Safari Privacy Overview

Learn how the Safari web browser protects your privacy.

November 2019

Contents

Key Safari Privacy Features

Intelligent Tracking Prevention
Intelligent Tracking Prevention uses on-device machine learning to block cross-site tracking, while still allowing websites to function normally.

Smart Search field
The Smart Search field minimizes the amount of data passed to third-party search engines. It doesn't send precise location data or cookies along with search data.

Private Browsing mode
Private Browsing doesn't save browsing history, protecting a user's privacy from other users who may share the same device.

Seamless integration with Apple Pay
Apple Pay is a privacy-centric payment method that doesn't share credit card numbers with Apple or merchants, while offering industry-leading security.

Passwords and syncing
iCloud Keychain enables users to easily sync passwords, credit card numbers, and autofill information across devices while keeping that information secure and without signing users in to any other services.

Introduction

Safari is the built-in browser on Mac, iPhone, iPad, and Apple Watch. Fast and energy efficient, Safari delivers innovative features while also protecting user privacy. Safari is built to ensure websites keep working as expected while blocking unwanted cross-site tracking. Safari also minimizes the amount of data passed to third parties like search engines, and it provides many other features to help protect privacy like Private Browsing and secure password management. Safari protects privacy without requiring users to change the default settings.

Privacy by design

Safari has been designed from the ground up to protect user privacy. Key privacy features like Intelligent Tracking Prevention (ITP) and fingerprinting defense are turned on by default, so there is no need to make changes in Settings or Safari preferences to benefit from these privacy protections.

Safari minimizes the amount of data collected by Apple and shared with third parties. Where possible, Safari's privacy protections are designed to process data on device. For example, ITP uses machine learning to classify tracking data locally so that browsing history isn't sent to Apple. Safari also limits the amount of information passed to search engines when a user searches using the Smart Search field. And Safari is designed to provide users with transparency and control around data that is shared. For example, if a user visits a website that wants to access location using Location Services on the device, or use the camera or microphone, Safari will ask permission from the user before granting access. Users can also customize these settings for each website to allow, not allow, or ask each time the site is visited. Safari is designed to hide the user's identity when sharing information with Apple. Analytics data shared with Apple is not attached to identifying information and, in some cases, is protected using differential privacy, a technique that obscures individual information while allowing Apple to analyze broader trends in web-browsing behavior. And Safari implements security best practices to protect user data.

Protection from cross-site tracking

In the years since the web was created, technology has been developed to track user behavior across websites for advertising purposes. Users experience this tracking in action when they look at a product online and then ads for that product seem to follow them around the web. Tracking is pervasive; some websites include 100 or more trackers from different companies on a single page.

What are cookies?
Cookies are small data files that websites save on a device. They can be used for a variety of purposes, including saving sign-in information so that a user can navigate the web without having to sign in to the same sites over and over again. They can also be used to store information about where users have been on the web for cross-site tracking.

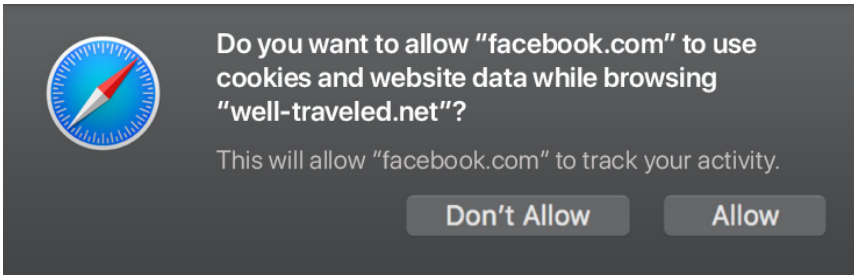
What are first-party and third-party cookies?
A cookie from a first-party website is saved to a user's device by a web page the user has visited. A third-party cookie is saved to the device by any other site or service, often for cross-site tracking.

Why is Intelligent Tracking Prevention necessary?
In 2005, Safari became the first browser to block third-party cookies by default. Since then, tracking companies have found new ways to track people using first-party cookies and other data. Intelligent Tracking Prevention was created to block tracking regardless of what kind of data is used.

Because tracking uses web technology that also provides features required for the proper operation of websites, simply blocking all of the functionality used for tracking can cause issues, including not being able to save sign-in information or remember items in a shopping cart.

In iOS 11 and macOS High Sierra, Safari added a feature called Intelligent Tracking Prevention to address this problem. The goal of ITP is to limit tracking while still enabling websites to function normally. ITP works by learning which domains are used to track a user and then immediately isolating and purging the tracking data that they attempt to store on the user's device. The process of learning about domains uses machine learning and happens on device, so it doesn't share the user's browsing history information with Apple. This on-device approach applies the same high standard to every website that is visited. And because ITP is turned on by default, there is no need to change anything in Settings or Safari preferences to receive tracking protection.

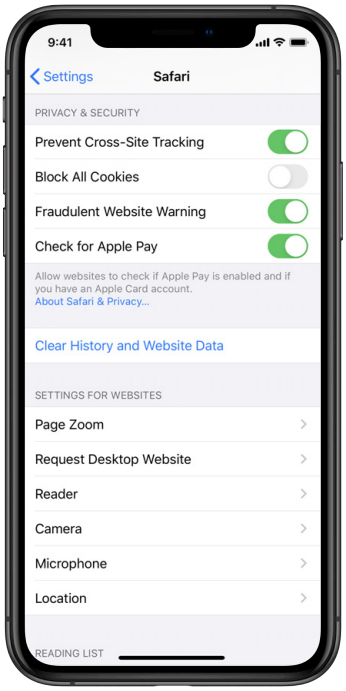
Social widgets embedded on other websites, such as Like buttons, Share buttons, and comment fields, can be used to track users even if they don't click them or use them. With ITP, Safari blocks this tracking by default, provides transparency and control, and asks users if they'd like to allow social widgets to access their identity. For example, if a user interacts with an embedded social plug-in, it can request access to the user's information with a permission dialog such as this:



Choosing Allow permits the social site to access the user's information while the user is browsing the news site. If the user navigates to a different site, the user will need to grant access again, which helps ensure that the user is in control.

Fingerprinting defense
In addition to blocking cookie-based tracking, Safari works to prevent advertisers and websites from using the unique combination of characteristics of a device to create a "fingerprint" to track the user online. Some of these characteristics include the device and browser configuration and the fonts and plug-ins that have been installed. To combat fingerprinting, Safari presents a simplified version of the system configuration to trackers so more devices look identical, making it harder to single one out. And unlike some other browsers, Safari doesn't add any custom tracking headers or unique identifiers to web requests. On other browsers, these headers can include things like location, sign-in status, account information, features enabled, and other data that can be used for cross-site tracking.

Privacy by default
Safari's key privacy features are enabled by default. For example, in iOS, Intelligent Tracking Prevention (shown in Settings as Prevent Cross-Site Tracking) is turned on by default. Camera, microphone, and location are set to ask for permission before granting access.



With macOS, Safari no longer supports most plug-ins, so they can't be used to attempt to uniquely identify a user. Fingerprinting protection is built into Safari and doesn't require any user action. Together, these anti-fingerprinting protections make a user's device look much more like other devices, providing "herd immunity" that dramatically reduces data companies' ability to identify a single device uniquely—and all without compromising the web-browsing experience. Apple believes the role of the web browser is to act as an agent on behalf of the user. This means that Safari will continue to evolve to prevent new forms of tracking.

Ad measurement that respects user privacy

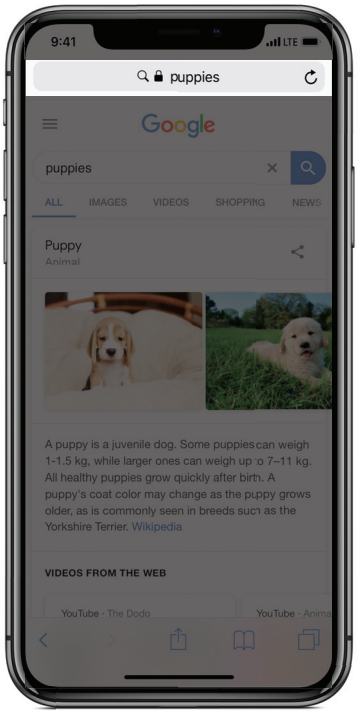
Apple understands that advertising is important for the economy of the web. Online advertising should not require privacy-invasive tracking and neither should advertising measurement. Unfortunately, ad click measurement has traditionally used tracking technology that infringes on user privacy. To address this, Safari now includes the ability to offer Private Click Measurement, an innovative way of doing ad click measurement that prevents cross-site tracking but still enables advertisers to measure the effectiveness of web campaigns. It is built into the browser itself and runs on device, which means that neither advertisers, merchants, nor Apple can see what ads are clicked or which purchases are made. This solution avoids placing trust in any of the parties involved—the ad network, the merchant, or other intermediaries—so none of them are able to track users as they click on ads and make purchases in Safari.

Private Click Measurement is built around a handful of privacy principles. First, a user should not be tracked for the purpose of ad click measurement. Second, only sites a user visits should be involved in measuring ad clicks and conversions—not third-party data companies. Third, the browser should act on the behalf of users and do its best to preserve their privacy. And fourth, the browser vendor should not learn about which ads users click or what they buy.

By allowing the browser to store information only on the device and report directly on the ad click, tracking technology is removed from the process. By limiting the amount of data collected by third parties, ad measurement is done in a privacy-preserving way without cross-site tracking. Matching of an ad click with a purchase is all done on device and is not reported to Apple.

Apple has proposed Private Click Measurement as a new web standard to the World Wide Web Consortium.

The Smart Search field and privacy
When a user searches using the Smart Search field, Safari doesn't send location or cookies to third-party search engines—just the minimum amount of information needed to complete the search.



Minimizing data sharing with the Smart Search field

The Safari Smart Search field enables a user to type website names, URLs, and search queries into one easy-to-use field at the top of the browser window. As the user types, it includes Safari suggestions for recommended websites, shows results from the user's bookmarks, history, and tabs, and provides relevant information from sources like Wikipedia.

To protect privacy, Safari limits the amount of data collected by the search engine when a user searches using the built-in Smart Search field. Safari sends only the minimum amount of information necessary to complete a web search to third-party search engines. For example, Safari doesn't send location or cookies, which can be used to track users across websites. In contrast, using the search bar on a search engine website may result in additional user information being stored.

Safari provides a choice of which search engine is used when typing search queries in the Smart Search field, including DuckDuckGo, a privacy-friendly option. Safari also offers search engine suggestions, provided by the default search engine provider, for completing searches as the user types. Users can turn off search engine suggestions in the settings for Safari, and no information will be sent to the default search engine until the Return key is tapped or pressed to send the full query. Similarly, in Private Browsing mode, Safari doesn't show search suggestions or pass any information to the default search engine while the user types in the Smart Search field.

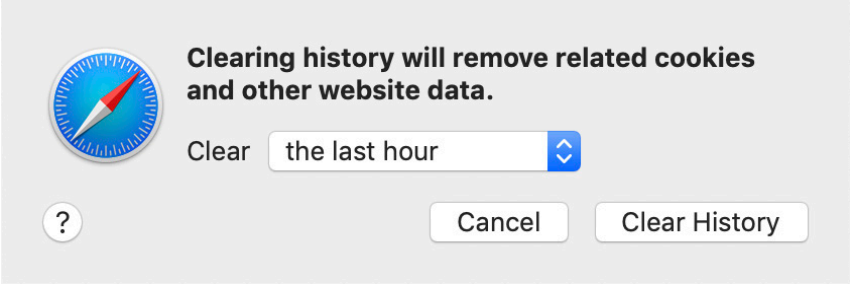
Browsing privately

Users sometimes want to keep their browsing data private from the people they share the device with or from people on a public device. Safari was the first browser to introduce a Private Browsing mode, which was first shipped in 2005. When a user searches using a Private Browsing window, Safari doesn't save a list of the web pages visited, add typed information to AutoFill, or store the list of downloads and searches in the Smart Search field (though downloaded items remain on the device). This means that users on a shared device won't be able to see which sites other users visited, what they searched for, or what they typed into web forms.

When in Private Browsing mode, browsing initiated in one tab is isolated from browsing initiated in other tabs, so websites can't track browsing across multiple sessions. And if iCloud Tabs sharing is used, Private Browsing windows are not passed to iOS devices or other Mac computers. Changes to cookies and other website data aren't saved, and extensions that support Private Browsing can stop storing data locally whenever the user has a Private Browsing window open.

Deleting history and other data

Outside of Private Browsing sessions, Safari saves history and website data to the device to enable helpful functionality, like allowing users to access their browsing history. This saved information includes a history of which pages have been visited, search history, as well as cookies and other website data like sign-in information. To provide the user control over what is saved on a device, Safari makes it easy to delete this data. With the Clear History feature, users can clear history and website data (including cookies) for the time period they choose.



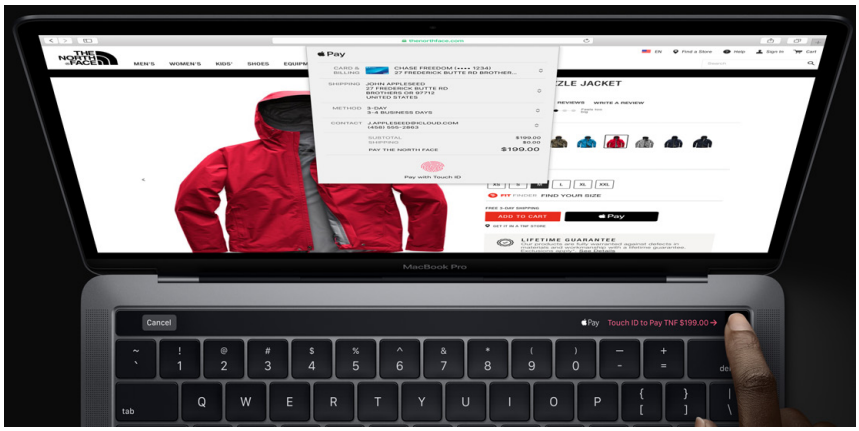
If Safari is enabled in the settings for iCloud and the user clears history and website data, history will also be cleared on other devices signed in to the same iCloud account. Website data will not be cleared on other signed-in devices. Clearing history won't change AutoFill information, and it will preserve content users have explicitly chosen to save, including their passwords, bookmarks, and Reading List items.

Secure payments on the web

Shopping online is one of the most common things that users do in a web browser. To make the process of paying easy, Safari provides seamless integration with Apple Pay, a payment method that is designed to protect privacy. In addition to web-based tracking, payments are also a major source of information for the data industry. For example, when a user makes a purchase with a physical credit card, information about the payment may be passed to companies that build profiles on users based on what they buy.

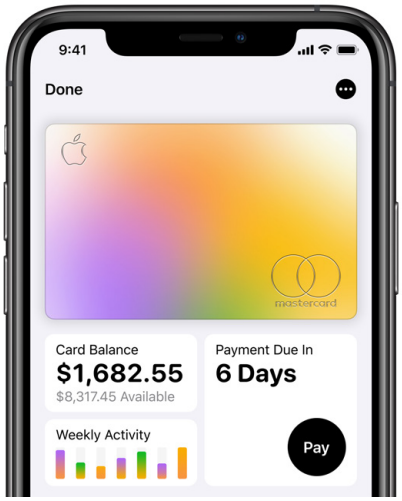
Many e-commerce websites now integrate Apple Pay, allowing users to pay by simply authenticating with their Apple device rather than entering their credit card information manually. For example, iPhone users can authorize Apple Pay using Face ID or Touch ID, and Mac users can authenticate using Touch ID on Mac models with the Touch Bar. For Mac models without Touch ID, the user can still complete the Apple Pay purchase using an iPhone or Apple Watch. When a purchase is made on a website using Apple Pay, a device-specific number and a unique per transaction security code are sent to the merchant rather than the actual credit card number and security code, so the user's real credit card information can't be compromised. And because card numbers are never shared with merchants, the actual card number can't be used to identify users across different websites. Apple Pay provides the merchant with only the minimum amount of information necessary to complete the transaction, such as a shipping address and the zip code to calculate tax and shipping, but not the billing address. Apple Pay also doesn't keep transaction information that can be tied back to the user. This further limits the amount of information that can be harvested by data companies during a purchase.

To protect users from unauthorized purchases, payments require biometric authentication using Face ID or Touch ID on device, which means that even if a user's iPhone, iPad, or Mac were stolen while unlocked, a thief wouldn't be able to make purchases.



To securely transmit payment information when paying on the web, Apple Pay receives the encrypted transaction and re-encrypts it with a developer-specific key before the transaction information is sent to the payment processor. This key helps ensure that only the website conducting the transaction can access

Apple Card
Apple Card has all the security of Apple Pay built in. Using Apple Card with Apple Pay is a great way to help keep transactions on the web private. As with all Apple Pay purchases, Apple won't know what a user bought, where the user bought it, or how much the user paid. And with Apple Card, our partner Goldman Sachs will never share or sell user data to third parties for marketing or advertising purposes.



the encrypted payment information. For additional security and to protect against fraud, websites must verify their domain every time they offer Apple Pay as a payment option. Apple sends the device account number to the website along with a transaction-specific, dynamic security code. Neither Apple nor the device sends the actual payment card number to the website, and the transaction-specific security code further protects against unauthorized transactions.

Sync and sign-in features that keep the user in control

Browsers are more convenient to use when information is synced across a user's different devices. For example, being able to access their history across devices means users can easily find the places that they've been on the web, regardless of whether they're on their phone or their computer. Safari provides a secure way to keep information in sync across devices while protecting privacy. Unlike other browsers, Safari doesn't have a browser-level sign-in that automatically signs the user in to all the browser vendor's online services. Instead, Safari enables users to easily sync passwords across devices while keeping their information secure using iCloud Keychain. iCloud sign-in is separate from other Apple sign-ins. This means that while other browsers may quietly sign in users to online services that track them, Safari helps users stay in control of where they're signed in.

iCloud Keychain also securely stores user names, passwords, and credit card numbers and keeps them up to date on a user's trusted devices. iCloud Keychain lets users autofill their information—like user names and passwords—on any device that they approve. It also stores credit card numbers and expiration dates so users can easily sign in to their favorite websites and quickly make online purchases if they choose to provide a credit card directly to the website. iCloud Keychain is end-to-end encrypted, so not even Apple can read the passwords stored there.

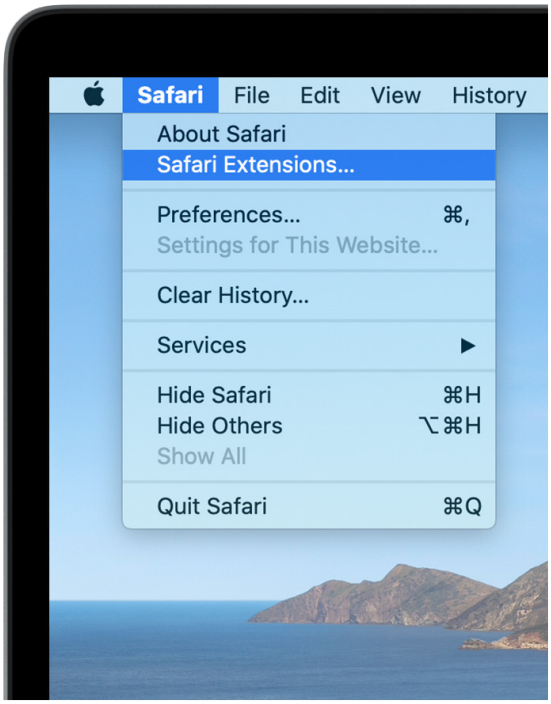
Safari also helps users create and manage passwords. When iCloud Keychain is enabled, Automatic Strong Password enables a user's devices to automatically create, sync, and enter unique strong passwords for sites and apps. Generated passwords are saved in a special Password AutoFill Keychain and synchronized across devices with iCloud Keychain. Saved passwords that have been used on more than one website or are considered weak are flagged so that users can easily update them to unique strong passwords. And if the user signs in to a website using a previously saved password that is very weak, the user is shown an alert strongly encouraging an upgrade to an Automatic Strong Password.

Providing the convenience and efficiency of one-tap sign-in while giving the user more transparency and control over personal information, Sign in with Apple is a privacy-friendly alternative to other single sign-on systems. Sign in with Apple allows users to set up an account and sign in to websites using the Apple ID they already have and gives them more control over their personal information. Websites can only ask for the user's name and email address when

setting up an account, and the user always has a choice: They can share their personal email address with an app or choose to keep their personal email private and use Apple's new private email relay service instead. This shares a unique, anonymized email address that forwards to the user's personal address so the user can still receive useful communication from the developer while maintaining a degree of privacy and control over personal information.

Extensions that respect user privacy

Safari Extensions are a great way to personalize the browsing experience and extend web browser functionality. Extensions can show helpful information about a web page, display news headlines, help users with their favorite services, change the appearance of web pages, and much more. The Safari browser extension architecture is designed with privacy in mind.



When installing an extension, users are informed about the information the extension can access. Content Blocker extensions, which allow users to block content and tracking data on websites, are enabled through APIs designed to protect privacy by disallowing the extension developer to access browsing data. And extensions that support Private Browsing can stop storing data locally whenever the user is in a Private Browsing window.

Improving Safari while respecting privacy

Analytics data helps Apple improve Safari when users share issues they experience with the product. Users are asked to opt in before analytics and usage data are collected, and data is sent to Apple with identifying information removed. The most sensitive information—such as the top-level domain of a website that has caused a crash—is collected using differential privacy, a technique that combines an individual user's information with that of many other users so that Apple can observe trends without identifying the browsing of any specific person. If users have opted in, they can view their analytics data that is sent to Apple in Settings in iOS and iPadOS, and in the Console app in macOS, and they can choose not to provide analytics data at any time.

Conclusion

Apple is committed to helping protect customers with leading privacy and security technologies that are designed to safeguard personal information. Safari is built with that commitment in mind. The following Apple privacy principles are deeply integrated into Safari:

- Minimize the amount of data collected by Apple and shared with third parties.
- Provide transparency and control around data that is shared.
- Protect the user's identity when sharing personal information—such as analytics data—with Apple.
- Implement security best practices to protect user data.

To learn more about Apple's commitment to privacy, go to apple.com/privacy.

© 2019 Apple Inc. All rights reserved. Apple, the Apple logo, Apple Pay, Apple Watch, Face ID, iPad, iPadOS, iPhone, Mac, macOS, Safari, and Touch ID are trademarks of Apple Inc., registered in the U.S. and other countries. Touch Bar is a trademark of Apple Inc. iCloud and iCloud Keychain are service marks of Apple Inc., registered in the U.S. and other countries. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. November 2019