**暗網探索**

**1.暗網的意思**

講暗網 (Dark Web) 之前，先來認識深網 (Deep Web)，深網又稱為深層網路，深網的意思是**存在著但不容易找到，找到也不一定能夠進去的網站**，像是需要註冊或是登入的私人網站、公司的數據庫、論文的數據庫、刻意隱藏內容的網站等等。

了解完深網是什麼之後，現在來說說常常被搞混的暗網，暗網必須通過**特定的瀏覽器或特殊授權**才能夠進入，舉例來說:在這100個建築物裡，有90家是我們可以看到的合法店家，但有10家是「不能曝光」 的店家，必須通過特定管道才能進入，這 10家就像是暗網，雖然說是「不能曝光」，但這可不一定就是血腥、暴力、色情等內容，也有可能是一些加密貨幣的交易、或是被政府打壓的網站等等。

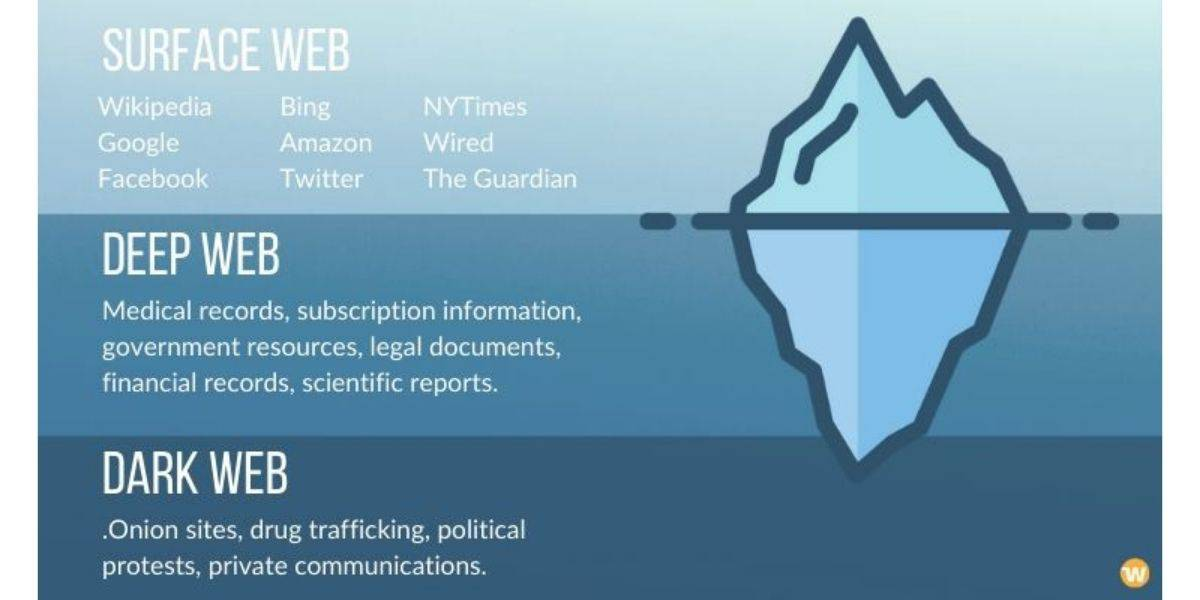
**2. 深網與暗網的差異**

一般我們能搜尋到的網站、深網、暗網實質上是在「同一個」名為「網路」的冰山中，我們搜尋到的網站則是冰山一角，還有很多我們看不到的網站存在海面下，也就是深網與暗網。

兩者的差異:

**深網**：你知道資料存在，但沒權限去存取 (例如 A 公司的資料庫、B 大學的資料庫)。

**暗網**：必須透過「設定」、「特定的瀏覽器」、「授權」等等，才 能夠存取。



**3. 安全的環境**

進入暗網前必須先做好各種準備，不代表說暗網就是那麼危險、恐佈的，僅僅是對於資安的一種慎重而己

畢竟有許多使用者即使沒到暗網，也會不小心進到釣魚網站、安裝了惡意程式等等。

第一點：使用一個完全乾淨的裝置，像是剛重灌完的電腦

第二點：選擇一個安全且值得信賴的 VPN，透過加密以及變換 IP 來保護主機位址

第三點：不要使用免費的 Wi-Fi

選擇乾淨的裝置是避免電腦中毒造成其他資料損毀，VPN 的網路協定能在不安全的網路上提供一個安全路徑，免費 Wi-Fi 通常沒有嚴格的加密，容易成為駭客攻擊的目標

VPN 也不能隨便選選，特別是免費的 VPN 具有風險，建議的 VPN 有 Surfshark 及 NordVPN、ExpressVPN，這三款是外媒評比最佳的 VPN，並且「不記錄使用者的資料」，這點對於要前往暗網的人來說格外重要。

**4. 暗網的瀏覽器**

一般我們常見的瀏覽器像 Chrome、Firefox、IE、Edge …等，是沒有辦法前往暗網的，而最為人知的就是透過 Tor Browser (洋蔥路由瀏覽器)，與其他的瀏覽器相比，最大的差別是 Tor Browser 在到達目的地網站之前，會先經過三個中繼的伺服器，也就是說你的 IP 位址會變更三次，從到達到隱藏自己真實 IP 的作用，不過由於經過三個中繼的伺服器，連線速度也會降低許多，既然有 Tor 來隱藏 IP 又為何需要使用 VPN 呢？最大的差別在於少了「資料加密」的過程以及「真實 IP」的部份，若是有心人士花時間反查你的 Tor 路徑，你的真實 IP 便會暴露，相當危險，而透過 VPN 再使用 Tor 的話，即使被反查最終也只會停在 VPN 的伺服器上，真實 IP 位址則是安全的。準備好值得信賴的 VPN，下載好 Tor Browser 之後，下一步就是前往暗網的入口，暗網上的網址和一般的網址有很大的不同，舉例來說:2gh3ftr1ce8cefc4q.onion，乍看之下就是一組亂數組成的網址，其實就真的是由亂數生成的，而最後面的 .onion 就是類似於 .com 這種域名的存在，而上面這組亂碼就是名為「DuckDuckGo」的搜尋引擎，在一般網路上它的網址是「duckduckgo.com」，而在暗網就是上面這組「2gh3ftr1ce8cefc4q.onion」，DuckDuckGo 就是類似於 Google 的東西，連上後就可以開始在暗網上搜尋資訊了。

**5. 暗網的趨勢**

Tor上最常見的代管內容是兒童色情，其次是黑市，而流量最高的網站專門用於殭屍網路營運，許多吹哨人網站都有線上論壇和政治討論論壇，近年來比特幣、詐騙和郵購相關服務的網站最豐富，其中加密貨幣相關話題為最熱門的，特斯拉在三月份宣佈接受加密貨幣，且可以購買自己的電動車，這家電動汽車製造商在2月份曾透露，已購買了15億美元的比特幣，雖然在5/14，特斯拉撤回了先前宣佈的計劃啟用比特幣購車的聲明，但這期間比特幣的價格飛漲，所以與比特幣相關交易在暗網上非常頻繁，這類帳戶的安全措施又寬鬆，加上大量的比特幣ATM可供用戶匿名提款，因此被駭客盯上，一個加密貨幣交易所Coinbase的帳號可以在暗網上賣到610美元（約新台幣17046元），再來使用比特幣滾筒進行洗錢成為新趨勢，一種常見的方法是使用數字貨幣兌換服務，將比特幣轉換為線上遊戲貨幣，然後再轉換回金錢，由此可見未來加密貨幣在暗網上會成為很熱門的趨勢。