither the funding nor the personnel to review and approve apps for its devices, and so planned to continue to rely on Apple and the App Store because it trusts us to comprehensively vet apps.

These agencies have all recognized that sideloading—downloading apps from outside the App Store—could compromise security and put government data and devices at risk.

And ***users*** have sent Tim Cook numerous emails expressing their fears that these changes will make their experience on iPhone less safe. These customers have told us that what they love and value about Apple and its products is our commitment to protecting their privacy and security, and that they fear the risks the new changes may bring to their own devices—and those of their families.

We heard—and anticipated—these concerns. That is why we implemented safeguards, and why we will work tirelessly to innovate to protect our users to the extent possible under the law.

Dear Tim

Real emails received by Tim Cook about changes to iPhone in the European Union

To: **Tim Cook**
From: **EU Citizen**
Subject: **Thank You**
Date: **January 27, 2024**

Thank you for leading a company that puts customers first, no matter if it's in regards to their privacy, health, or human rights.

As an EU citizen, ... I will not be allowing sideloading on my devices

To: **Tim Cook**
From: **Apple Customer**
Subject: **Deeply concerned by recent EU legislation**
Date: **January 28, 2024**

I've been a happy Apple customer and user for well over a decade. I truly believe what Apple created is magical. I don't want to see the day when I am forced to download a 3rd party store when the developer of an app I want to use chooses to circumvent the App Store and forces me to sign up to theirs, or use 3rd party payment app if my bank decides it doesn't want to support Apple Pay anymore. It all currently works like magic and is a pleasure to use.

I sincerely hope yourself and Apple continues to stand up for what's right and continues to deliver best customer experience around and that we never see the iPhone full of 3rd party App store like Samsung or Google phones.

To: **Tim Cook**
From: **EU iPhone User**
Subject: **Concerns European Digital Markets Act**
Date: **January 27, 2024**

Recently, there has been significant discussion about iPhones opening up to alternative app stores, following the European Digital Markets Act. As a consumer, this development concerns me. **I chose the iPhone for its strong commitment to privacy and security, a hallmark of Apple's philosophy.**

I understand that, under the new regulations, I am not obliged to download apps from outside the App Store. However, I would prefer an option that would allow me to avoid even the possibility of encountering apps from external sources, including avoiding pop-ups or notifications about them. Essentially, I seek to maintain the iPhone's current user experience, where the App Store is the sole source for apps.

Could Apple consider introducing a feature that lets users like me restrict their iPhones to only download apps from the Apple App Store? This option would uphold a consumer's right to choose the level of security and privacy they are comfortable with, which I believe is in line with fair competition principles.

To: **Tim Cook**
From: **Apple User**
Subject: **Sideloading**
Date: **January 16, 2024**

Can you even guarantee security to people who don't want sideloading on their devices?

Surely lot of people prefer getting normal applications as usual. A way to unaccept side-loading and having « normal Apple applications » on instal-lation would be a nice way.

Google Program Prevents Sideloading

Android has allowed sideloading since its inception, but it appears Google has recognized this practice puts high-security users at risk.

Google designed its Advanced Protection Program for users whose "accounts contain particularly valuable files or sensitive information" and strongly recommends "journalists, activists, business executives, and people involved in elections" enroll in the program. One of the core features of the program is that it prevents sideloading to help fight off "harmful downloads." Enrollees in the program are only able to install apps from "verified stores, like Google Play Store and your device manufacturer's app store."

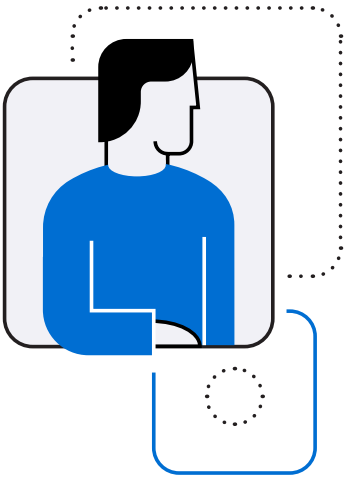
The Risks That Are Reduced (But Not Eliminated) by Apple's Safeguards for App Distribution and Alternative Payment Systems

These safeguards will help keep EU users' iPhone experience as secure, privacy-protecting, and safe as possible—although not to the same degree as in the rest of the world. This section provides more detail on the categories of risks that these safeguards will seek to address.

NOTARIZATION

Notarization aims to detect malicious apps by identifying serious threats to user security, privacy, and safety. For example:

- One common way that malicious apps find their way onto devices is through ***social engineering***—by manipulating users into granting access to their device by pretending to be something they are not, including by imitating popular, legitimate apps. Notarization seeks to reduce this threat by checking to see if the way an app presents itself through its metadata accurately represents how it works during the review. Notarization will analyze apps with the goal of stopping these sorts of malicious pretenders from making their way onto devices.



As just one example, through its combination of human and automated review, Apple identified a set of apps that were found to be impersonating a legitimate ad platform in order to steal login credentials. Notarization will check for malicious apps like these. Human review is essential to catch these schemes—automated review cannot check for attacks designed to manipulate users.

- Bad actors can also ***misrepresent their intentions*** to the user in order to convince them to willingly provide access to protected areas of their iPhone, such as Location Services, HealthKit (which stores health data), microphone, camera, contacts, photos, and more. Bad actors could use that illicitly gained access to target users with ***ransomware***, where the bad actor gains access to a user's files and encrypts them, decrypting them only after a ransom payment is made, or threatens to release the files publicly unless they receive money—which can lead to the loss of access to critical files, financial harm if the user pays the ransom, or emotional and psychological harm if the user's private notes, photos, and other files are made public. Notarization, and especially our human reviewers, will also look to identify and block malware which may try to deceive users about why it is requesting their permission to access other parts of iPhone—permission which is essential for the malicious app to access data beyond its tightly controlled sandbox.

- Bad actors could also use that fraudulent access to deploy ***consumer spyware***, a genre of malware that is installed on a device without the end user's knowledge and steals sensitive information, including contacts, photos, and videos. Consumer spyware can be used to violate the privacy of an intimate partner, or by hackers seeking to extract monetizable data like business secrets, or to obtain leverage over the user as part of some other criminal scheme. Bad actors can also sell such sensitive data without user permission, including in violation of the user's rights or Apple's privacy-protecting policies. Notarization, and our human reviewers, will also look for apps that hide their true purpose and capabilities in order to deploy consumer spyware.

- Developer tools themselves have the potential to contain malicious software, whether they are knowingly malicious or become infected, posing a threat to the users and developers alike. Malicious SDKs that a developer knowingly or unknowingly includes in their app could collect location data and sell it to unscrupulous entities, opportunistically collect protected data that the app itself has obtained legitimate user consent for; or attempt to clandestinely track a user across websites and apps without permission. Notarization will review apps to identify if they have compromised developer tools embedded into their apps—like those SDKs—that we know contain ***malware***, which protects developers themselves from threats from malicious actors who could offer infected developer tools that contain and propagate malware.

More on Threats from Sideloading

You can read more about how bad actors can try to use sideloaded apps to threaten users' security, privacy, and safety—especially absent Apple's new safeguards—in the 2021 "Building a Trusted Ecosystem for Millions of Apps" papers: "A Threat Analysis of Sideloading" and "The Important Role of App Store Protections."

To: **Tim Cook**
From: **Apple User**
Subject: **Disappointed**
Date: **January 15, 2024**

Pretty soon you will have nothing to differentiate you from anyone else. This decision is going to affect so many of my friends and family who rely on the iPhone's ability to protect them from bad actors. I am going to have a hard time justifying them spend the money on an iPhone now.... I am not sure if you will read this personally, but I hope Apple has some way of keeping people safe if this is the path they plan to take.

- Malicious apps can even pose ***physical harm*** to users. Notarization will review apps for these risks. For instance, Notarization will check if apps encourage harm to users or others, catching "challenge apps"—like a variety of apps built by bad actors in response to a dangerous online challenge that assigned tasks to users over a 50-day period to encourage them to commit suicide. These apps were designed to gradually introduce elements of self-harm, with the final challenge requiring the "player" to kill themself. Apple caught and rejected these apps from iOS. Notarization aims to continue to keep dangerous apps like this off iOS.

REQUIREMENTS FOR ALTERNATIVE APP MARKETPLACES

The eligibility criteria for operating an alternative app marketplace will help prevent other types of malicious conduct from harming users on iOS by requiring ongoing monitoring. Although Apple provides the safest and most secure mobile computing platform in the world—as independent experts have repeatedly confirmed[7]—bad actors will always try to circumvent our protections. Despite sophisticated tools and expert review teams, persistent and ongoing monitoring is necessary to catch cutting-edge, disguised malicious apps that are not detected by Notarization in the first instance.

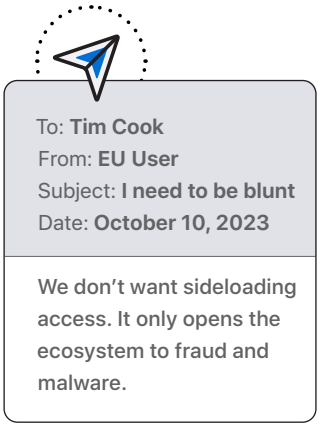
We have also seen apps that can transform themselves from unremarkable to malicious ***after*** they clear review. Apps that might appear benign—and thus pass Notarization—could be triggered by an external signal that turns on malicious features post-approval, transforming into crypto scams, copycats, money laundering tools, or worse. These are called **bait and switch apps**. These apps might include a component that renders information from the developer's server—so that the cybercriminal could change the user interface served to the user after Notarization so the app becomes malicious.

Or an app might contain obfuscated code that does not immediately appear malicious, but is triggered by an external condition, such as geolocation, IP address (that is, if it is not being opened in locations or by devices that could be Apple employees), or how long it had been since submission (that is, long enough that the bad actor thinks the app will likely have completed Notarization). For example, an app that appeared during Notarization to be a calculator—and thus passed Notarization—could contain code unknown to Apple that, after the app passed Notarization, turned it into an illegal gambling app.

Those apps are only able to be identified through ongoing monitoring. Indeed, through ongoing monitoring, Apple has caught the following apps that became malicious after they got onto the App Store:

- An app that presented itself as an app that provided travel information and services but, after approval, switched to an illegal loan app by an unverified service provider.
- A popular adult chat app that was secretly embedded with ransomware; the app first requested access to the user's contacts list—and then, if user did not pay a ransom, the app threatened to notify all users in their contacts list about their use of the adult chat app.
- An app that presented itself as one that provided information about animals but, after approval, switched to an app that facilitated illegal gambling.

Apple performs this ongoing review for apps distributed through the App Store and can quickly remove any malicious app we identify. Some of those protections will be deployed in the new landscape in the EU. These include automated tools that attempt to detect if apps have changed since Notarization, such as by periodically installing and launching apps as if they were installed through an alternative app marketplace. However, Apple also uses other signals, including marketplace-specific signals, such as data analysis of user reviews and downloads on the App Store. We cannot use those marketplace-specific signals to perform this ongoing review for apps distributed on alternative app marketplaces, leaving us with many fewer tools to understand when an app may have turned malicious. As a result, alternative app marketplaces must commit to monitoring for malicious apps in order to protect users from these very real threats.



And without criteria to ensure marketplaces are legitimate businesses that have the resources necessary to distribute apps on behalf of developers, dangerous marketplaces could also easily find their way onto users' devices. These could include scam marketplaces that set up shop for a short period of time, convince users to purchase fake or counterfeit apps, and then close the marketplace—becoming very difficult to track—before users realize they have been scammed. It could also include marketplaces that are unable to meaningfully monitor the apps they offer for security, privacy, and safety issues. Or it could include marketplaces that operate without any clear financial means at all, facilitating transactions between developers and users only to shut down due to lack of resources, leaving users without any remedies if they encounter issues with the apps they have downloaded from the marketplace, need to request a refund, or report a scam. Apple developed criteria to minimize the risk of such dangerous app marketplaces, while retaining options for legitimate marketplaces.

To: **Tim Cook**
From: **Apple Customer**
Subject: **Please DO NOT ALLOW SIDELOADING OR THIRD PARTY APP STORES on iOS17 or later iOS updates**
Date: **January 11, 2023**

I'm sending this email to let you know that most users including me across the world hope you don't allow side-loading. As I know, a lot of users will leave the iOS ecosystem if apple allows sideloading.
I have used Apple devices for more than 10 years, and I believe App Store is the core of iOS/iPad OS devices.
It will be a disaster for current and future iOS users If you guys allow sideloading on iOS...
I believe you know much better than me how harmful and dangerous it is to allow sideloading to the iOS ecosystem.

APP INSTALLATION SHEETS

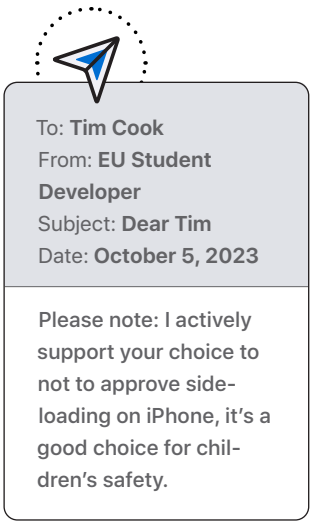
The app installation sheets also inform users and help users avoid scams and social engineering attacks. Bad actors often try to trick users into downloading malicious programs—including through copycat apps, scams spread using social media, fake system updates, email phishing methods, advertising on legitimate-looking websites, and many other malicious tactics. For example, bad actors may falsely present apps on websites that then direct users to an alternative marketplace, which in turn permits the developer to misrepresent their app. Because app installation sheets will help to inform each user about what it is they are downloading and from where, they will substantially reduce—but not eliminate—the risk that bad actors will trick users into downloading a malicious app.
These sheets will also help safeguard against—but likewise cannot fully prevent—apps that misrepresent themselves on alternative app marketplaces. App marketplaces could choose not to have rules regarding how an app markets itself on its platform. In those marketplaces, not only could an app market itself as a totally different app, but it could also set out different pricing or subscriptions than it will actually charge the user, or falsely represent that it has different features or services. The app installation sheet, which reflects the data that the developer submits about their app and that is then checked for accuracy during Notarization, creates a backstop so that users can be informed of how the app appeared and what its stated purpose was when it was submitted to Apple for review.

INFORMATION ABOUT ALTERNATIVE PAYMENT OPTIONS

For alternative payment options, our informational banners will help inform users of the inevitable risks that may arise, such as specific predatory techniques that Apple's secure commerce system prevents. Our system protects against malicious actors that use intentionally confusing designs and text to trick users into purchases or subscriptions on terms they didn't intend or understand, or that make it nearly impossible for the user to cancel. In addition:

- Because all apps on iOS that sell digital goods and services within the app have—until now—used Apple's secure commerce system, Apple has been able to ensure that users can easily cancel every subscription they sign up for with one simple tap. And through the StoreKit developer framework that powers In-App Purchase, Apple ensures that the pricing and terms of the in-app purchase are exactly what the developer has configured on their SKU in App Store Connect. Regardless of how the app might market its pricing and terms, the user is always presented with confirmation of the price they will be charged before conducting the purchase. Without this system, apps may make it difficult for users to figure out how to cancel their subscriptions in order to disincentivize those users from leaving, or use misleading tactics to trick them

into subscribing on terms or at prices the user did not understand in the first place—like through misrepresenting how long a free trial is, or how often or how much a user will pay for the subscription.[8]

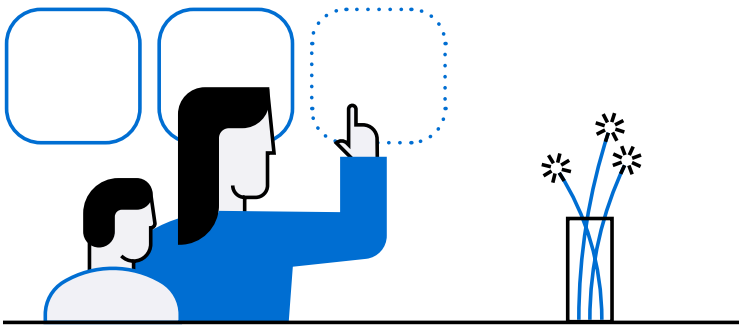


- The App Store's secure commerce system helps prevent apps from charging more for a digital good than they disclose. When the app is submitted to Apple for potential inclusion in the App Store, it must include the price of its digital goods and services. Apple can test whether that app is actually charging the amount it advertised to the user—and can check if an app is egregiously overcharging for the digital goods or services delivered. We have taken action on hundreds of apps in the last year for their manipulative pricing. As part of the standard, consistent checkout flow for digital goods and services using In-App Purchase, Apple's commerce system APIs also make sure the app displays the price that it submitted to Apple to the user (along with other submitted product information and important purchase terms) before the user completes the purchase, so the user knows what they'll be charged, whether or not the app disclosed the true amount to them. Without this system that users have relied on, the user may not have the assurance that the price the developer is marketing is an accurate representation of what they will ultimately pay.

- Apple further protects children and families through services like **Ask to Buy**, which requires parental approval on every item that their children want to buy or download onto iPhones, so parents can feel secure that scammers are not targeting their children.

- Apple's anti-fraud measures protect users from fraudulent developers, but they also protect developers from fraudulent users (such as those who transact with stolen credit cards), including through Apple's analysis of its payment system data to identify trends and developments, which allows Apple to root out scams and unscrupulous individuals.

- The App Store's commerce system can also help make sure apps deliver what they promised. When a user makes a purchase through Apple's system, that transaction is written to a user's purchase history. If the app does not deliver digital goods or services after the user pays, Apple can use the transaction



Dear Tim

Real emails received by Tim Cook about changes to iPhone in the European Union

To: **Tim Cook**
From: **Apple User**
Subject: **No Android**
Date: **April 21, 2023**

We are very satisfied with iOS because it is not like Android, it has high security, it has a user-friendly interface and it never slows down, but we heard from sources that sideloading is possible in iOS 17 and it can be downloaded from stores other than the App Store. It can also be downloaded. Please stop doing this. We just want to download from the App Store and ensure our security. Please do not enable sideloading. We want iOS to be like the old one, with strict rules and extremely high security.

To: **Tim Cook**
From: **EU Apple User**
Subject: **From a concerned Apple user and EU citizen**
Date: **October 24, 2023**

I am feeling increasingly more concerned and scared about my digital privacy and online safety in the EU. As an EU citizen and Apple user I always believed to have had the perfect balance between regulatory protection (like GDPR) and Apple safety features (like App Tracking Transparency and App Store). However, recently... that has changed.

Me, my family, friends and colleagues are Apple users and specifically picked the Apple ecosystem for our work and free time because of how the products and software is designed to be private and secure. Plus of course the safety features introduced over the years. It is a scary idea but it looks like new regulation from the EU Commission would compromise many of those safety and security features I currently rely on.

To: **Tim Cook**
From: **EU iPhone User**
Subject: **Sideloading EU**
Date: **January 25, 2024**

I really hope that you will offer me as an EU Client the option to not use any sideloaders. I want to rely on the proven App Store and not some nonsense...

To: **Tim Cook**
From: **EU Apple User**
Subject: **Concerns and Suggestions Regarding EU's Sideloading Mandate**
Date: **January 26, 2024**

I am writing to express my concerns about the recent requirement imposed by the European Union (EU) for Apple to allow sideloading on iOS devices. I understand that this decision has been made in the interest of promoting competition and consumer choice, but I believe it raises important privacy and security considerations.

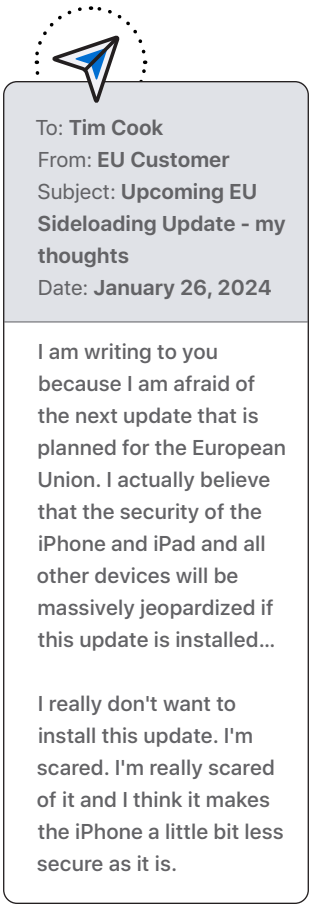
... The App Store has been a trusted source for iOS applications, providing a level of confidence and security that is crucial in today's digital age. Personally, I have always felt safe knowing that the apps I download from the App Store undergo strict vetting processes to protect my device and personal information.

However, with the introduction of sideloading, there is a potential risk of users unknowingly installing malicious or unverified applications from external sources, compromising the overall security of iOS devices. This shift could expose users to various cybersecurity threats, and I am concerned about the potential consequences of sideloading on iOS.

history to validate whether the transaction took place and take action against apps that do not fulfill their end of the transaction. Without this history, Apple will not be able to assist users if apps renege on a transaction.

- Apple also has thousands of AppleCare agents that users can call for assistance with refunds or other customer support. These agents will not be able to provide support for purchases made through alternative payment systems.

Users have come to rely on the benefits and protections provided by Apple's secure and private commerce system after using it to buy digital goods and services for the better part of two decades. The informational banners will keep users informed that they need to be on the lookout for deceptive techniques that, until now, Apple has protected them from.



The Role of Alternative App Marketplaces and Alternative Payment Processors in Further Reducing Risks

In the coming months, many users in the EU will be able to download apps onto iOS from alternative app marketplaces and make payments using alternative payment processors. This will mark a sea change from the way things have always worked on iPhone. Because users trust Apple to keep their devices protected, they have not had to worry about whether their source of third-party apps or their in-app payment system posed a threat to them. Users will no longer be able to assume that protection.

Apple is taking substantial, meaningful measures to protect users in the EU in the new world of alternative distribution and alternative payments that the DMA has opened. But the scope of these measures is necessarily limited by the law. Apple must therefore pass responsibility for the user protection functions it is no longer permitted to carry out on its own to the alternative app marketplaces and payment processors themselves.

That means alternative app marketplaces and alternative payment processors have a likely unavoidable role to play in protecting users—even if users do not want to use them. Many users have reached out to us to ask whether they can simply opt out of the changes that Apple announced to comply with the DMA. And some commentators have argued that users are under no obligation to take advantage of the new options Apple is making available in the EU if they do not want to; instead, these commentators say, users can simply continue downloading apps exclusively from the App Store.

To: **Tim Cook**
From: **EU iPhone User**
Subject: **Customer from the European Economic Area**
Date: **January 23, 2024**

It was my free choice to purchase an Apple iPhone, and I did so because I feel more secure with iOS than with a device running Android. Now, my actual question: Wouldn't it be possible for me as a customer to have the freedom to choose whether I install the iOS version intended for the European market in the future, or whether I can install the iOS version used in the rest of the world?

An Android app used SMS phishing to trick people into sideloading an app that masqueraded as a legitimate postal service app, but then stole sensitive information from the device. It repeated this scam by masquerading as mail services in several different countries. Because it ran slightly different apps for each scam, it would be harder for each marketplace to detect this pattern.[10]

Users will also likely have no choice but to set up multiple accounts with each app marketplace and alternative payment option they use. This will not only be inconvenient to the user and degrade their experience—it will also increase the risk that their data will be stolen. The more accounts a user has, the more different places their personal and financial information is stored, which increases the risk of that data being exposed in a data breach—which is increasingly likely to happen.[9] In addition, users could become even more conditioned to indiscriminately share their information and trust app distributors—even when the distributors may not be legitimate. A bad actor could fool a user by posing as a legitimate app marketplace on a website off iOS, tricking the user into providing payment or their information—only after which the user would discover that the bad actor never had a marketplace at all.

But in practice, users in the EU will lose the choice to solely remain on the App Store and keep all of Apple's industry-leading protections, even if that is what they would prefer. Some developers will choose to make their apps exclusively available on alternative app marketplaces. These could include apps that users' jobs or schools require, or that they need to stay connected with family and friends—apps that users have to download, even if they would prefer not to use alternative app marketplaces. **Developers will ultimately control where huge numbers of EU users must go to obtain the apps they need**, whether or not users are satisfied with the protections provided by those stores. Despite our best efforts, many users may not notice or understand that developers are directing them to download apps from an alternative app marketplace, in spite of the users' preference not to transact with that marketplace.

DECISIONS FOR ALTERNATIVE MARKETPLACES AND PAYMENT PROCESSORS

In the EU, every user's security, privacy, and safety will depend in part on two questions. First, are alternative marketplaces and payment processors capable of protecting users? And, second, are they interested in doing so? The measures that Apple is implementing will establish an important baseline, but that does not mean they are sufficient on their own. Users' experiences will vary significantly based on how each marketplace and payment provider chooses to conduct their business. This opens up opportunities for differentiation, and, just as the DMA intended, Apple intends to vigorously compete to ensure that the App Store remains the most safe, secure, and privacy-protecting option for consumers. But it also creates potential gaps.

App Store Signals

150 million
transactions each day including all free & paid app downloads and in-app purchases

3.12 million
ratings and reviews each day

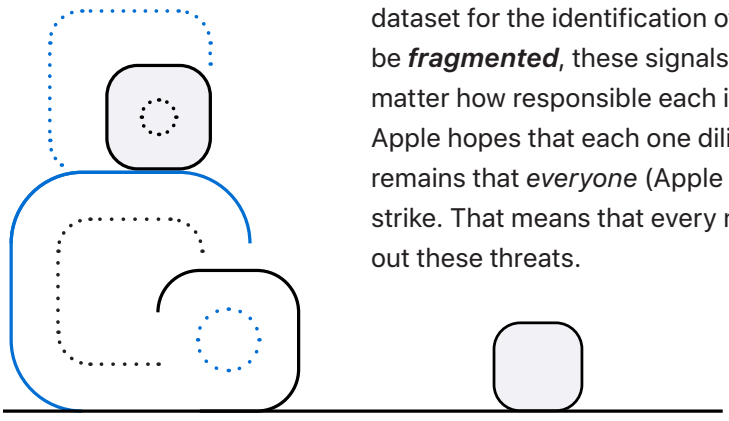
Operating the App Store for the better part of two decades has been an enormous undertaking. We work constantly to find and stop bad actors and their ever-evolving malicious apps. In addition to the thousands of engineers who create the hardware and software intended to prevent bad actors from harming users, hundreds of full-time Apple employees participate in App Review, reviewing apps in over 80 languages across three time zones. Each year, we review over 6 million app submissions. In the last full year for which data is available, Apple approved nearly 4.5 million apps and rejected 1.6 million more—many because they did not perform properly on the device, and some because they violated our security and privacy rules. This persistence is a major reason why iOS has remained the safest mobile computing platform in the world since it was launched—and why most bad actors have concluded that trying to infect iOS with malware is not a worthwhile investment of their time, energy, and resources.

Even with our experience and round-the-clock human reviewers, we pulled more than 185,000 apps from the App Store per year because they were later discovered to have violated Apple's Guidelines. To find and remove these apps, Apple carefully monitors the App Store itself—where *every single day* more than 150 million transactions occur and more than 3.1 million ratings and reviews are submitted—to identify problematic apps. Apple considers a variety of indicators in its monitoring. These include user reviews, reports through our Report a Problem tool, feedback to the thousands of AppleCare agents supporting users, and suspicious patterns in the data—like unusual activity in reviews, sudden spikes in the number of downloads, or unusual purchase behaviors. It is only by paying close attention to these signals that Apple's team can root out bad actors.

These include apps described on page 20 that turned into an unverified loan app, adult chat ransomware attack, the illegal gambling app that Apple has caught.

Alternative app marketplace operators will now have to undertake ongoing monitoring necessary to protect EU users from bait-and-switch and other malicious apps outside of the App Store.

Even if alternative app marketplaces dedicate significant resources to this monitoring work, it will be harder to identify these malicious apps than it was before the DMA. Until now, all of these app and developer trustworthiness signals could be found and analyzed in one place—the App Store— establishing a rich dataset for the identification of bad actors. But because app distribution will now be ***fragmented***, these signals will be spread across multiple marketplaces. No matter how responsible each individual app marketplace operator may be—and Apple hopes that each one diligently monitors for malicious actors—the fact remains that *everyone* (Apple included) will receive fewer signals when bad actors strike. That means that every marketplace will inevitably be less efficient in rooting out these threats.



To: **Tim Cook**
From: **iPhone User**
Subject: **Keep Apple's iOS closed please**
Date: **January 27, 2024**

If I wanted an open-source operating system like Google or Samsung I would have bought them. The main—and I can't say this loud enough, main—reason I buy and have an Apple phone is because you are a closed iOS and the iOS is more secure than Android. But if you are going to open the gates and no longer be as safe, then I might as well switch over. Please keep iOS closed, please.

Apple has long been concerned with protecting developers and the app ecosystem from unethical and malicious pirated apps. These so-called "cracked" apps—some of which are paid apps which have been modified to be available for free, and some of which have had their code rewritten to include modifications not intended by their creators—not only steal from hardworking developers and violate their rights, but also pose severe risks to users. These pirated apps are often a vector for malware.

In the weeks following our announcement of the changes required by the DMA, we've been working with a number of developers interested in building alternative app marketplaces. We are excited to see what they build. **But we've also learned about bad-faith developers who seem interested in these changes only so they can build marketplaces that steal other developers' IP and distribute pirated apps.** One developer actually scheduled a meeting with Apple to ask us about the changes we're making in response to the DMA, which we answered in good faith—only to later discover that the developer was associated with a notorious distributor of pirated software, and that they had illegally recorded the conversation and posted it online. Unfortunately, their questions appear to have been intended to probe for the best ways to take advantage of Apple's upcoming changes in the EU in order to build an official marketplace for pirated apps on iOS.

Over the last fifteen years, we have spent significant time and engineering fighting bad actors like these, who have tried to exploit every opportunity they can find to steal and distribute our developers' IP. But Notarization won't check to see if the apps on an alternative app marketplace infringe on others' IP, meaning it will be much harder to catch and prevent pirate distributors from making marketplaces that check for IP violations in name only. **These bad-faith distributors have been some of the loudest voices calling for alternative distribution for just this reason.** In fact, after we contacted the developer who illegally recorded their conversation with Apple, the developer actually argued that the DMA prohibits Apple from taking action against them to prevent their distribution of pirated apps on iOS.

DECISIONS ON CONTENT AND BUSINESS MODEL RULES

Each alternative app marketplace will develop its own market standards for content, business models, and more—and some content and business models that Apple has always protected users from will become available on iPhone. This is what the DMA intended: marketplaces will be able to offer apps that Apple would not have allowed on the App Store. For instance, none of Apple's new user protections will evaluate whether apps contain adult content, whether gambling or cryptocurrency exchange apps have the required licenses, or whether apps with user-generated content have content moderation policies. We will not consider whether apps are encouraging the reckless use of weapons or whether they are seeking to profiteer from national and global crises like epidemics. Each app marketplace will have to decide whether it will allow those kinds of content and businesses on their marketplaces, and how much to invest in enforcing their rules to ensure apps that violate them stay off their platforms.

DECISIONS ON PROTECTIONS FOR USERS AND THEIR KIDS

Alternative app marketplaces will also have to decide what protections to provide users of their platforms—especially parents and kids. For instance, **Ask to Buy** prevents children from buying or downloading items onto their iPhones without parental approval, and Apple prominently displays an app's age rating on its download page on the App Store. The App Store also requires developers to provide Privacy Nutrition Labels on their app listings, which explain to the user

On Android devices, many different pornographic apps and games are available to sideload, including app marketplaces specifically for adult content.

Apple has removed apps from the App Store for being primarily used to facilitate anonymous cyberbullying. One such app was being used to send anonymous messages to middle-school age children telling them they hoped they killed themselves.[11]

Apple has identified apps during App Review that appear at first to be innocuous but contain signals in their metadata indicating nefarious intent—such as one app that initially posed as a language program, but contained hidden signals that it planned to transform into an unlicensed gambling parlor after making it on to the App Store. Apple found and rejected this particular app.

Apple requires cryptocurrency exchanges on the App Store to be properly licensed everywhere they do business. It regularly rejects apps that are impersonating cryptocurrency exchanges but instead intend to defraud users, or that attempt to operate as unlicensed exchanges by submitting the app under the guise of a legitimate app.

Many popular game apps targeted at children incorporate in-app purchases, including of in-game currency, power-ups, loot boxes, and more. Without features like Ask to Buy, children can spend hundreds of dollars on these purchases without a parent noticing. For example, just last year the U.S. Federal Trade Commission ordered a game developer "to pay $245 million to consumers to settle charges that the company used dark patterns to trick players into making unwanted purchases and let children rack up unauthorized charges without any parental involvement."[12]

Apple does not permit apps that aim to profit from national crises—like the COVID-19 pandemic—on the App Store. It removed an app that promoted private parties during the pandemic despite stay-at-home orders, and required contact-tracing apps to stop using their public health function to sell ads. Apps like these could be allowed on alternative app marketplaces.[13]

how an app will collect their data and track them ***before*** the user downloads the app onto their device. None of those features are mandatory for alternative app marketplaces. Marketplaces can choose to offer similar protections—or they can choose not to.

Apple's commitment to protecting user privacy means that on its Privacy Nutrition Labels, an app has to declare what data the app is collecting and linking to a user. Existing app marketplaces on other platforms do not require that sort of clear disclosure of tracking.

Although we hope that alternative app marketplaces will meaningfully invest in protecting user security, privacy, and safety, we cannot guarantee it. Their business models may provide varying incentives to create protections for users. For example, alternative app marketplaces that have business models based on the collection and sale of user data would have a commercial incentive not to offer features like Privacy Nutrition Labels, which facilitate informed user consent to the collection and use of their data. This would leave users on that marketplace less educated about their options to protect their data privacy. Those app marketplaces also would have no incentive to continue investing in innovative new ways to protect users' privacy—as Apple continues to do for users on the App Store.

DECISIONS ON PAYMENTS SUPPORT FOR CUSTOMERS

In 2021, the US Federal Trade Commission fined a membership-based online learning tool $10 million dollars because it did not adequately disclose that consumers would be charged indefinitely after an initial free trial period ended, and it required a lengthy and confusing process to cancel the subscription. Under Apple's subscription tools today, a user can cancel a subscription like this in one click—but other marketplaces might not provide that service.[14]

It will be up to each individual marketplace, app developer, and/or alternative payment processor to provide payments support to users. Some may provide excellent consumer protections, but others may not. In all such cases, however, Apple will no longer be able to help users who fall into subscription traps or are tricked into making an unintended purchase—Apple's many AppleCare agents will have no ability to provide support for a payment system that Apple does not control. These choices will introduce enormous complexity for users who understandably think that they can continue to contact Apple for support after purchasing a digital good or service through an app available on the App Store—but instead find that Apple cannot help them because the developer has chosen a different payment solution. That is why it is so important for users to have as much information as possible before engaging in such a transaction. Apple has a role to play in supporting users transacting through alternative payment options, including through the information it provides, but third parties implementing these solutions do as well—if they do not, the users will be worse off for it.

NEW INCENTIVES FOR CYBERCRIMINALS

While these changes bring new opportunities for competition, they will also inevitably create new and lucrative markets for malicious actors. Malicious actors have long struggled to gain access to iPhone because of its best-in-class security and privacy protections. Apple's integrated approach to platform security has put the iOS ecosystem out of the reach of commodity malware—in fact, cybercriminals have never succeeded in getting a single widespread consumer

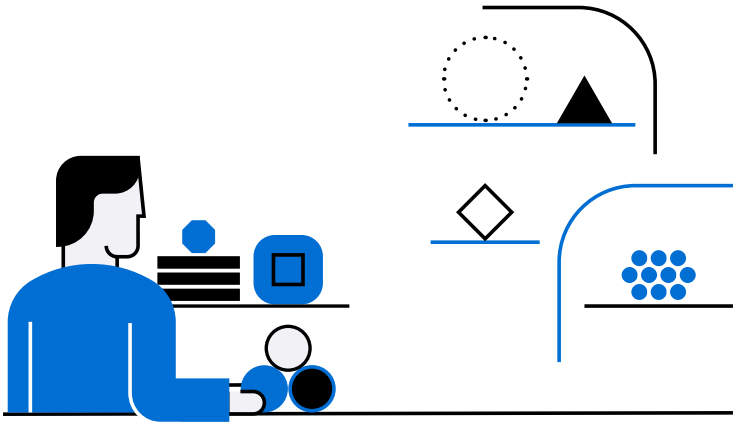
To: **Tim Cook**
From: **iPhone User**
Subject: **3rd Party Apps**
Date: **February 20, 2023**

I love how secure iOS on iPhone is over Android and would like the option to not allow 3rd party apps to be downloaded once the option arrives. Maybe a do not allow check box in settings?

malware attack on iOS. They have learned that Apple's integrated approach to platform security makes most malware infection attempts a lost cause. The production and distribution of malicious software requires significant resources, and iPhone's strong defenses have prevented these efforts from seeing meaningful return on investment, further lowering the device's attractiveness as a target.

In the same way, Apple's proactive and ongoing monitoring has made it more difficult for ongoing scams to gain a foothold on iOS. For instance, we take action to prevent otherwise legitimate apps from being used to facilitate scams, like the "pig butchering" scam which tricks users into depositing funds for investment into a scam brokerage account on a legitimate investing app. When we learn about such scams, we contact the developer of the legitimate app to stop the scams from proliferating on that app. Our actions have made iOS apps less attractive to scams like these as well.

The new changes to iPhone in the EU will alter the calculus for bad actors who previously did not seek ways to exploit iOS and its users because of the relatively lower returns available to them. Alongside new options for developers, these changes create new entry points—and potential vulnerabilities—for scammers and cybercriminals. These increasingly creative actors pose sophisticated threats. Many rely on social engineering to trick users into giving away their most personal and sensitive information through means that anyone could fall for—even the savviest user. With easier access to iPhone users through alternative app download channels, the return on their investment increases, making attempts to target iPhone relatively more lucrative overall. For all the reasons we have described, including Apple's inability to test for fraudulent overcharges outside of its commerce system and the fragmentation of marketplace signals, it will take longer to catch scammers or other bad actors—and we cannot guarantee that alternative app marketplaces will take the same swift action against them that we would. This leaves users exposed to potential bad actors for longer, and may give those bad actors more space to find creative ways to trick users.



This creates an incentive for bad actors to build new schemes and invent new malware that targets iOS users. These bad actors will gain the ability to move their apps from one alternative app marketplace to another, creating opportunities to use the same scam again and again on marketplace after marketplace—or even potentially on the same marketplace with minor changes. All of this increases the likelihood that bad actors will see a return on their investment on iOS, incentivizing even more malicious development. Perhaps most concerning, this newly incentivized level of criminal investment in building tools, services, and infrastructure to target iOS users risks spilling over and lowering the cost of attacking even those users who only use the App Store.

Let's be clear: Apple builds multiple layers of security into its devices and systems. We will do everything possible to reduce these risks. But for all the reasons explained, the risks will increase.

Apple is committed to a secure, privacy-protecting, and safe user experience on iPhone. That commitment continues even as we have put changes into place to comply with the DMA, so that we are doing everything we can to protect users in the EU. Even if the EU experience will not be the same as the one we are able to offer elsewhere, these new tools and processes will help us fight against the risks that these changes create.

Notarization will help prevent users from being exposed to malicious apps that contain malware like ransomware or consumer spyware, that trick users into exposing more of their information than they intend, or that risk their own safety. App installation sheets will allow users to receive accurate information about the apps they're downloading, so that users will be less likely to be tricked into installing a fake app or an app with terms they didn't understand. Requiring alternative app marketplaces to conduct ongoing monitoring will help stop malicious apps from spreading unchecked. And informational sheets about alternative payment systems will let users know that they now need to be on the lookout for fraud and scams intended to trick them into overpaying for what they requested.

These protections help ensure that users will continue to have an enriching, safe, and transparent iPhone experience, where the user is in control of their own data. And they will continue to make iPhone the most secure, most privacy-protecting, and safest smartphone available in the European Union today—giving users the great product they expect from Apple.

Sources

1. *Survey: Nearly half of Android users consider switching to iPhone over security and privacy concerns,* 9to5Mac (Aug. 16, 2022), https://9to5mac.com/2022/08/16/android-users-consider-switching-iphone/.

2. *App Store developers generated $1.1 trillion in total billings and sales in the App Store ecosystem in 2022*, Apple (May 31, 2023), https://www.apple.com/newsroom/2023/05/developers-generated-one-point-one-trillion-in-the-app-store-ecosystem-in-2022/.

3. For more information, *see Apple announces changes to iOS, Safari, and the App Store in the European Union,* Apple (Jan. 25, 2023), apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/.

4. *App Store stopped more than $2 billion in fraudulent transactions in 2022*, Apple (May 2023), https://www.apple.com/newsroom/2023/05/app-store-stopped-more-than-2-billion-in-fraudulent-transactions-in-2022/.

5. *2022 App Store Transparency Report*, Apple (2023), https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf.

6. Steve Jobs recognized this very issue in 2007. *See* Steve Jobs, *iPhone SDK Letter* (Oct. 17, 2007), *available at* https://tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter.

7. *Threat Intelligence Report 2023*, Nokia, https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/.

8. *See* European Consumer Centre Germany, *Tips against subscription traps on the internet*, https://www.evz.de/en/shopping-internet/internet-fraud/subscription-traps.html.

9. Stuart Madnick, *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase* (Dec. 2023), https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

10. *Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading*, Apple (Oct. 2021), at 14.

11. Elizabeth Cassin*, Sarahah: Anonymous app dropped from Apple and Google stores after bullying accusations*, BBC (Feb. 25, 2018), https://www.bbc.com/news/blogs-trending-43174619.

12. *FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges*, FTC (Mar. 4, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making; *Kids Mobile Gaming Report: More Than Two-Thirds of Parents Worry Kids Overspending on In-App Purchases*, Sell Cell (June 5, 2020), https://www.sellcell.com/blog/more-than-two-thirds-of-parents-worry-kids-overspending-on-in-app-purchases/.

13. *App promoting private parties amid COVID-19 removed from Apple App Store,* Bus. Insider (Dec. 30, 2020), https://www.businessinsider.in/tech/apps/news/app-promoting-private-parties-amid-covid-19-removed-from-apple-app-store/articleshow/80020920.cms; Khadeeja Safdar & Kevin Poulsen, *Google, Apple Struggle to Regulate Covid-19 Tracing Apps*, Wall St. Journal (June 5, 2020), https://www.wsj.com/articles/why-google-and-apple-stores-had-a-covid-19-app-with-ads-11591365499.

14. *Children's Online Learning Program ABCmouse to Pay $10 Million to Settle FTC Charges of Illegal Marketing and Billing Practices*, FTC (Sept. 2, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing.