尽管 cookie 已成为使用互联网的正常和必要部分，但NordVPN的新研究表明，一半的美国用户在他们访问的每个网站上都“接受所有 cookie”。

对于那些不熟悉的人，HTTP cookie 或浏览器 cookie 是您访问网站时存储在浏览器中的一段数据。启用 cookie 后，网站将记住您的偏好以及您在上次访问期间所做的任何小改动。

虽然大多数 cookie 都是安全的，并且公司使用它来在其网站上提供更多个性化，但有些 cookie 可用于在未经您同意的情况下跟踪您。同时，cookie 甚至可以被监视或用于伪造用户的身份，以便攻击者可以访问他们的在线帐户。

NordVPN 的数字隐私专家 Daniel Markuson 在新闻稿中提供了关于 cookie 带来的危险的进一步见解，他说：

“人们需要知道 cookie 会在线跟踪您。即使您使用 VPN 隐藏您的 IP 地址，cookie 也可以跟踪您的在线行为并形成您身份的部分 ID。此外，第三方可以出售您的 cookie。一些网站通过提供第三方 cookie 来赚取收入。这些都不起作用——它们的目的是从您的数据中获利。此外，cookie 是一个漏洞。如果浏览器设置错误或访问错误的网站，cookie 可能会给您的浏览体验带来安全漏洞，”

防止 cookie 跟踪您

现在大多数网站在页面底部都有一个弹出窗口要求用户“接受所有 cookie”的原因是什么？以便运营它们的企业能够遵守数据隐私法，例如欧洲的GDPR和加利福尼亚的CCPA。

大多数网站仍允许您在不接受所有 cookie 的情况下浏览和访问其内容，而其他网站则允许您指定要接受哪些 cookie。尽管如此，如果您想完全避免使用 cookie，还是有一些方法可以做到的。对于初学者来说，大多数浏览器都具有让您自动阻止不必要的 cookie的功能。但是，您可以通过使用隐身模式浏览更进一步。虽然它不会保护您的隐私，但隐身模式将允许您在不保存 cookie 或历史记录的情况下访问网站。

不过，为了获得额外的保护，您应该考虑在浏览时使用VPN来隐藏您的 IP 地址，如果您希望在线搜索保持私密性，这可能至关重要。NordVPN 最近还推出了新的威胁防护功能，其中包括一个跟踪器拦截器，以防止第三方 cookie 收集有关您的浏览习惯的数据并为您创建详细的个人资料。

使用匿名浏览器或具有内置隐私保护功能的浏览器（如Mozilla Firefox ）也可能是值得的。启用后，Firefox 的全面 Cookie 保护功能会通过为用户访问的每个网站创建一个单独的 cookie jar 来阻止 cookie 在网络上跟踪用户。

Cookie 长期以来一直是互联网的重要组成部分，但随着谷歌一直致力于其隐私沙箱的工作，这种情况可能很快就会改变，目的是永久取代 Cookie。在那之前，您应该继续三思而后行，然后再接受您访问的每个网站上的所有 cookie。