沒有 cookie 的網頁在關閉不會儲存任何與使用者相關的訊息，因此在沒有 cookie 的幫助下每次登入社群軟體都要重新輸入密碼，而 cookie 則可以儲存一些資訊以解決這個問題，在 cookie 到期之前都會記著使用者的資訊，除此之外 cookie 還有一些特性，例如：資訊儲存在客戶端、連線時會自動帶上及能夠設置專屬路徑，而利用設置到期時間這個特性也可以用來刪除 cookie。

然而這麼方便的功能仍有一些安全的隱憂，例如訪問 http 瀏覽器時，會自動將 cookie 回傳給伺服器，而 http 網頁並沒有加密，也就是以明文傳輸，因此黑客有可能截取使用者的資訊，然而使用加密的協議 https 仍然也有可能會被盜取資訊，因為黑客也有可能將他的伺服器偽裝成真正的伺服器，使用者則主動將 cookie 發給黑客的伺服器。

如果 cookie 的網域與使用者所瀏覽的網站網域相同，稱為第一方 cookie，為當下瀏覽的網站所建立的 cookie，而近年各大瀏覽器逐步淘汰第三方 cookie，是為與使用者主要瀏覽網址的網域不相符的來源建立的 cookie，主要被廣告業者廣泛使用並具有跨網站是別用戶和資訊同步的特性，但是涉及到使用者隱私因此逐漸被禁用，而在這種趨勢下，廣告商等第三方 cookie 使用者則轉而利用第一方 cookie 來達成第三方 cookie 的成效，例如 google analytics 仍然是使用第一方 cookie 來達到用戶身分識別。