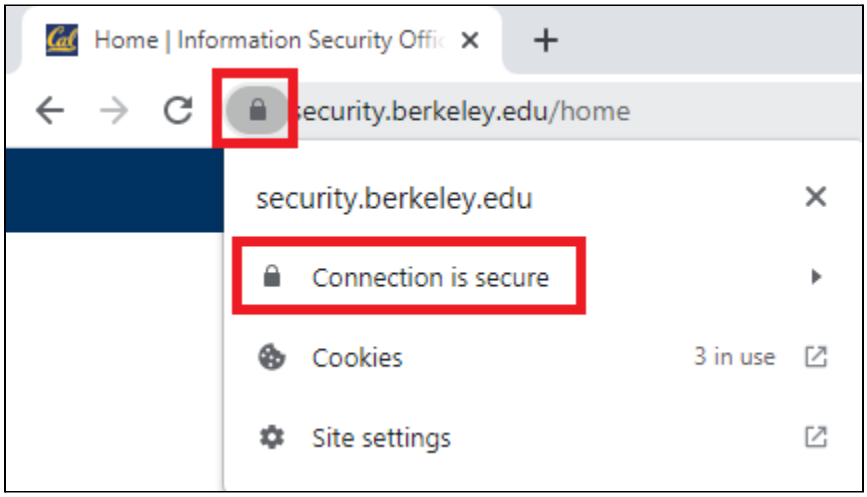
MSSND #4: Use of Authentication

Web Browsers: Chrome

Check for HTTPS

Always be certain that HTTPS is being used for the authentication session (look for a lock in the URL field); otherwise, credentials will be exchanged unencrypted and exposed to potential attackers.

1. **URL Bar > Check for Padlock**



Protecting your online accounts

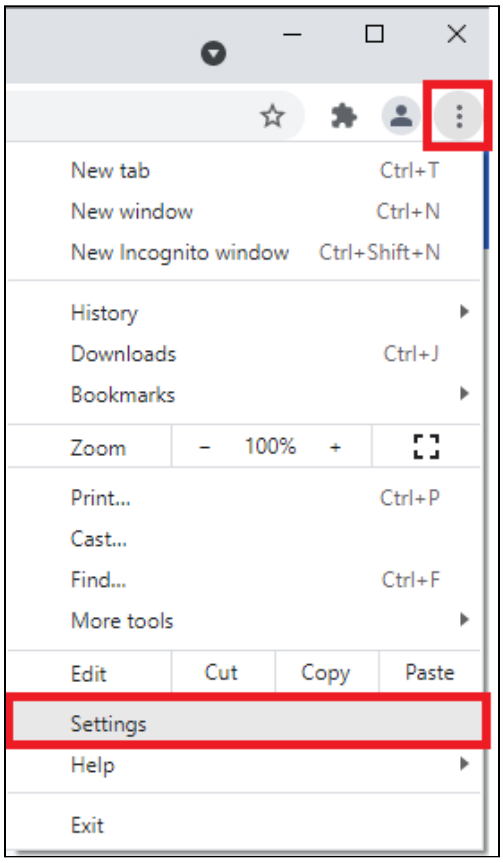
Authentication helps keep unauthorized people from using your online accounts. However, once you have signed into online accounts on a web browser, you might remain signed in even after you are done using the browser. If someone gets access to your device, they can then access your accounts through stored credentials in the web browser.

Steps you can take:

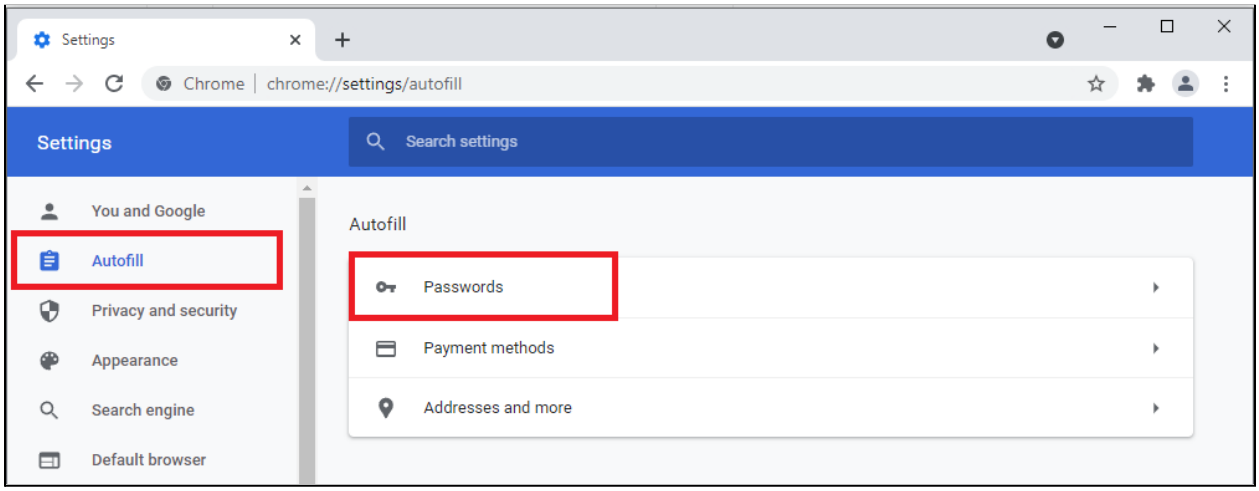
1. Turn off "Offer to save passwords" and save your passwords to a password manager
    - LastPass premium password manager is now available to students, staff, and faculty
        - LastPass is a browser plugin that allows you to securely save passwords and autofill them later
        - Go to https://calnetweb.berkeley.edu/calnet-me/lastpass-premium/lastpass-quick-start-guide
2. Clear the browsing data
    - This will remove stored passwords and other sign-in data, autofill form data (things you type into webforms, like your name and address), and other browsing history.
3. Use an incognito session instead
    - Chrome Incognito mode opens a private browsing session.
    - Chrome won't save your browsing history, cookies and site data, or information entered in forms.
    - It is important to close all incognito windows in order for your private browsing session to be closed. If an incognito window is left open on the device, your signed in accounts will still be accessible.

Turn off “Offer to save passwords”

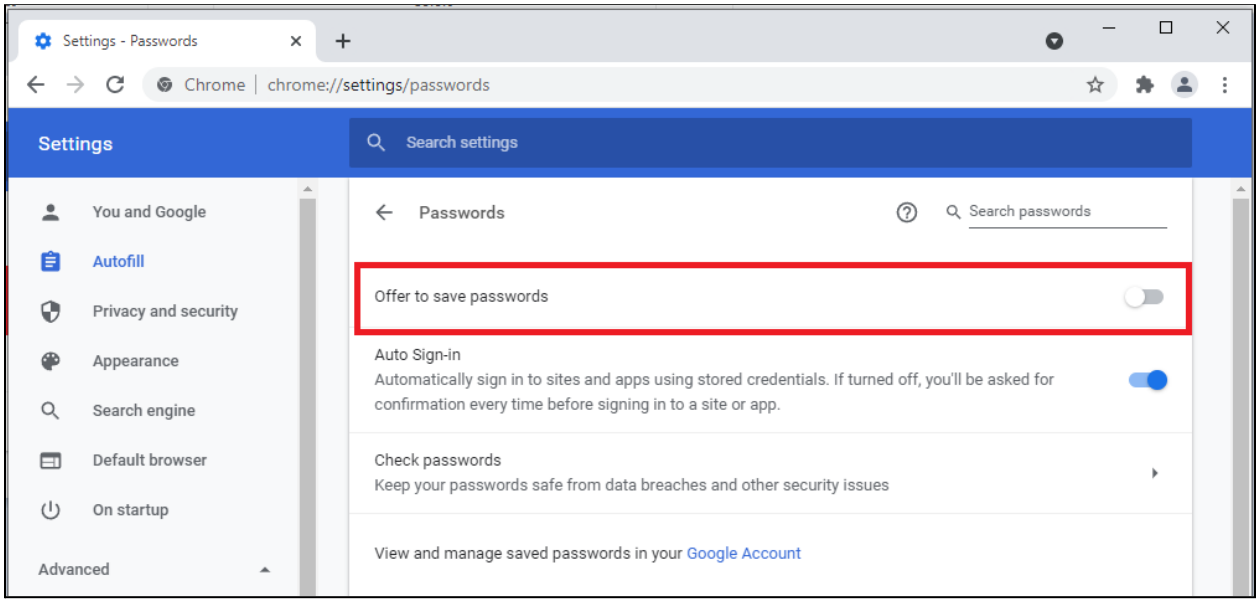
1. **Three dot menu > Settings**



2. **Autofill > Passwords**



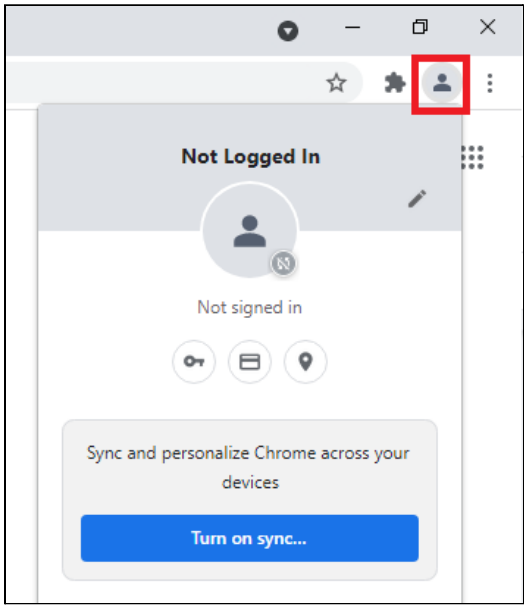
3. **Uncheck “Offer to save passwords”**



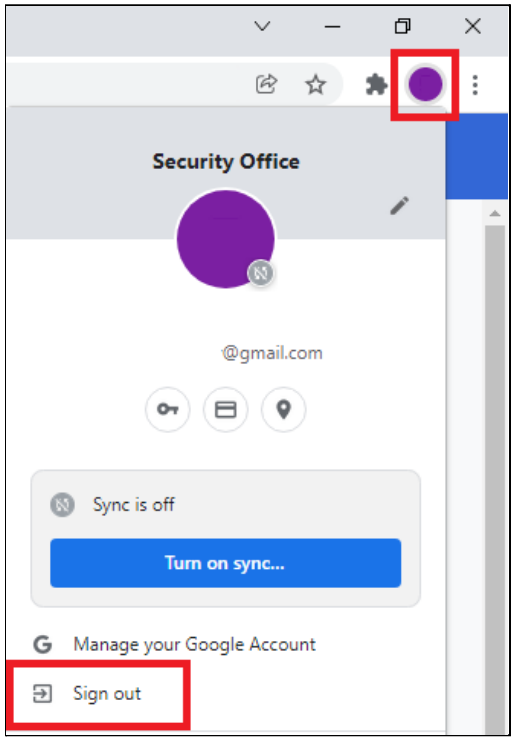
When to clear browsing data

Check if you are logged in to the browser, synced with the browser, or not signed in.

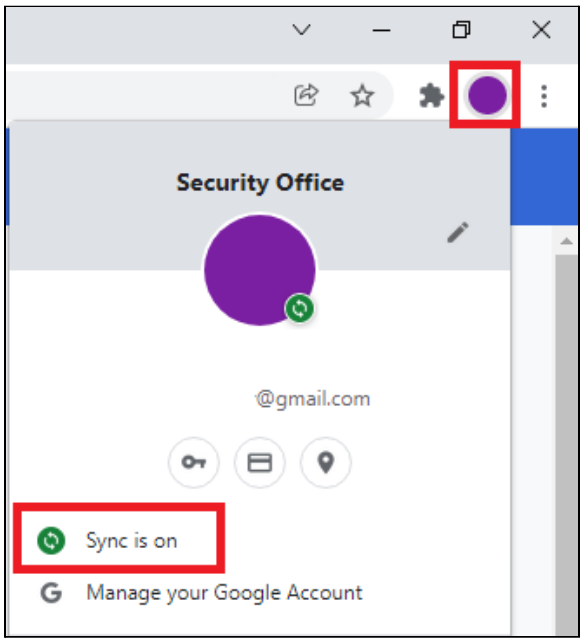
Not Signed In:



Signed In but Not Synced:



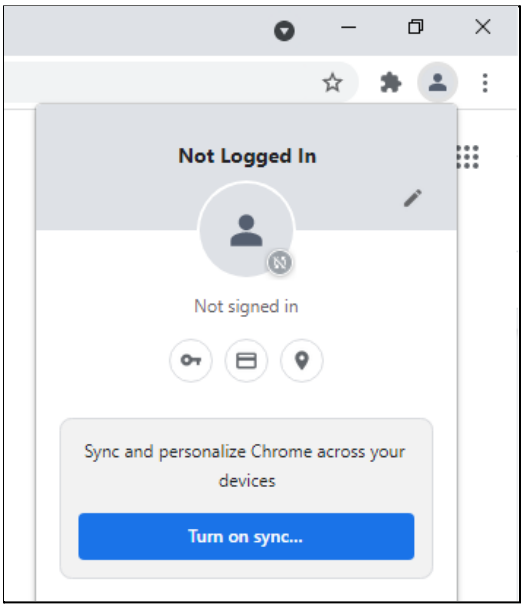
Signed In and Synced:



- If you are not signed in or synced, clear the browsing data
- If your account is signed in but not synced, sign out and clear the browsing data
    - Even after you sign out, your browsing data is stored with the web browser and must be cleared.
- If your account is synced with the browser, unsync your account. If you do this, you do not also need to clear browsing data
    - When your account is synced, your browsing data is stored with your account information in the cloud, and once you unsync the browser does not retain your browsing data.

Sign out of Google Chrome

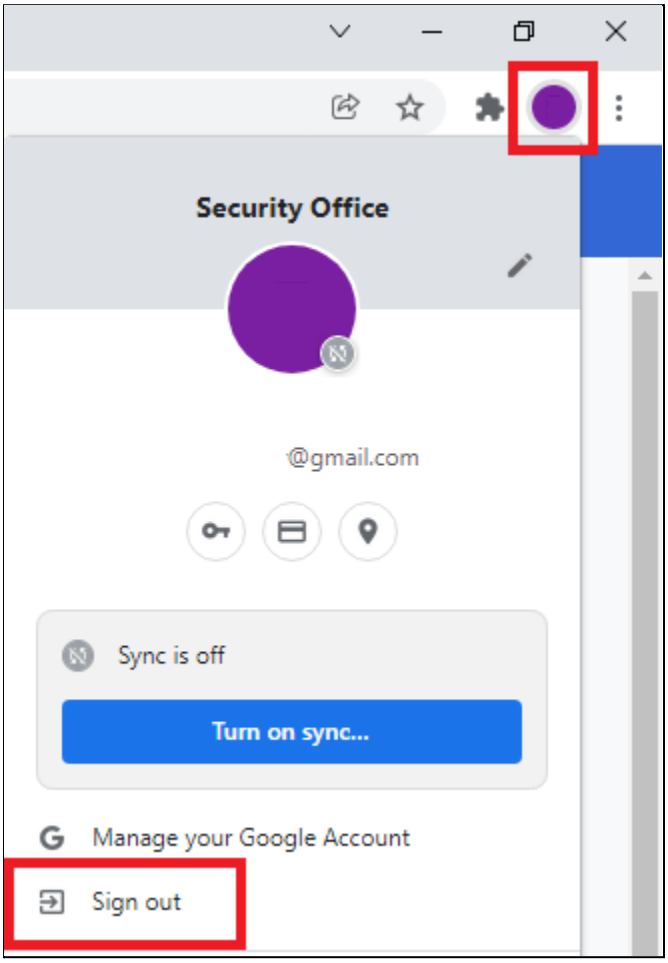
Not Signed In:



1. **Clear browsing data (see below)**

If your Google account is signed in but not synced:

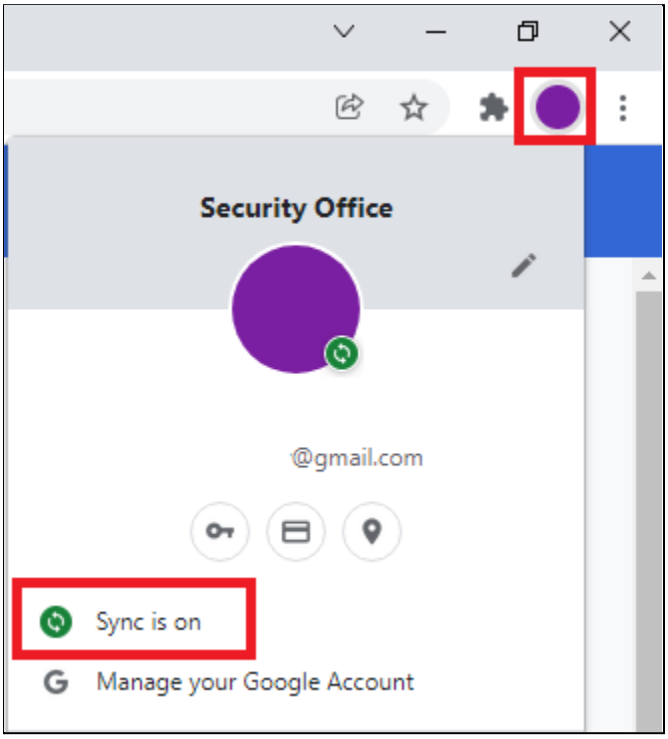
1. **User Icon > Sign Out**



2. **Clear browsing data (see below)**

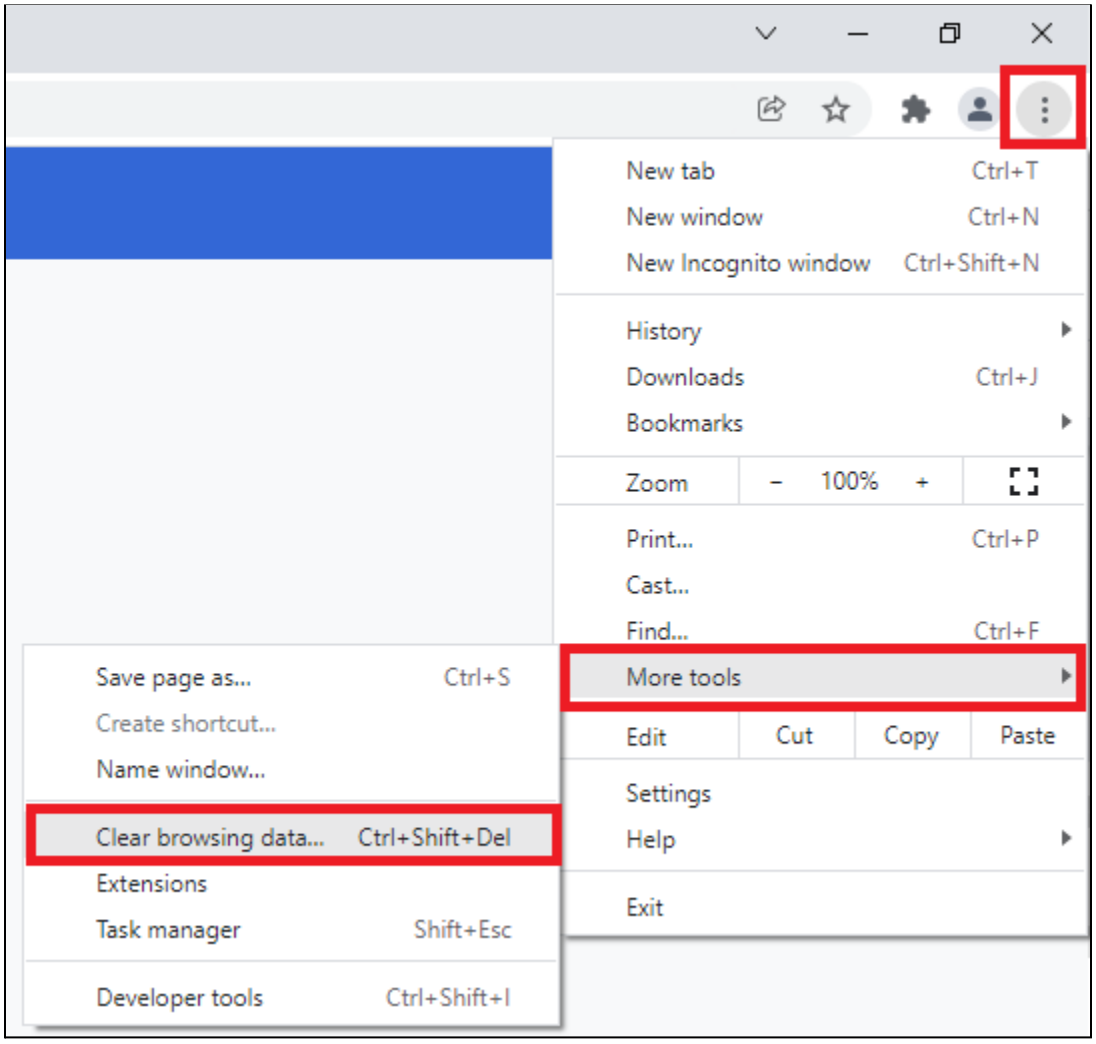
If your Google account is signed in and synced:

1. **User Icon > Sync is on > Turn Sync Off**

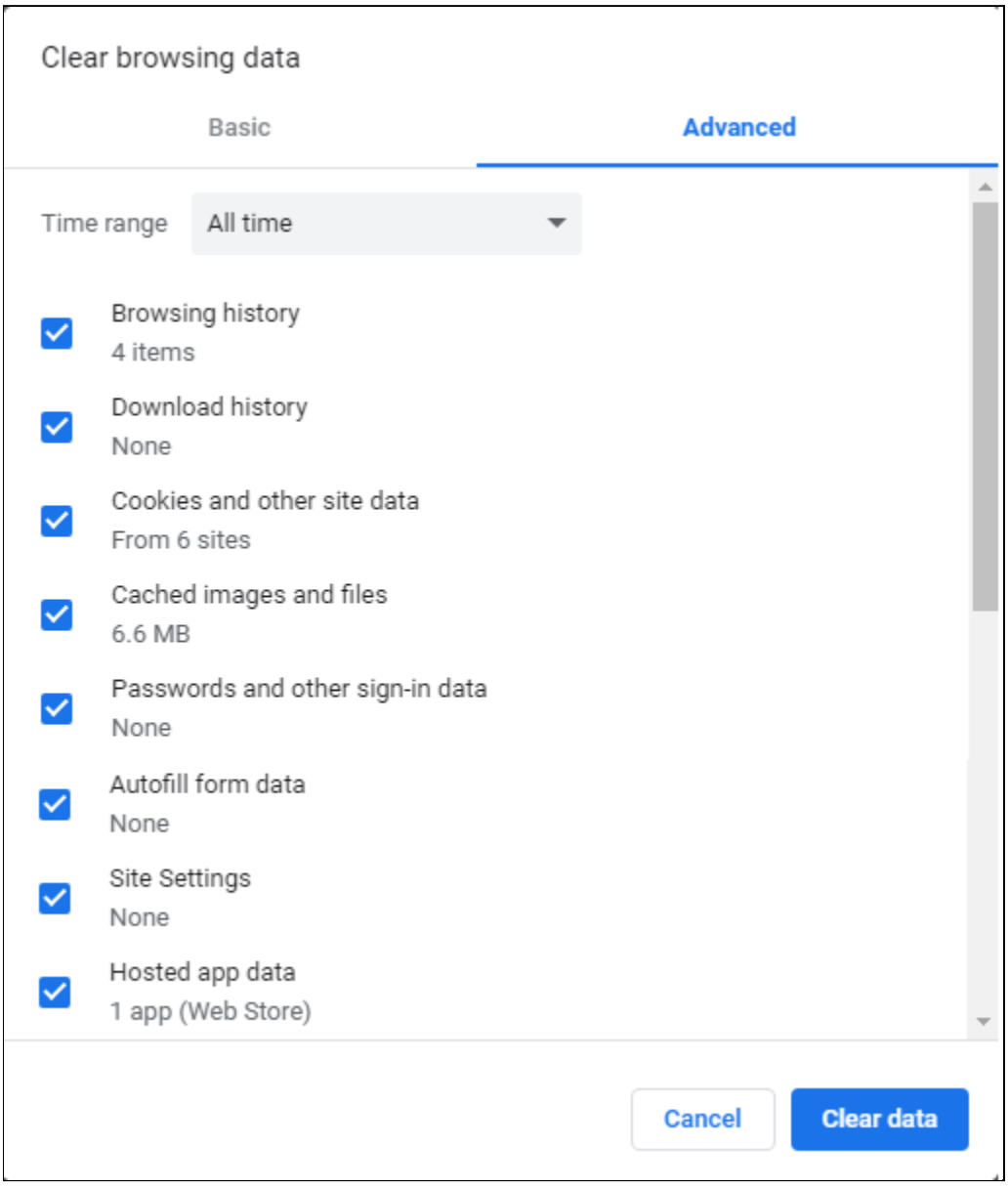


Clear browsing data

1. **Three dot menu > More tools > Clear browsing data**



2. **Advanced > Select all options > Time Range: All Time > Clear data**



Open an Incognito window

1. **Three dot menu > New Incognito window**