

其中的英文換成形狀相近的數字(如將英文字母o換成數字0)或將某些官網文字連結，請慎防。

※提醒8

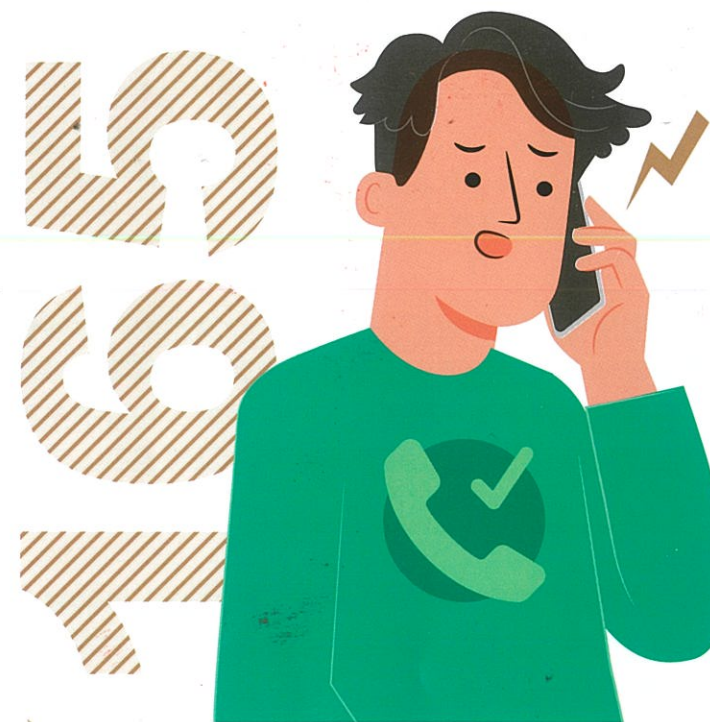
數發部已建置「111政府專屬短碼簡訊平臺」，做為行政部門發送簡訊的信賴管道，並協調各大電信業者在簡訊發送端檢核把關，目前已有122個政府機關完成導入。民眾收到手機簡訊時，只要認明111短碼，即可確認內容來自政府機關，可避免被詐騙集團偽冒的政府簡訊所騙。

如何查詢警示帳戶？

請撥打內政部警政署165反詐騙專線
或利用書面郵寄、網路向財團法人金融聯合徵信中心申請查詢。



內政部警政署 165全民防騙網



我要報案！

請撥打內政部警政署反詐騙專線 **165** 或撥 **110** 報案。

臺灣高等檢察署關心您 臺灣臺中地方檢察署

金融帳戶防詐指引

為什麼 我會莫名其妙成為 詐騙、洗錢案的被告



臺灣高等檢察署 編印

小心！詐騙集團會用盡一切方法騙取您的金融帳戶資訊，作為犯罪使用，常見手法如下

一、投資詐騙

詐騙者常假冒社會知名人士，以網路或社群軟體推播投資(教學)廣告，標榜內線消息、高報酬、零風險等，誑騙民眾加入群組或下載來歷不明的APP、誘騙匯款，投資標的則多為飆股、仙股、未上市公司股票、虛擬貨幣等金融商品。詐騙者會烘托交易熱絡假象，有些更會讓受騙者取得小額利益，目的是逐步鬆懈心防，使受騙者變現資產加碼投資(如配合不肖代書業者誘使以不動產抵押借貸)待榨乾資產後即消失無蹤，受騙者畢生積蓄付諸流水。提醒您，投資必定有風險，請保持理性判斷，並應向金管會核准的證券商、期貨業或投信投顧業者，購買合法金融商品。

二、網購詐騙

詐騙者會利用真假網購交易，誘騙民眾提供金融帳戶資訊，但該帳戶卻遭利用作為洗錢犯罪的金流跳板，典型案例如第三方交易詐欺犯罪。請慎選網購交易對象，務必了解對方的交易評價及信用，並請以相對安全的【貨到付款】或【信用卡付款】等方式支付款項，降低風險。

三、求職詐騙

請留心網路或Facebook等社群軟體上的徵才廣告，內容如果是短時間可以獲得大量報酬、無工作經驗、只需提供帳戶就能獲得報酬，但工作內容卻沒有詳細說明、讓求職者以加入LINE等社群軟體方面進行線上面試等，這些有極高的可能都是詐騙。詐騙者會以薪資匯款需認證金融帳戶為由，讓求職者寄送金融帳戶存摺、提款卡、密碼，但實際上是蒐集作為人頭帳戶。

四、貸款詐騙

詐騙者會以代辦貸款的廣告訊息，吸引急需金錢的民眾，以此取得民眾身分證明文件、金融帳戶存摺、提款卡、密碼。也常見藉口幫信用不良的民眾美化財務，將大筆金錢匯入其金融帳戶，但實際上都是贓款，再誑騙該民眾協助提領或匯款到第二層帳戶，以達到收受贓款、隱匿金流的

目的。所以民眾如有資金需求，應洽詢合法的金融業者，勿聽信市井傳言，以免受騙。

五、交友詐騙

詐騙者會在社群網站或交友軟體以虛假帳號偽裝不同身分，逐步博取民眾的感情與信任，並以各種謊言騙取金錢，或要求提供帳戶作為收受款項使用，例如佯裝因在國外工作，以沒有臺灣帳戶，請受騙者以自己帳戶協助收款，但實際上是將詐欺贓款匯入帳戶，再誑騙協助提領或匯款到第二層帳戶，不可不慎。

六、假冒熟人詐騙

詐騙者會突然來電冒充親友，謊稱遇到緊急情況(如醫療需求、車禍賠償、遭遇黑道押人討債、投資周轉等理由)，誘騙匯款或提供帳戶資訊。

七、假冒檢警詐騙

詐騙者擅長偽裝假冒檢察官或警察，以涉及刑案製造心理恐懼，謊稱：遭盜領存款、涉嫌洗錢、個人資料被冒用等，進而以「保管金錢、監管帳戶」為由，要求匯款或操作ATM。提醒您，檢察官、警察不會以電話通知監管帳戶，更不會要求匯款、收取現金或存簿。這些都是詐騙，請勿相信。



一旦被當成人頭帳戶，將面臨嚴重的法律責任及後果

刑事責任

112年5月19日立法院三讀洗錢防制法增訂第15條之2，**明定任何人無正當理由，不得將金融帳戶、帳號(含向虛擬通貨平台及交易業務之事業申請的帳號、向第三方支付服務業者申請的帳號)交付、提供予他人使用。**

在下列情況下，**行為人將面臨3年以下有期徒刑、新臺幣(以下同)100萬元以下罰金的刑事處罰：**

- 1、「賣」帳戶帳號(期約或收受對價)。
- 2、交付、提供之帳戶或帳號合計3個以上。
- 3、曾受警察機關**裁處告誡後，5年以內再犯。**

※何謂正當理由？

依本條但書規定，符合一般商業、金融交易習慣，或基於親友間信賴關係，即屬有正當理由。

請特別注意：

本條立法理由已言明，**以申辦貸款、應徵工作為由**交付或提供帳戶、帳號予他人使用，並不符合所謂一般商業習慣，**非屬正當理由**。因為申辦貸款、應徵工作，通常僅需提供個人帳戶之帳號資訊即可(為收受貸放款項或薪資)，並不需要交付、提供具有支付功能所需之金融帳戶存摺、金融卡、密碼、印章等物品。

附帶說明

行為人如單純提供、交付自己的提款卡及密碼委託他人代為領錢、提供帳號予他人轉帳給自己等，因為仍屬本人金流，並非本條所規定之交付、提供「他人」使用。

行政及金融管制措施

一、裁處告誡

113年3月1日頒布施行的洗錢防制法第15條之2第6項帳戶帳號暫停限制功能或逕予關閉管理辦法，**新增裁處告誡，自告誡當日起5年內，已開立、新開立的帳戶，功能會受到下列限制：**

- 1.各帳戶每日轉帳、提領上限為1萬元。電子支付帳戶每日累積匯兌上限為1萬元，每月累計代理收付金額為3萬元。
- 2.禁止使用網路銀行。

- 3.虛擬通貨平台帳號經結清後逕予關閉，不得開立新帳號。
- 4.銀行得拒絕臨櫃交易或開新帳戶。
- 5.縱經調查允許新申請成為第三方支付業者的賣方客戶，亦不再受有虛擬帳號服務，且於同一業者僅限開立一個帳號、自然人於同一業者僅限代表一家法人，撥款天數不得短於交易請款日起算20日，每日收款金額上限為2萬元，每月累積收款上限為20萬元。
- 6.查證期間，得先暫停帳戶功能。若5年內再犯，限制或關閉期間重新起算5年。

二、警示帳戶

只要有詐騙案被害人報案主張受騙匯款到您的金融帳戶，帳戶就會被列為警示帳戶，所有的存提匯款、網路交易等功能全部都被取消，銀行也會拒絕幫您開立新帳戶。

三、衍生管制帳戶

於此同時，您在其他銀行金融帳戶的電子交易功能(提款卡、網路轉帳及電子支付等)，會全部被取消(但臨櫃交易原則不受影響)。

請遵守金融秩序，個人金融帳戶、證件資料及帳號密碼，務必妥善保管，勿輕易交付他人

一、妥善保管金融帳戶

請妥善保管金融帳戶的帳號、存簿、提款卡、各類密碼、印章等，切勿提供給陌生人或來歷不明的人士。

二、定期檢查金融帳戶交易資訊

請經常檢查金融帳戶交易資訊，才能及時發現異常，並請確保所有交易都是由自己進行。如有使用金融機構APP，建議設定帳戶交易提示功能，以便能第一時間發現並阻止異常交易。如發現任何可疑交易，請立即聯繫金融機構處理。

三、妥善保管個人身分證明文件

請妥善保管國民身分證、健保卡、護照、台胞證、駕照等文件，如有遺失、遭竊，請洽各主管機關依法辦理掛失、補發程序。詐騙者一旦取得您的身分證明文件，即可冒名申辦金融帳戶、行動電話門號等，影響重大，請務必慎重保管。

四、妥善保管各類網路帳號密碼資訊

現代人的生活離不開網路與手機，從Facebook、LINE、Instagram等社群軟體、Google及Apple帳號、各類購物網站，至金融機構提供的網路銀行、第三方支付業者平台等，均需輸入使用者帳號、密碼驗證。因此各類網路使用所需的帳號、密碼，請依照資訊使用安全原則，設定足夠強度、長度的密碼，以保障資訊安全，並請妥善保管，以免遭盜用作為犯罪使用工具。

當被列為警示帳戶，該怎麼辦？

一、保存證據

請保存並提供可疑為詐騙者的相關資料給警方偵辦，例如購物網站資訊、通訊軟體對話截圖、電話簡訊、對方電話號碼等資訊。

二、立刻報警

請檢附證據資料向警方報案，索取報案三聯單，並完整說明經過，以供後續查證。

經裁處告誡或帳戶被警示時，該如何救濟？

一、裁處告誡

警察機關裁處告誡為行政處分，不服者，得於接獲書面告誡次日起30日內，提起訴願(繕具訴願書經由原處分機關向訴願管轄機關為之)。對訴願決定不服者，於決定書送達後2個月內，向高等行政法院提起行政訴訟。

二、警示帳戶

原則上，警示帳戶只有在該詐欺、洗錢案件偵查終結(檢察官為不起訴處分、緩起訴處分)或法院判決執行完畢後，才能向原通報機關申請解除。另警示期限屆滿(自通報時起算2年)，如原通報機關未為延長通報，自動失其效力。

面對無所不在的詐騙，該如何因應？

※提醒1

隨時代演進，詐騙者即使僅有金融帳戶號碼，也能作為詐騙使用。請務必謹慎保管，勿輕信他人而告知。

※提醒2

警察機關已與金融機構建立臨櫃關懷制度，面對行員詢問轉帳用途時，請安心接受行員的詢問與協助。如有異常，警察機關會通報檢察機關續處。

※提醒3

陌生來電者會偽裝為您久未聯絡之親友，謊稱更換新號碼或要求重新加LINE好友，或與您攀談獲取個人訊息。請小心來電者身分，一律掛斷電話，勿輕信而提供個人訊息或以對方提供的新聯繫管道進行接洽。

※提醒4

陌生來電者也會帶脅迫或恐嚇，要求保持秘密，不要將資訊告訴他人，製造心理壓力及恐懼。當遇到這種情形，請保持冷靜，一律掛斷電話，切勿以對方提供的電話或管道查證。請透過政府機關學校、公司行號的官方網站資訊、104查號台(網路或電話)或可信任的親友等進行訊息查證。如陌生來電講述的信息涉及親友人身安全，請洽當地警察機關尋求協助。

※提醒5

NCC已推動攔阻境外偽冒來話機制及國際電話語音警示等措施，針對來電顯示前4碼為「+8860至8」的門號全面攔阻。但近來也有以「+67」和「+102」的電話施詐，且詐騙者也會持續透過國內人頭門號傳遞虛假訊息，請對陌生的境外來電保持警戒。

※提醒6

詐騙者慣常冒用社會知名人士身分，在網路或社群媒體上張貼購物、理財投資、心理測驗、網路遊戲等諸多訊息，目的均在誘使民眾點選進入詐騙網頁，進行商品購買，或加入投資理財群組進一步施詐，請勿因名人效應而受騙。

※提醒7

詐騙者會製作以假亂真的【釣魚式詐騙網站】，假借各種政府補助申請、商品市場調查有獎活動等，誘騙您點選輸入個人或金融帳戶資訊。

- 1.請保持對【亂數】網址存疑(即網址編碼是一堆數字符號，沒有任何意義，非公司或政府機關的英文單字縮寫)。
- 2.一般網址識別可以看網址結尾，政府單位是.gov.tw、教育單位是.edu.tw、企業是.com.tw。但詐騙者也會把