Cache

In computing, a cache (/kæʃ/ (About this soundlisten) kash,[1] or /ˈkeɪʃ/ kaysh in Australian English[2]) is a hardware or software component that stores data so that future requests for that data can be served faster; the data stored in a cache might be the result of an earlier computation or a copy of data stored elsewhere.
https://en.wikipedia.org/wiki/Cache_(computing)

By the way, not only browsers are caching sites, but also proxy servers are doing that. The proxy server loads the site once and on a repeated request it provides the users with a cached version of the page on the server. This significantly speeds up the loading of the website by the user. If someone replaces the site's cache at the server level, users can download a malicious version of the site. This attack is called Web Cache Poisoning, we will talk about it in more detail in the chapter on proxy servers.

Source: https://book.cyberyozh.com/security-professionals-point-view-about-browser-cache/

Incognito Window

Incognito mode stops **Chrome** from saving your **browsing** activity to your local history. Your activity, like your location, might still be visible to: Websites you visit, including the ads and resources used **on** those sites.
Incognito Mode is an excellent method of hiding your personal information from anyone else who is using the same computer as you do. Additionally, it is a smart way to avoid staying logged in while using public computers and networks. It's also a neat way to hide your browsing history from anyone who would frown upon some websites you are visiting.

However, it's important to remember that Incognito mode doesn't provide complete privacy. You can still leave a trace on your Google account if you log in during Incognito mode use. Furthermore, Incognito mode browsing is not the same as using a Virtual

Private Network. Incognito mode can cover your tracks, but only from those in your immediate vicinity. Therefore, browse carefully.
https://www.uscybersecurity.net/incognito-mode-are-you-really-incognito/#:~:text=Incognito%20Mode%20is%20an%20excellent,using%20public%20computers%20and%20networks.

Access control

Shared drives use a similar permission model as other content in Drive. Unlike files in My Drive, content located within a shared drive is owned by a group of users. For more information about permissions, refer to Share files, folders, and drives.
https://developers.google.com/drive/api/v3/about-shareddrives#:~:text=but%20not%20both.-,Access%20control,files%2C%20folders%2C%20and%20drives.

Google fully understands the security implications of providing cloud storage services and powering businesses in the cloud. One of the key questions to ponder when deciding to adopt Google Drive cloud storage is: Can you provide better security than the service provider when it comes to protecting your data? For many, the economics favor Google.

Google's robust global infrastructure, industry-leading knowledge in building secure cloud infrastructure and applications at scale, huge investment in data security, along with a high concentration of dedicated security expertise, puts them in a position to offer better security than the consumers themselves. For most computer users, Google Drive is more reliable, automatically backed up, relatively safe from ransomware, and almost certainly more secure from theft. In general, the benefits largely outweigh the risks.

When you upload files to Google Drive, they are stored in Google's secure data centers. Google Drive encrypts data at rest in the Drive, and data in transit to and from the Drive.

Google uses 128-bit or 256-bit AES keys (depending on the type of storage device) to encrypt data at rest in Google Drive, which helps in protecting the confidentiality of the data stored in Google Drive. But it's important to point out that Google is also in possession of the encryption keys, and can potentially decrypt your files at will.
https://www.comparitech.com/blog/information-security/google-drive-secure/#:~:text=For%20most%20computer%20users%2C%20Google,in%20Google's%20secure%20data%20centers.