

緊貼最新防騙資訊 反覆求證 識破百變騙術



騙徒無處不在，無孔不入，電騙、網騙、網戀、各種虛假的投資信息，每日狂轟濫炸，排山倒海充斥着日常生活，市民稍有不慎隨時中招，損失慘重。據警方早前的數據顯示，今年首三季錄得3523宗網上投資騙案，比去年同期上升近1.6倍，損失金額增2.2倍，約

21.3億元。受害人除了普通市民，還有教授、醫生、投資顧問、銀行董事等專業人士。

恐懼、無知、寂寞和貪心是人性的弱點，亦是騙徒向你埋手的切入點，編造不同的騙案劇情，配合心理技巧，令你墮入騙局。時代進步，騙徒也在不斷更新騙術和手段，市民只有時刻提醒防備，切勿輕信突如其來的短訊，牢記便宜莫貪，不斷更新及認識最新防騙資訊，反覆求證，做個「百騙不侵」的精明市民。



大公報記者 盛德文、黃山（圖、文、視頻、網上圖片）

「這些不法歹徒的騙術真是層出不窮，無所不用其極，令人防不勝防，對發來的訊息都無砸信心，因為這些短訊都不知哪些是真、哪些是假，稍不小心就隨時中伏，現在即使收到真短訊都敢當真，真是令人氣憤！」從事地產物業投資的張先生向大公報記者滿腹怒氣說道。

釣魚短訊網站無孔不入

騙徒利用手機釣魚短訊行騙愈來愈猖獗，市民接到愈來愈多來歷不明、五花八門的釣魚信息。據本港警方資料顯示，今年首九個月接獲3569宗釣魚騙案，損失金額約8910萬元，而張先生就是其中一名損失3萬元的釣魚短訊受害人。

今年7月9日中午，張先生手機突然收到一條附有網址連結的短訊，指其積分到期有禮物換。他以為是電訊商發送的短訊，隨手點入連結，出現疑是電訊商的網站，內裏展示了很多只需1元便可換取的禮品，由於自己是該電訊商的長期客戶，不虞有詐的他按指示輸入電話號碼、個人資料、信用卡號碼和卡背後的CV號碼，隨即便彈了一個加1元的連結並要求填密碼，當他輸入密碼後，立即獲信用卡公司發短訊通知，成功交易了3萬元，緊接着又彈出第二條標示2萬元要輸入密碼的連結，「原本以為交1元的，怎知卻突然變成交易3萬元。」此時，張先生才恍然醒悟，中了騙徒釣魚短訊的伏，即時報銀行為止交易不果，遂報警求助。

張先生表示，平日都收到不少類似的短訊，不過因為忙，無理會，那天剛好休息點入連結，豈料



▲立法會議員江玉歡的兒子早前收到假冒的WhatsApp更新軟件短訊，賬號被騎劫並向親友借錢，幸好發現得早，避免損失。



▲網戀是常見詐騙手法之一，騙徒會在社交媒體中扮成俊男美女或專業人士結識受害人，發展網上情侶後，就會以不同藉口索要金錢。



損失。

江玉歡表

示，數周前20

多歲的兒子收

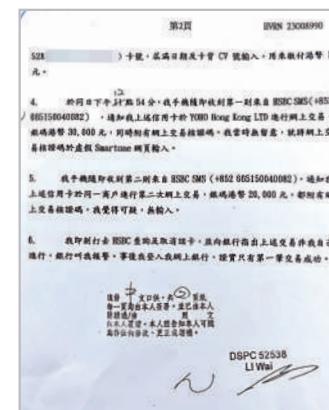
到假冒的WhatsApp更新軟件短訊，不小心

點入連結，手機賬戶好快便就被騎劫了，並冒充兒子向羽毛球教練和爺爺嬪嬪借錢。當時教練已準備

好轉賬2萬元，所幸臨尾一刻致電兒子確認時，發

覺受騙及時終止轉賬。騙徒更致電兒子的爺爺嬪嬪借錢，所幸他當時正陪爺爺嬪嬪晚飯，當場揭穿騙

案。



▲專家提醒，市民在使用程式時，不要輕易輸入電話號碼、信用卡號碼等個人資料。網上圖片

毒App款多難辨真假 勿胡亂下載

加強防範

看見平價旅遊套餐、電子產品、包車服務、入油優惠等貼文或訊息，可能是黑客偷走你金錢的第一步！」警方「守網者」Facebook專頁顯示，由9月至11月初接報至少六宗有關報案，受害人均被社交平台廣告或白撞WhatsApp訊息吸引，輾轉被誘騙在安卓(Android)手機下載「第壹商城」、「港澳商城」、「88雜貨舖」等毒App後，網上銀行存款遭轉走，合共損失68萬元。

案情透露，一名中年男子看到一個名為「金歐旅遊」的專頁出售平價旅遊套票，經WhatsApp聯絡客戶服務員。對方向男子發送連結，要求男子安裝「港澳商城」App，並登記會員取得優惠。男子不虞有詐，下載毒App並輸入銀行戶口登入憑證，銀行賬戶隨即被轉走24萬元。

兌換店職員失100萬人民幣

警方表示，這類毒App含有惡意程式碼，安裝時取得事主允許完整操作權限後，黑客便可遙距操控手機，取得手機的SMS短訊、擷取鍵盤按鍵紀錄，甚至執行手機內的任何App。黑客還會不定期製作各類社交專頁和更改毒App名稱，甚至把毒App包裝成不同款式的

工具，例如視頻播映工具，與真App幾可亂真，令使用者減少防範。市民近期如在搜尋器或瀏覽器輸入「WhatsApp」字眼時，有機會出現以廣告形式置頂連結的虛假網頁版，用家一旦誤登入以「WhatsApp」包裝的假網站，輸入電話號碼、驗證碼等，賬號即被騙徒騎劫，並隨機向聯絡人發出借錢訊息，甚至再去騙取其他人的WhatsApp賬號，擴大詐騙對象人數。

一名兌換店職員無辜被捲入漩渦，騙徒騎劫其WhatsApp賬戶後，假扮他與一名有生意來往的聯絡人通訊，以人民幣兌換率非常優惠為藉口，騙取對方把100萬元人民幣存入兩個指定內地戶口，直至同日下午，聯絡人與兌換店職員溝通時才揭發騙案。



▲警方提醒市民，應到官方網站下載軟件，確保安全。網上圖片

家庭式「網戀」團夥 喰155人2100萬元

騙財偷心

今年11月5日至11日期間，警方東九龍總區展開打擊網絡投資騙案的「鑽鋒」行動，一周內拘捕223人，涉及265件案件，金額達1.8億元。案中共有328名受害人，其中一名80歲的婦人損失超過910萬元。

該名曾任職電梯設計工程師的婦人，在網上放租物業時，遇上自稱是銀行數字資產高級分析師的騙徒，誘騙女事主在虛擬貨幣投資網站投資，事主先後40多次存入款項投資，最後被騙逾910萬元。

此外，「網上情緣」亦是騙徒常使用的招數。警方今年5月破獲一個家庭式營運的「網上情緣」詐騙團夥，合共拘捕10男5女。該家庭式詐騙集團以本地男性為主要目標，集團成員假扮不同國籍的人士誘騙受害人，然後詐稱財困、染病及繼承遺產等不同藉口進行詐騙。由去年1月至今年5月案發，共騙取155人逾2100萬元。

另一名「網上情緣」受害者為63歲任職投資經理的男子，早前在網上交友平台認識一名女子後，發展網上情緣，女子聲稱是虛擬貨幣投資專家，誘騙事主投資。去年12月至今年1月，受害人共轉賬約1200萬元至對方指定的賬戶，其後未能取回款項，懷疑受騙報警。

星洲銀行App 遇可疑阻截登入

他山之石

電騙案猖獗，警方與銀行攜手採取各種把關措施，防止罪犯得逞。

金融界立法會議員陳振英昨日在一個電台節目上表示，新加坡在上月起推出新措施，要求各銀行的流動理財應用程式(App)加入阻截功能，一旦偵測到手機內有來歷不明的應用程式時，便不允許登入(login)銀行的程式。他認為新加坡的做法實際又有效，值得本港參考，建議由監管機構牽頭，聯同所有銀行採取有關措施。

港銀行近數月阻止200宗騙案

陳振英又指，就近期的騙案，警方與各大銀行採取各種有效措施，包括審視一些過往只用作收取騙款的傀儡戶口，並通知曾轉賬至有關戶口的人士，數月內已成功勸阻約200名受害人繼續轉賬。

銀行業亦會共享傀儡公司戶口的資料，下一階段將研究共享個人傀儡戶口的私隱問題。業界還會就大額交易進行額外認證或與客戶確認交易，期望防止騙案發生。

四種常見詐騙手法

1 電話騙案

一味靠嚇，令你思想混亂不能作出理智決定。假扮內地執法人員稱受害人在內地犯法，要求支付金錢作保證金，或交出網上銀行賬戶號碼及密碼作調查用，並出示「假證件」、「假調查令」、「假拘捕令」等威脅受害人，若拒絕合作將會被拘捕。

2 求職騙案、刷單賺佣圈套

世途險惡，不要太天真，搵快錢變中伏。騙徒利用「高薪厚職」、「無需經驗」、「彈性工作」等字眼，在社交媒體發放招聘廣告，聲稱只要在購物網站將貨品放入購物車並將截圖發給騙徒，再將購物金額轉賬到騙徒的銀行賬戶，就可賺取佣金並獲退回購物金額。當受害人執行大額刷單任務並墊支大筆購物款後，騙徒便逃之夭夭。

3 網戀騙案

小心不期而遇的網上邂逅，令你賠上一生積蓄兼亂心智。騙徒會在社交媒體中扮成俊男美女或專業人士結識受害人，然後噓寒問暖，發展網上情緣後，以不同藉口索要金錢，如送名貴禮物給受害人但需繳交關稅；家人身患絕症要醫藥費；出現財務危機急需現金周轉等。

4 投資騙案

貪心會衝昏你頭腦，令你孤注一擲。騙徒會自詡投資達人，透過社交媒體結識受害人，推介虛假投資應用程式，聲稱掌握升跌規律，或有內幕消息，只要跟隨提供的貼士在程式內投資，就會有所斬獲。不過，所謂「零風險高回報」、「必賺投資應用程式」最後都血本無歸。謹記：「贏粒糖，輸間廠」，若有必勝投資，為何要與你分享？

懷疑受騙及求助途徑

24小時熱線

防騙易：18222

網上查詢

防騙視伏器：

<https://cyberdefender.hk/scameter/>

防騙視伏App：

輸入平台賬戶名稱或號碼、收款賬戶、電話號碼、電郵地址、網址等，評估詐騙及網絡安全風險

資料來源：警方反詐騙協調中心