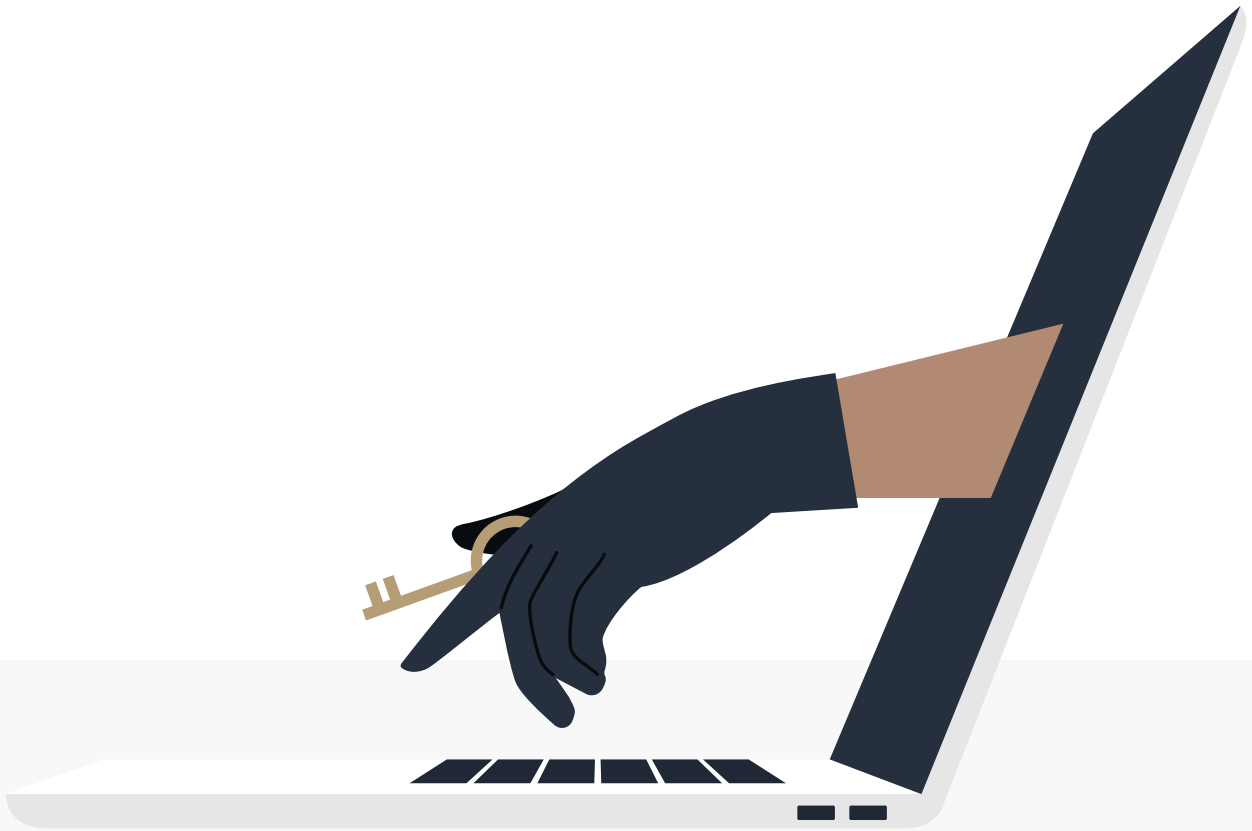
十大技巧用于防範

冒充詐騙

Traditional Chinese | 繁體中文



Australian Government | Be Connected Every Australian online.

Australian Government | National Anti-Scam Centre | SCAMWATCH

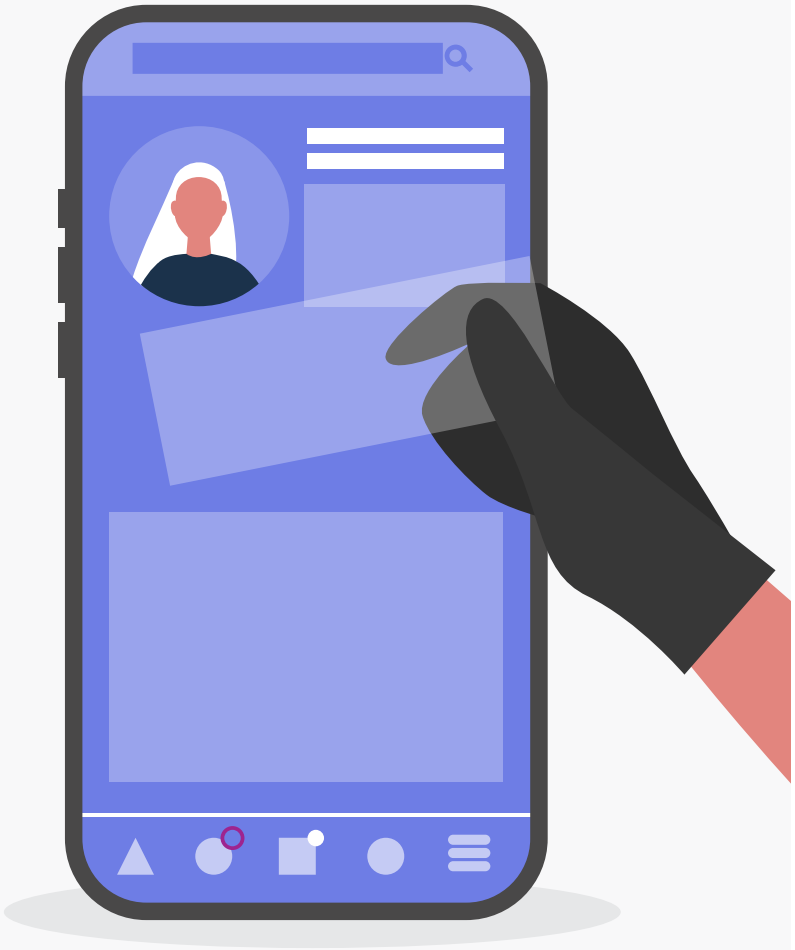
現今詐騙手法日益精密複雜。過去可透過拼寫錯誤或文法不通輕易識破，但隨著技術進步**詐騙行為已更難辨識。**

澳洲國家反詐騙中心已聯合政府部門、產業專家、執法機構及社區組織共同打擊詐騙。您亦可採取以下措施自我保護。保持對新型詐騙手法的認知是最佳防禦方式，從而 能夠識別出詐騙的跡象。

Be Connected 與國家反詐騙中心 (National Anti-Scam Centre) 的 Scamwatch 合作提供本指南，協助您識別冒充詐騙、加強防護，並在受害時知道如何求助。

本指南所有案例均為真實詐騙案件。

本指南的內容



什麼是冒充詐騙？

冒充詐騙旨在偽装成您所熟悉的合法組織。它們可能看起來像是來自您的銀行、網際網路服務提供商、政府部門、零售商、，甚至是您認識的“親友”。

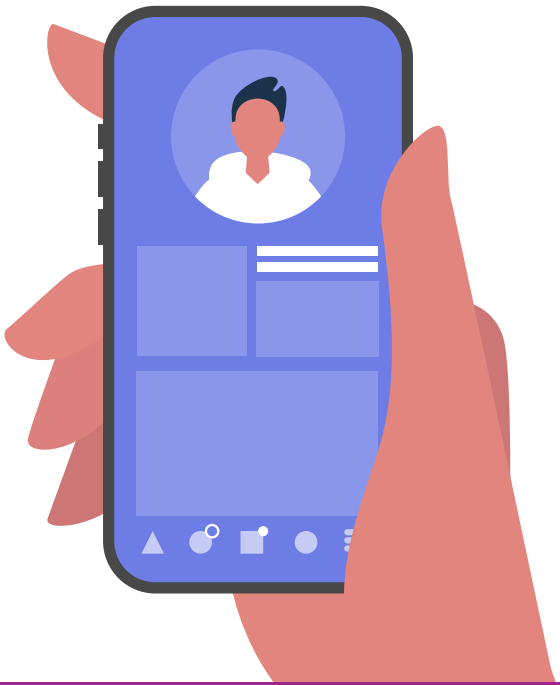
詐騙者會冒充您信任的人，利用您的緊迫感，誘騙您支付金錢或提供個人資料，例如重要密碼、信用卡或銀行等詳細資料。

詐騙者會使用多種方法與您聯繫，包括短信、電話、電子郵件、社交媒體帖子以及看起來與官網完全相同的假網站。

什麼是偽裝？

詐騙者會利用技術偽裝成您信任的機構來電或發送訊息。這被稱為“偽裝”。

請對任何主動索取密碼等個人資訊或要求付款的聯繫保持警惕。直接聯絡該機構進行求證。



常見的各種偽裝技術包括：

01. **來電顯示偽裝：**詐騙者更改其來電顯示，顯示與實際使用的電話號碼不同的號碼，使來電看起來像是來自一個合法的 號碼。

02. **簡訊偽裝（或 alpha 標籤）：**詐騙者會篡改來電顯示為機構名稱（例如 AusPost）。它可以使詐騙簡訊混入一個機構的真實對話紀錄或貼子中。

03. **電子郵件偽造：**詐騙者會更改他們的電子郵件地址或發件人姓名，使電子郵件看起來像是來自可信來源。他們會偽造寄件人顯示名稱或竄改電子郵件域名，通常是通過更改或添加合法域名中的字母或數字（例如，@amaz0n.com、而不是 @amazon.com）。

常見的冒充詐騙手法

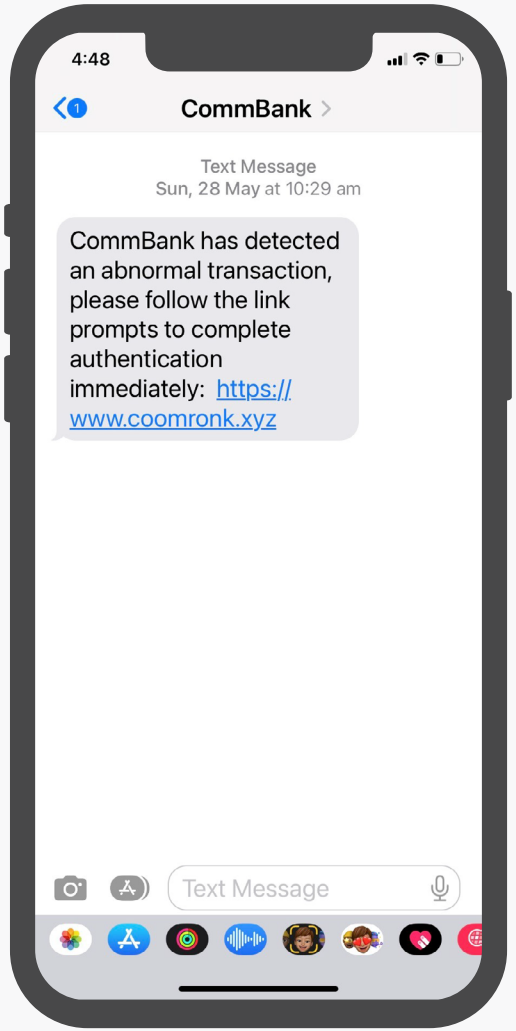
冒充銀行詐騙

- 您接到自稱銀行安全部門的來電 / 簡訊。通知您偵測到可疑交易，聲稱您的帳戶已被入侵。他們敦促您將資金轉至“安全帳戶”或配合“調查”。
- 您收到一條簡訊或電子郵件，要求點擊連結驗證帳戶的訊息。該連結會將您導向一個偽造網站，用于竊取您的用戶名、密碼及其他個人訊息。

如何辨識此類詐騙？

當銀行偵測到您的帳戶有可疑活動時，可能會與您聯繫，但絕對不會要求您將資金轉至其他帳戶。銀行絕不會透過您未主動請求的簡訊、電子郵件或電話，向您索取任何帳戶帳戶或個人詳細信息，包括您的密碼、PIN 碼或一次性驗證碼。

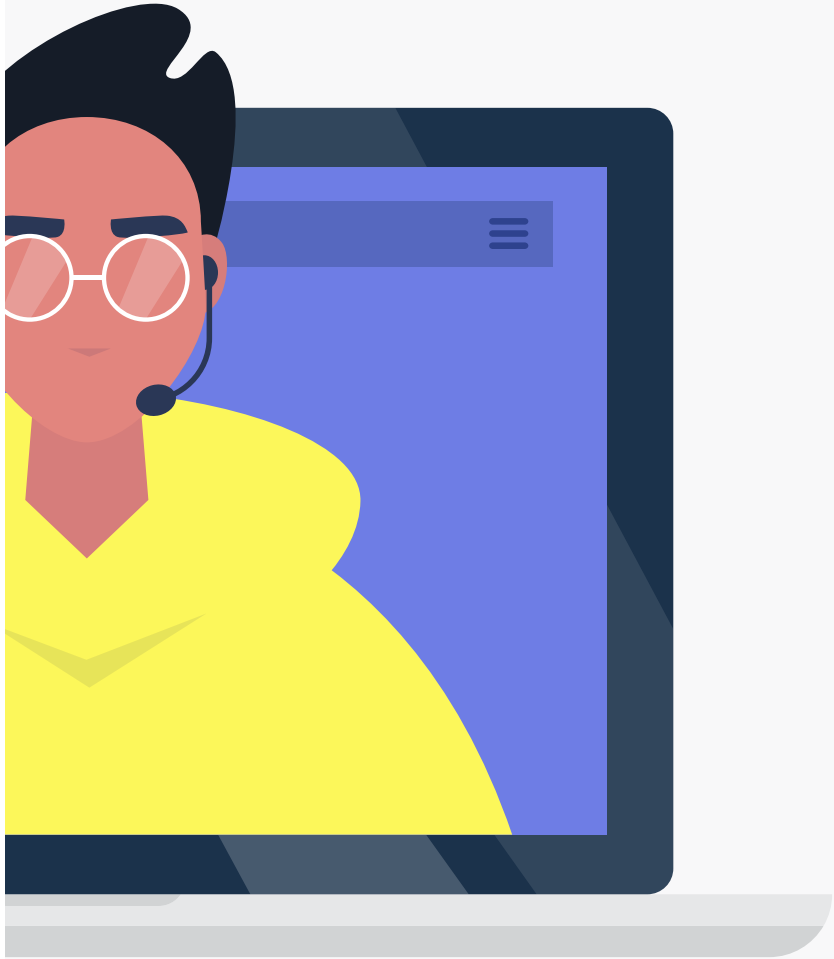
詐騙者可能偽造來電顯示，使其看起來與銀行官方號碼相同，請勿以此作為您正在與誰通話的憑證。對方可能掌握您的部分個人資料，但這些資料很可能是通過欺詐手段獲得的。



來自偽造號碼的銀行詐騙簡訊實例，要求您點擊連結驗證您的詳細資料。

技術支援詐騙手法

- 詐騙者可能自稱是網路服務供應商、電信公司或電腦公司的工作人員，並聲稱您網路或電腦出現問題。他們可能聲稱您的網路 / 電腦遭到入侵、感染病毒 、系統運行緩慢或服務即將中斷 他們會誘導您下載應用程式或軟體，以便他們遠端控制您的電腦，從而「修復」問題。
- 您的電腦螢幕出現警告訊息，要求您立即 撥打指定電話號碼，以解決偵測到的問題。



如何辨識此類詐騙？

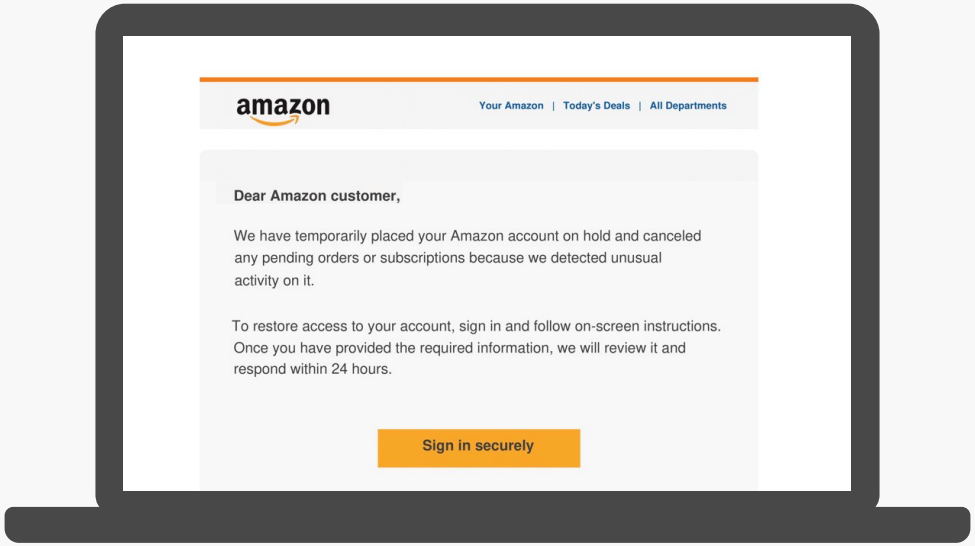
正規公司絕不會致電通知您網路連接或電腦出現問題（他們會等待您在出現問題時主動聯繫他們）。他們絕不會要求您下載任何具有遠端存取功能的軟體或應用程式。

點擊彈出視窗右上角的「×」關閉訊息。若無法關閉，請嘗試點擊視窗外的空白區域或直接關閉網頁。若仍無法關閉彈出視窗，對于 Windows 電腦，按住 ALT 和 F4 強制關閉瀏覽器。對于 Apple 電腦，從 Apple 選單中選擇「強制結束」，然後選取要關閉的瀏覽器 .

帳號停權詐騙手法

您收到自稱來自 Amazon、PayPal 或 Netflix 等知名機構的電子郵件或簡訊。通知您帳號因可疑活動已被暫停，要求您點擊連結確認身份以恢復使用。

詐騙者利用恐嚇手段誘導您前往偽造的網站，藉此竊取您的用戶名、密碼以及銀行或信用卡資料等個人資訊。



聲稱來自 Amazon 的詐騙電子郵件範例，促請您點選連結以提供您的個人資訊。

如何辨識此類詐騙？

Amazon、PayPal 和 Netflix 等正規企業絕對不會透過未經您請求的電子郵件或簡訊中的連結，向您索取密碼、銀行或信用卡資料等個人資訊。雖然各機構聯繫客戶的方式不盡相同，但最安全的做法是對這類郵件、簡訊或電話保持高度警覺。

若不確定訊息的真實性，請直接透過網路搜尋該機構的官方聯絡方式進行確認。切勿使用訊息、電子郵件或電話中提供的聯絡資料。

常見恐嚇話術

詐騙者常使用以下緊急話術促使您立即行動：以下是一些他們可能會說的話來吸引您的注意：

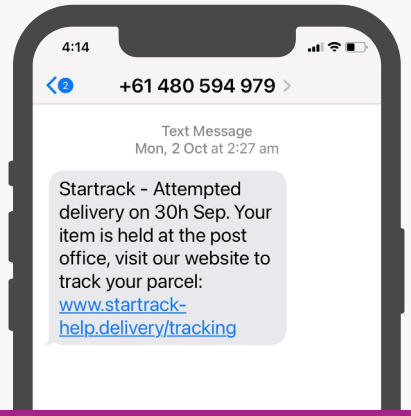
- 偵測到異常帳戶活動
- 發現未經授權的登入嘗試
- 您的帳號已被封鎖/凍結
- 您的付款遭拒
- 無法驗證您的帳單資訊

包裹無法遞送詐騙

您收到自稱 Australia Post 或 FedEx 等快遞公司的電子郵件或簡訊，聲稱您的包裹因故無法遞送。要求您支付額外運費或「更新資料」才能收取包裹。

如何辨識此類詐騙？

澳洲郵政、聯邦快遞（FedEx）及其他正規物流公司絕對不會透過簡訊 / 電子郵件索取個人資料或要求支付任何費用。如果您正在等待送貨，最好通過官方 APP 或訂單確認郵件中的追蹤編號查詢。如果您沒有追蹤編號，請直接致電快遞公司客服確認您包裹的狀態。



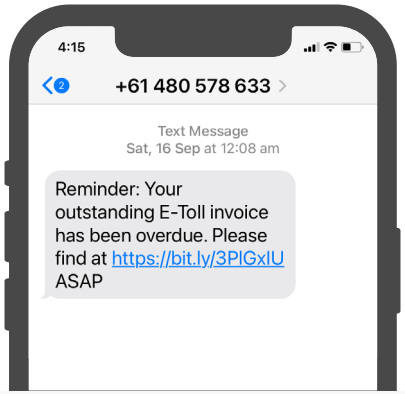
快遞公司詐騙簡訊範例。

收費道路詐騙

您會收到自稱收費道路營運商的簡訊，通知您通行費逾期未繳。您必須立即處理以避免罰款。簡訊中包含的付款連結會將您導向專門竊取財務資料的偽造網站。

如何辨識此類詐騙？

若收到“拖欠道路通行費“或”帳戶餘額不足”的簡訊，這可能是詐騙。請直接登入收費機構官方網站或 APP 上的個人帳戶查詢最新的交易紀錄。



收費道路詐騙短信範例。

虛假投資詐騙手法

您可能會看到看似由名人或財經網紅背書的絕佳投資機會。承諾高額回報且幾乎零風險。當您進一步詢問時，會被引導至專業製作的網站，並收到精心設計的宣傳資料。

如何辨識此類詐騙？

優惠好到難以置信？那麼它很可能是騙局！詐騙者慣用「限時優惠」等話術迫使您倉促決定，以免「錯失良機」。警惕附「見證評價」或「高回報保證」的電郵 / 廣告。

提供服務的「顧問」聲稱無需持澳洲金融服務 (AFS) 牌照。即使他們提供了牌照號碼，也應親自核實持有人身份。

虛假網站詐騙手法

您在 Facebook 上看到知名 BBQ 烤爐品牌廣告，標價僅 100 澳元，而正常售價 900 澳元）。您點擊進入零售商網站後，發現信用卡付款需支付 2.99% 手續費，因此選擇銀行轉帳以獲得額外 5% 折扣。雖然收到確認郵件，但最終根本收不到燒烤爐。

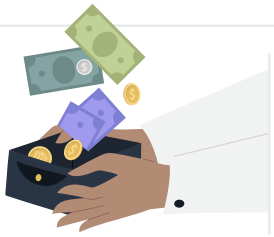
如何辨識此類詐騙？

假網站的價格過於誘人、付款方式異常，還有其他可疑之處，例如網址試圖模仿官方商店的網址（例如 webberbbqs.com 假冒正牌 weber.com）。

詐騙集團也會在社交媒體和 Google 等搜尋引擎上購買“贊助廣告”，點擊這類廣告時務必保持高度警惕。

十大技巧用于防範

01. 對陌生來電保持警覺。讓陌生來電號碼轉接至語音信箱。



02. 在回應不明來歷的通訊並提供個人或財務資料前，務必停一停、想一想。問問自己：這是否會是騙局？

03. 提防使用恐嚇手段的電郵。檢查顯示名稱與電郵地址是否相符。它們匹配嗎？例如，寄件人」顯示為「Amazon Support」，但電郵地址卻是 amazonsupport830@gmail.com。

04. 不要只因為短信出現在你認識的機構過往訊息對話框中，便輕易相信。這仍可能是詐騙訊息。

05. 若對收到的訊息或來電存疑，應直接聯絡相關機構核實。透過他們的官方網站或您智慧型手機或平板電腦上的安全應用程式與對方聯繫。

若對任何機構或網站存疑，請在搜尋引擎輸入「機構名稱 + 詐騙」進行查證。

06. 切勿向電話中的任何人透露密碼、PIN 碼或一次性驗證碼，即使對方自稱來自銀行或政府機構，並能說出您的帳戶資料。

07. 切勿點擊簡訊中的鏈接。即使部分連結可能無害，但謹慎為上。對于電郵中的附件及鏈結，除非您完全確認寄件人身份，否則亦應同樣處理。

08. 切勿聽從陌生來電者的指示下載任何應用程式或安裝軟件，以免對方訪問您的裝置。請立即掛斷電話。

09. 切勿透過電子郵件或簡訊中的連結登入您的線上帳戶。相反，應直接在瀏覽器輸入公司網址，或使用其安全應用程式訪問您的帳戶。

10. 在線上付款前，務必檢查網站網址（是否官方網站？）、留意異常付款方式，以及網站底部「關於我們」、「送貨及退貨」等欄位是否存在措辭不當或資料缺失的情況。

懷疑自己受騙了？
求助通道

遭受詐騙可能造成財務損失和心理壓力，請務必迅速尋求幫助和採取行動。您可以採取以下步驟：

1. 立即聯繫銀行阻止可疑交易。
2. 聯絡 IDCARE，這是專為受到詐騙或身份盜竊影響的人提供的免費支援服務。致電。1800 595 160，或造訪 idcare.org
3. 立即更改所有密碼並設定高強度新密碼。
4. 向 Scamwatch 舉報詐騙案件，幫助他人避免受害：scamwatch.gov.au/report-a-scam
5. 為自己尋求支持。如果您覺得不方便與朋友或家人談話，請聯絡 Lifeline 或 Beyond Blue 進行保密談話。若您已遭受重大金錢損失，請立即聯繫國家債務熱線 (National Debt Helpline) 尋求協助。

   Beyond Blue：1300 22 4636（24 小時服務），或造訪 beyondblue.org.au

   Lifeline：13 11 14（24 小時服務），或造訪 lifeline.org.au

   國家債務熱線：1800 007 007（工作日，上午 9:30 至下午 4:30）或造訪 ndh.org.au

更多資訊

請點選下方圖塊了解更多：

播客節目
《識破冒充詐騙陷阱》

播客節目
網路詐騙徒最怕你知道的事

主題
詐騙識別和規避指南

主題
高階線上安全指南

專題文章
攔截騷擾電話全攻略

專題文章
身份盜用：什麼是身份盜用及其防範措施

《防詐騙小手冊》(Little Book of Scams) 是一項國際認可的反詐騙工具，可幫助您了解各種常見詐騙手法，并提供防護對策保護自己免受詐騙。

訪問 Scamwatch 網站，掌握最新詐騙警訊與防護建議。

關於 Be Connected

Be Connected 是澳洲政府推動的數位能力培育計劃，致力於透過免費電腦課程、短期線上課程等多種形式，提澳洲年長者的數位技能、自信心及網路安全意識。Be Connected 該計劃網站與學習內容由 eSafety 網路安全專員負責管理。

關於 Scamwatch

Scamwatch 由國家反詐騙中心負責運作，該中心成立的目的是使澳洲成為詐騙分子更難下手的目標。它通過教育社區如何識別、避免和報告詐騙行為，提高人們對詐騙的認識。反詐騙中心透過分析詐騙通報資料，並與政府部門、執法機關及民間企業合作，共同打擊與預防詐騙活動。