公務機密 資訊安全維護

網際網路無國界 慎防機密由此洩

資安時事案例

駭客正在覬覦您的個人資料，您該如何預防?

遇到變更匯款帳號 一定要撥電話確認 列印

個人資料保護法

個資當事人的權利

輕鬆學資安

電腦安全駭客

數位學習 107年資安動畫金像獎

童話故事也要慎防詐騙

https://www.youtube.com/watch?v=lSmd-V5XdRI

駭客正在覬覦您的個人資料，您該如何預防?

2019 年 07 月 30 日 Trend Labs 趨勢科技全球技術支援與研發中心

人們的生活越來越數位化，從購物、社交、通訊、到電視欣賞和玩遊戲，現在都能舒舒服服地透過桌上型電腦、筆記型電腦或行動裝置來完成。不過，要享受這樣的便利，我們必須提供一些個人資料來獲得服務。不論是提供簡單的姓名和電子郵件地址，或者進一步提供更敏感的資訊，如：身分證字號和信用卡卡號，這些所謂的身分識別資訊 (PII) 一旦提供給他人，都有可能讓我們暴露在危險當中。為什麼？因為駭客隨時都在覬覦這些資料，隨時都在想辦法竊取這些資料來讓他們獲利。

哪些資料可能面臨風險？

追根究柢，駭客的最終目的就是為了賺錢。雖然他們也可能利用網路勒索或勒索病毒 Ransomware (勒索軟體/綁架病毒)來達成目的，但最普遍的作法還是竊取資料來賺錢。駭客一旦偷到您的身分識別資料與金融資訊，就會將這些資料拿到黑暗網路賣給犯罪集團來從事各種詐騙。犯罪集團可能利用買來的網路銀行登入資訊進入您的帳戶、掏空您的存款。或者，也可能冒用您的身分來申辦信用卡，讓您欠下鉅額負債。

在美國，身分冒用是消費者日益面臨的一項嚴重威脅。光 2018 年就有 1,440人受害，造成 17 億美元的損失，此金額是 2016 年的兩倍以上。

正如我們前面所提，駭客會盡可能蒐集更多個人身分識別資訊。他們蒐集到的資料越多，就越能拼湊出您的完整身分，輕鬆騙過您所往來的機構，這些資料包括：姓名、地址、出生年月日，以及一些更重要的資訊，如：身分證字號、銀行帳戶細節、信用卡資料、醫療保險等等。

網路帳號大多會記載這些資訊，當然，廠商會使用密碼來加以保護，所以駭客才會費盡心思想要猜測或竊取您的帳號登入資訊。即使是一些您認為駭客不會有興趣的帳號，也可能為駭客帶來財富。例如，您的 Uber 帳號登入資料就可能被駭客竊取之後拿到網路上販賣，而買到您帳號的人就能免費搭車。還有，如果您的 Netflix 帳號登入資料被偷到網路上販賣，買到您帳號的人就能免費使用這項影片串流服務。

現在，駭客甚至會直接駭入各大機構的網路，直接竊取您的個人資料。過去就曾發生過多起超大型資料外洩事件，如：Uber (影響全球 5,700 萬用戶) 和 Yahoo (影響全球 30 億用戶)。除了大型機構之外，駭客也可能針對您個人來發動攻擊。有時，駭客會利用他們手上已經掌握的資料來製造一些網路釣魚攻擊，誘騙您提供更多資料，例如報稅詐騙與性愛勒索。甚至，當駭客已經掌握您某個帳號的密碼時，他們會試圖登入您在其他網站的帳號，看看您會不會在其他網站上使用相同的帳號密碼。

雖然，銀行最後很可能會賠償您因身分遭冒用所蒙受的損失，但除此之外，您還可能面臨其他嚴重後果，因為網路資料竊盜及後續的詐騙很可能會讓您：

必須自行承擔重新辦理身分的花費。

承受心理壓力：75%的受害者表示患有嚴重的憂鬱。

信用評等下降。

花費許多時間和精力來解決盜刷爭議或爭取賠償：根據估計，受害者在遭受攻擊之後平均需要約六個月的時間與 200 的工作時數來重辦自己的身分。

接下一頁

我該如何預防？

所幸，您有許多簡單的步驟可以確保資料安全無虞，而且絕大多數都不用花錢，例如：
針對每一個網站和應用程式都使用較長、較難猜測、且非重複的密碼。您可借助一套網路密碼管理員軟體來協助您儲存這些密碼，在您需要登入時隨時取用。
每當廠商通知您的帳號可能遭到外洩時，請立即變更密碼。
可以的話，盡量使用雙因子身份認證（2FA）或多重認證 (2FA/MFA) 來提升您的登入安全。
當您要輸入個人身分識別資訊時，請務必確定網址列顯示的網址是否以「HTTPS」為開頭。
小提醒: FBI在今年六月提出警告：不要以為HTTPS網站很安全，有些暗藏網釣攻擊,駭客為了避免 Chrome 對釣魚網站提出不安全網站的警告,2018年大約有49%的釣魚網站會使用 https 進行加密,網址列的掛鎖圖示代表著這網頁傳輸的資料獲加密保護，並非100%證明這網站是安全的。
針對不請自來的電子郵件或訊息，切勿點選其中的連結或開啟附件檔案。如果有疑問,即使收到了看似熟係聯絡人的郵件，應該直接打電話或寄郵件予該名聯絡人，而非直接回信。
小心避免在社群媒體上分享過多的個人資料或金融資訊。
僅從官方應用程式商店下載應用程式，如 Apple App Store 或 Google Play。
當您連上公共的 Wi-Fi 網路時，切勿登入任何敏感的帳號 (如銀行、電子郵件信箱)，除非您經由 VPN 連線。
在 PC 和行動裝置上安裝一套您信賴廠商的防毒軟體，此軟體應具備網路釣魚與垃圾郵件雙重防護。
所有的作業系統與應用程式都應該隨時保持在最新版本以盡量減少駭客可利用的漏洞。
隨時留意自己所有的金融交易，如此，一旦發生身分遭到假冒的情況才能迅速察覺。
當發生與您的信用相關的資料外洩事件時 (如 Equifax 事件)，請立即透過 Equifax、TransUnion、Experian 及 Innovis 查詢自己的信用狀況，必要時可申請凍結自己的信用。
原文出處：Hackers Are After Your Personal Data – Here’s How to Stop Them

接上一頁

遇到變更匯款帳號 一定要撥電話確認

自由時報 2019年8月1日

〔記者姚岳宏／台北報導〕使用電子郵件雖便利但安全堪慮，易遭攔截冒用，專家提醒，若交易方突然要求更改匯款帳戶及帳號資料，務必循原有連絡方式再次確認，以免成為詐騙集團眼中的肥羊，蒙受巨大損失！

趨勢科技公司調查顯示，最常遭鎖定的產業是相當倚賴電子郵件進行交易溝通的電子業、製造業及食品零售業，手法往往是竄改成與公司高階主管（如執行長、總經理等）類似的電子郵件帳號，如l及i、w及vv、m或rn，或在長串英文字母中增加或減少一個字母等方式使之混淆。

歹徒駭入後，通常不會馬上行動，先潛伏一段時間、觀察雙方往來郵件伺機而動，等時機成熟，隨即模仿原本往來郵件語氣，發信給企業客戶或員工。

警方提醒，遇到變更匯款帳號時，應撥打電話進一步確認，同時使用合法授權防毒軟體，定期更新密碼，最好每個應用程式都設定不同密碼，以免歹徒駭到一組密碼，就能無限暢遊各網域，被害人長期被駭而不自知。

圖解個資法

個資當事人的權利

▶個資當事人擁有以下權利

1. 查詢或請求閱覽
2. 請求製給複製本
3. 請求補充或更正
4. 請求停止蒐集、處理或利用
5. 請求刪除

不得預先拋棄或以特約限制

▶可拒絕當事人行使權利的情形

可拒絕查詢、提供閱覽或製給複製本的情形：

1. 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
2. 妨害公務機關執行法定職務
3. 妨害該蒐集機關或第三人的重大利益

個人資料正確性有爭議時，可拒絕當事人請求停止處理或利用的情形：

1. 執行職務或業務所必需
2. 經當事人書面同意

iThome

文 /吳其勳

Computer Security Hacker

電腦安全駭客

資料出處：教育部全民資安素養網站

電腦安全駭客是指擁有電腦與網路知識的駭客，這樣駭客懂得網路運作原理與其資安風險，比如在一個有IPS的網路環境，他知道如何避開IPS的偵測與阻擋進行攻擊。