

OUCH!

您的每月安全意識通訊

虛擬專用網 (VPN)

概觀

當您不在家時，例如當您在當地餐館或咖啡店或在酒店或機場旅行時，您可能會發現自己需要使用公共Wi-Fi進行互聯網訪問。但這些公共網絡有多安全呢？誰又正在觀看或記錄您在網上做的事情？也許您甚至不相信您家裡的ISP（互聯網服務提供商），並希望確保他們無法監控您在網上做什麼。使用稱為VPN（虛擬專用網絡）可以保護您的在線活動和隱私。VPN是一種為您的在線活動創建專用加密隧道的技術，這使得任何人都難以觀看或監控您在線進行的操作。此外，VPN有助於隱藏您的位置，使您訪問的網站更難以確定您所在的位置。

它是如何操作的？

VPN通過創建到您選擇的VPN提供商的專用加密隧道來工作。您的所有在線活動都會通過此隧道，然後將您的目的地變成VPN提供商的網絡。例如，如果您位於佛羅里達州坦帕市連接到德國慕尼黑的VPN服務器，那麼您連接的任何網站都會認為您從德國慕尼黑連接。VPN很容易使用。第一步是找到您信任的VPN提供商，然後創建一個帳戶（這通常需要您購買他們的服務）。擁有帳戶後，即可下載，安裝和配置其VPN軟件。安裝和配置後，您將一如既往地連接到互聯網。VPN軟件將默默地創建您的加密隧道並開始保護您的隱私，而您甚至沒有留意到。

選擇VPN提供商

您的在線活動的安全與隱私與所選VPN提供商一樣重要。一定要選擇一個值得信賴的產品。以下是選擇VPN服務提供商時的關鍵點。



日誌記錄：尋找一些關注隱私，而且不保留任何日誌的服務。如果您的VPN服務提供商沒有收集任何日誌，那麼任何人都很難回去看您在網上做了什麼。



基於公司的位置: 不同的VPN提供商位於不同的國家/地區。請務必選擇位於具有嚴格隱私要求的國家/地區的VPN提供商。位於隱私法很少或較弱的國家/地區的VPN提供商可能會被迫提供他們收集的信息。



服務器: 尋找具有位於您所需國家/地區或城市中的服務器的VPN服務。一些VPN提供商在全球擁有數千個服務器和位置。您是否需要使您的連接看起來像是來自特定國家/地區，您的VPN提供商是否可以提供這些連接？



兼容性: 尋找適用於不同電腦和移動設備的服務。例如，您可以使用Windows筆記本電腦，平板電腦和iPhone。您將需要一個適用於所有這些設備的VPN服務。



避免免費: 對“免費”VPN服務要非常謹慎，他們如何賺錢和保持業務？免費服務可能會收集和出售您的信息。

VPN是幫助保護您的在線隱私的絕佳方式。但是，VPN無法保護您的電腦，設備或在線帳戶。因此，即使您使用的是VPN，也要確保始終遵循基本的安全步驟，包括確保更新設備，使用屏幕鎖定以及始終為所有帳戶使用強大的唯一密碼。

客座編輯

Phil Johnsey ([@peakreflections](#)) 是Palm Beach County的一名IT專業人員，在安全，取證和審計方面經驗豐富。他還是SANS註冊的數字取證，安全要素和OUCH社區評審委員會成員。他的執著於把幫助人們把安全簡單化。



參考資料

- 使密碼簡單化: <https://www.sans.org/u/Sd8>
- 保護您的移動設備: <https://www.sans.org/u/Sdd>
- 阻止惡意軟件: <https://www.sans.org/u/Sdi>

OUCH! 由SANS Security Awareness發行刊登，遵從 Creative Commons BY-NC-ND 4.0 (創意公用授權條款4.0版)。在不更改本刊物內容的前提下，你可以自由分享此月刊或使用於你的安全意識計劃。有關翻譯或更多諮詢，請聯絡 www.sans.org/security-awareness/ouch-newsletter。編輯委員會：Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | 翻譯：巴珊珊