Australian Banking Association

保證你自己的安全：
警惕詐騙

以新冠病毒疫情為由的詐騙活動有可能在未來數月裏越來越多。

詐騙犯用假電子郵件、電話或短信試圖竊取個人資料。他們假裝來自你的銀行、世界衛生組織、政府部門、慈善機構或合法商業機構，比如旅行社、供電公司、電話或網路公司、或你本地超市。

保護你自己

你的銀行永遠不會發電子郵件或短信詢問任何帳戶或財務細節，包括更新你住址或電話/手機/網上銀行的登錄細節。

政府部門及其它合法機構永遠不會要你點擊一個鏈結來更新資料。如果可疑，請教朋友或家人，或直接聯繫相關機構進行詢問。

如果陌生人給你打電話索要個人資料，馬上掛電話。直接給有關公司打電話，問他們是否給你打過電話。

永遠不要打開陌生人或機構發的附件。永遠要警惕聽起來好得難以置信的提議或索要太多資料的提議。

銀行會給予幫助，以下情況應馬上聯絡銀行：

- 你在接詐騙電話、回復詐騙電子郵件或短信時透露了你的銀行資料
- 你不小心點擊了任何鏈結或下載了任何附件
- 你注意到帳戶裏出現不尋常交易。

如何識別詐騙

- 叫你更新或確認個人資料，包括住址、出生日期、銀行帳戶資料、稅號、個人識別號或密碼。
- 電子郵件或短信包含可疑鏈結。如果你不確定，請朋友或家人幫忙。
- 叫你馬上付錢或付押金。
- 如果一種提議聽起來好得難以置信，那很可能就是假的。
- 電子郵件與公司名稱不吻合。
- 打電話的人要求遠端進入你電腦。

Australian Banking Association

www.ausbanking.org.au

保護財務資料不被騙取的重要提示

- 掛掉可疑電話，代之去公司網站或找出他們的電話號碼，直接給他們打電話。
- 永遠不要把密碼或個人識別號告訴別人。用密碼保護你的設備。如果你和別人共用一台電腦，永遠不要保存密碼，永遠要記得退出你的帳戶。
- 定期檢查你的銀行帳戶，以便及時發現可疑交易。
- 避免在購物時刷卡。輕敲或插入卡片通常更安全。
- 取消信用卡提現功能。
- 請教銀行保護你帳戶的最好方法。
- 如果你認為受到詐騙，馬上向銀行報告。

騙子有很多行竊方法，主要包括：

Phishing（網絡釣魚）– 假裝來自一可信管道（比如銀行、慈善機構或政府部門），用電子郵件或短信竊取你的個人資料。訊息看上去像真的，通常叫你在假網站上輸入個人資料或叫你點擊一個鏈結 – 這會讓騙子進入你的電腦並竊取你的個人資料。

網上購物詐騙 – 詐騙犯裝成真實網店，要麼透過一個假網站、要麼透過一個真實零售網站上的一條假廣告。假的網店網址通常會要求非同尋常的付款方式，比如要求透過匯票、電匯、國際轉賬或禮品卡立即付款。

投資詐騙 – 詐騙犯自稱是股票經紀人或投資經理，提供財務或投資諮詢服務。他們會叫你交錢投資一個可能是真的、也可能是假的項目，然後騙走你的錢。

遠端登錄詐騙 – 詐騙犯謊稱你的電腦或網路連接有問題或感染了惡意軟體。他們會試圖說服你安裝一種應用軟體或讓他們進入你的電腦。然後他們會竊取你的個人資料或要求你“付費”解決問題。

交友約會詐騙 – 詐騙犯與你形成某種關係，勒索錢財。他們長期與你發展關係，然後會叫你把財產轉到他們名下或要求成為你遺囑的受益人。他們還經常問你要錢，以解決某種健康、旅行或家庭問題。

有用鏈接：

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/