狙殺鏈的步驟	惡意行為	矯正措施	監控措施
傳遞	使用者收到網路釣魚郵件。	評估企業需要使用到哪些附加檔類型，像 *.js* 之類的文件就可能是有危害的，且很少會從外部來源遞送。 建立郵寄黑名單和灰名單（如 Spamhaus 和 dnsbl）阻擋已知的惡意郵件伺服器。	灌輸使用者「信任但要驗證」的觀念。 部署 Ad-Blocking Filetypes，依照檔案大小及類型封鎖已知的惡意程式，例如過濾規則設為超過 22MB 的 *.scr* 檔案或超過 15MB 的 *.js*。
漏洞利用	使用者下載一支 JavaScript 或內有巨集指令的 Word 文件。	利用群組原則停用巨集和惡意的檔案類型，確保任何端點保護都已安裝並更新到最新版本。	監控代理伺服器的日誌，尋找非預期的檔案存取行為，例如從某部威脅情資黑名單中的伺服器取得 JavaScript 檔案。 使用代理伺服器或 IDS（對明文資料）監控已知的解密後字串。
安裝	載荷在使用者的機器上執行（Lucky、Cerber 和 CryptoWall 會使用內建的 Windows Cypto API 進行加解密）。	保留備份檔案（不要恆常掛載）以便檔案被加密後，可以利用備份檔輕鬆還原。 依照不同的作業系統，使用者的機器上應該執行如 Little Flocker（*https://www.littleflocker.com*）之類的「檔案系統防火牆」，限制個別處理序對檔案的存取權限，例如可以限制 MS Word 可以存取，但 IE 就無權存取。 有一些實驗性質的工具可以封鎖加密型的勒索軟體，例如 Decryptonite（*http://bit.ly/2miUj3w*）。	發現 Windows Crypto API 在短時間內大幅增加。 網域出現大量的數字或者有意義的字串比例下降。

樹系

樹系是機構的安全性範圍，並定義系統管理員的授權領域。

—摘自微軟 Technet

雖然許多機構只利用一個樹系定義一個網域，也有一些大型企業歷經收購許多小型公司而形成如圖 10-2 的足跡。對於大型樹系，在不同網域間存在不同的安全存取管制，並不容易取得平衡。

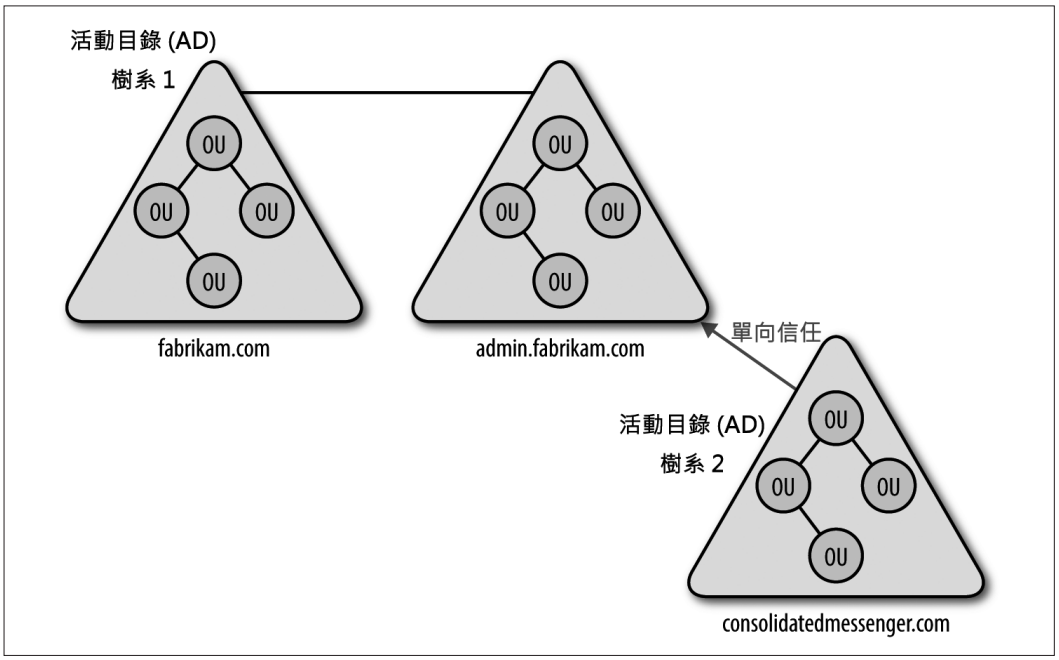

圖 10-2　樹系可以是單個網域或多網域的集合

定期更新

就和伺服器的情況一樣，工作重點是確保端末設備安裝修補程式，以減少系統錯誤及降低漏洞數量。盡量降低端末設備上的漏洞數量，就可以減少攻擊者的技術選項，也能防止某些類型的惡意軟體自動攻擊。

不同的平臺有不同的修補方式，這和企業的管理方式有很大關係。自攜設備（BYOD）系統的選用及管理，和傳統由雇主提供設備的方式有很大不同，這些差異包括硬體、作業系統、應用程式。

微軟 Windows 環境

從推出 Windows 95 以來，微軟就提供 Windows 更新服務，該服務經歷多次改變，最終以半自動的方式將修補內容發送到端末設備。該網站可以讓執行 Windows 的電腦根據執行中的作業系統版本下載更新和修補程式，但這項服務主要針對消費型和 BYOD 市場，且常常需要使用者自己動手，使用者可能因此拒絕或延後更新，且沒有提供系統管理員關於修補程式的部署狀態。

過去微軟以系統管理伺服器（SMS）、微軟營運管理員（MOM）和 Windows 伺服器更新服務（WSUS）為企業用戶提供更新服務，允許系統管理員將修補程式派送給環境中的工作站，而不需依賴 Windows 更新或微軟更新。然而，這些系統已不再是標準應用了。

撰寫本書時，對於執行 Windows 10 的端末設備微軟建議改用商務用 Windows 更新（Windows Update for Business；*http://bit.ly/2lYsI4f*）。可以透過端末設備的群組原則或移動式裝置管理（MDM）設定使用商務用 Windows 更新服務，而不是消費者模式的 Windows 更新服務。

圖 13-6　從被駭的 @AP Twitter 帳號發出假的推文

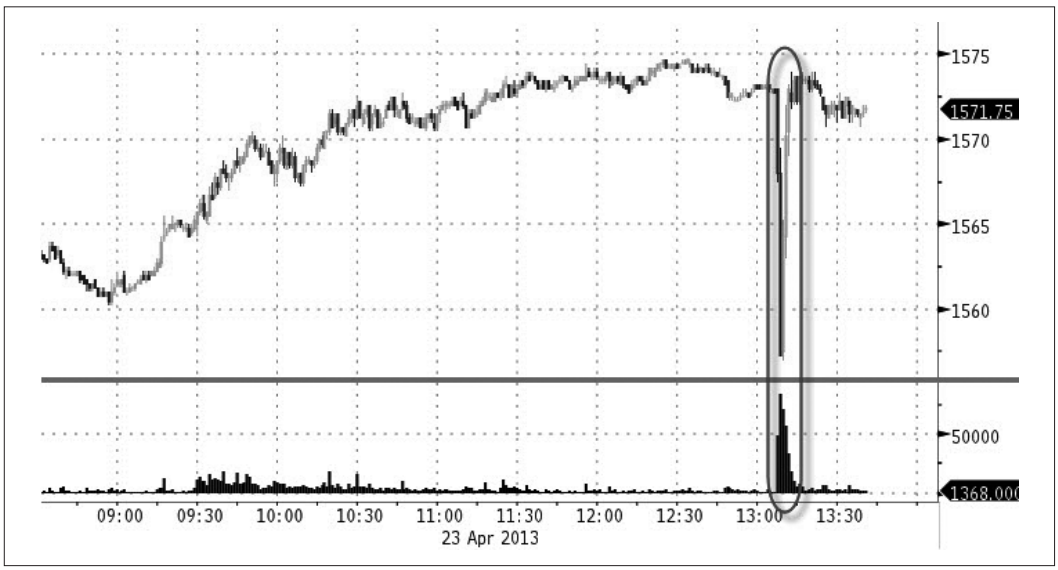

圖 13-7　推文發出後造成股市暴跌

路由器

上面的建議也都適用於路由器，但有些針對路由器的特定安全考量值得更深入討論。

路由器通常以存取控制清單（ACL）提供基本的封包過濾選項，ACL 和簡單的防火牆規則非常相似，允許路由器根據簡單的準則（如 IP 位址）拋棄封包，為了避免影響路由選擇性能，ACL 型的路由器一般不會維護封包狀態，也不夠聰明，但還是有一些用途：

- 基於管理的目的，除了來自授權管理路由器的特定網路封包（如來自網路監控中心或堡壘主機的封包），否則封包的目的位址沒有理由是路由器的 IP 位址，因此，ACL 可以將目的地是路由器的所有流量拋棄。
- ACL 能替其他設備或網路做粗略過濾，例如刪除指向防火牆的流量。
- 有關安全設備的碎裂封包問題其來有自，攻擊者可以使用碎裂封包規避 IDS 等工具的檢測，藉由拋棄碎裂封包，就可將這種技術侷限在區域網路裡。但要在網路上施作這種 ACL 之前，應該先了解對網路的影響，因為某些網路本來就會產生合法的碎裂封包。

根據來源廠商和預設組態，路由器可能具有動態路由協定，如內部閘道器協定（IGP）、路由信息協定 V2（RIPv2）、增強型內部閘道器路由協定（EIGRP）或開放式最短路徑優先（OSPF）。如果適當運用，這些協定可以動態確認兩個主機之間最快的繞送路徑，以及繞過故障的設備、鏈路和網段；如果設置不當，攻擊者可以利用這些協定，經由他控制的惡意裝置來繞送流量，並竊聽封包內容或啟動中間人攻擊。

每個協定的複雜性都可以自成一個章節，但就像服務一樣，為避免被濫用，用不到的路由協定就該停用。動態路由協定的正確組態不該只依靠供應商，而是要適用於你的網路架構。

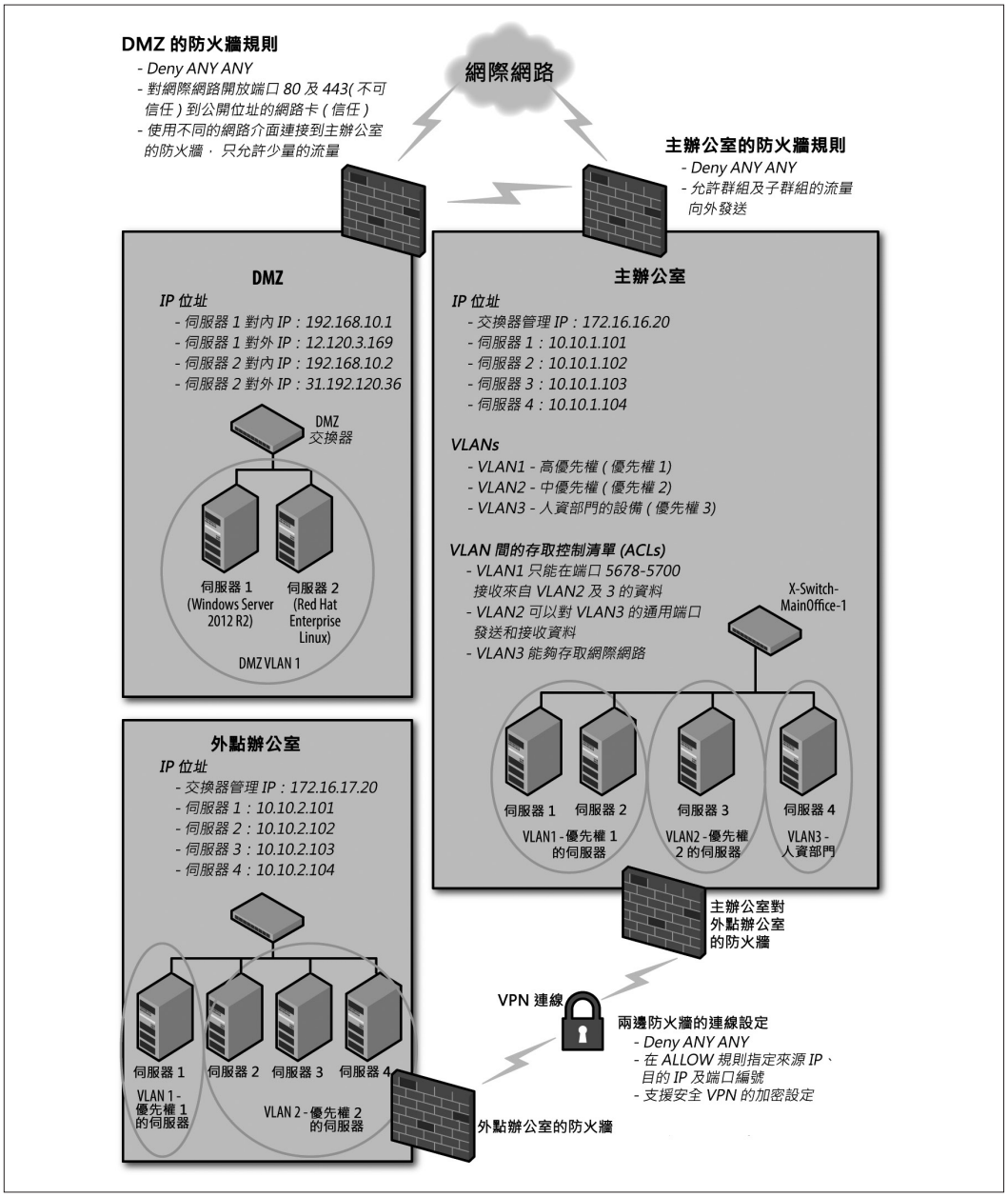

圖 15-1　實體和邏輯網路的例子

比照這種方式再執行其他資料轉化，如 IP 位址解析、探索伺服器上執行的網站、GeoIP 位置等。

也可以利用此網域搜尋感興趣的檔案及電子郵件位址，此項功能會利用不同的 Google Dorks 爬找各種 Office 檔案（參考見圖 18-5）。

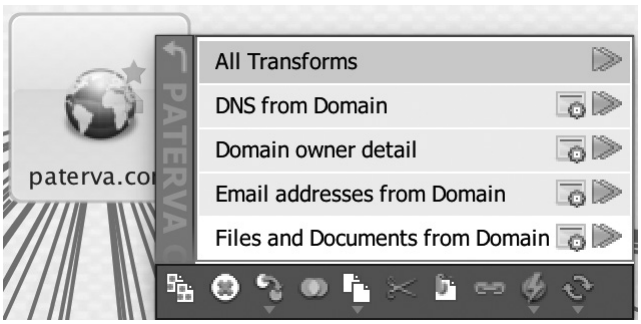

圖 18-5　選擇「All Transforms」可能發生資料超載，但會看到許多有趣的結果產出

執行全面性掃描可能會得到過多資訊而造成不必要的干擾，不僅耗用大量時間，圖形畫面也會充斥許多價值性不高的資料。你可以試著對某個網域執行「All Transforms」體驗看看。

recon-ng

「…是用 Python 寫成的全功能 Web 勘查框架，透過完整的獨立擴充模組、資料庫交互參照、內建功能、互動式操作和命令，Recon-ng 提供一個強大的環境，可以針對網際網路的公開來源進行快速、徹底勘查。」[3]

3　*https://bitbucket.org/LaNMaSteR53/recon-ng*

現在就指定一份網路清單到 Shodan 上搜尋，使用搜尋字串「net：209.87.112.0/24」找到在美國的 23 個不同服務，圖 18-18 顯示位於美國的所有 HTTP、HTTPS 和 DNS 伺服器，Shodan 可以從這裡鏈結到網站或顯示特定 IP 位址上的詳細資訊，雖然 Shodan 沒有將每組 IP 位址的 65535 個端口都編入索引，但確已索引常用的部分，這樣可以讓資料更具一致性。

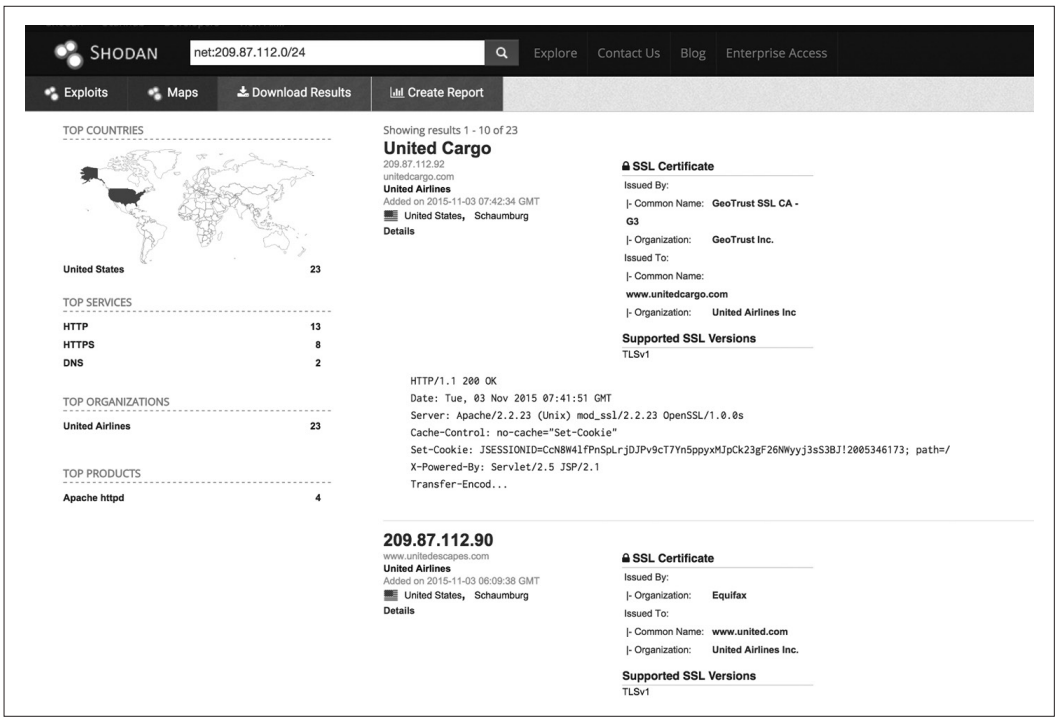

圖 18-18　利用 Shodan 查詢網路區段的結果

在 Shodan 官方的圖書（*https://leanpub.com/shodan*）可以找到完整的搜尋語法及 API 使用指南。

部署排污伺服器或黑洞 *DNS*

如圖 21-2 所示，DNS 排污伺服器（*http://bit.ly/2m2hiwb*）會假裝成官方 DNS 伺服器，用來對抗提供惡意軟體和病毒的不良網域，當用戶端嘗試查詢惡意網址時，它回應一組無法繞徑的虛擬位址，確保用戶端不會連接到惡意網站。可以利用惡意軟體分析程序，從已知的 C&C 伺服器收集惡意的網域名稱，開放資源網站也會利用回應原則區域（RPZ）的 DNS 紀錄提供惡意 IP 及釣魚網站的資訊。

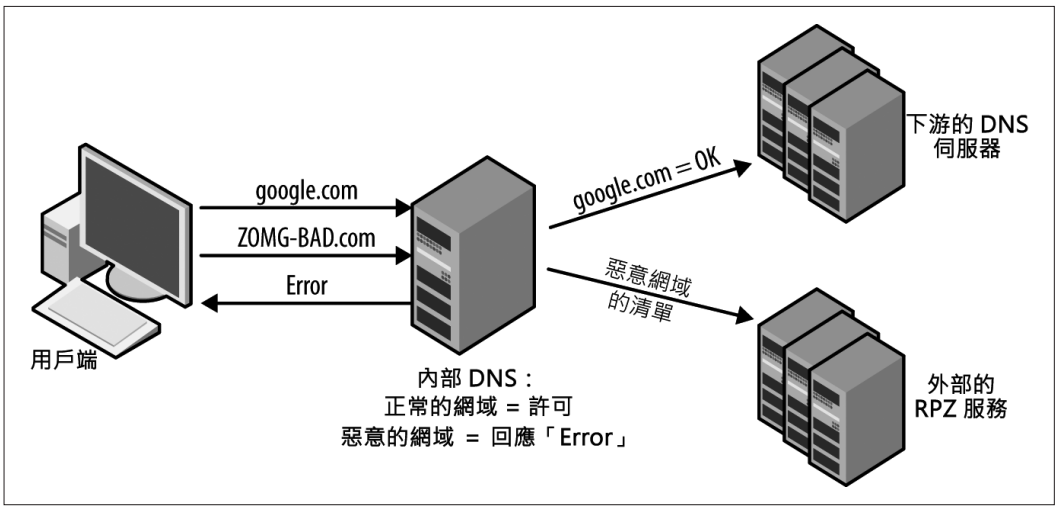

圖 21-2　DNS 排污架構圖

DNSSEC

DNS 安全擴充功能提供 DNS 資料的解析器來源身分驗證機制，建議一般機構不要部署這項功能，它具有極高的風險，但成效有限。不僅會削弱 DNS 能力，還提供駭客利用大量安全 DNS 封包的可靠 dDoS 放大攻擊來源。

隱式安全

所謂隱式安全就是以非標準的方式「隱藏」資產、服務或程式的一種防護手段，雖然其本身並沒有安全防護功能，但可以當作額外的加強措施。

該做的事：

- 將服務設定在非標準端口上，將網頁管理的登入頁面之監聽端口從 443 改成 4043，或者將 ftp 伺服器的端口改成 2222。
- 變更本機管理員帳號名稱。
- 重新設定服務的迎賓訊息，不要揭露伺服器的作業系統和版本資訊。

不該做的事：

- 封鎖 Shodan 掃描或其他網際網路爬蟲存取公共 IP，因為只禁止某個服務的資料不被索引，並不表示駭客就找不到它。前面提過你可以藉用 Shodan 的服務來協助找出安全漏洞。
- 在資料中心和設備機櫃貼上明顯的「網路資料中心」標籤。
- 將未通過弱點掃描的服務或設備，直接掛載到網際網路上。

網路釣魚的訓練投影片

你可以利用此範本或者自行編製的投影片，做為網路釣魚活動之後，使用者自我學習的教材，也可以用在平常的教育訓練。

你已經被駭了！

別驚慌！這只是一個測驗（真正的測試是來自攻擊者）。（點擊箭頭可看到更多資訊！）

發生了什麼事？為什麼會這樣？

- 你知道嗎？真正的攻擊者一直在對我們的網路進行同樣的嘗試。
- 在攻擊者取得我們的病人個資之前，我們寧可把自己鍛鍊得更強壯。
- 無論部署多麼先進的技術來防護網際網路安全攻擊，最好的防禦總是團體中具有警覺心的成員（就是你！）。
- 課堂上講的只是一種治療理論，它絕不是第一個病人，實際練習才可以更安全。

社交工程入門

電腦非黑即白、不是開就是關，而人類不一樣，很不幸地，我們成了攻擊鎖定的目標：

- RSA（資安公司）在 2011 年因電子郵件而被入侵（*http://bit.ly/2lEpV4b*）
- HBGary（資安公司）在 2011 年因重複使用密碼、電子郵件而遭到入侵（*http://bit.ly/2lEj7Dn*）
- 2010 年駭客利用 Aurora 入侵 Google / Adobe（*http://bit.ly/2lEkFxa*）

如果現在被入侵，也沒啥大不了

- 如果連在電腦公司工作（特別是資安防護）的人都被攻陷，那麼面對類似的攻擊，你可能也束手無策。
- 我們需要做更好的準備，這是一次練習的機會。

不要自責、不要慚愧，只是…

- 在醫療機構服務的你，傾聽及信任人們的心聲是你的天職，真的很偉大！
- …但社交工程就是利用你純真的天性和對人性的信任去營造情境（我也愛我們的病人！）、提出請求（請給我密碼），並常常利用高層的名義讓你感到迫切被需要（*CEO* / *CIO* / *CNO* 都希望這樣做！）。

當下一次再遇時，要謹記…

- 如果這封信不是你所預期的，就算寄件者看起來是認識的人，也請不要點擊鏈結或開啟附檔。
- 如果覺得與工作有關，請回信給寄件者，並詢問更多詳細內容（確認發信者的身分及目的）。
- 如果網站要求你輸入個人資訊（例如密碼），但你無法確認該網站的真實性，請電洽 IT 人員幫忙。

因為一定還會有下一次

- 如果網站外觀看起來似乎沒有問題，請確保它是一個安全網站（*https://* 的網址在網址列上會出現上鎖的鎖頭）。