Internet Applied (Settings & Security)

Browsing Data:

When you browse the internet, your internet browser will collect browsing data to optimize your user experience, and to provide information to the web services you are accessing.

Browsing data includes your browsing history, cookies, cache, and more, such as autofill settings and download history.

Browsing History

When you browse the internet, the browser stores a record of the websites you have visited. This is the browsing history.

This enables us to utilize the long press on the back button, or for Google to auto-fill websites as we begin to type them in the address bar.
It also enables Google to autofill certain fields, like your address or username for a particular website.

You may wish to view your browsing history to remember what webpage you visited last Tuesday to pay your bill, or to get back to a page that you accidentally closed out of.

Accessing your Browsing History

To access a log of your browsing history, click on the three dots next to your avatar in the top right corner of Chrome to access settings.

From there, you can select “History.” Alternatively, you can press the CTRL key and H.

You will now be shown a record of your browsing history. This is arranged reverse chronologically by date.
To access any link, simply click the title of the webpage.

You also have the option to use the search box to find an item in your browsing history. If you utilize this feature, know that it is not very sophisticated, so you’ll need to be as minimal as possible in your search.

Cookies and Cache

When you visit a website, information about your device, visit, and preferences are stored in a small document known as a **cookie**.

This is required when a webpage needs remember who you are and what you were doing to continue as you browse from page to page. For example, adding an item to your shopping cart, or logging into an account.

Cache is a memory of components on a webpage that you've visited. This memory is saved so that when you visit a webpage again it can load faster.

Clearing your Browsing Data

It is important to clean up your browsing data from time to time. This is a good habit to protect your personal information.

You may also wish to clear browsing data when:

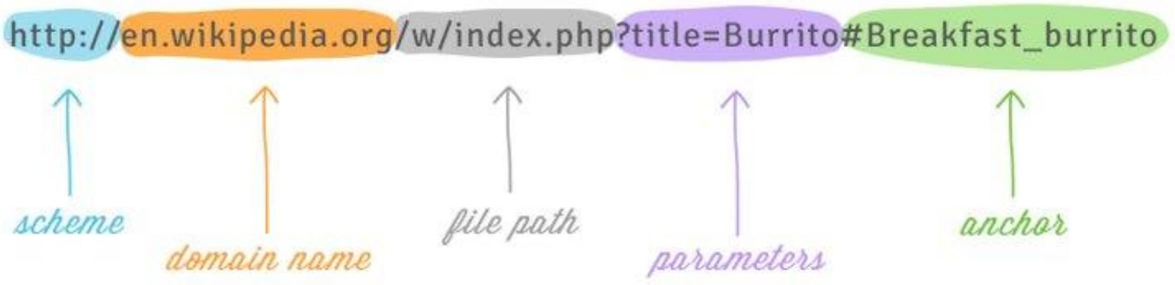
- You've logged in on a computer that doesn't belong to you,
  (The library computers do this automatically)
- You don't want websites to have information about your device, visit, or other parameters.
- You're having issues on a website page (especially on payment pages).
- Your browser is running slowly.
- You changed your login information.

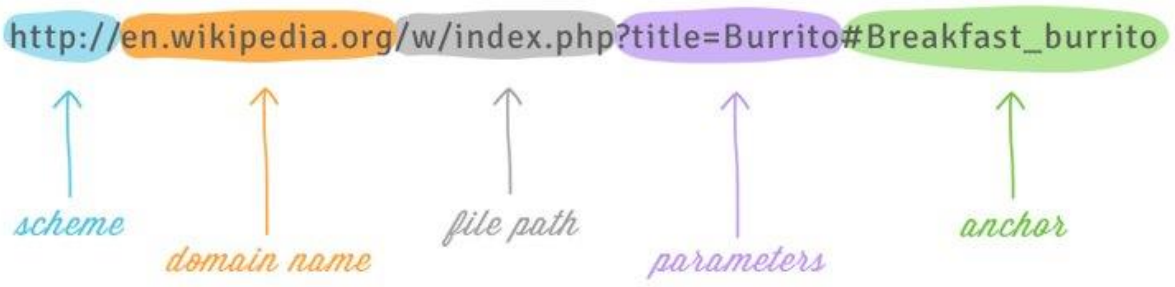
To clear your browsing data:

- Click on the three dots next to your avatar
- Click "Settings"
- Scroll down and click "Advanced"
- At the bottom of the section titled "Privacy and Security," select "Clear Browsing Data"
- Select how far back you would like it to go
- Click "Clear Data"

Understanding URLS

A URL is made up a few components.


http://en.wikipedia.org/w/index.php?title=Burrito#Breakfast_burrito
scheme
domain name
file path
parameters
anchor


http://en.wikipedia.org/w/index.php?title=Burrito#Breakfast_burrito
scheme
domain name
file path
parameters
anchor

(image via gcfglobal.org)

You won’t need to know all of these by name, but it’s helpful for you to begin to spot and understand the use of the domain name to ensure that you can locate the pages you’re trying to reach, and that you are navigating to legitimate websites.

Note that if you are given a very specific URL, you must **enter all of the parts exactly as they appear.** Google Chrome will do its best to help you, but for very specific URLs it's not always possible.

Checking the Link Destination on Search Results

Whether you're trying to type in a URL, or you are clicking on a link, you can get a really good idea of where you're going by knowing how to read the URL.

Scenario: I need for 1040 for federal taxes, I type in "1040 tax form" into the Google Chrome address bar. This pulls up a few search results. The top result sounds like it should be the most relevant, but when I look at the link destination, I see that it would take me to TurboTax to file online. The link I actually want (irs.gov) is the third result listed!

Checking the Link Destination on a Webpage or Email

Checking where your links go is not only a good practice for the safety of your personal information and device, it's also helpful when you aren't sure what to click on a page!

To check the destination of a link, hover your mouse over it, and look in the bottom right corner of the browser screen. You will be able to see the full URL. This works on most links (to webpages or downloads) and even on buttons.

HTTP vs. HTTPS

HTTP stands for Hypertext Transfer Protocol, whereas HTTPS stands for Hypertext Transfer Protocol **Secure.**

The places where your most sensitive data is stored (such as the login for your bank, loan providers, insurance providers, etc.) **can and should** have a https:// that proceeds the domain name.

Check your URL to ensure that this is present. This can also help protect you from websites that may seek to steal your information.

If you can't see it, you can check for a padlock on the left hand side of the address bar, or you can double click inside of the address bar to display the full URL including the URL scheme.

Phishing

Phishing is an attempt to secure personal information, such as login credentials, by baiting users to click on links and enter this information. These are usually in the form of email, but can also appear as ads.

Some attempts appear very obviously suspicious upon first glance, however others are trickier to spot. Learning to recognize attempts and practicing a healthy amount of skepticism while using the internet will help to protect your accounts and information.

If you ever receive an email and are genuinely unsure if it's a phishing attempt or not, try one of these:

- If the message is concerning an online account (accessed through a login) do not click the link in the email. Open a **new tab** and go directly to the website and log

in.
If there are any immediate actions you need to take, you will either see a message on the website or will be prompted to upon success log in.

- If it's something else and you're still not sure, ask a librarian!

Browser Extensions

Browser extensions allow you to customize your web browsing experience.

There are a variety of extensions out there, each with a specialized function (usually to enhance productivity).

- Social media (Pinterest, Facebook)
- Online Shopping (Amazon)
- Security extensions (password managers, ad blockers)
- And **many** more

Generally, most extensions through the Google Chrome webstore are safe and have been evaluated by Google. However, extensions can make your information vulnerable, because you are giving consent for the extension to view and access your information.

Keep the following in mind when using or installing browser extensions:

- Only add browser extensions that you directly access through the **Google Web Store**.
- The more extensions that you add to your browser, the more **vulnerable** your information is.
- **Research** your browser extension. Do you recognize the developer?
    - Many extensions require creating an account login associated with it to access the service, ensure you feel comfortable sharing what you do.
- **Remove** any extensions you aren't using.
- Extensions that provide free services (such as PDF editors) may simply be **free trials**.

(De Leon, Nicholas. Browser Extensions: How to Stay Safe. 2018, Nov. 9)

Using an Adblocker

Google Chrome by default will block most severely obtrusive and otherwise malicious ads. However, through normal web browsing you will still encounter many ads that may make it difficult for you to access content.

Consumer Reports has researched and evaluated several ad blocking extensions. Type in the link from the additional resources page to read more about the advantages and disadvantages of each of these ad-blocking extensions:

- Adblock Plus
- Disconnect
- Ghostery
- Privacy Badger
- UBlock Origin

Accessing the Web Store

To access the Google Web Store, click on the **three dots** next to your avatar to see the options menu.

Mouse over **More Tools** section, and click **Extensions** from the menu that pops out. Then click on the **three lines** in the top left corner.

There should be a link at the bottom of this sidebar that says **“Open Chrome Web Store”**

Viewing and Removing Browser Extensions

To access all installed browser extensions:

- Three dots by the avatar
- Select “More Tools"
- Select "Extensions" on the bottom left-hand sidebar

To remove an unwanted extension, click on "remove."

To turn an extension on or off, click on the switch in the bottom right of the content block.

Additional Resources:

https://www.consumerreports.org/digital-security/to-protect-against-websites-that-spy-on-you-get-an-adblocker/
A comprehensive comparison of adblocking extensions available, and a guide on how to use them from Consumer Reports.

https://www.consumerreports.org/digital-security/web-browser-extension-privacy-digital-security-advice/
An assessment on how an adblocking extension may protect your digital privacy, via Consumer Reports.

https://www.grahamcluley.com/good-idea-clear-browser-history-cookies/
A guide on how and why you should clear your browsing data from the browser.

https://www.consumerreports.org/money/how-to-protect-yourself-from-phishing/
A guide from Consumer Reports on how to spot and avoid phishing scams.

https://edu.gcfglobal.org/en/internet-tips/
A guide on tips for using the internet that covers many of the topics we did today.