洗錢手法再升級！

詐團改用「釣魚網頁+電子支付」 騙取電支帳戶

民眾淪人頭洗錢工具

詐騙集團洗錢手法再度翻新！過往詐團多以收購或騙取實體金融帳簿、卡片作為洗錢工具，近期警方發現，詐騙集團已將目標轉向「**電子支付工具**」，利用假一頁式網頁、假快遞、假客服等釣魚手法，誘騙民眾交付個資與關鍵驗證碼，隨後強行綁定「**電子支付帳戶**」進行洗錢，導致無辜民眾在不知不覺中淪為詐欺共犯。

中部一名許姓女子，於今年 6 月中旬，在臉書（FB）購買縫紉機，隨後收到賣家訊息，宣稱將透過黑貓宅急便配送商品，對方隨即傳來一個極度逼真的假快遞網頁連結（https://www.t-cat.vom.tw.lsp.shop/...），要求被害人點擊進入填寫配送資料。

被害人依約填寫後，詐團食髓知味，再度假冒黑貓宅急便名義，聲稱「帳戶遭到凍結，導致物流作業異常」，指引被害人點擊網站上的客服連結。被害人點擊後被引導加入一個虛假的 LINE 客服帳號。該假客服以「需進行實名制認證以解凍帳戶」為由，誘騙被害人提供身分證字號、出生年月日及銀行帳戶帳號。隨後，詐團利用這些個資

在後台發動電子支付綁定程序，被害人在未察覺異狀下，將手機剛收到的簡訊驗證碼一併交付給假客服。

直到 2 天後，被害人愈想愈不對勁，主動向銀行申請凍結帳戶，但為時已晚，詐團早已利用騙來的個資與驗證碼，成功綁定了**「街口支付」**、**「愛金卡（icash Pay）」**及**「全盈+PAY」**等數個主流電子支付工具，並將該帳戶作為詐欺贓款的洗錢轉帳管道，帳戶在當時已被灌入大量異常金流，才驚覺遭詐並向警方報案。

刑事警察局呼籲：

「電子支付工具」因具備開戶便利、轉帳迅速等特性，已成為詐騙集團眼中的洗錢新寵，民眾網購時務必提高警覺，切勿點擊來路不明的簡訊、網頁連結。**簡訊驗證碼（One Time Password，簡稱 OTP）等同於網路交易的個人簽名與通行密碼，在任何情況下都絕不可交付給任何人**，民眾若發現帳戶有異常登入或綁定情形，應立即聯繫銀行掛失，並撥打 165 反詐騙專線或 110 報案求助，以免淪為詐騙集團的洗錢工具。