

OUCH!

全民資訊安全意識月刊

# 暗網

## 概述

您也許曾聽過某人或媒體提起「暗網」一詞，並好奇「何為暗網？」或「關於暗網，我應該做甚麼嗎？」我們現在就向您解釋什麼是暗網，及它所代表的意義。

## 何為暗網？

暗網由網路上各式系統組成，其設計目的是安全及匿名地溝通或分享資訊。單一的「暗網」並不存在，它並不像Facebook由單一組織運作。取而代之，暗網是不同系統與網路之多樣集合，由不同成員出於各種目的管理。此類系統仍與網路連結且屬於網路的一部分，然而，一般而言，您無法透過一般的搜尋引擎找到它們。通常您需要在電腦上安裝特殊的軟體，方能找到或接觸它們。Tor (The Onion Router) 專案是其中一例。為了連接至暗網，您需要下載並安裝洋蔥瀏覽器 (Tor Browser)。當您利用洋蔥瀏覽器連結網站伺服器時，您的加密流量將流經同樣在使用此瀏覽器的其他電腦。當流量在這些電腦間跳動時，來源IP位址將隨之改變，這意謂著您連上網站的同時，您的線上活動是匿名化的。其他暗網的例子包括Zeronet、Freenet及 I2P。

## 誰在使用？

網路罪犯是暗網的最大宗使用者。他們於暗網經營網站及論壇以匿名及安全地進行犯罪活動，如購買藥物或販賣數以萬計遭駭的數據。舉例來說，某一群網路罪犯駭入銀行或線上購物商店，他們竭盡所能地竊取資訊，接著將其賣給暗網上的另一群網路罪犯。

暗網還是有一些正當的用途。例如，在審查制度氾濫的國家，人民可透過暗網網路來分享資訊並看見世界發生的大小事，與此同時，又能保護自身隱私及維持匿名。新聞記者、吹哨人(告密者)及在乎隱私的人可善用暗

網來增加自身的匿名程度並繞過審查。此外，這些人不僅可利用類似洋蔥瀏覽器的技術進入暗網，更可匿名瀏覽普通的網際網路。

## 我該做甚麼？

提醒您除非有特定的理由非要存取暗網不可，否則能避則避。多數暗網網站用於非法目的，其中又有許多網站會利用您的電腦做為端點來達成他們的目的，且某些情況下您的電腦可能會被探測或攻擊。有些公司提供監測服務，讓您知道您的姓名或其他資訊是否曾被網路罪犯盜用，並在暗網被發現。此類服務的實際價值令人懷疑。保護自己的最佳之道是假設您的部分資訊已經在暗網被網路罪犯利用，結論是：



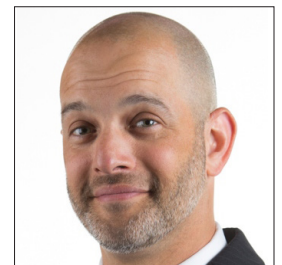
- 對任何假扮成官方單位強迫您採取行動，如繳交罰金之類的來電或電子郵件心生警惕。罪犯甚至可能利用他們發現的與您有關之資訊來設計個人化攻擊。
- 監控您的信用卡和銀行狀態。可以的話甚至對所有交易執行設置警訊。如此可讓您察覺是否發生任何金融詐騙。若您真的察覺到有異狀，立即向您的信用卡公司或銀行回報異常。
- 凍結您的信用紀錄。這不會影響您使用信用卡，且是保護自己，避免身份遭冒用的最有效步驟之一。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站

<http://www.tsc-tech.com/>或臉書@tsctech了解更多訊息。

## 客座編輯

Micah Hoffman(@WebBreacher)是焦點資安有限公司(Spotlight Infosec LLC)的首席調查員，他是SANS認證的SANS公開來源情報(OSINT)課程導師及作者。Micah的計畫、教材軟體及教學風格展現了他對於網路及公開來源情報的熱忱。



## 參考資源

個人化詐騙: <https://www.sans.org/u/RfW>  
社交工程攻擊: <https://www.sans.org/u/Rg1>  
身分冒用: <https://www.identitytheft.gov>  
信用凍結: <http://photo.udn.com/money/story/5599/3381794>  
洋蔥瀏覽器: <https://www.torproject.org/>  
SANS 公開來源情報(OSINT)課程: <https://sans.org/sec487>

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，您能夠自由分享此月刊或使用於您的安全認知計劃。有關翻譯或其他資訊，請聯絡 [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter)。  
編輯委員會：Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | 翻譯群：宋亞倫、顧君毅、葉力維、戴興望、李彥鋒