

6蚊釣魚騙局 幫緊你？呃緊你！

訛稱包裹派遞失敗更新地址 500人遭套取信用卡資料



◆警方記者會解構騙徒手法及展示搜獲的證物。

香港文匯報記者劉友光 攝

「包裹XXXX號派送失敗，請前往<https://xxx.com>確認您的地址以便再次安排送貨。」相信有很多市民近月都收到這種手機SMS短訊。這是香港本地詐騙集團針對港人的「服務式釣魚」新騙局，騙徒假冒香港郵政和不同快遞公司發短訊，引誘市民進入偽冒網站更新地址「以完成送貨服務」，由於短訊來自本地手機，以及需用信用卡支付僅僅6元手續費，令常用網購服務的市民頓感「安心」，詎料「一鍵按入」變荷包「大出血」，其信用卡快速被綁定到騙徒的手機電子錢包上，然後被騙徒到商店瘋狂掃貨。警方近日拘捕8名騙徒，揭發他們在一個月內發出100萬個附有超連結釣魚詐騙短訊，套取500名市民信用卡資料，當中有183人已被騙270萬元。

◆香港文匯報記者 蕭景源

警方昨日公布案情指出，這是警方首次發現有本地騙徒利用實名登記的電話卡，在香港本地設置詐騙短訊發放中心，目標也是香港本地的信用卡用戶，其犯罪手法涉及到快遞元素，市民更應加倍小心。

警方指，因大部分市民都有用電子銀包或信用卡網購的習慣，網購通常也隨之附帶快遞服務，市民可能使用過不同的快遞公司，因此，騙徒漁翁撒網式發放詐騙信息，令不少潛在受害人在收到詐騙短訊後，容易自動「對號入座」上當受騙。

其次，是騙徒用6元手續費「釣大魚」，低額手續費令市民解除戒心，以為就算被呃也就損失6元，但其實騙徒的終極目標是騙取信用卡資料。雖然案中單一最大損失12萬元，最少損失600元，但騙徒向全港市民發放海量短訊，將令上當者倍增。

月發百萬短訊 誘入偽冒網站

警方調查並破解該本地犯罪組織的犯案手法，發現騙術自今年8月開始，在香港設立不同據點，假冒香港郵政及不同快遞公司，隨機向市民發送SMS電話短訊，短信附有超連結連至偽冒的網站，並要求市民繳交低額的手續費，以便完成送貨。犯罪集團利用從收債集團得來的市民身份證等個人資料，在網上向電訊商實名申購手機SIM卡，然後安排人到便利店領取SIM卡。為了增加市民上釣機會，騙徒利用俗稱「貓

池」的電話數據機，同時插入數十張SIM卡，每日都發出大量假冒快遞公司欺詐短訊，由今年9月30日至11月8日，一共用300張SIM卡發出超過一百萬個欺詐短訊，高峰時一張SIM卡在3小時內發出逾7,000個短訊。這些欺詐短訊附帶一個超連結，訛稱有包裹派遞失敗，需要更新地址，誘使市民點擊該連結進入偽冒的快遞公司網站。

當市民進入偽冒網站更新地址後，騙徒打出信息要求市民用信用卡支付港幣6元的手續費，誘使受害人輸入信用卡資料，同時騙徒將有關信用卡資料綁至騙徒手機的電子錢包，這時發卡銀行會向市民發出一一次性驗證碼，此時虛假網站就會彈出一個版面，要求市民輸入一次性驗證碼，聲稱為該6元手續費交作授權。

「釣起」500張信用卡 涉款270萬

當市民輸入該驗證碼後，騙徒就成功將市民信用卡資料綁至他們自己手機的電子錢包。及後，騙徒安排俗稱「車手」的同黨，持電子錢包在全港各區購物，當中包括手機、電器、現金券及點數卡，每名「車手」每次交易可獲取500元至1,000元報酬，相信他們在3個月內，至少利用183名受騙市民的信用卡資料，在全港進行500次購物，令市民共損失270萬港元。

網罪科探員深入調查及情報分析，由11月7日

您的快遞配送無人簽收，派遞員派送失敗。請更新您的地址：
<https://hksfteq.com>

◆騙徒以漁翁撒網的方式發送釣魚短訊。

至9日展開代號「黑雷」行動，在旺角、筲箕灣、銅鑼灣、荃灣及葵青的酒店及住宅單位，以「串謀欺詐罪」共拘捕8名本地男子（17歲至44歲），包括集團主腦及骨幹成員。行動中，警方檢獲一部「貓池」機、3部電腦、25部手機；另於旺角的酒店內檢獲295克懷疑氯胺酮，並在主腦身上起回19萬元現金。

警方亦在騙徒電子裝置內發現超過60名香港市民的個人資料，相信將會被用作登記購買電話卡。此外，警方發現500張信用卡資料，當中有部分已被綁綁騙徒的電子錢包購物，相信有500人中招，只是騙徒仍未成功用來綁綁電子錢包購物。

理心」，扮子女向父母索要「保釋金」，這種騙案往往亦令市民在情急下受騙。

至於網上情緣騙案靠的是「氹」，騙徒有耐心和長時間偽裝關心，令受害人有「被愛」的感覺，繼而做出各種非理性的行為，並會產生「確認偏見」，再陷入投資等陷阱。

而騙徒偽冒快遞公司、衛生防護中心、社會福利署或金融機構套料行騙，則利用了服務性行業的特點，令市民覺得可能與大額金錢無關，所以「唔上心」而輸入個人資料，最終因小失大。

詐騙短訊「煩過鬼」 中伏3天「嚟多鑊」

李女士：幸記賬卡戶口無大額存款

李女士向記者展示手機短訊說，今年10月3日，她接獲一個標稱是DHL快遞的短訊，指其有包裹因派發地址錯誤，要求按入短訊內一條超連結登記資料。由於她本身有使用DHL服務，所以不以為意便按指示按入，並輸入了銀行卡資料，並在頁面填寫地址及繳付15元手續費，由於金額不大，她於是照付。及後，她思前想後覺得有可疑，於是按短訊提供的包裹編號，進入DHL的包裹追蹤網頁查核，發現並沒有此包裹編號，懷疑受騙，遂致電DHL查詢及求助。DHL職員相信她已受騙，建議她馬上取消信用卡資料，以免蒙受損失。不過，李女士指自己使用的是記賬卡，戶口沒有大額存款，故騙徒沒法盜取金錢。不過，3天後，她的手機又接獲同樣的包裹派送短訊，她未有理會，令她感到非常無奈，認為「騙徒如鬼魂纏身」。

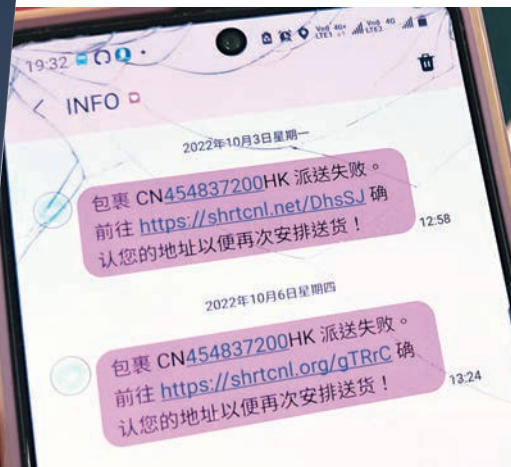
年約30歲的文員張先生表示，近年經常有類似騙案的新聞報道，因此他自己也十分警惕，因為涉及的騙術種類繁多，難以逐一掌握，但騙案基本上萬變不離其宗，「（騙徒）唔係擇錢就擇料」，他索性對所有可疑來電、短訊及超連結一概拒接拒看，所以沒有被騙經歷。不過，他一名朋友的姐姐曾收到這些詐騙短訊，要求她輸入個人資料，所幸她醒目，即時致電其弟查詢，被「點醒」後才免受騙。

◆香港文匯報記者 蕭景源



張先生

「釣魚短訊」騙財解構



◆李女士展示電話騙案短訊。香港文匯報記者 攝

由嚇到氹再扮服務 騙徒「劇本」屢「進化」

香港文匯報訊（記者 蕭景源）據警方網絡安全及科技罪案調查科和警方臨床心理專家分析總結，時下流行各類電訊和網上騙案，基本與「網絡釣魚」息息相關，最終目的都是為了套料和直接騙財。警方提醒市民，防騙的關鍵要「心快手慢」，給自己爭取時間冷靜思考，先查證後行動。

騙徒的釣魚手段，通常有語音電話、偽冒網站、短訊、電郵及App五大類，並在不同時期根據社會議題使用手段，運用「社交工程」技巧，編造不同劇本攻克市民心理防線。例如騙徒利用「假冒官員」就是靠「嚇」，通過「建立權威」，令受害人產生恐懼和孤立，「猜猜我是誰」則利用「嚴重性」、「迫切性」和人的「同