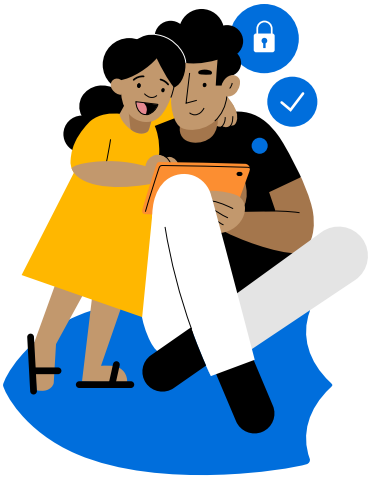


Building a Trusted Ecosystem for Millions of Apps

The important role of App Store protections

June 2021

2007

"We're trying to do two diametrically opposed things at once: provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. This is no easy task."

Steve Jobs, 2007[1]

2016

"Use the official application marketplace only. Users should … not [download applications] from third-party sources, to minimise the risk of installing a malicious application. Users should not sideload applications if they do not originate from a legitimate and authentic source."

European Union Agency for Cybersecurity (ENISA), 2016[2]

2017

"The best practices identified for mitigating threats from vulnerable apps are relevant to malicious and privacy-invasive apps. Additionally, users should avoid (and enterprises should prohibit on their devices) sideloading of apps and the use of unauthorized app stores."

U.S. Department of Homeland Security Report, 2017[3]

Today, our phones are not just phones; they store some of our most sensitive information about our personal and professional lives. We keep them with us wherever we go, and we use them to call and text with loved ones, take and store photos of our children, give us directions when we're lost, count our steps, and send money to friends. They are with us in happy times, and in times of emergencies.

We designed iPhone with this in mind. We built the App Store to give developers from around the globe a place to build innovative apps that can reach a growing and thriving global community of over a billion users. Nearly two million apps are available for users to download on the App Store, with thousands of apps added every week. Given the sheer scale of the App Store platform, ensuring iPhone security and safety was of critical importance to us from the start. Security researchers agree that iPhone is the safest, most secure mobile device, which allows our users to trust their devices with their most sensitive data. We built industry-leading security protections into the device, and we created the App Store, a trusted place where users can safely discover and download apps. On the App Store, apps come from known developers who have agreed to follow our guidelines, and are securely distributed to users free from interference from third parties. We review every single app and each app update to evaluate whether they meet our high standards. This process, which we are constantly working to improve, is designed to protect our users by keeping malware, cybercriminals, and scammers out of the App Store. Apps designed for children must follow strict guidelines around data collection and security designed to keep children safe, and must be tightly integrated with iOS parental control features.

And when it comes to privacy, we don't just believe it's important – we believe it is a fundamental human right. That principle guides the high privacy standards we build into our products: we collect only the personal data strictly necessary to deliver a product or service, we put the user in control by asking them for permission before apps can access sensitive data, and we provide clear indications when apps access certain sensitive features like the microphone, camera, and the user's location. As part of our continued commitment to user privacy, two of our newest privacy features – privacy labels on the App Store and App Tracking Transparency – give our users unprecedented control over their privacy, with increased transparency and information to help them make informed choices. Thanks to all these protections, users can download any app on the App Store with peace of mind. This peace of mind also benefits developers, who are able to reach a wide audience of users who feel confident downloading their apps.

Did you know?

Apple reviews all apps and updates on the App Store to intercept those that could harm users. This includes apps that contain inappropriate content, invade user privacy, or contain known malware, which is software used for bad or dangerous purposes.

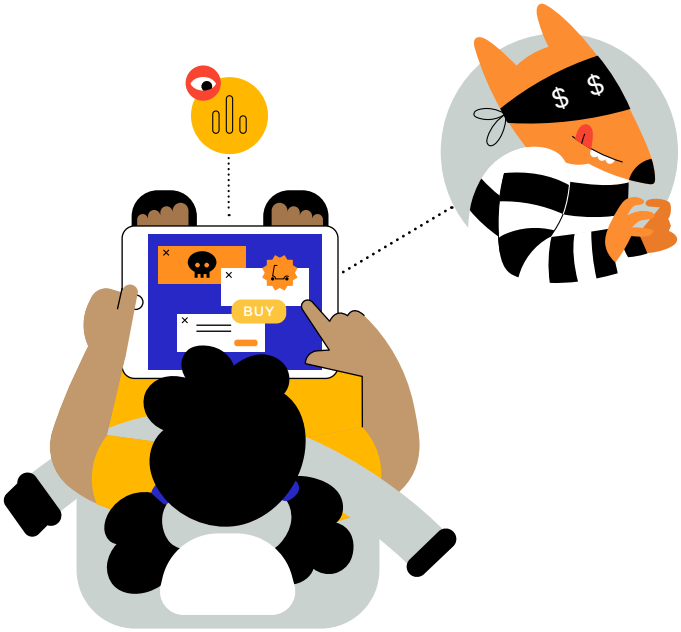
A study found that devices that run on Android had 15 times more infections from malicious software than iPhone, with a key reason being that Android apps "can be downloaded from just about anywhere," while everyday iPhone users can only download apps from one source: the App Store.[4]

This approach to security and privacy has been highly effective. Today, it is extremely rare for any user to encounter malware on iPhone.[5] Some have suggested that we should create ways for developers to distribute their apps outside of the App Store, through websites or third-party app stores, a process called "sideloading." Allowing sideloading would degrade the security of the iOS platform and expose users to serious security risks not only on third-party app stores, but also on the App Store. Because of the large size of the iPhone user base and the sensitive data stored on their phones – photos, location data, health and financial information – allowing sideloading would spur a flood of new investment into attacks on the platform. Malicious actors would take advantage of the opportunity by devoting more resources to develop sophisticated attacks targeting iOS users, thereby expanding the set of weaponized exploits and attacks – often referred to as a "threat model" – that all users need to be safeguarded against. This increased risk of malware attacks puts all users at greater risk, even those who only download apps from the App Store. Additionally, even users who prefer to only download apps from the App Store could be forced to download an app they need for work or for school from third-party stores if it is not made available on the App Store. Or they could be tricked into downloading apps from third-party app stores masquerading as the App Store.

Studies show that third-party app stores for Android devices, where apps are not subject to review, are much riskier and more likely to contain malware as opposed to official app stores.[6] As a result, security experts advise consumers against using third-party app stores because they are unsafe.[3,7] Allowing sideloading would open the door to a world where users may not have a choice but to accept these risks, because some apps may no longer be available on the App Store, and scammers could trick users into thinking they are safely downloading apps from the App Store when that is not the case. Sideloading would expose users to scammers who will exploit apps to mislead users, attack iPhone security features, and violate user privacy. It would also make it more difficult for users to rely on Ask to Buy, a parental control feature that allows parents to control their children's app downloads and in-app purchases, and Screen Time, a feature to manage their and their children's time with their devices. Scammers would have the opportunity to trick and mislead kids and parents by obfuscating the nature of their apps, making both features less effective.

In the end, users would have to constantly be on the lookout for scams, never knowing who or what to trust, and as a result many users would download fewer apps from fewer developers. Developers themselves would become more vulnerable to threats from malicious actors who could offer infected developer tools that contain and propagate malware. Developers would also be more vulnerable to piracy, undermining their ability to get paid for their work.

Let's look at how a family's everyday experience using their iPhone would be different with sideloading. We'll follow the day of John and his 7-year-old daughter, Emma, as they navigate this more uncertain world.



A sideloaded game bypasses parental controls

Emma asks John if she can play a game that she heard about from her friends at school. John looks for the game on the App Store, but the developer has only made it available on third-party app stores. This makes John uneasy, but he downloads it because Emma really wants to try the game, and the third-party app store claims the app is appropriate for children. Later, on their way to the park, when Emma is playing the game in the backseat of the car, the app bombards her with links to outside websites and targeted advertisements. John had added his credit card information to buy Emma a starter pack when he downloaded the game, but he didn't realize that the Ask to Buy parental controls would not work with this sideloaded app. While she is playing, Emma purchases many extra turns and special items, not realizing that her dad had not actually approved those purchases. The app also has embedded third-party trackers, which collect, analyze, and sell Emma's data to data brokers, even though the app is marketed for kids.

Real-world attacks on platforms that allow sideloading

Android apps aimed at children were discovered to be engaging in data collection practices that violated kids' privacy. These apps continue to thrive and target Android users on third-party app stores, even though they were removed from the Google Play Store.[8]

Malicious actors have placed inappropriate or obscene ads on apps targeted at kids.[9]

Real-world attacks on platforms that allow sideloading

Sideloaded apps on Android have been known to carry out "locker" ransomware attacks. These malicious apps, if installed, lock users out of their phone or target their photos, unless they agree to pay a ransom.[10,11]

Android users have been tricked into using insecure methods to download fake versions of apps like Netflix and Candy Crush. These fake apps, either when given access or by exploiting platform vulnerabilities, can spy on Android users via the microphone, take screen shots of their devices, view location, text messages and contacts, steal users' login credentials, and make changes to users' phones.[12,13,14] Others have been used to steal banking credentials and take over users' bank accounts.[15,16,17,18]

A recent ransomware scam involves an Android app masquerading as a COVID-19 contact tracing app. If installed, it encrypts all personal information, leaving an email address to contact if the user wants to rescue their data.[19]

One app found on third-party Android app stores tricks users by pretending to be a system update. Once installed, the app displays a "Searching for update" notification, as it gets access to and steals the user's personal data, such as messages, contacts, and pictures.[20,21]

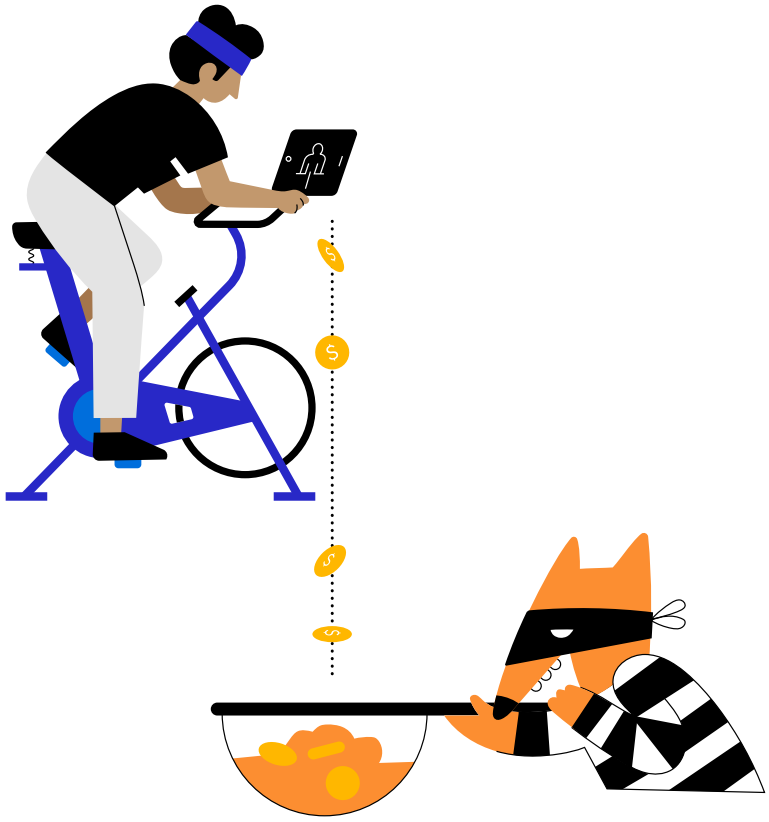
At the park, the copy-cat filter app John had sideloaded threatens to delete all of his photos unless he pays up

When John and Emma are at the park, John sees an ad for a selfie filter app from a well-known app developer that looks like it would be fun to use with Emma. The ad takes him to a page to download the app that looks like the app developer's page on the App Store, so John thinks he is protected, and does not realize he is actually downloading a copy-cat version of the app from a third-party app store. Because John thinks the filter app came from a well-known, trusted developer, he grants it permission to access his photos. Once the app starts running, however, he realizes he's made a mistake – the app threatens to delete all of the photos on his camera roll unless he enters his credit card information and pays a ransom. iPhone on-device protections give John control over which apps are allowed to access his photos, but in this case the sideloaded app tricked him into granting access to his photos by posing as a selfie filter app.

Real-world attacks on platforms that allow sideloading

Research shows that pirated apps published on third-party app stores cost developers billions in lost revenue per year.[22]

Pirated and otherwise illegitimate apps are widespread on Android. Such apps include gaming apps that allow cheating (e.g., a pirated version of Pokémon Go with the ability to simulate one's location), apps modified to provide pirated access to premium content or features, and illegal gambling and adult-content apps.[23,24,25]

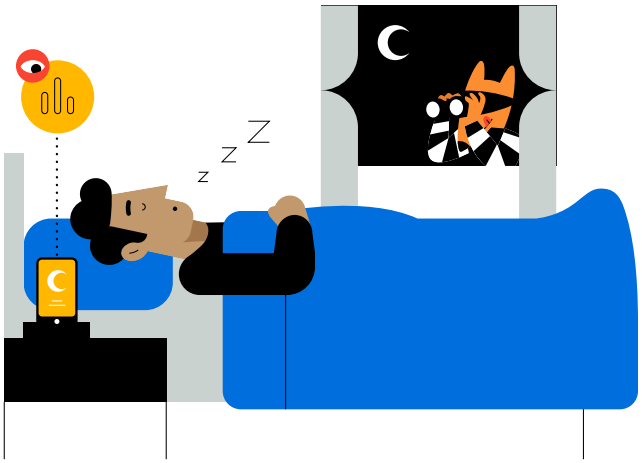


John unknowingly downloads a pirated app from a third-party app store

John's friend loves a fitness app she's been using and she sends him a referral for him to try it out. But the referral only works if he downloads the app through a third-party app store, not through the App Store. He downloads the app, signing up for a monthly subscription. However, what neither of them had realized was that this app had been pirated. That means that the money he pays every month is not going to the developer who designed and built the app, but rather, going to the scammers who stole the app. John believed he was doing the right thing – supporting the developer of this awesome fitness app – but instead he was lining the pockets of scammers, unknowingly supporting a fraudulent scheme that deprives developers of their earnings.

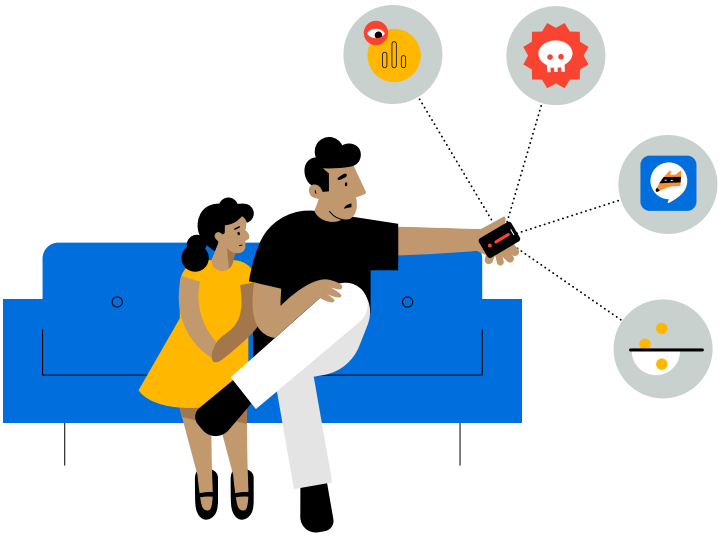
Learn more about Apple's privacy protections

To learn more about how the App Tracking Transparency and privacy labels on the App Store give you control and transparency on how apps collect and use your data, read **A Day in the Life of Your Data** and visit **apple.com/privacy/control.**



A sideloaded app violates John's privacy

John heard about a new sleep tracking app that he'd like to try, but it is not available on the App Store. He downloads it from a third-party app store, signs up using his email address, and starts using it to monitor his sleep quality. The app claims that it keeps its users' health and usage data completely private, and does not link it with outside data or share it with third parties. However, this claim turns out to be completely false. Because the app was sideloaded, the app developer was free to do whatever they wanted, so the app tracked John using his email address without asking for his permission. This allows the developer to link his data with information collected from other apps and sell his health data to data brokers, without user permission and without having to worry about being stopped.



iPhone is used every day by over a billion people – for banking, to manage health data, and to take pictures of their families. This large user base would make an appealing and lucrative target for cybercriminals and scammers, and allowing sideloading would spur a flood of new investment into attacks on iPhone, well beyond the scale of attacks on other platforms like Mac. Scammers would be galvanized to develop tools and expertise to attack iPhone device security. The App Store is designed to detect and block today's attacks, but changing the threat model would bypass these protections. Scammers would then use their newly developed tools and expertise to target third-party stores as well as the App Store, which would put all users at greater risk, even those who only download apps on the App Store. The additional distribution channels introduced by sideloading provide malicious actors expanded opportunities to exploit system vulnerabilities, thereby incentivizing attackers to develop and disseminate more malware.

This means that users like John, who had grown to take the safety and protection of iPhone and the App Store for granted, would have to constantly be on the lookout for the ever-changing tricks of cybercriminals and scammers, never knowing who or what to trust. In some cases, John may have no choice but to take a risk by sideloading an app that is not available on the App Store from a third-party store, or he may be tricked into doing so. In the most serious cases, sideloaded apps pretending to be something they're not – for example, claiming to be an Apple software update or disguising their download page to look like the App Store – could attempt to break iPhone on-device protections to get access to protected data like messages, photos, and location. In light of all these risks and scams, John would be a lot more cautious about which apps to download. In the end, he would download fewer apps, and stick to those from a few trusted developers, making it harder for new, smaller developers to reach users with innovative new apps. He would not have the peace of mind that comes with knowing that apps on his iPhone are the safest options for him and his daughter.

Did you know?

Users who are worried about their security and privacy are more likely to download fewer apps and to delete apps from their devices.[26,27,28] A less secure ecosystem, in which users do not feel safe downloading apps, could mean users are less likely to try out innovative new apps or take a chance on apps coming from new or lesser-known developers. This could blunt the growth of the app economy, harming both users and developers.

Apple's security layers and App Review protect John, Emma, and their devices

To protect iOS users from malicious apps and provide the world's best platform security, we take a multi-pronged approach, with many layers of protection. iOS poses unique security challenges because users continuously and frequently download new apps onto their devices, and because iOS devices need to be safe enough for children to use unsupervised. This means that we take a heightened approach to security on iPhone compared to Mac, because the population of users, as well as their behaviors and expectations, are different.

- **As on Mac, we use automated software to scan apps for known malware, preventing them from ever making it onto the App Store and thus ever reaching or harming users.**
- **Additionally, app developers are required to submit a description of their app and its features.** This information is reviewed by a team of experts for accuracy during the App Review process, and is presented to users when they evaluate whether to download an app. This process creates a high barrier against the most common scams used to distribute malware: misrepresenting the malware as a popular app, or claiming to offer enticing features that are not actually provided.
- In addition to verifying whether the app's features work as described and whether the app's App Store page is accurate, **these experts also manually check that the app doesn't unnecessarily request access to sensitive data and evaluate that apps targeted at children comply with stringent data collection and safety rules.**
- **In cases where an app makes it into the App Store but is later discovered to violate our guidelines, we work with the developer to quickly resolve the issue.** In dangerous cases, involving fraud and malicious activity, the app is immediately removed from the App Store and users who downloaded the apps can be notified of the app's malicious behavior.
- **If a user has an issue with an app downloaded from the App Store, Apple Care is available to provide support and issue refunds.**

The goal of App Review is to ensure that apps on the App Store are trustworthy and that the information provided on an app's App Store page accurately represents how the app works and what data it will access. We are constantly improving this process: we update and refine our tools and our methodology continuously.

Once users download an app through the App Store, they are able to control how that app functions and what data it is able to access, using features such as App Tracking Transparency and permissions. Parents can further control what their kids buy with the Ask to Buy feature, how much time they spend on certain categories of apps with Screen Time features, and what data they share. Users are also able to centrally manage all app-related payments, and are able to easily view and cancel subscriptions that are paid for via In-App Payments. These controls could not be fully enforced on sideloaded apps.

In addition to the protections provided by App Review, we design our devices' hardware and software to provide a last line of defense in case a harmful app is downloaded on the device. For example, apps downloaded on iPhone from the App Store are "sandboxed," meaning they are not able to access files stored by other apps or make changes to the device unless explicitly permitted by the user.

The best defense relies on a combination of all layers – robust App Review to help prevent the installation of malicious apps, and robust platform protections to limit the damage malicious apps can inflict. The security designed into iOS provides users with powerful protections that are the best of any consumer device, but those protections are not engineered to protect against choices a user might be tricked into making. App Review gives teeth to App Store policies designed to protect users from apps that may attempt to harm them or trick them into granting access to sensitive data. And, in the very serious instances of malicious apps trying to bypass on-device protections, App Review makes it harder for them to get on users' devices in the first place.

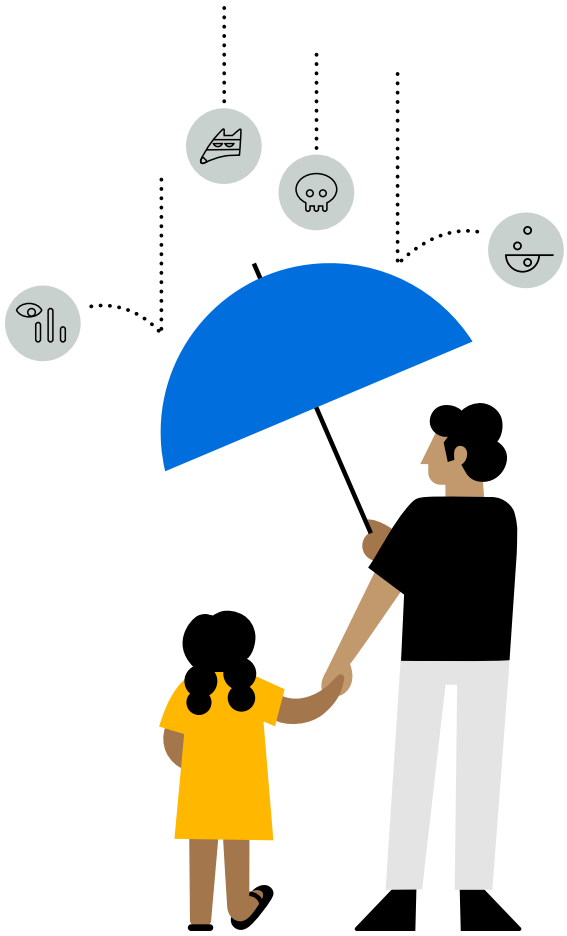
The end result is that security experts agree iPhone is the safest, most secure mobile device. Apple's many layers of security provide users with an unparalleled level of protection from malicious software, giving users peace of mind.

App Review

Through the App Review process, we work to ensure apps come from vetted sources and are free of known malicious components. We also check that the apps aren't trying to trick you into making unwanted purchases or providing access to personal data. We screen developers and users, expelling those who misbehave. While App Review processes do not prevent the distribution of every single low-quality app, we continue to innovate and improve its technology, practices, and processes.

Apple's app protections in action in 2020

- **100,000 new apps and updates are reviewed every week** on average by a team of over 500 dedicated experts, who review apps in different languages.
- **Nearly one million problematic new apps and a similar number of updates were rejected or removed:**
  - More than 150,000 for being spam or copycats, or misleading users
  - More than 215,000 for violating privacy guidelines
  - More than 48,000 for containing hidden or undocumented features
  - About 95,000 for fraudulent violations, predominantly for including "bait and switch" functionalities to commit criminal or other forbidden actions
- **Apple stopped over $1.5 billion in potentially fraudulent transactions.**
- **Apple expelled 470,000 teams from the Apple Developer Program for fraud-related reasons.** It also rejected nearly 205,000 developer enrollment attempts over fraud concerns.
- **Apple deactivated 244 million customer accounts due to fraudulent and abusive activity, including fake reviews.** It also rejected 424 million attempted account creations due to fraudulent and abusive patterns.



App Review gives John peace of mind when he downloads apps

The App Store security and privacy features give John peace of mind when he downloads apps for himself and his daughter. He knows that Apple screens 100% of apps on the App Store for known malware, and that, compared to other devices, it is extremely rare for users to encounter malicious software on iPhone.

Learn more about Apple's protections

To learn more about how Apple protects your security and privacy on the App Store, visit **apple.com/app-store.**

To learn more about how Apple protects your location data, read the **Location Services White Paper.**

To learn more about parental control on iOS, visit **apple.com/families.**

Frequently Asked Questions

What is sideloading?

"Sideloading" is the process of downloading and installing apps on a mobile device from a source other than the official App Store, such as a website or third-party app store. To protect user security and privacy, we designed iPhone from the beginning not to allow sideloading for everyday users.

What is a threat model?

A threat model is the set of attacks and vulnerabilities that users need to be safeguarded against. Different devices, users, and environments have varying threat models, and security needs to be built with this in mind. The App Store is a crucial component of protecting against the iPhone threat model. It is a trusted place for users to securely download apps that are reviewed by Apple, from known developers who must abide by Apple's guidelines.

Would allowing sideloading from websites and third-party app stores on iPhone threaten users who only download apps from the App Store?

Yes. By providing additional distribution channels, changing the threat model, and widening the universe of potential attacks, sideloading on iPhone would put all users at risk, even those who make a deliberate effort to protect themselves by only downloading apps through the App Store. Allowing sideloading would spur a flood of new investment into attacks on iPhone, incentivizing malicious actors to develop tools and expertise to attack iPhone device security at an unprecedented scale. Having developed expertise in ever more sophisticated attacks, malicious actors would use it to target third-party stores as well as the App Store, putting all users at greater risk. Additionally, even users who prefer to only download apps from the App Store could be forced to download an app they need for work or for school from third-party stores if it is not made available on the App Store. Or they could be tricked into downloading apps from third-party app stores masquerading as the App Store.

What is Apple's App Review process?

We use a combination of sophisticated technology and human expertise to carefully review every app and every update to evaluate whether they adhere to the App Store's strong guidelines on privacy, security, and safety. We rely on human expertise when automated review is not enough to detect specific issues, such as privacy violations or apps for children that do not adhere to our strict guidelines. The guidelines have changed over time to respond to new threats and challenges, with the goal of protecting users and providing them with the very best experience on the App Store. 100,000 new apps and updates are reviewed every week on average by a team of over 500 dedicated experts around the world.

What is being reviewed?

All apps and updates submitted to the App Store are subject to the App Review process.

What parental controls are available on Apple devices?

We design features that allow parents to have control over how kids use devices. Screen Time gives parents a better understanding of the time kids spend using apps, visiting websites, and using devices. Screen Time also lets parents set the amount of time kids can spend each day on categories of apps and websites. Additionally, Ask to Buy allows parents to approve or decline kids' app purchases and downloads right from their device. Ask to Buy has a fifteen-minute timeout to prevent subsequent purchases.

What are App Tracking Transparency and privacy labels on the App Store?

These new features provide users greater control over their data and their privacy. App Tracking Transparency requires apps to get the user's permission before tracking their data across apps or websites owned by other companies. With privacy labels on the App Store, we require every app on the App Store to give users an easy-to-view summary of the developer's privacy practices, giving users key information about how an app uses their data.

Sources

1. Jobs, Steve, "Third Party Applications on the iPhone," October 17, 2007, accessed via tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

2. ENISA, "Vulnerabilities - Separating Reality from Hype," *European Union Agency for Cybersecurity*, August 24, 2016.

3. Griffin, Robert Jr., "Study on Mobile Device Security," *U.S. Department of Homeland Security*, April 2017.

4. Nokia, "Threat Intelligence Report 2020," *Nokia*, 2020.

5. Johnson, Dave, "Can iPhones get viruses? Here's what you need to know," *Business Insider*, March 4, 2019.

6. Symantec, "Internet Security Threat Report, Volume 23," April 2018.

7. Golovin, Igor, "Malware in Minecraft mods: story continues," *Kaspersky*, June 9, 2021.

8. Lunden, Ingrid, "Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations," *Tech Crunch*, October 23, 2020.

9. Henry, Josh, "Malicious Apps: For Play or Prey?" *United States Cybersecurity Magazine*, 2021.

10. Schwartz, Jaime-Heather, "How to protect your Android phone from ransomware – plus a guide to removing it," *Avira*, August 13, 2020.

11. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices," *ThreatPost*, June 24, 2020.

12. Owaida, Amer, "Beware Android trojan posing as Clubhouse app," *WeLiveSecurity by ESET*, March 18, 2021.

13. Desai, Shivang, "SpyNote RAT posing as Netflix app," *Zscaler*, January 23, 2017.

14. Peterson, Andrea, "Beware: New Android malware is 'nearly impossible' to remove," *The Washington Post*, November 6, 2015.

15. Palmer, Danny, "This Android trojan malware is using fake apps to infect smartphones, steal bank details," *ZDNet*, June 1, 2021.

16. O'Donnell, Lindsey, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks," *ThreatPost*, April 21, 2020.

17. Stefanko, Lukas, "Android Trojan steals money from PayPal accounts even with 2FA on," *WeLiveSecurity* by ESET, December 11, 2018.

18. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World," *Cybereason*, July 1, 2020.

19. Stefanko, Lukas, "New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor," *WeLiveSecurity by ESET*, June 24, 2020.

20. Yaswant, Aazim, "New Advanced Android Malware Posing as 'System Update'," *Zimperium*, March 26, 2021.

21. Aamir, Humza, "Beware of this newly discovered Android spyware that pretends to be a system update," *TechSpot*, March 29, 2021.

22. Koetsier, John, "The Mobile Economy Has A $17.5B Leak: App Piracy," *Forbes*, February 2, 2018.

23. Koetsier, John, "App Developers Losing $3-4 Billion Annually Thanks To 14 Billion Pirated Apps," *Forbes*, July 24, 2017.

24. Maxwell, Andy, "Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit," *TorrentFreak*, January 8, 2021.

25. Campaign for a Commercial-Free Childhood, "Apps which Google rates as safe for kids violate their privacy and expose them to other harms," December 12, 2019.

26. J.P. Morgan, "2020 E-commerce Payments Trends Report: Japan," *J.P. Morgan*, 2020.

27. Deloitte, "Trust: Is there an app for that? Deloitte Australian Privacy Index 2019," 2019.

28. Gikas, Mike, "How to Protect Your Privacy on Your Smartphone," *Consumer Reports*, February 1, 2017.