

有關防範偽冒語音訊息來電、虛假電郵、偽冒網站及偽冒手機短訊的重要提示

南洋商業銀行(「南商」)特別提醒客戶慎防偽冒南商的語音訊息來電、虛假電郵、偽冒網站及偽冒手機短訊等，客戶在任何情況下必須小心保管個人資料。

本行特此提示客戶注意以下事項:

1. 本行不會透過電話、電郵或手機短訊，要求客戶提供任何敏感的個人資料(包括登入密碼及只用一次的密碼)，客戶切勿向可疑來電者或第三者提供個人資料。
2. 本行不會透過預錄語音訊息、電郵或手機短訊，通知客戶其銀行或信用卡賬戶出現異常或已遭凍結，並要求客戶輸入其個人資料，或聯絡職員以核實身份。本行提醒客戶不要單憑來電顯示、電郵地址、網址、手機短訊或訊息內容辨別訊息發出者的身份。
3. 若客戶對來電者的身份存疑，應要求對方提供聯絡電話及姓名等資料，以便核實，過程中切勿披露任何個人資料。
4. 若客戶需核實任何以本行名義撥出的電話、發出的電郵、網址或手機短訊，請致電南商客戶服務熱線 (852) 2622 2633 (選擇語言後按“0”)或親臨本行任何一家分行查詢。
5. 客戶使用網上銀行或手機銀行服務時，應在瀏覽器網址欄內直接鍵入本行網址(www.ncb.com.hk)，並不應透過來歷不明的電郵提供的超連結，登入網上銀行或手機銀行。

有關網上銀行的保安資訊，請瀏覽：

http://www.ncb.com.hk/nanyang_bank/resource/si_tc.pdf

如客戶懷疑曾向任何可疑人士披露個人資料，請即致電本行客戶服務熱線 (852) 2622 2633 (選擇語言後按“0”)或親臨本行任何一家分行查詢，或直接聯絡香港警方。

如客戶不欲收到本行的電話銷售來電，客戶可致電南商客戶服務熱線 (852) 2622 2633 (選擇語言後按“0”)或親臨本行任何一家分行，以行使其拒絕直銷的權利。



請瀏覽香港金融管理局網頁

<https://www.hkma.gov.hk/chi/smart-consumers/beware-of-fraudsters/> 內
之宣傳影片及相關資料，以了解更多提防詐騙資訊。

隨提示附上「有關防範偽冒語音訊息來電、虛假電郵、偽冒網站及偽冒手機
短訊的注意事項」，以供參考。

南洋商業銀行有限公司謹啟
2020年11月

有關防範偽冒語音訊息來電、虛假電郵、偽冒網站及偽冒手機短訊的 注意事項

情景(一) 提防詐騙的措施

應該

- ✓ 就可疑來電，要求對方提供聯絡電話及姓名等資料，以便核實
- ✓ 致電本行客戶服務熱線或親臨本行分行，以確認電話、電郵、網址或手機短訊的真確性
- ✓ 使用網上銀行服務時，直接鍵入本行網址
- ✓ 登入本行網站/網上銀行時，注意版面有否出現異常情況(例如要求輸入信用卡號碼、有效期、卡背檢驗碼、只用一次的密碼或個人資料)

切勿

- ✗ 輕易將敏感的個人資料 (特別是登入密碼及只用一次的密碼) 透露予第三者
- ✗ 單憑來電顯示、電郵地址、網址、手機短訊或訊息內容辨別訊息發出者的身份
- ✗ 透過來歷不明的電子郵件提供的超連結，登入網上銀行及手機銀行

情景(二) 懷疑曾向可疑人士披露個人資料的處理

應該

- ✓ 即時致電本行客戶服務熱線或親臨本行分行，與本行職員聯絡
- ✓ 保持冷靜，儘快通知香港警方

切勿

- ✗ 嘗試自行處理，遲遲未有通知本行職員或香港警方

懷疑被騙

請即打
防騙易諮詢熱線



反 詐 騙 協 調 中 心

ADCC
Anti-Deception Coordination Centre
反 詐 騙 協 調 中 心

ANTI-SCAM
防騙易
18222

提防電騙

1

預錄語音

騙徒以預錄語音致電市民，聲稱為速遞公司、銀行、政府部門或其他機構等，然後要求市民按鍵選擇收聽語言

懷疑被騙
請即致電
18222

2

聲稱市民涉及刑事案件

市民被轉駁至假冒的內地執法人員，該騙徒聲稱市民在內地犯法，需要提供其網上銀行資料作快速審查，以協助其洗脫嫌疑。過程中，騙徒能夠向受害人展示其相片、姓名及身份證等個人資料

3

操控網上理財戶口及轉走存款

騙徒會要求受害人下載應用程式或要求受害人到偽冒網站，並在程式或網站輸入網上銀行資料。受害人最終被轉走戶口內所有存款

陌生來電

即刻收線

同你講錢

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

ANTI-SCAM
防騙局
18222



ADCC

Anti-Deception Coordination Centre

反詐騙協調中心

防騙易諮詢熱線 18222



核實來電 提防電騙

如有懷疑:

請致電 **18222**

聯絡 **反詐騙協調中心**

如遇到緊急事故, 請立即致電 999



香港特別行政區政府
香港警務處



www.police.gov.hk/adcc/

提防假冒官員
切勿向他人透露
網上銀行帳戶
及密碼



ANTI-SCAM
防騙易
18222

HELPFUL
TIPS!

最新手法

1

要求提供網上
銀行帳戶及
密碼

騙徒會要求受
害人提供網上
銀行帳戶及
密碼



2

要求前往騙徒
提供的假網頁

騙徒會提供一
個連結連接至
假網頁，並要
求受害人輸入
網上銀行
帳戶及密碼



3

要求下載可疑
手機應用程式

騙徒會要求受
害人下載應用
程式，並要求
受害人輸入網
上銀行帳戶及
密碼



騙愛玩家 哋到埋身



行騙伎倆

- ⚠ 假肖像
- ⚠ 假甜言蜜語
- ⚠ 假投資應用程式

即掃QR Code
同我展開激情對話!



18222

www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「網戀投資騙案」三步曲

1 搭訕

騙徒扮成「高富帥」透過社交媒體或交友程式向受害人搭訕。繼而自稱是投資達人，並向受害人展示自己生活無憂的照片，以降低受害人的戒心。

2 網戀投資

騙徒開始對受害人甜言蜜語。當成功令受害人以為自己是網上情人後，便向受害人推介一些虛假的投資應用程式，並聲稱可提供內幕投資貼士，受害人於是下載程式，之後依從騙徒指示將投資金額存入騙徒提供的個人銀行戶口或虛擬貨幣錢包。

3 「贏粒糖輸間廠」

受害人依照騙徒的投資貼士在投資應用程式內投資。最初，騙徒會令受害人嚐到甜頭（獲利），使其放下戒心。受害人加大投資金額，但最後發覺根本不能取回投資金額和利潤。

懷疑受騙

即打 18222
www.adcc.gov.hk



ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

電騙之王 哋到埋身



行騙伎倆

- ⚠️ 假冒執法人員
- ⚠️ 製造恐慌「先嚇你·後幫你」
- ⚠️ 展示個人資料換取信任

而家你犯咗法！
即掃QR Code同你化解



☎️ 18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「假冒官員電話騙案」三步曲

1 預錄語音

騙徒以預錄語音致電市民，聲稱為速遞公司、銀行、政府部門或其他機構等，然後要求市民按鍵選擇收聽語音。

2 聲稱市民涉及刑事案件

市民被轉駁至假冒的內地執法人員，該騙徒聲稱市民在內地犯法，需要提供其網上銀行資料作快速審查，以協助其洗脫嫌疑。過程中，騙徒能夠向受害人展示其相片、姓名及身份證等個人資料。

3 操控網上理財戶口及轉走存款

騙徒會要求受害人下載應用程式或要求受害人到偽冒網站，並在程式或網站輸入網上銀行資料。受害人最終被轉走戶口內所有存款。

懷疑受騙

即打 ☎️ 18222
www.adcc.gov.hk



ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

假工祭司 呢到埋身



行騙伎倆

- ⚠️ 強調零經驗及高薪厚職
- ⚠️ 以社交媒體廣告作招徠
- ⚠️ 呢你個人資料申請貸款

大把筍工俾你揀
即掃QR CODE



☎️ 18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「匯款員式求職騙案」三步曲

1 「高薪厚職」作招徠
騙徒在社交平台或網站刊登招聘廣告，聘請專人協助外國公司轉移資金到香港，並以「合法」、「搵快錢」、「彈性工作時間」和「高薪厚職」等字眼作招徠。

2 騙取受害人的資料借貸
受害人按招聘廣告的聯絡方法以社交媒體或即時通訊軟件聯絡騙徒。對話中，騙徒指示受害人傳送身份證、住址證明、銀行卡或月結單的副本。之後，騙徒用上述資料以受害人的名義向銀行或財務機構借貸。

3 誘騙受害人交出貸款
其後，貸款轉帳到受害人的銀行戶口，騙徒向受害人訛稱該筆款項是外國公司的資金，並要求受害人交出款項。騙徒取得款項後便逃之夭夭，而受害人則負上債務。

懷疑受騙

即打 ☎️ 18222
www.adcc.gov.hk



ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

釣魚特工 哋到埋身



行騙伎倆

- ⚠ 假連結
- ⚠ 假網站
- ⚠ 假訊息

你個銀行戶口有問題
即掃QR CODE檢查戶口設定



☎ 18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「網絡釣魚騙案」三步曲

1 設置釣魚網站

黑客仿照政府部門、銀行、網上付款服務商、網上零售商等機構的網站，並製作一些外觀一樣的釣魚網站。無論如何相似，偽冒網站的域名和真正的網站必會有所不同，偽冒網站的功能很多時也不齊全。

2 向大眾發放釣魚訊息

黑客發放偽裝由上述機構發出的電郵或電話短訊(SMS)。這些假電郵及短訊的行文及格式都和官方的電郵及短訊非常相似，內容一般是指機構發現了和受害人相關的異常情況(例如是發現受害人的網上銀行戶口新增了一名登記收款人)，以引誘受害人按動附上的假連結作出修正。

3 受害人被引導至虛假網站

受害人按動假連結進入釣魚網站後被要求登入網站。受害人輸入其個人、信用卡或網上銀行戶口資料。騙徒掌握以上資料後，會直接從受害人的銀行戶口或信用卡竊取金錢。

懷疑受騙

即打 ☎ 18222
www.adcc.gov.hk



ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

虛App神棍 狂噬億金

行騙伎倆

- ⚠️ 利用社交媒體結識受害人
- ⚠️ 誘騙受害人進行假投資
- ⚠️ 令受害人獲得甜頭後加注



跟我買賺硬！
即掃QR Code



防騙易熱線
18222
www.adcc.gov.hk

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

「網上投資騙案」三步曲

1

利用社交媒體結識受害人

騙徒利用社交媒體接觸受害人，與其混熟後，表示自己是投資達人。

2

誘騙受害人進行假投資

騙徒向受害人推介虛假的投資應用程式供其下載，並聲稱掌握程式的買賣規律。受害人下載該程式後，騙徒便教受害人聯絡程式的客戶服務員，以安排開戶。受害人之後按指示將款項或加密貨幣存入指定的個人銀行賬戶或電子錢包，並在程式進行買賣。

3

受害人獲得甜頭後加注 最後血本無歸

起初，騙徒讓受害人獲利，將利潤存入受害人的銀行賬戶，以獲取信任。受害人加大投資，但其後向客服申請取回本金及利潤時，卻被不同藉口拖延，或被要求存入更多錢方能取回款項。受害人最後血本無歸。

懷疑受騙



ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

即打 18222
www.adcc.gov.hk

數碼 KEY

睇緊啲

你的戶口有一筆港幣50,000元的
預設轉帳，請按此連結確認：
172.80.bank/login

揸 LINK 前

要三思

銀行不會透過短訊或電郵超連結，引領客戶到網站或流動應用程式進行交易，
或要求客戶提供任何敏感個人資料(包括登入密碼和一次性密碼)。



HONG KONG MONETARY AUTHORITY
香港金融管理局

陌生來電

可疑網店

筍工招聘

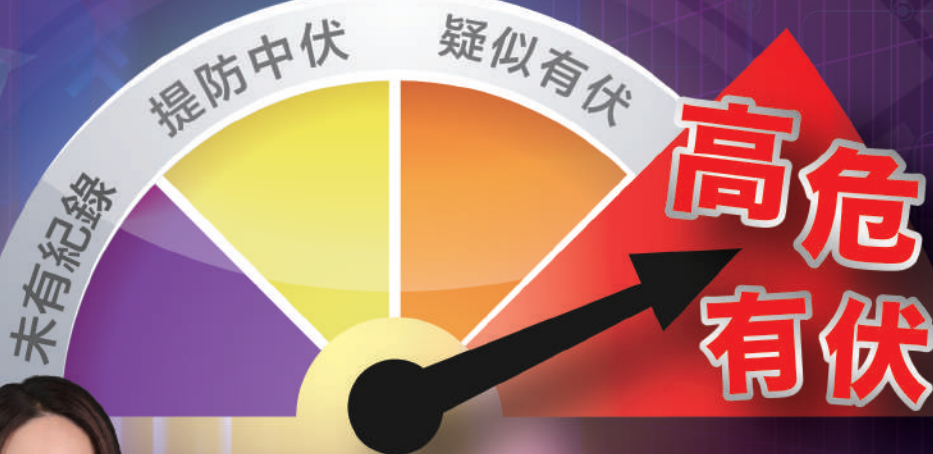
白撞訊息

必賺投資

係咪呢緊你？ Check 吓

防騙視伏器

即上 CyberDefender.hk



輸入資料，揭穿詐騙陷阱！



一站式詐騙陷阱搜尋器

電話號碼
平台用戶名稱
社交帳號
網址
收款賬號
電郵地址 IP 地址

網頁

Facebook

Instagram

YouTube



CYBER 守網者
DEFENDER

懷疑受騙

即打18222

緝
戀

寂寞

恐懼

來電靠嚇

貪心

無知

刷單圈套

騙局誘惑

捉心理騙局

誘惑到你萬劫不復!

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

