民國 114 年 6 月 12 日

內政部警政署刑事警察局新聞資料

■新聞稿 1 則　□背景資料　份　■照片 3 張

□請立即發布　■請於 114 年 6 月 15 日發布

提交 OTP 碼要小心 詐騙集團盜刷、盜領一空

現今民眾日常使用手機時，時常會收到 OTP 驗證碼的簡訊訊息，但多數人對其用途及安全意涵認識不足，很容易遭詐騙集團趁虛而入，透過假冒訊息或釣魚網站誘騙提交 OTP 驗證碼。一旦民眾誤信詐術並交出 OTP 碼，不僅可能導致信用卡遭盜刷，甚至會使銀行帳戶遭綁定至詐團控制的行動支付平臺，造成重大財務損失。

中部一名王姓婦女於 114 年 5 月中旬，接獲一則冒用知名銀行的釣魚簡訊，簡訊內容聲稱其帳戶需於月底前「實名驗證」，否則將停用相關金融服務，並附上偽造該銀行官方網站的惡意連結（https://ctbcbankebs-vastly.com/u，已停止解析）。王婦點擊連結後，網頁要求她輸入所持信用卡號、有效期限、卡片背面安全碼（CVV），接著又提示需輸入手機簡訊收到的「OTP 驗證碼」，王婦依指示操作，但系統不斷顯示錯誤，要求需重新驗證並再次輸入 OTP 驗證碼，導致她連續輸入 3 次，直至接獲銀行客服來電詢問是否有進行海外刷卡交易，王婦才驚覺信用卡已遭盜刷，經清點發現，信用卡於杜拜之網路商店被盜刷 3 次，合計共損失新臺幣（下同）32 萬餘元。

另北部一名陳姓男子於 114 年 3 月中旬在 PTT 社群出售二手手錶時遭詐騙集團鎖定，對方假扮買家，指定陳男須以某貨運物流平臺交易，騙稱該物流平臺會在訂單成立後匯款給陳男。為取信被害人，詐

騙集團再傳送網域名稱仿冒官方物流公司的釣魚連結（https://www.kerrytil.top，已停止解析），誘使陳男點擊。陳男陷入該詐術，在該網頁填寫出貨資訊後卻顯示訂單遭凍結，並跳出提示稱須完成四大電子支付工具的綁定驗證，才能解除限制。陳男信以為真，遂使用自己名下的四家銀行帳戶，嘗試綁定 iPass MONEY、悠遊付、街口支付與 icash Pay 等支付平臺，並依頁面指示提交 OTP 簡訊驗證碼，豈料綁定後，陳男帳戶內資金即遭快速轉出盜領，雖於事後察覺異常並緊急聯繫銀行要求取消綁定，但仍不幸遭詐損失近 40 萬元。

刑事警察局提醒，OTP（One-Time Password）一次性密碼是網路金融交易中驗證本人身分之重要安全機制，民眾在收到 OTP 簡訊時務必詳讀內容，特別注意其中是否包含交易幣別、金額及用途等資訊，若與實際操作不符，切勿將 OTP 密碼輸入至任何網頁或告訴他人，以防落入詐騙陷阱。另近期發現釣魚連結不再僅透過簡訊傳送，亦已擴及電子郵件與假買家詐騙中，此類釣魚連結常偽冒的官方網站包含遠通電收（稱未繳停車費）、金融機構（稱帳戶需驗證）、公家機關（催繳水電費或罰鍰）、電商及物流平臺（偽造刷卡交易或綁定他人電子支付）。民眾在日常查看簡訊、電子郵件，或使用通訊軟體及社群平臺等網路活動時，務必慎防來路不明的訊息，除應仔細檢查訊息發送來源外，並應比對陌生連結與官方網站之網域名稱是否一致，同時善用 Whoscall 或趨勢科技防詐達人等防詐 APP 辨識連結功能，如對陌生訊息仍感到存疑，請立即停止任何操作，並撥打 165 反詐騙諮詢專線或官方客服求證。

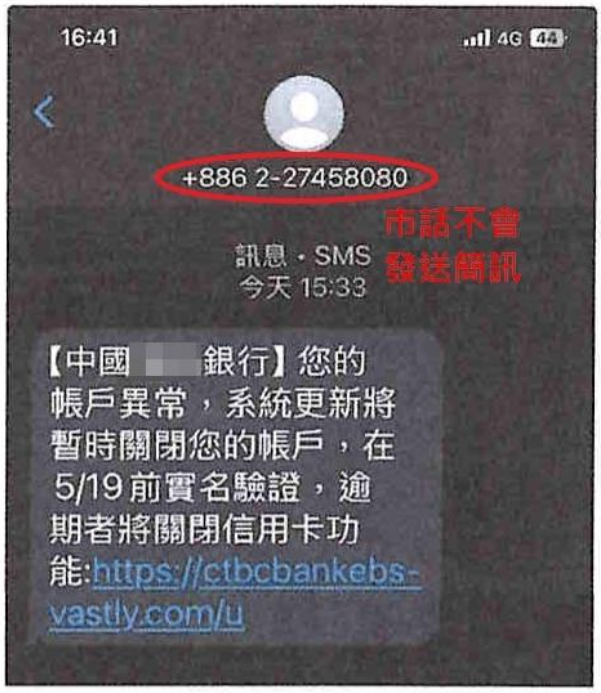
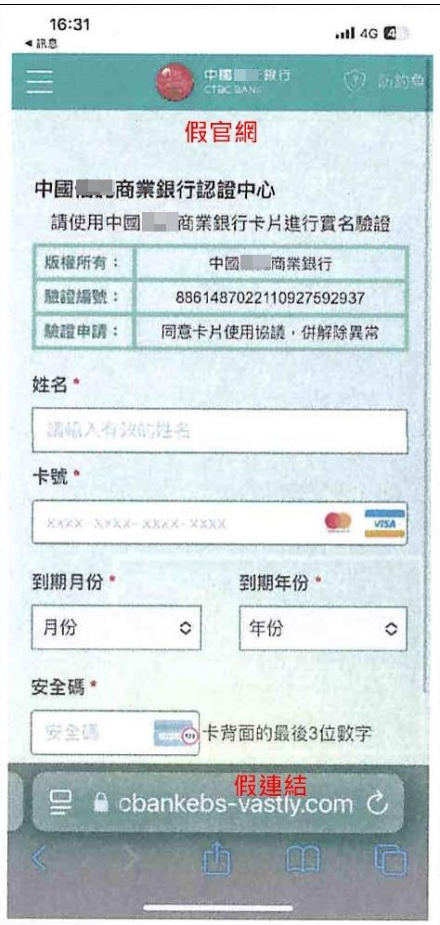
<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>圖 1 - 釣魚連結假冒知名銀行。</td>
<td>圖 2 - 釣魚連結騙取信用卡個資</td>
</tr>
</table>

圖 3－於釣魚連結輸入 OTP 碼，信用卡即遭海外盜刷

圖 4－釣魚連結務必查證