介紹

你不能阻止政府監視你，這是人們普遍的一個誤解。你可以。不要讓政府鎮壓的恐懼阻止你發表意見。 Ritser隱私工具包旨在幫助你保持安全和保持知情的狀態。

互聯網是怎麼辦到的

互聯網上的所有計算機都有一個IP地址，用來互相通信。網站也有IP地址，但是為了讓瀏覽互聯網變得更容易，它們也有域名（例如www.facebook.com以及www.google.com)鏈接到他們的IP地址。當你的計算機想轉到www.google.com執行搜索時，它獲取與之有關聯的IP並與該計算機通信以獲取信息，在這個情況下會是你的Google搜索結果。

您的ISP（互聯網服務提供商）將你的計算機連接到互聯網。你可能有一個調製解調器，通過電話、電視或光纖電纜連接到ISP的網絡。因為你的互聯網通過他們的基礎設施，他們可以看到你傳輸的所有數據和你將信息發送到了哪個IP地址。

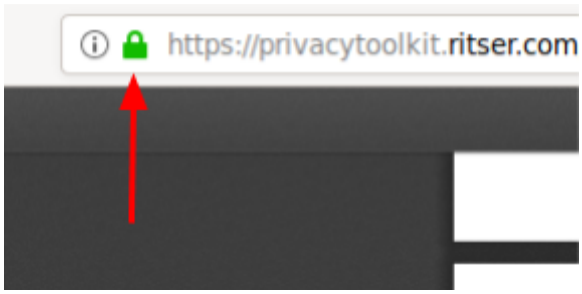
但這並不代表他們必須知道你在訪問哪些網站。如果你使用HTTPS加密數據，他們將看不到正在進行的操作，包括URL (www.google.com/search?q=news）。他們只知道你要連接的IP地址，你連接的時間，以及你發送的加密數據的大小。

政府可以追踪到什麼

我們來看看政府/ISP能追踪到什麼。假設你使用的是HTTPS而不是Tor，你的政府可以追踪你使用的網站和時間。這意味著他們可以知道你在晚上7點38分時訪問了IP地址www.facebook.com，但他們不知道你訪問了哪些頁面或個人檔案。他們只知道你游覽過www.facebook.com。

如果你不使用HTTPS，你的政府也可以追踪你發送到網站的內容。這包括密碼和各種URL。

你怎麼知道你使用的是HTTPS？通常，當你使用HTTPS瀏覽時，瀏覽器會顯示如下所顯示的鎖符號。



HTTPS的工作原理是對瀏覽器和網站之間的數據進行加密。這意味著它使用數學算法來確保這些數據在傳輸過程中是不可讀的。現代加密算法被認為是安全的，因為即使是最強大的情報機構也無法破解它們。

未加密的連接（沒有S的HTTP）如下所示：

從: 70.210.154.182

到：103.190.246.203 (baidu.com)

時間: 4:42 AM 2020-09-02

數據 (70字節):

遊覽的網站: baidu.com/account

用戶名: alex2

密碼: password

加密連接（HTTPS）如下所示:

從: 70.210.154.182

到：103.190.246.203 (baidu.com)

時間: 4:42 AM 2020-09-02

數據 (68字節):

o866)F(Yu~1]TEjP47h6(vIEs!dq_'|/Sl^ZMbFriN_"LejUyUYZ%d?sRx;F##Coq9M&

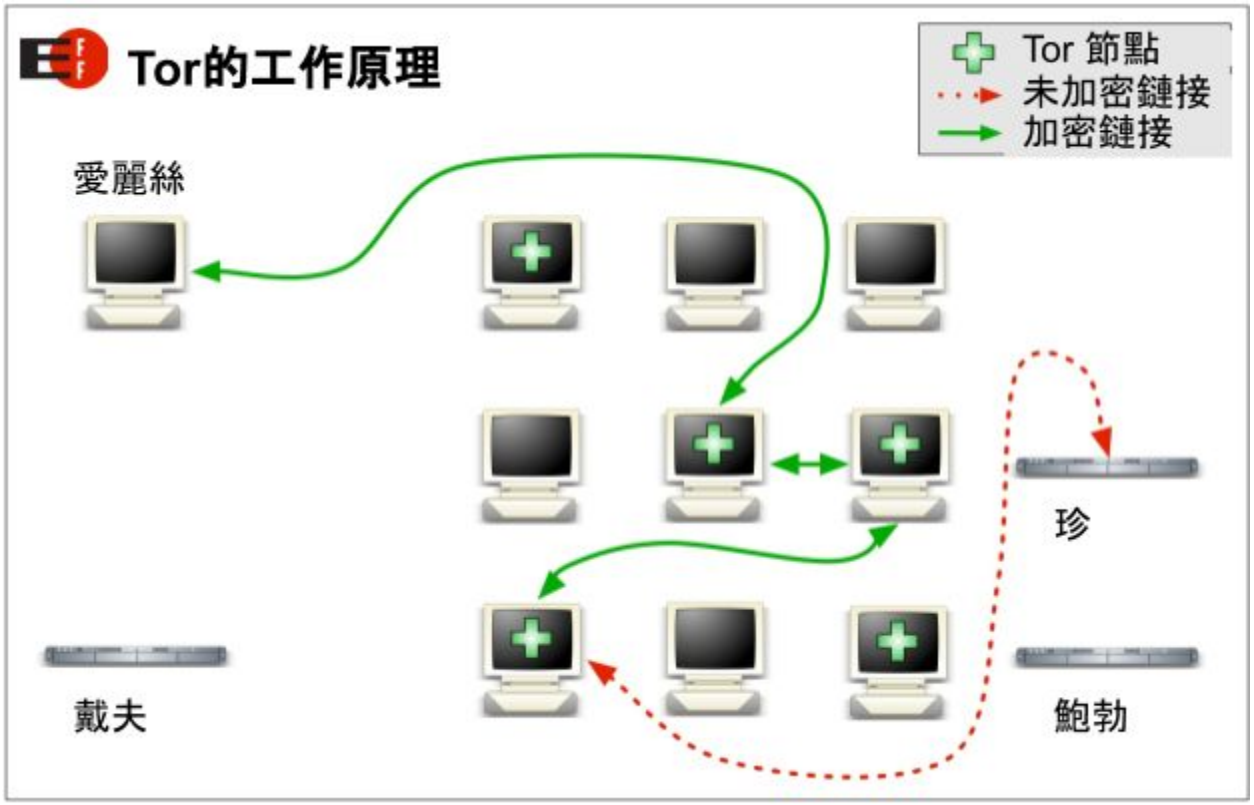
政府可以在網站主人的幫助下追踪什麼

然而，HTTPS並**不**阻止網站向警方提供你的數據。你在互聯網上訪問的每個網站都可以看到你的IP地址。如果一個網站決定給政府你帳戶背後的IP地址，**他們可以用它來找到你的真實地址。**重要的是要確保當局找不到你的在線帳戶背後的IP地址。

Facebook、Reddit和Google等大型網站都有處理政府要求用戶數據的程序。這個過程通常是透明和公平的，因為他們通常不理會獨裁政府的法律。例如，谷歌在2014年至2018年間處理了3個埃及用戶數據請求。他們全都否認了。

在網站上隱藏你的身份

然而，把你的安全交給跨國盈利性公司不是一個明智的想法。如果你生活在一個國家，而你的身份被暴露了，你的安全就會受到威脅，那麼最好使用Tor（包含在本工具包中）。 Tor通過在你的網絡流量到達網站之前由其他計算機發送它，從而隱藏起你的IP地址。網站將能夠看到最後一台計算機的IP而不是你的。你的政府會知道你在訪問Tor，但他們不知道你通過它發送了什麼，也不知道你在和誰交流。



使用Tor的另一個好處是，由於ISP不知道你正在訪問哪些網站，所以他們無法封鎖它們。

Tor不是絕對可靠的。如果政府知道你的大致位置，而網站所有者告訴他們你在使用Tor，他們可以在你瀏覽網站的同時，查看訪問Tor的人，以獲得你的真實身份。聯邦調查局以前也這樣做過，但這不應該成為一個問題。如果你擔心這個，你可以使用公共WiFi。

旁注：VPN在在線保持匿名方面不如Tor有效。

顯而易見的

通常人們被抓不是因為政府獲得了他們的IP地址。而是他們向互聯網上提交的東西，顯示了他們的身份或向他們的朋友透露了他們的身份。人們被抓是因為愚蠢的錯誤。以下是一些你應該經常做的事情：

1.提交故事時，含糊其辭，編造細節。一小部分信息，比如你兄弟姐妹的數量，可以用來揭露你的身份。

2.在網上提交照片時要**非常**小心。從你上傳的所有照片中刪除EXIF數據，並驗證是否沒有可用於識別你的詳細信息。

3.如果其他人使用你的電腦，確保你的瀏覽記錄沒有被保存。不要將任何可能洩露身份的內容保存到計算機中。

4.不要用你的真名註冊那些你用著匿名身份的賬戶。

5.不要向現實生活中認識的人透露你的匿名身份。

6.不要向你通過匿名身份認識的人透露你的真實身份。

結論

如果你使用匿名的Reddit或Facebook賬戶，你有時還可保持安全。但如果你的生活依賴這些公司的話，你可能不會想要信任這些公司。如果你想自信地保持匿名，使用Tor。 PrivacyTools是其他以隱私為目標的軟件的一個很好的資源。

記住：只有你能對自己的安全負責。