
提防各種騙局



網絡釣魚詐騙

在網絡釣魚詐騙中，受害人會在網站或社群媒體平台（如 Carousell、Facebook 或 TikTok）上見到看似為是合法機構（如政府機構或銀行）發布的廣告。這些廣告會展示一些好得令人難以置信的優惠。一旦受害人通過廣告中提供的聯繫方式接觸騙徒，騙徒就會向受害人發送連結（通常是透過 WhatsApp、Telegram 或 SMS 等通訊軟件平台），並要求受害人在該網站輸入個人的銀行憑證。

該網站實際上是一個偽裝成合法的詐騙網站；事實上，騙徒利用它來竊取受害人的個人敏感資訊。受害人只有在其銀行帳戶被他人使用未經授權的交易時，才會意識到自己已被騙了。



假朋友詐騙

您會接到一個陌生的電話號碼，對方硬要你猜猜他是誰？這就是利用「假朋友」引誘受害人跌入陷阱的方法。一旦你於對話中說出朋友的名字，騙徒就會立刻假冒該身份，並要求受害人在聯絡人清單中以此號碼取代其之前的號碼。這類騙徒亦可能會假裝是您失散多年的好友，請求您幫忙的解決緊急的財務問題。

保護自己的方法

騙徒常常會利用受害人的情緒進行詐騙。他們可能會試圖恐嚇你，讓您感到迫切地需要做決定或讓你覺得自己會錯過某些優惠或獎賞。請您務必保持警惕，並採取保護自己的措施。

<p>在社群媒體上收到未經請求的私人訊息（或寄件者聲稱是認識您的）嗎？</p>	<p>謹記驗證寄件者的身份。如果寄件者自稱是一個組織，請致電該公司的電話熱線進行核實。</p> <p>如有任何疑問，請向可信賴的朋友或家人徵詢意見。</p>
<p>在網站見到一些看起來好得令人難以置信的優惠？</p>	<p>請務必瀏覽網站的評論以認證該網店或賣家的可信度。謹記只跟信譽良好的網店或賣家購物。</p>
<p>透過社交訊息平台收到賣家發送的連結，並要求點擊連結接以分享敏感資訊或進行付款？</p>	<p>請勿在未經驗證的網站輸入您的銀行憑證或透過該網頁付款，包括任何透過社交訊息平台（例如 WhatsApp、Telegram）發送給您的網站連結。</p>
<p>提示您授權可疑付款或收到您未進行的購買交易通知？</p>	<ul style="list-style-type: none">● 除非您清楚知道目的，否則切勿授權交易（包括需要登入的要求）。● 為了及時收到通知，請確保我們的記錄中是您最新的聯絡資料。請務必仔細閱讀我們發送給您的通知。如果您發現您沒有進行的交易，請立即通知我們。● 考慮設定較低的每日交易限額 - 這可以阻止大量資金在未經您授權或許可的情況下從您的帳戶中轉出。