HISTORY OF WEBBROWSER

* A web browser is a software application for retrieving, presenting and traversing information resources on the World Wide Web.
* It further provides for the capture or input of information which may be returned to the presenting system, then stored or processed as necessary.
* The method of accessing a particular page or content is achieved by entering its address, known as a Uniform Resource Identifier or URI.
* This may be a web page, image, video, or other piece of content.
* Hyperlinks present in resources enable users easily to navigate their browsers to related resources.
* A web browser can also be defined as an application software or program designed to enable users to access.

EARLY 1990s

* The first web browser, WorldWideWeb, was developed in 1990 by Tim Berners-Lee for the NeXT Computer (at the same time as the first web server for the same machine)[29][30] and introduced to his colleagues at CERN in March 1991.
* Berners-Lee recruited Nicola Pellow, a math student intern working at CERN, to write the Line Mode Browser, a cross-platform web browser that displayed web-pages on old terminals and was released in May 1991.
* Early web users were free to choose among the handful of web browsers available, just as they would choose any other application—web standards would ensure their experience remained largely the same.
* The browser wars put the Web in the hands of millions of ordinary PC users, but showed how commercialization of the Web could stymie standards efforts.
* Both Microsoft and Netscape liberally incorporated proprietary extensions to HTML in their products, and tried to gain an edge by product differentiation, leading to a web by the late 1990s where only Microsoft or Netscape browsers were viable contenders. In a victory for a standardized web, Cascading Style Sheets, proposed by Håkon Wium Lie, were accepted over Netscape's JavaScript Style Sheets (JSSS) by W3C.

LATE 1990s

* In 1996, Netscape's share of the browser market reached 86% (with Internet Explorer edging up 10%); but then Microsoft began integrating its browser with its operating system and bundling deals with OEMs.
* Within 4 years of its release IE had 75% of the browser market and by 1999 it had 99% of the market.
* Although Microsoft has since faced antitrust litigation on these charges, the browser wars effectively ended once it was clear that Netscape's declining market share trend was irreversible.
* Prior to the release of Mac OS X, Internet Explorer for Mac and Netscape were also the primary browsers in use on the Macintosh platform.
* Unable to continue commercially funding their product's development, Netscape responded by open sourcing its product, creating Mozilla.
* This helped the browser maintain its technical edge over Internet Explorer, but did not slow Netscape's declining market share. Netscape was purchased by America Online in late 1998.

IN 2000

* At first, the Mozilla project struggled to attract developers, but by 2002, it had evolved into a relatively stable and powerful internet suite.
* Mozilla 1.0 was released to mark this milestone.
* Also in 2002, a spinoff project that would eventually become the popular Firefox was released.
* Firefox was always downloadable for free from the start, as was its predecessor, the Mozilla browser.
* Firefox's business model, unlike the business model of 1990s Netscape, primarily consists of doing deals with search engines such as Google to direct users towards them – see Web browser#Business models.
* In 2003, Microsoft announced that Internet Explorer would no longer be made available as a separate product but would be part of the evolution of its Windows platform, and that no more releases for the Macintosh would be made.
* AOL announced that it would retire support and development of the Netscape web browser in February 2008.
* In the second half of 2004, Internet Explorer reached a peak market share of more than 92%.

Security:

Web browsers are popular targets for hackers, who exploit security holes to steal information, destroy files, and other malicious activities. Browser vendors regularly patch these security holes, so users are strongly encouraged to keep their browser software updated. Other protection measures are antivirus software and avoiding known-malicious websites. To ensure user safety and privacy, browsers may also need to execute a security policy to make sure that the specific web applications being accessed on the browser do not have any access to private areas of data.

Vulnerabilities:

Some of the main threats that web browsers seem to face are system compromises and data theft.When the system is compromised, the rendering engine is the main detector of this type of threat. Data theft describes the stealing of “local network or system data.”

Changes to Due to growing concerns about privacy, large companies like Apple and Google have started to hinder data for advertisers. In 2017, Apple released a new version of Safari that made it harder for advertisers to track people on websites. By 2023, Google plans to block cookie trackers on its own web browser, Google Chrome.

Data:

According to some privacy studies, major web browsers like Google Chrome and Apple Safari allow the companies that own the browser to track the locations and identity of the user. Other data that might be tracked through a web browser might include:

* Law enforcement tracking digital trails on web browsers to solve crimes.
* Web Analytics uses users’ data to improve performance on a web page.
* Advertisers use data to create targeted ads to increase user interaction.

Cookies:

First-Party Cookies:

First-party cookies are domain hosted and are used to provide a better web experience. These cookies also allow owners to collect analytics data and keep language settings.

Third-party Cookies:

Third-party cookies are a tool advertisers use to target ads on a web browser browser based on the customer's preferences and interests. Specifically, these types of cookies are used for tracking across websites sites and are created on a different domain than the website the person is visiting.Third-party cookies can also allow for services like live chats.