

Google Chrome and Privacy

Last modified: March 20, 2012

Google Chrome provides users transparency and control over the information managed by the browser.

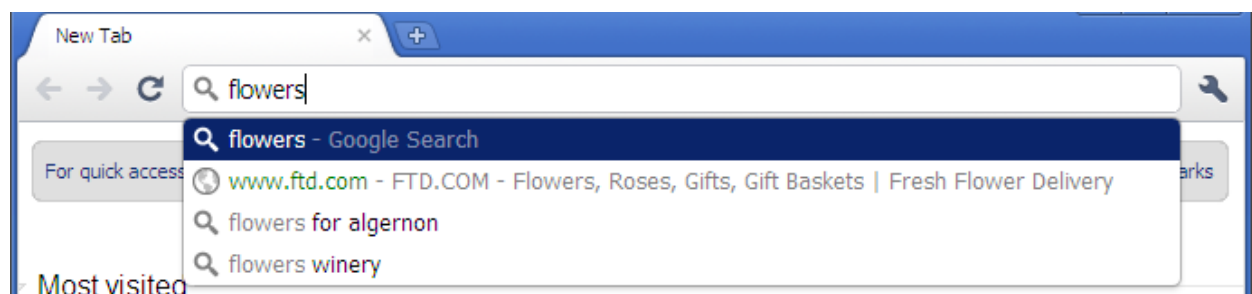
This document describes why, how, and when Google Chrome communicates with Google and your chosen default search engine, as well as how you can enable or disable certain features. Here we're focusing on the desktop version of Chrome. Details regarding Chrome OS can be found in the [Chromebook Privacy Notice](#).

If you have questions about Google Chrome and Privacy that this document doesn't answer, please contact the privacy team at privacy@chromium.org. We'd be happy to hear from you.

Omnibox Predictions

Google Chrome uses a combined [web address and search bar](#) (we call it the "omnibox") at the top of the browser window.

When you type in the omnibox, your [default search engine](#) can make searching faster and easier by automatically predicting websites and searches that are likely completions of what you have entered so far.



In order to provide the predictions, Chrome sends the text that you have typed into the omnibox to your default search engine. Your IP address and certain cookies are also sent to your default search engine with the request. You can [configure your default search engine](#) in Chrome's options.

If Google is set as your default search engine, then a randomly selected 2% sample of

requests are logged in order to help improve the prediction feature. Google drops cookies and the last octet of the IP address from these logs within 24 hours.

If you select one of the suggested queries, Chrome will send your original query and the position of the suggestion you selected, along with the search request. This information helps improve the quality of our suggestion engine, and is logged and anonymized in the same manner as [Google web searches](#).

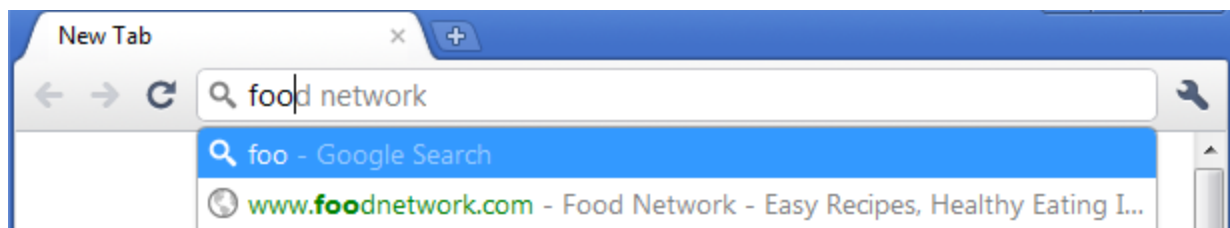
If you use a different search provider as your default search engine, your queries will be sent and logged under that provider's privacy policy.

You can [disable omnibox predictions](#) by unchecking the box in the “Privacy” section of the “Under the Hood” tab of Google Chrome's options.

Note: If you have the “[Chrome Instant](#)” feature enabled, the behavior of predictions in the omnibox will be different. This behavior is described in the “Chrome Instant” section, below.

Chrome Instant

The “[Chrome Instant](#)” feature is disabled by default but can be enabled from the “Basics” tab in [Chrome's options](#).



With Chrome Instant enabled, search results and in-line predictions appear instantly (before you press Enter) as you type in the address bar, if supported by your default search engine. The feature requests search results as you type, so the text you type may be logged as search terms. The specifics of the logging behavior depend on your default search engine.

If Google is your default search engine, the logging behavior is as follows: query text that you enter into the Omnibox is treated by default as “partial query data,” meaning that it is stored for up to two weeks and then deleted. The text is only treated as a full search if you either select a prediction from the address bar menu, explicitly submit a search by pressing

Enter, click on the search results page, or pause for three or more seconds without editing the query text.

For some helpful examples of Google's logging policies for Chrome Instant, see our ["Logging policies for Chrome Instant" help center article](#).

Google search locale

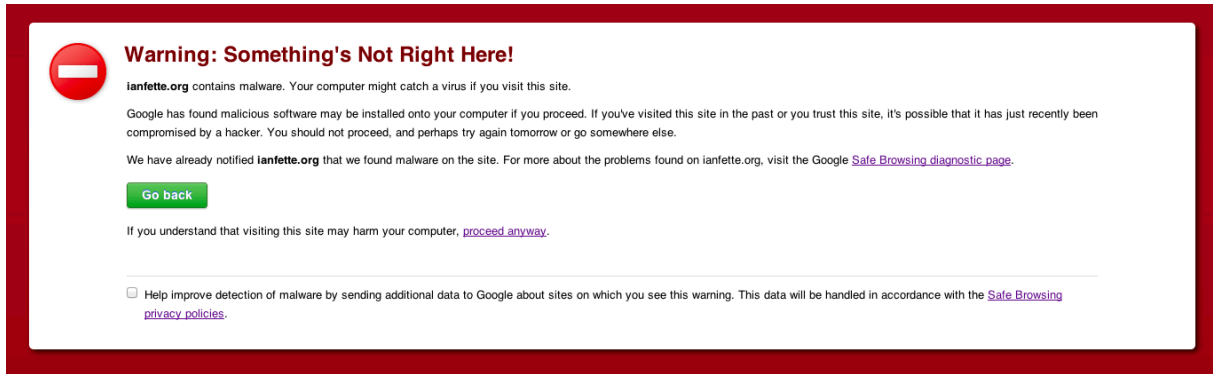
If Google is set as your default search engine, Chrome will try to determine the most appropriate local address for Google search queries conducted from the [omnibox](#). For example, if you were in Germany, this would cause your omnibox searches to go through google.de, instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTP request to google.com would be (see the [description of "server logs" in the Privacy FAQ](#) for details). If you do not have any cookies from google.com, this request will not create any.

Phishing and malware protection

Google Chrome includes a feature called Safe Browsing to help protect you against [phishing and malware attacks](#). This helps prevent evil-doers from tricking you into sharing personal information with them ("phishing") or installing malicious software on your computer ("malware"). The approach used to accomplish this was designed specifically to protect your privacy and is also used by other popular browsers.

Safe Browsing checks URLs against a list of known-bad websites that is maintained locally on your computer and updated regularly. If the URL matches against the local list, a partial fingerprint (a hash prefix) is sent to Google for verification that the URL is indeed dangerous. Chrome also contains some client-side logic that can detect bad behavior on sites that don't appear on the Safe Browsing list. If a site looks suspicious, Chrome will query Google with the full URL for further information. You may or may not get a warning depending on the combination of client-side checks and additional information available from Google's server-side data.



If you do get a malware warning, you can opt-in to send additional data to Google that helps us expand the coverage of the Safe Browsing service. If you opt-in, Chrome will send a report containing the URL and contents of the website, as well as the URL of the page which directed you to that site. While opted-in, this data will be sent every time you receive a malware warning in order to verify whether the site is still serving content that may exploit users. This data is sent over SSL, and includes neither data from sites you visit in Incognito mode, nor data originally sent over HTTPS. To see how this feature looks like you can visit our test page: <http://ianfette.org/>

Safe Browsing also checks the URL of executable files that you download against a list of known-good URLs maintained locally on your computer and updated regularly. Chrome trusts executables that match URLs in the whitelist, and also those downloaded from the local network, or signed by a trusted authority. Executables that don't fall into one of these buckets are considered untrusted. In this case Chrome sends the downloaded URL, a hash of the downloaded file, the IP of the download server, and the referer URL to Google for further verification.

For all Safe Browsing requests, the transferred data is logged in its raw form for up to two weeks. After at most two weeks, Safe Browsing will delete the raw logs, storing only calculated data in an aggregated form which does not include your IP addresses or cookies.

You can disable phishing and malware protection by [unchecking the box](#) in the "Privacy" section of Google Chrome's options. Please be aware that Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software if you disable this feature. We really don't recommend turning it off.

Navigation error tips

Google Chrome can show tips to help guide you to the page you were trying to reach in cases where the web address cannot be found, a connection cannot be made, the server returns a very short (under 512 byte) error message, or you've navigated to a parked

domain.

Google Chrome will first check the address against a locally-stored list of suspected parked domains. If there is a match, Chrome sends a partial fingerprint (a hash prefix) of the URL to Google for verification that the domain is indeed parked. This uses the same methodology as the Safe Browsing service (see the “Phishing and malware protection” section, above).

In the case of other navigation errors, the URL of the web page you're trying to reach is stripped of all GET parameters, and then sent to Google in order to retrieve navigation tips. This information is logged and anonymized in the same manner as [Google web searches](#). The logs are used to ensure and improve the quality of the feature.

You can [disable navigation error tips](#) by unchecking the box in the "Privacy" section of Google Chrome's options.

Google Update

Google Chrome uses [Google Update](#) to keep you up to date with the latest and most secure version of Chrome. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is [open source](#).

Google Update requests include information that helps us understand how many people are using Chrome and how often they use it. The information sent includes whether Google Chrome was used in the last day, the number of days since the last time it was used, and the total number of days that Google Chrome has been installed. Google Update also periodically sends a non-unique four-letter tag to Google which contains information about how you obtained Google Chrome. This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is shared with everyone who obtained Google Chrome the same way.

A similar system is in place to keep extensions and applications that you've installed via the Chrome Web Store up to date. These requests include similar information (the application id, when the application was last used, and how long it's been installed). We use these update requests to determine the aggregate popularity and usage of applications and extensions.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which is independently updateable. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (for example “fmeadaodfnidclnjhlkdgjkolmhmfofk”). Requests for component updates

contain these IDs and the components' versions -- as every installation uses the same ID, these are not personally identifiable.

Installed Applications and Extensions

Installing an application or extensions from the Chrome Web Store directly or via an [inline installation](#) flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you're logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

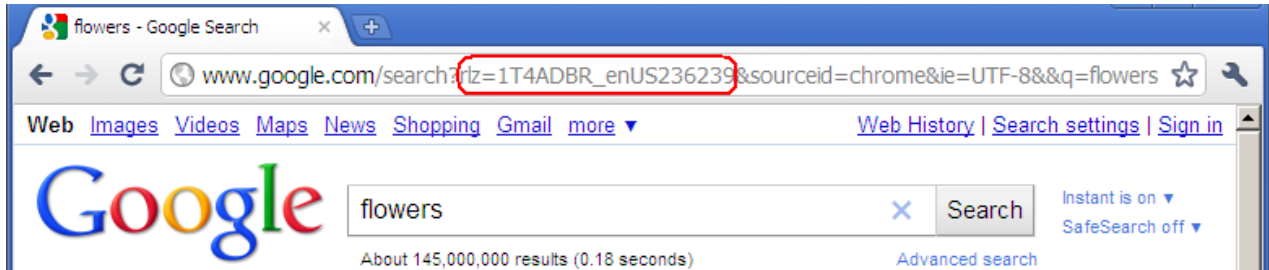
Installation token

In order to measure the success rate of Google Chrome downloads and installations, a randomly generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. It is generated for every install, is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

Promotional tags and tokens

Due to compliance with contractual obligations, installations of Google Chrome that are obtained from promotional campaigns send non-unique information regarding the campaign's effectiveness to Google. Installations of Google Chrome obtained by directly visiting www.google.com/chrome do not send this information.

The information includes a non-unique promotional tag that contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. The tag looks similar to "1T4ADBR_enUS236US239", and the article ["How To Read An RLZ String"](#) makes it clear exactly what information is being passed along. This non-unique tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to help us measure the searches and Chrome usage driven by a particular promotion.



Installations of Google Chrome obtained via promotional campaigns also send a token when you first launch Chrome and when you first search from Google. The same token will be sent if Chrome is later reinstalled and is only sent at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner.

Google Chrome uses a software library called "RLZ" to generate and send this information. The RLZ library was fully open-sourced in June 2010. For more information, please see the [In the Open, for RLZ](#) post on the Chromium blog.

You can opt-out of sending this information to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome.

Usage statistics and crash reports

You can opt-in to sending [usage statistics and crash reports](#) in Google Chrome. This feature is off by default.

Optional: Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. [Learn more](#)

Sending this information to Google helps us improve the features and stability of Google Chrome.

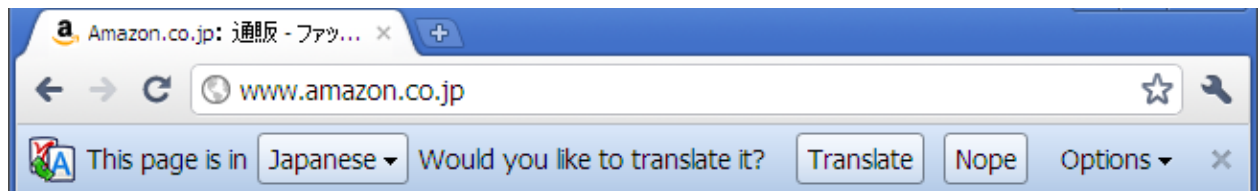
Usage statistics contain aggregated information such as preferences, user interface feature usage, responsiveness, and memory usage. These statistics do not include any personal information. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information depending on what was happening at the time of the crash.

If you enable this feature, Google Chrome stores a randomly generated unique token, which is sent to Google along with your usage statistics and crash reports. This token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics.

You can enable or disable the feature in the "Privacy" section of Google Chrome's options. Details are available in the ["Usage statistics and crash reports"](#) help center article.

Translate

Google Chrome's built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Automatic translation [can be disabled at any time](#) in Chrome's options in the "Web Content" section of the "Under the Hood" tab.

Language *detection* is done entirely using a client-side library, and does not involve any Google servers. For *translation*, the contents of a web page are only sent to Google if you explicitly decide to translate it by clicking "Translate" on the bar, or if you've previously chosen "Always translate" for a given language via the translate bar Options menu.

If you do choose to translate a web page, the text of that page is sent to Google's [translation service](#) for translation. Your cookies are not sent along with that request and, if the page you are on is encrypted with SSL, Google Chrome also sends the translation request over SSL. This communication with Google's translation service is covered by the [Google privacy policy](#).

Sign In to Chrome

Google Chrome provides the optional ability to [synchronize your browser state](#) (such as your bookmarks, themes, history, and extensions) across multiple computers via your Google Account. You can see what information is stored for your Google Account from the Chrome Sync section of the [Google Dashboard](#). Furthermore, using the same dashboard,

you can disable synchronization completely and delete all the associated data from Google's servers.

The feature can be enabled or disabled at any time in the "Sign In" section of the "Personal Stuff" tab of Chrome's options. Signing into Chrome will automatically log you into the associated Google Account, and allow you to choose which data types get synchronized and which don't. For example, you could choose extensions and bookmarks, but not themes.

If you choose to synchronize passwords, Chrome encrypts them with a key generated from your Google account's password before sending them over a secure SSL connection to Google's servers for storage. You may choose to set a distinct passphrase to perform this encryption instead. Note that when you set a distinct synchronization passphrase, encryption and decryption takes place entirely on your computer. Google never knows your passphrase, and if you lose it, Google can't help you retrieve your data.

Autofill

Google Chrome has a [form autofill feature](#) that helps you fill out forms on the web more quickly. Autofill is enabled by default, but can be disabled at any time in Chrome's options in the "Personal Stuff" tab.

If Autofill is enabled, and you encounter a web page containing a form, Chrome will send some information about that form to Google. This information includes a hash of the web page's hostname together with form identifiers such as field names, the basic structure of the form, and Chrome's guess at each field's data type (that is, "field X looks like a phone number, and field Y looks like a country"). This is necessary to help Chrome match up your locally stored Autofill data with the contents of the form, and to improve the quality of form filling over time.

If Autofill is enabled, and you *submit* a form, Chrome sends the data types you actually used for filling in the form in order to improve its guesses over time. The actual text you typed into the form is not sent.

You can manage your Autofill entries via [Chrome's options](#), and edit or delete saved information at any time. Chrome will never store credit card information without explicitly asking you and getting confirmation first.

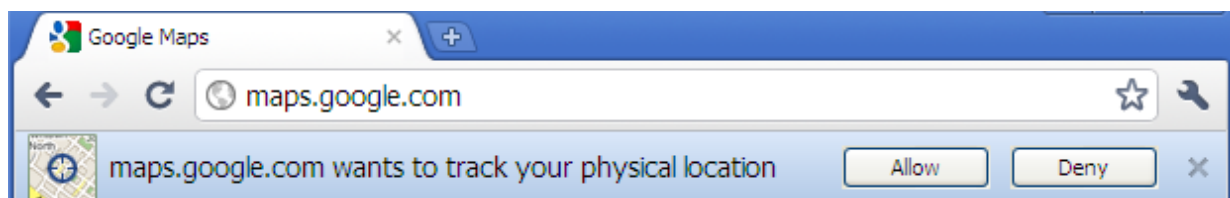
Also, if you choose, Autofill data can be [synced](#) as part of your browser settings (see the "Sign In to Chrome" section in this document). If you choose to sync autofill information,

the field values will be sent as described in “Sign In to Chrome”; otherwise, the field’s values are not sent.

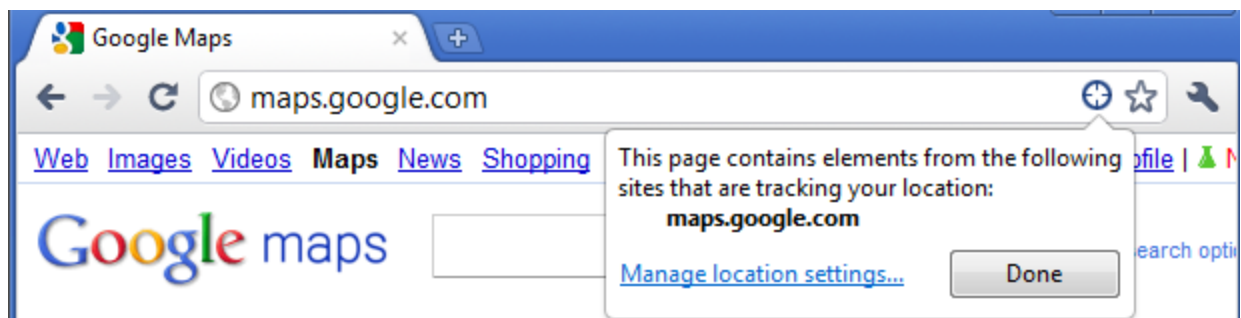
Geolocation

Google Chrome supports the [Geolocation API](#), which provides access to fine-grained user location information.

By default, Chrome always asks you when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.



Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In [Chrome’s options](#) in the “Under the Hood” tab, clicking “Content Settings” and scrolling to the “Location” section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

If you do choose to share your location with a web site, Chrome will send local network information to Google Location Services (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you’re not using them), and your computer’s IP address. The requests are logged, and aggregated and

anonymized before being used to operate, support, and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see ["Practical Privacy Concerns in a Real World Browser"](#) written by two Google Chrome team members.

Speech to Text

Chrome supports two mechanisms for converting speech to text: input elements that contain a `x-webkit-speech` attribute, and the [experimental speechInput extension API](#). Both of these mechanisms use Google's servers to perform the conversion. Using the feature sends an audio recording to Google, along with your default browser language and the language settings of the page that triggered the query. Cookies are *not* sent along with these requests.

If you have opted-in to sending usage statistics (see above), Chrome will send some additional information to help find and fix problems with the service, including the URL of the website using the API, your operating system, and the manufacturer and model of your computer and audio hardware.

Google Cloud Print

The [Google Cloud Print](#) feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google's servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google's servers.

A print job will be downloaded by either a Chrome browser ("Connector") or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP's ePrint, for example).

The print job is deleted from Google's servers when any of three criteria is met:

- 1) You delete the print job

- 2) The job has been printed and marked as printed by the printer/connector
- 3) The job has been queued on Google's servers for 30 days

You can manage your printers and print jobs on the [Google Cloud Print website](#).

SSL certificate error reporting

Chrome contains a list of expected SSL certificate information for a variety of high-value websites in an effort to [prevent man-in-the-middle attacks](#). For Google websites in particular, Chrome will alert Google to a possible attack by sending information about the SSL certificate chain to our security team if the certificate provided by the web server doesn't match the expected signature.

App Notifications

Applications installed in Chrome may send notifications if you allow them to. The notification's text is sent over a secure channel from the developer to Google, and then from Google to you. Google servers handle the notifications as plain text, and retain up to five notifications per application in order to ensure delivery to users.

If you opt-in to notifications for an application, Chrome provides the application with a "channel ID" which can be used to send you information. The same ID is returned to each application that uses notifications for a given user.