公務機密

資訊安全維護

防駭不注意，隱私落滿地

不輕易使用免費或不明WIFI無線上網　避免個資遭竊

資安時事案例

◎**臉書資安事件 企業應引以為戒**

◎伊朗駭客假冒Gmail和Yahoo發送釣魚郵件

個人資料保護法

輕鬆學資安

◎electronic Cash電子現金

數位學習 106年資安動畫金像獎

我要成為資安王!

臉書資安事件 企業應引以為戒

工商時報 劉懿慧／台北報導

臉書（Facebook）爆發用戶個資遭濫用，估計約有5,000萬人受影響，勤業眾信風險管理副總林彥良指出，近年數位空間的隱私保護與資安法規發生革命性翻新，本次事件也牽涉歐盟通用資料保護規則，可被視為敲醒數位時代隱私與資安保護浪潮的又一響鐘，企業應引以為戒。

林彥良表示，企業檢視個資保護作為有三大關鍵，第一是定期檢視隱私保護機制，包括公開透明的告知與明確的同意，且定期實施資料外洩應變演練等作業；再者，應落實委外安全管理，例如盡職調查、合約安全要求、資料安全管理、定期安全評估與現場實地稽核等。

最後，企業必須全面落實預設隱私保護，將預設隱私嵌入業務營運流程，並定期或於業務流程、資訊系統發生重大變更時，實施隱私衝擊評估，確保隱私保護機制持續有效，以落實數位時代隱私與資安保護。

安侯建業數位安全服務負責人謝昀澤表示，5月歐盟新版GDPR（個資法）上路後，若「臉書事件」重演，所面臨的罰鍰恐將達全球營業額4%以上。謝昀澤指出，此一事件並非駭客入侵竊取個資的傳統資安事故，而是社群網路服務因營業模式或協作廠商的管理疏失與不當利用，所導致的「侵害用戶隱私權」事件。

此類事件檢討的關鍵重點並不在企業的防毒、防駭，謝昀澤認為，重要的是，這些新科技媒體產業能否修正隱私保護的重大瑕疵與缺陷流程，並升級成能兼顧隱私保護的產品或服務，這項轉型能否成功，也攸關其他類似臉書的互聯網大帝國，能否持續壯大的關鍵因素。

(工商時報)

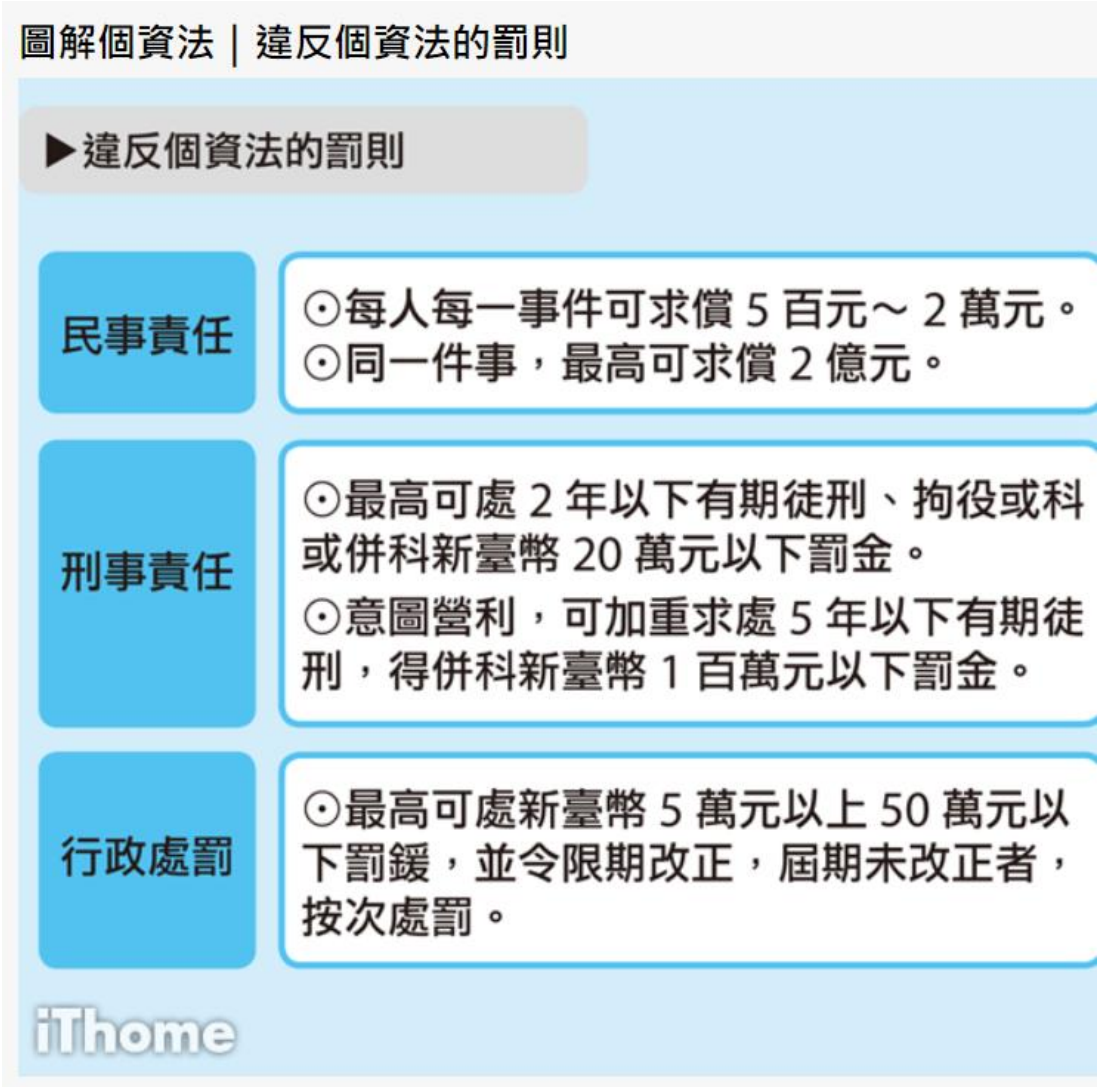
伊朗駭客假冒Gmail和Yahoo發送釣魚郵件

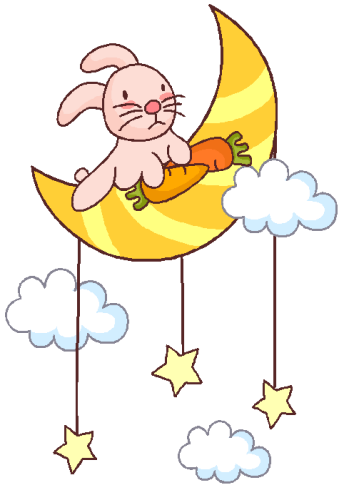
安全研究公司Certfa Lab發現最近有親伊朗政府的駭客向美國政府官員、社會運動人士和記者發送釣魚郵件，甚至連Gmail、Yahoo Mail等服務的雙因素驗證(Two Factor Authentication, 2FA)也能成功繞過，突顯2FA技術安全性堪慮。Certfa Lab表示，11月間偵測到有精準網釣攻擊郵件，對政治人物、記者或人權人士發送以「notifications.mailservices[at]gmail.com」、「customer[at]email-delivery.info」為標題的釣魚郵件，通知他們的Gmail或Yahoo Mail信箱帳號遭未授權存取，請其立即點擊信中連結了解詳情。和其他網路釣魚攻擊一樣，該信會將受害者導向假的Gmail或Yahoo Mail網頁，要求用戶驗證帳號、密碼以便登入下載檔案。為此駭客還架了一個以假亂真的Google Drive網頁以搏取受害者信任。此外，為了躲避Gmail的檢查，網釣郵件還以圖片為信件主題。信件中並嵌有一個隱藏圖片檔，讓用戶上鉤時立即通知駭客。

根據網釣郵件來源網域，研究人員判斷這是源自伊朗政府支持的駭客組織Charming Kitten，可能和美國對伊朗實施的軍事和經濟制裁有關。研究人員已通報Google撤下駭客Google Site網頁。這次攻擊較特別的是，透過釣魚信件的隱藏圖片，駭客會獲知用戶上當，且同步於真正Gmail和Yahoo Mail登入頁中輸入檢查是否正確。即使如果郵件啟用了簡訊、像Google Authenticator等驗證app的2FA，也可以依此竊取2FA驗證碼。此外，為免打草驚蛇，駭客不會變更用戶密碼，以便未來還可以用上這些郵件帳號。這次的網釣攻擊連2FA都能成功繞過，突顯2FA的安全風險，研究人員認為最保險的方法是使用YubiKey等FIDO (Fast Identification Online)標準的硬體驗證金鑰。Google已經於2014年支援FIDO硬體安全驗證，而包括Google Chrome、Microsoft Edge與Mozilla Firefox等瀏覽器也承諾支援FIDO2身分驗證規格，降低使用者連上釣魚網站的風險。

圖解個資法

違反個資法的罰則





electronic Cash

電子現金

資料出處： i-Security

電子貨幣的一種，為了因應電子商務的廣泛運用所發展出替代實體現金的交易方式。使用者能於網路上設立專屬的電子帳戶，每當在網路上購物後，可直接透過電子帳戶扣除帳戶裡的錢。而電子帳戶中的錢即為電子現金。