

內政部警政署刑事警察局新聞資料

短短 10 日 詐團冒充一卡通 iPASS MONEY 詐 172 件 獲利近 900 萬 刑事局示警 詐團改冒用悠遊付行騙

從今年 10 月 10 日起，民眾陸續收到誣稱「一卡通 iPASS MONEY」的 Email 或釣魚簡訊，佯稱更新會員資料、iPASS MONEY 消費回饋等緣由，邀請民眾點入仿冒一卡通官網的詐騙頁面，報案人不疑有他，點擊「立即參加活動」按鈕後，於網站輸入姓名、身分證字號、iPASS MONEY 密碼及電話號碼後，旋即遭盜刷。

雖然詐騙案件皆為小額盜刷，但今年 10 月 10 日迄今共有 173 件報案，短短 10 日民眾遭詐總金額達 872 萬元，其中最高遭跨境交易 21 筆共盜刷 18 萬 3,572 元。刑事局進一步分析，該類詐騙網站的網址為了仿冒一卡通官網，雖有出現 https://***.ipass-***.***，但網址 ipass 前後皆有出現其他亂數字母，如：<https://ipass-spayx.net/ipay/#/page/index>、<https://ipass-walletb.com/twpay/#/page/success>，而非官網乾淨的 <https://www.i-pass.com.tw/>，混淆民眾視聽，加上以消費回饋、帳號功能調整或更新會員資料為由，導致民眾不疑有他紛紛遭詐。

刑事局雖已將民眾報案的假網站停止解析，但分析資料發現，自 10 月 21 日起，詐團改用「悠遊付」名義相同手法傳送 Email 或釣魚簡訊，同樣謊稱更新帳戶、儲值回饋等理由，要求民眾填寫個人資料、密碼、手機號碼及 OTP 驗證碼，陸續因盜刷而進線 165 報案。

刑事局呼籲公司企業，如有建置蒐集個人資料之伺服器主機，應強化資安、提升防火牆防毒功能，以防止客戶資料外洩，造成民眾財損與恐慌，並提醒民眾，接收 Email 或簡訊應仔細辨明網址，相

關操作應至官方網站查證真偽，且各項資料更新未涉購物消費，都不應輸入 OTP 驗證碼，如被要求輸入 OTP 驗證碼，皆須留心信用卡遭盜刷。