

公務機密

資訊安全維護

別讓歹徒用個資拼湊出你的全貌



資料來源:教育部全民資安素養網

資安時事案例

百家電商洩個資「去年詐騙吸70億」！
行政檢查僅1成、無人遭罰

小心臉書變Spy？五動作設定保護隱私

個人資料保護法

如何保護網路上的個人資料？

資訊安全防護

2023資訊安全新知不可不知

數位學習

103年度資安動畫金像獎 瑪莉的資安生活

百家電商洩個資「去年詐騙吸70億」！ 行政檢查僅1成、無人遭罰



周刊王CTWANT | 中國時報胡欣男、張薔 2023年3月13日

[周刊王CTWANT] 政府部門和企業個資外洩燒不停，連帶讓詐騙居高不下，去年全台詐欺財損近新台幣70億。刑事局科技研發科指出，電商平台頻傳個資外洩，1年來函請行政院數位發展部等7個部會對業者發動「行政檢查」，不僅檢查的比例僅約1成，且裁罰掛零，行政怠惰與企業罔顧資安，已淪為詐騙幫凶。

政院官員表示，警方函送各部會之案件，應依照個案情形作判定，並不是函送就會裁罰，若要裁罰必須要有前提，若有先進行改善，也不會構成裁罰條件，因此要看個案情形；現在規定是先進行早期的柔性輔導，不是移送就會裁罰，若說各部會故意不罰，說法未必客觀。

刑事局分析165反詐騙諮詢專線報案資料發現，近期駭客假冒「蝦皮拍賣」、「旋轉拍賣」等交易平台進行釣魚網站攻擊，盜取網路交易個資，然後進行「解除分期付款」詐騙。從達官顯要到升斗小民，都有被騙案例。

警方表示，蝦皮、旋轉是新加坡外商公司所有，在台灣僅少數行政管理人員，更無設置專業資安團隊協助帳號、密碼遭盜用後的防護。警方統計2網路平台迄今已蟬聯5周的高風險賣場1、2名，已由刑事局依違反《個人資料保護法》函送主管機關數位發展部查處，並於去年12月底由數發部實施「行政檢查」要求限期3個月改善，但迄今均未有具體作為。

為此，刑事局除定期在165網站公布「高風險賣場」，提醒消費者注意外，也主動針對疑似個資外洩電商進行訪視與追查，情節嚴重者依《個資法》及《行政院及所屬各機關落實個人資料保護聯繫作業要點》通報目的事業主管機關裁處。

令警方沮喪的是，去年6月至今年2月為止，警方將蝦皮、旋轉拍賣、博客來、生活市集、ONE BOY、大大寬頻等100家，涉及數發部、交通部、衛福部、教育部、經濟部、文化部和通傳部業管的個資外洩電商，函送7部會，要求業者改善，裁罰數竟掛零。

根據《個資法》，非公務機關個資外洩可處5萬元以上、50萬元以下罰鍰，並限期改正。7部會收到警方函送資料，發動行政檢查，要求改善者僅11家，另78家是書面通知改善，且均無裁罰紀錄。

警方指出，個資外洩是詐騙的源頭，詐團利用駭客竊取消費個資，偽冒公司客服以解除分期付款的詐術，誘騙民眾至ATM或網銀轉帳。

警方感嘆，個資外洩造成的詐騙案，2個月件數可達近千件，財損逾1億元，相比業者不投入資安成本，最重也才罰50萬，根本不成比例。

行政院官員坦言，裁罰額度最高僅50萬，確實太低，政院未來修法將提高裁罰額度，國發會已在研議，目前可以思考的修法方向，比如個資洩漏情節重大者，可以先裁罰，後要求改善，若不改善，繼續重罰。

你小心臉書變Spy？ 五動作設定保護隱私

教育部全民安素養網 更新日期:2022.3.30

人們常常開玩笑說，臉書太懂我們，就像是在「監控」一樣。事實上，臉書掌握著我們的使用者數據，還真的非常了解我們，只是這種「了解」可不見得是件好事。

像是《紐約時報》就曾經披露，有公司在未經使用者的許可之下，取得並保留 5,000 萬臉書使用者的個資。2021年初，臉書更有超過 5 億個資外洩，連創辦人的電話都沒有倖免！

究竟，在我們幾乎每天使用的服務中，要如何保護自己的個資呢？
臉書登入超好用？小心資料全都露！

臉書對現代人來說，就像是一張超方便的「數位名片」，只要交換了帳號，便能知道對方的各種資訊。同時，我們也常透過臉書來登入其他網站或遊戲，這樣「一個帳號走天下」的方式，為生活帶來了不少便利。

然而，當我們授權其他軟體使用，或是本身在用臉書的時候，其實透漏了非常多自己的重要資訊，內容包括：電話號碼、真實姓名、性別、居住地、感情狀態、職業、生日和 email 等等。

掌握這些資料，不但能拿來用作詐騙等用途，甚至有可能被有心人士拿來偽造、冒用身分，令人防不勝防。

一步一步設定，保護重要資訊！





不過，這些其實是可以避免的，透過以下幾個方向，讓我們一起為自己的臉書來場「健康檢查」：

一、檢查第三方應用程式授權：

前文中說到，我們常常授權各式各樣的第三方應用程式存取臉書資料，到底要在臉書公開哪些內容，務必再三確認。至於那些來源不明，或是久未使用的應用程式，則最好移除它們的存取權，避免個人資料外洩。

二、不讓臉書掌握你的興趣偏好：

臉書的重要收入來源便是廣告，當它越了解你，便越能將你的喜好賣給廣告主，讓你不知不覺就掉入過度消費的陷阱。想要避免這種情形，可以在「廣告設定」中調整，別讓臉書透過紀錄你的行為，不斷推送相關內容。

三、加裝廣告攔截程式：

跟前一點息息相關，透過進一步在瀏覽器中加裝廣告攔截程式，例如經《紐約時報》測試的Disconnect或Privacy Badger，這些程式能讓我們多一分保障，避免碰到帶有病毒的行動廣告。

四、定期清除瀏覽紀錄和 cookie

定期主動清除你在網路上留下的足跡是很重要的，千萬不要偷懶。可以自訂一個好記的週期，時間到了就清理，避免被人看透透。

五、少貼文、少分享、取消按讚

無論是 po 文、分享或按讚的行為，都能讓臉書記下你的喜好，所以盡可能避免這些主動的行為，也是保護自己的好方式。

就算臉書天天滑，個人資料保護也不可忘！

「早上起來滑一下、晚上睡前滑一下」是許多人使用臉書的日常，就算我們很難脫離臉書生活，還是要記得使用這些服務有可能帶來的負面效應，在享受服務的同時，也別忘了時時提醒自己，不要在毫無所覺的狀況下把自己給「賣」了出去。

為自己訂下個鬧鐘吧！下次「開滑」之前，先確定隱私設定都做好了，才能在開心上網的同時，也保護好自己喔！

如何保護網路上的個人資料？



個人資料是什麼？為何要保護個人資料？

各位同學有聽過「個人資料保護法」嗎？你知道這一項法律和我們有什麼關係嗎？「個人資料保護法」主要是用來保護我們的「個人資料」安全，這裡提到的「個人資料」，包括我們的姓名、生日、身分證號碼、聯絡方式等等，只要是可以讓別人知道我們身分的資料，都算是「個人資料」。

為什麼我們的「個人資料」需要被保護呢？這是因為，如果我們的個人資料被別人知道了，可能就會接到很多廣告信或是廣告電話，如果是被歹徒知道就更糟糕了，歹徒可能會假冒我們的身分去做壞事，讓我們的親朋好友被騙，造成金錢上的損失，或是和我們一樣，個人資料也被歹徒騙走，這樣歹徒又可以拿他們的資料去詐騙更多人了。

如何保護在網路上的個人資料？

既然個人資料很重要，我應該如何保護在網路上的個人資料，不要讓它被偷走呢？平常我們上網的時候，常常會需要在網路上留下個人資料，像是加入成為某一個網站的會員，或是在網路上買東西、參加抽獎活動，各位同學可以注意一下你使用的網站是不是有提供「隱私權聲明」或是「隱私權政策」這一類的說明，在這個頁面裡，網站的管理人員會告訴上網的人你在這個網站輸入的個人資料會怎樣被使用和保護，這些說明文字通常有點困難不容易理解，各位同學可以請家長或老師解釋給你聽，幫助你一起判斷這個網站是不是可以信任的，再決定要不要在網站留下資料，絕對不要想說看不懂就算了，就直接填寫資料喔！

謹慎點選網路上的超連結

網路上還有一些會偷走我們個人資料的陷阱，也就是所謂的「惡意連結」，這些「惡意連結」常常會假裝是好聽的音樂或是好玩的小遊戲，欺騙我們去點選下載，當我們點選之後電腦可能會中毒，歹徒就可以利用電腦病毒把我們存在電腦裡的個人資料和其他重要資料通通搬走。在這裡要提醒各位同學，當你要點選網路上的連結時，一定要先停下來想一想，確定這個連結是可以信任的、安全的再點選喔！



2023資訊安全新知不可不知

面對變化多端的資安威脅，企業該如何制定資訊安全的防護策略和規劃預算的分配呢？我們將2023年的資安趨勢整理成以下4類提供給大家參考。

1.層出不窮的各種類資安攻擊手法

隨著IoT、5G、AI等各類新興技術快速地發展，與之相關的網路資訊安全威脅變化與攻擊頻率也愈加頻繁。如有漏洞或未及時修補的問題，非常容易成為駭客的攻擊目標。

2.資安人才資源的短缺

隨著許多商業行為與業務都更加依賴數位化及網路化，網路和資訊安全也越發重要，要有效的應對各類型資安風險與駭客攻擊，就必須具備專業的資安人員及防護工具，因此資安人才將會是重要的資源。

3.因地緣政治連帶的資安風險

近期俄羅斯入侵烏克蘭，兩國都頻繁透過資訊戰來影響局勢的發展，而台灣與中國的兩岸關係也很容易隨時事而產生變化，在美國眾議院議長裴洛西訪台期間，台灣的資訊設備遭受網路攻擊的事件比過往更高出約23倍；因此政治因素帶來的資訊安全風險也是必要的考量因素。

4.持續進化的法規監管

在過去幾年，世界各國對於個資的保護越發重視，因此監管要求不斷地提高，包括處理資料隱私的法律，更加重視資料保存與使用上的安全性。所以企業更需留意自身的資安規範是否能持續合規。