內政部警政署刑事警察局新聞資料

刑事局示警：輸入「**21*」，自己的電話全被詐團轉接！假檢警詐騙再升級，2 天盜刷 260 萬、股票 105 萬遭變現!

刑事局表示，假檢警詐騙手法出現重大變化，已不再只是透過電話或視訊「做筆錄」騙取個資，而是進一步操控民眾手機通訊功能，攔截所有來電，進而突破金融防線。警方指出，詐騙集團現已結合「來電轉接」與「金融盜刷」，形成新型態「金融接管」犯罪模式，危害程度遠超以往。

新北市一名劉姓上班族於今年 1 月接獲假冒門諾醫院來電，對方謊稱其證件遭冒用，涉及盜領管制藥品，隨後再由假冒警察及書記官透過通訊軟體接續聯繫，要求配合調查並進行視訊筆錄。在對方層層話術誘導下，被害人逐步提供個人資料、信用卡資訊、網路銀行及證券帳密，落入詐騙陷阱。

詐騙集團接著要求被害人購買新手機，並提供不明網址指示下載 App。對方再提供一組帳號密碼，要求被害人登入後，將名下所有信用卡逐一感應綁定，聲稱是為了「查證金流」。警方指出，這並非正常調查程序，而是詐騙集團為掌握支付工具、準備後續盜刷所設下的重要步驟。

真正關鍵則發生在「來電轉接」。詐騙集團隨後指示被害人操作手機，輸入「**21*」加指定門號，完成來電轉接設定。警方強調，這是整起詐騙得逞的核心關鍵，一旦設定完成，被害人的來電將全面轉往詐騙集團控制的電話，包括銀行針對異常交易所撥打的查證電話，也會直接落入詐騙集團手中。此時即使銀行主動關懷或進行安全確認，也可能由詐騙集團冒充本人回應，使金融防護機制形同失效。

在成功掌控通訊後，詐騙集團隨即展開盜刷行動，短短 2 天內密集盜刷多家銀行信用卡，共 19 筆交易，金額高達新臺幣 260 萬餘元。由於查證電話遭轉接攔截，詐騙集團得以冒充本人回應，讓盜刷順利完成。

更令人震驚的是，詐騙集團並未就此停止，隨後再登入被害人證券帳戶，迅速變賣持股，套現約新臺幣 105 萬餘元。整起案件總損失高達 366 萬餘元，從信

用卡到投資資產全面遭侵害。

警方強調，假檢警詐騙已從過去「騙資料、騙匯款」，升級為「買新手機、下載不明 APP、綁定信用卡、設定來電轉接、接管金融驗證」的複合型犯罪。民眾一旦依指示輸入「**21*」並設定指定門號，等同將自己的電話與驗證通道交給詐騙集團，風險極高。

刑事局呼籲，凡接獲要求下載不明 APP、綁定信用卡，或輸入「**21*」設定來電轉接或以其他方式設定轉接等，應立即中止操作並提高警覺；切勿提供信用卡、網銀及證券帳密等敏感資訊。另提醒相關業者及機構，除強化風險警示與異常交易監測，應儘速共同研擬防制對策。民眾如遇可疑情形，請立即撥打 165 反詐騙專線查證，或至 165 打詐儀錶板查詢相關案例。