Here are some tips for protecting your privacy when using Google.
If you don't want Google to keep a record of the sites you visit, you can delete individual searches or all of your search history. You can also tell Google not to save your future activity.

To do this, choose "Your data in Search" in the Settings Menu. This will bring you to your "Search History" page.

On this page, click “manage your search history.” Here you can delete individual searches by clicking the X next to each one.

Next, click “Controls” in the left sidebar. Here you can click the button to tell Google not to save your history for websites and apps. You can also click on specific Google products (like Google Maps, Google Chrome, or Google News) to delete data from each of those.

You can find more options by clicking "manage all web & app activity.” Here you can turn on auto-delete, and select a time frame for deleting your older search history automatically.

Another thing to know is that you can search while signed out of your Google account, but your history can still be saved in your browser by the use of cookies. For a more private search, use "private browsing,” also called "incognito mode" in some browsers.

Most browsers have this choice in the "File" menu: select New Private Window. When you're browsing in this mode, there will be no cookies set, no browser or search history stored, and no information saved that you've entered in forms. This is handy especially when you share a computer with others in your household, who may want to snoop around in your search history.

One thing to know is that even in private mode, you are not completely private. Google reminds you of this on their help screens.
According to Google,
"Your activity might still be visible to: websites you visit, website you sign in to, your employer, school, or whoever runs the network you’re using, and your internet service provider."
This is because websites keep logs that list the IP addresses of computers that visit them. People responsible for a university or company network also keep logs. Your internet service provider keeps logs as well.

To keep your activity private from these sources, you'll need to use other tools, like a VPN or TOR.

VPN stands for “virtual private network.” It’s software that encrypts your internet traffic. This is especially useful when you’re on a public wifi network, such as a coffee shop or airport. You can use CEU’s VPN to connect securely to CEU’s network when off-campus. Remember that your VPN provider, such as CEU, can still see your traffic.

For a more complete level of privacy, it’s recommended to use software called TOR in addition to a VPN. TOR stands for “the onion router.” It’s a volunteer-run service that provides both privacy and anonymity online by masking who you are and where you’re connecting from. It can be slow, so it's not the best service for everyday browsing, but it is useful in certain situations.

Some people associate TOR with nefarious uses, but there are many legitimate uses for it. If you’re interested in learning more about this, see "Normal people use TOR," for examples of use by journalists, activists, whistleblowers, and business people doing competitive intelligence.

There are some additional privacy tools worth using. You can use private search engines like Duck Duck Go or StartPage. These engines don’t track your searches. On your mobile phone a good browser to use for private searching is Firefox Focus. This app comes with strong privacy protections turned on by default.
To learn more about search privacy, see the private browsing page of our guide, “Google Search Techniques.”