

留意偽冒 Gmail 「已攔阻可疑登入」釣魚信件

發布時間：2015/4/10 下午 12:02:38

刑事警察局 165 反詐騙諮詢專線近期接獲民眾檢舉，指稱其 Google 電子郵件(或稱 Gmail)接獲疑似假冒以 Gmail 公司名義發送之釣魚信件，內容為「已經成功攔阻帳號免遭到駭客入侵，並明確標明入侵時間、IP 與地點」，要求郵件使用者點選信件下方【重設密碼】選項，實為竊取民眾帳號、密碼。由於近年 Google 服務跨越電子郵件、行動電話作業系統、行動軟體(Google Play)及電子錢包(Google Wallet)等領域，均由帳號、密碼控管，遂成駭客覬覦目標。

本次所發現之網路釣魚信件，不僅可躲過 Gmail 系統垃圾信攔截偵測，且利用 Gmail 電子郵件本身有攔截異常登入行為，透過變造類似內容來取信民眾，此手法早期係由外國駭客產生並演變，當民眾 Gmail 帳號密碼遭到竊取後，駭客便利用該帳號設定之信用卡支付購買商品(如 APP 軟體或遊戲寶物等)或竊取電子郵件內容向第三人發送詐騙信件，目前 165 反詐騙諮詢專線雖未接獲因 Gmail 遭竊取後衍生之詐騙個案，惟仍呼籲民眾應多注意可疑電子郵件，避免受騙。當民眾接獲異常登入訊息之電子郵件，首先可透過 Gmail 電子郵件瀏覽頁面最下方【上次帳戶活動時間】及點選【詳細資料】，以瞭解最近登入的 IP 與使用瀏覽器情形，核對帳戶是否遭到入侵，另外也可使用 Gmail 所提供之免費『兩步認證』工具，透過帳號、密碼外之第三道動態密碼安全機制，防止遭到入侵。另外若民眾發現疑似接獲釣魚電子郵件時，可前往官方網站(<https://support.google.com/accounts/answer/6063333?hl=zh-Hant>)查證並對於惡意電子郵件進行申告停權，切莫未經查證貿然連結陌生網址並輸入個人帳號、密碼，造成後續隱私及財產權遭受侵害。近期 165 反詐騙諮詢專線針對最新詐騙手法建立多元宣導管道，民眾可透過 165 LINE 官方宣導帳號 (@tw165)、165 反詐騙臉書粉絲專頁

(<https://www.facebook.com/165bear>) 或 165 官方網站(www.165.gov.tw)
查詢最新訊息，以提升全民反詐騙意識，降低被害風險。

(內容摘自內政部警政署 165 網站)

國軍退除役官兵輔導委員會政風處關心您!