流動銀行
及線上支付服務
最新安全威脅與防範措施

Latest security threats and measures in Mobile Banking and Online Payment

科技罪案數字

1

- 網上戶口盜用
- 網上購物騙案
- 信用卡盜用

最新安全威脅與真實案例

2

- 線上支付- 安全威脅與案例警示
- 流動銀行 - 安全威脅與案例警示

銀行業防禦措施與個人防禦策略

3

- 銀行業防禦措施
- 個人防禦策略
- 遠離網路購物陷阱 網上購物三不原則

1. 科技罪案數字

PUBLIC

科技罪案數字

網上戶口盜用

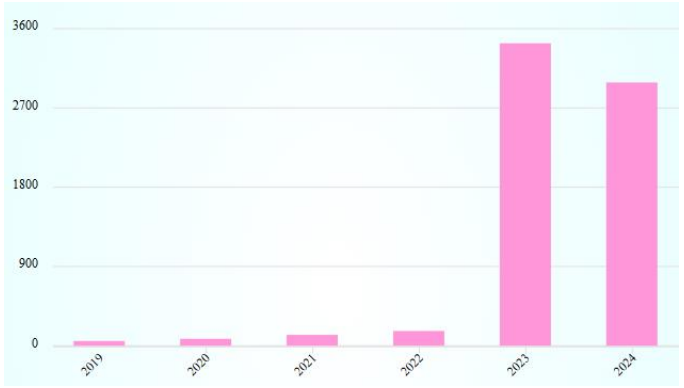
2023年8月開始出現新型帳戶騎劫手法。新手法利用釣魚白撞訊息，後來演變為「搜尋器優化中毒」的攻擊。 2024年一共發生2,989宗，損失金額達9千萬。

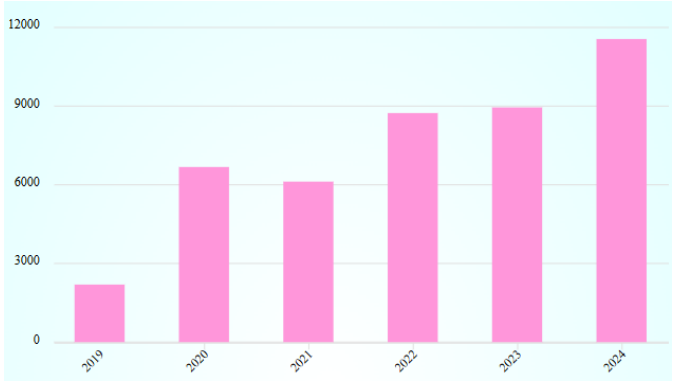
網上購物騙案

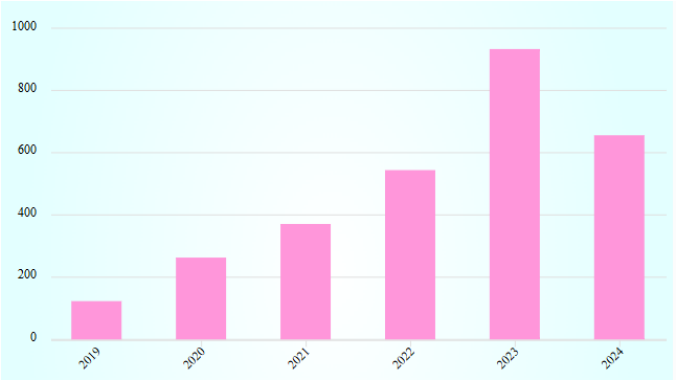
網上購物騙案是2024年各類型騙案的第一位，一共發生11,559宗，損失金額達3億5千萬，比2023年增加一倍。騙徒通常以限購、減價、外地代購等吸引買家，並拒絕當面交收，受害人轉賬付款後賣家便會失去聯絡；另外騙徒亦會假裝買家，提供虛假匯款收據來騙取貨品甚至金錢，所以在網上無論「買」或「賣」都要小心。

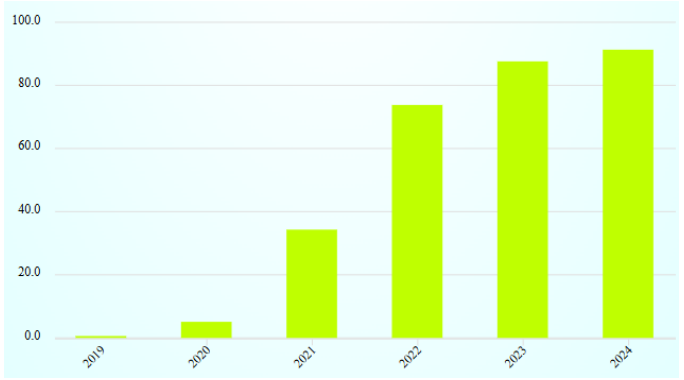
信用卡盜用

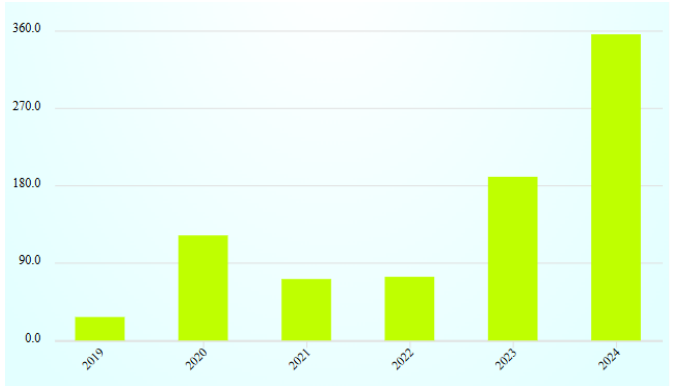
你的信用咭資料包括咭號碼、到期日及保安碼，一旦落入不法分子手上，資料便可能被盜用，因而蒙受損失。 2024年一共發生656宗，損失金額達1千萬。

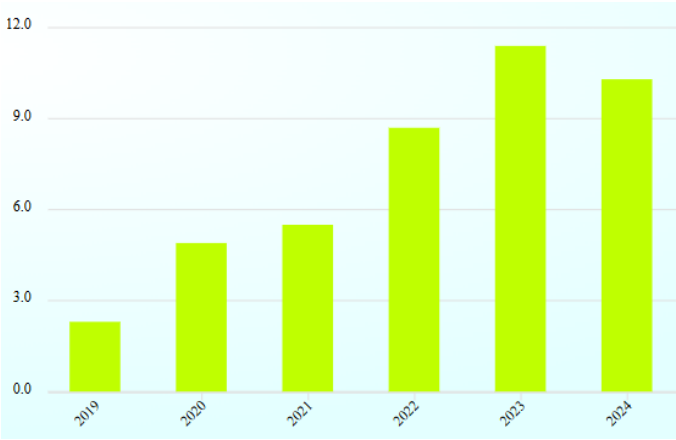












Source: CyberDefender (守網者）

2. 最新安全威脅與真實案例

線上支付安全威脅

1. 釣魚攻擊(Phishing)

假冒銀行短信及自動生成釣魚網站，偽冒銀行登入頁，例如偽裝成銀行的「賬戶異常」連結

2. 虛假投資App

冒充熱門理財平台如虛假「港股通」App誘導入金

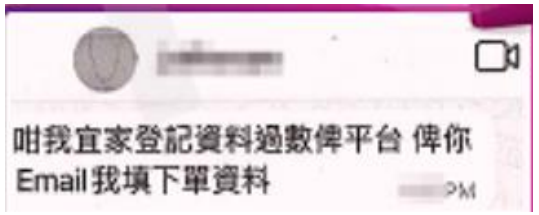
3.支付漏洞（二維碼劫持）

篡改商戶支付二維碼（案例：2024年某茶餐廳二維碼點餐系統遭植入惡意程式，盜取信用卡資料）

4. AI（人工智能詐騙）騙案

利用 深度偽造技術(Deepfake)和聊天機器人等技術來欺騙受害人，使詐騙手法更逼真、更具欺騙性。
E.g. 語音騙取轉帳授權，模擬親友/客服聲音

假(1)



假(2)

假(3)

carousell

案例分析(1)
假冒買家在網上拍賣平台詐騙

港女Carousell賣牙刷遇騙徒 誤點擊釣魚連結失$80萬積蓄

手法

騙徒在Carousell平台假扮買家，聲稱經平台付款會有保障。騙徒表示如果賣家從來沒有通過平台收取貨款，需先提供電郵地址，並按照指示登記資料。賣家不熟悉平台功能，因而提供了電郵地址；部分賣家還提供電話號碼給騙徒。隨後，賣家**收到虛假電郵，內容顯示買家已成功付款，並要求點擊「繼續」超連結，以登記資料完成收款**。其實該超連結連接假冒的Carousell網站。騙徒教導賣家在該網站輸入個人資料、網上銀行帳戶名稱、密碼及一次性密碼（OTP），並且通知賣家不要登錄手機銀行App，只要在交易頁面選擇接收短訊就可以收到該一次性密碼。

就這樣，賣家的銀行戶口便給騙徒完全操控了。
當賣家完成以上步驟，以為會收到貨款時，騙徒已經將賣家的銀行存款全部轉走。

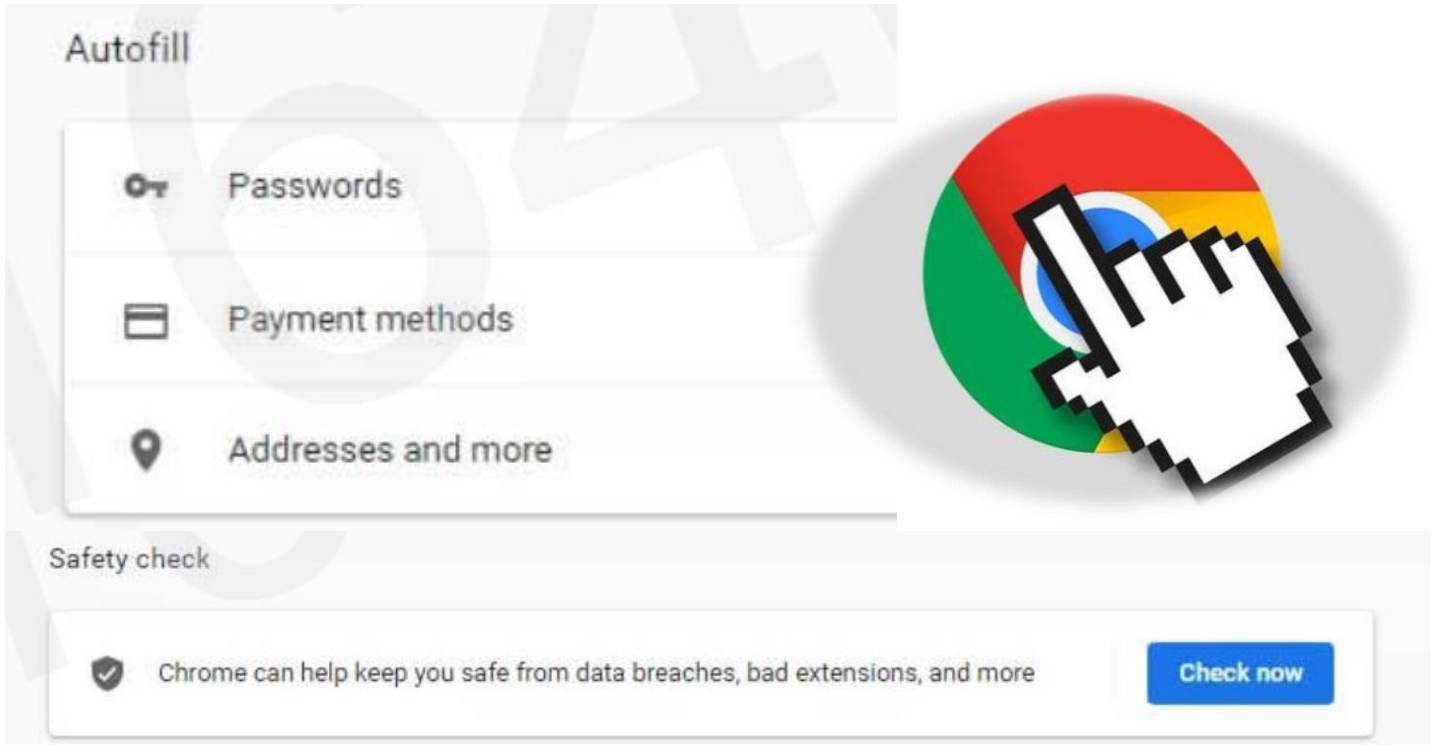
案例分析(2)
AI聲紋技術冒充他人

有聲未必係真人　騙徒以AI聲紋冒充他人　事主遭呃走1.45億元 |

一名受害人擬向內地公司購入一批加密貨幣挖礦機，雙方及後以手機通訊程式WhatsApp洽談。期間，受害人收到疑似對方公司財務經理的WhatsApp語音訊息，不虞有詐，按對方指示分別三次將總值約1.45億港元的加密貨幣USDT存入指定的加密貨幣錢包。
受害人其後發現受騙。調查發現，對方公司財務經理曾經在手提電腦上進入虛假的WhatsApp頁面，懷疑其WhatsApp 帳戶因此被盜，遭人以AI模仿財務經理聲紋，製作語音訊息詐騙他人。

惡意瀏覽器擴充功能(Extensions) -竊取自動填充的支付信息

- 高達66%的瀏覽器擴充功能具有高/極高等級的權限
- 研究人員發現Chrome與Safari等瀏覽器的自動填入功能可能潛藏網釣風險，駭客可藏匿表格資訊，看起來只要求填入姓名及電子郵件，實際上卻可獲得使用者所儲存的所有個人資訊，例如電話號碼，支付信息。
- 芬蘭一位白帽駭客Viljami Kuosmanen在GitHub上發佈了一個演示，展示了攻擊者如何利用擁有自動填充功能的瀏覽器、惡意外掛程式和密碼管理器等工具的過程中，如果使用者的瀏覽器中帶有自動填充功能，當他們填寫表格(只要求填入姓名及電子郵件）並提交后，就會將所有資訊，包括隱藏的個人資訊發送給駭客。



流動銀行安全威脅

1.AI驅動的社交工程攻擊	• 攻擊者利用生成式AI（如ChatGPT）製作高度個人化的釣魚訊息，模仿銀行官方語言風格，甚至生成虛假客服語音（深度偽造）誘騙用戶提供敏感資訊 • 案例： 偽造銀行簡訊通知「異常登入」，附帶AI生成的連結導向高仿登入頁面。
2. 進階銀行木馬變種	• 覆蓋攻擊（Overlay Attack）：木馬程式偽造登入介面，竊取帳密及生物識別資料。 • 自動轉帳系統（ATS）：自動攔截驗證碼並操控轉帳。
3. 惡意SDK與第三方庫漏洞	• 風險來源：銀行APP整合的廣告或分析SDK存在漏洞，導致數據外洩。 案例：2023年某銀行APP因第三方SDK漏洞遭中間人攻擊，數千用戶會話令牌被竊。
4. 供應鏈攻擊與API濫用	• 風險場景： 攻擊者入侵銀行合作的第三方服務商，植入惡意代碼。 逆向工程銀行API，偽造交易請求。
5. 公共Wi-Fi與中間人攻擊	• 威脅：駭客透過偽造免費Wi-Fi竊取銀行會話Cookie或注入惡意代碼 • 「自動連接Wi-Fi」功能
6. 深度偽造（Deepfake）語音詐騙	• 模仿親友或銀行職員聲音，要求緊急轉帳 • 案例:2024年香港發生多起假冒銀行經理語音釣魚案件
7. SIM卡劫持	• 通過偽造身份補辦SIM卡獲取OTP（需運營商配合）

欺詐網上銀行登入畫面截圖

明報新聞網

即時港聞

2025年2月18日星期二

四家銀行被冒充網站及釣魚電郵詐騙 (17:51)

上一篇 下一篇

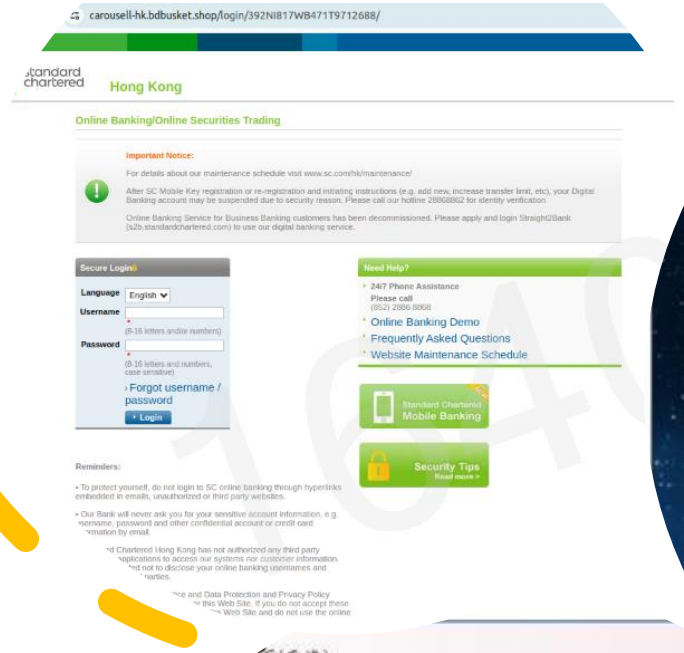
四家銀行被冒充網站及釣魚電郵詐騙

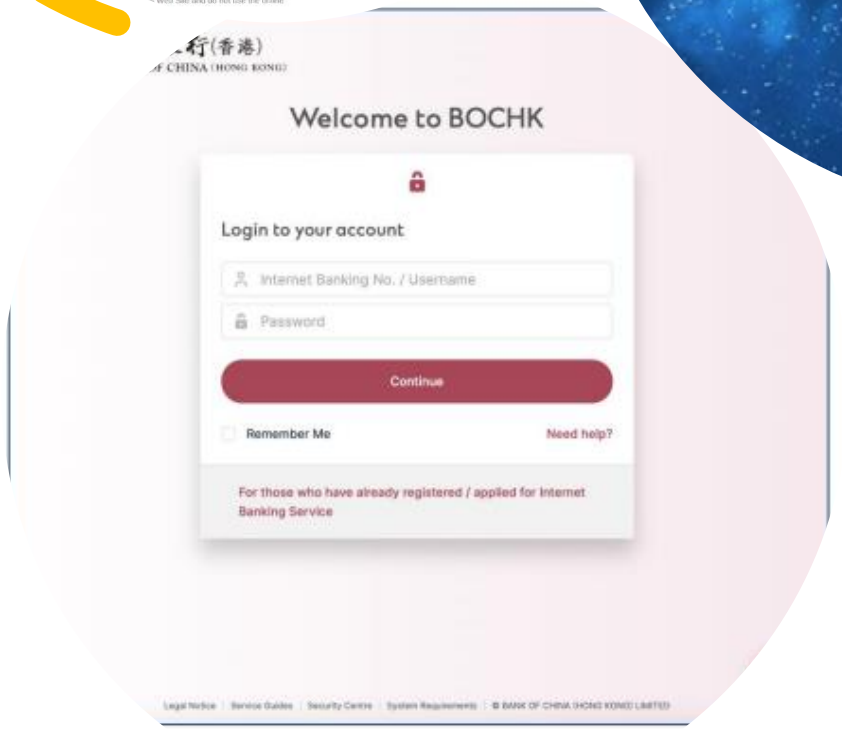
香港金融管理局今日（18日）表示，留意到有騙徒冒充中國建設銀行（亞洲）、交通銀行（亞洲）、中國銀行（香港）、創興銀行四家銀行行騙，涉及偽造欺詐網站、網上銀行登入畫面、偽冒電郵等多種手法。

金管局表示，騙徒透過偽造欺詐網站、網上銀行登錄畫面冒充中國建設銀行（亞洲）和創興銀行，交通銀行（香港）亦遭偽造欺詐網站，另有騙徒冒充中銀（香港）偽造釣魚電郵進行詐騙活動。

金管局提醒公眾，銀行不會透過短訊或電郵超連結，引領他們到其網站進行交易，更不會以電話、電郵及手機短訊，包括超連結方式，要求客戶提供包括登入密碼和一次性密碼在內的任何敏感的個人資料。

任何人士若曾向該網站或登入畫面提供其個人資料，或曾透過該網站或登入畫面進行任何交易，應利用有關新聞稿中的聯絡資料聯絡有關銀行，及聯絡香港警務處刑事總部資訊中心（電話：2860 5012）。





Android裝置受惡意軟件侵害

- 惡意軟件騙案日趨猖獗，當中涉及騙徒欺騙受害人於Android裝置下載並安裝含惡意軟件的應用程式，取得受害人Android裝置的存取權限並進行未經授權交易。調查發現，騙徒會透過社交媒體 / 訊息發布虛假廣告，推銷特別優惠，例如訂購日用品、音樂會門票、度假套票等等。要求受害人從非手機官方應用商店下載仿真購物應用程式，以獲取相關優惠，但實際上卻是含有惡意軟件的虛假應用程式。一旦Android 裝置被掌控，騙徒便能登入受害人的銀行應用程式，盜取各項敏感個人資料及作未經授權的交易。
- 在銀行新安全措施之下，如果你的裝置中安裝了來自非手機官方應用商店的應用程式；以及這些應用程式獲授予過多的權限，例如螢幕共享或完全控制您的裝置，你的流動應用程式可能會被暫停使用。
- 檢查您裝置的無障礙設定，評估已授予應用程式之權限是否必要。 如有懷疑，請關閉這些應用程式的無障礙設定（前往裝置設定 > 協助工具 / 無障礙設定）或將其刪除，以保障您的戶口安全；以及繼續使用流動應用程式。

3. 銀行業防禦措施與個人防禦策略

銀行業防禦措施

技術升級

- **生物認證**
  銀行等全面採用「面容ID/指紋登入」，取代傳統密碼。

- **AI即時監控**
  金管局要求銀行部署AI系統偵測異常交易（如突然跨境轉賬），2023年攔截**78億港元**可疑交易。

客戶自主管理工具

- **交易限額設定**
  客戶可自訂每日轉賬上限（如分級設定FPS/跨境轉賬限額）。
- **即時警示系統**
  任何交易即時推送通知（含地理位置），部分銀行允許客戶透過短信阻截交易。

教育與協作

- **反詐騙模擬測試**：銀行主動發送「模擬釣魚郵件」教育客戶。

- **長者支援計劃**：銀行與社福機構合辦「流動理財安全班」，教導識別假客服電話。

監管合作

- **快速凍結機制**
  與警方合作「止付機制」，2023年凍結4.3億港元詐騙款項。
- **「可疑帳號警示」**
  可疑賬戶列入共享數據庫（如金管局「防騙視伏器」）。

- **銀行一旦發現任何欺詐網站**、偽冒電郵或類似的詐騙事件，試圖誘使其客戶透露敏感個人資料，會迅速發出新聞稿通知其客戶（如其認為此舉符合客戶最佳利益），以及向金管局匯報。

個人防禦策略

1. 你的密碼有幾強?

- 使用密碼管理員，避免重複密碼。
- 啟用「 雙重認證（2FA）」、「 多重認證（MFA）」並定期更新密碼。

2. 設備安全

- 關閉iOS/Android的“自動連接Wi-Fi”功能。
- 定期檢查App許可權（如是否允許“短信讀取”）。
- 定期檢查手機銀行App的登入記錄。
- 不點擊不明連結
- 只從官方途徑 (如App Store)下載手機app
- 小心選擇給予app的存取權限，如被要求收集通訊錄、相機、位置等，應份外留神
- 時常將系統更新至最新版本

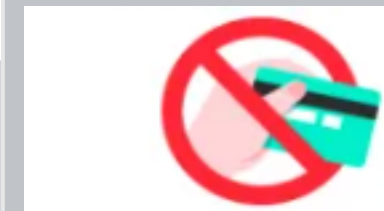
3. 交易習慣

- 掃碼支付前核對商戶名稱（如轉數快FPS顯示全名）。
- 設置交易限額（尤其信用卡綁定電子錢包時）。

4. 資源推薦

- 舉報平台：**「防騙易18222」**
- 守網者 / 下載**「防騙視伏器」**
- 「網絡安全資訊站」亦不時提供資訊保安公眾活動的消息、專家之言、以及由專業機構所提供的資訊保安故事等，讓公眾獲悉最新保安資訊。

遠離網路購物陷阱 網上購物三不原則



不隨意提供個人資料與銀行資訊

保密個人資料與銀行資訊，切勿輕易與他人分享。例如：證件號碼、信用卡/提款卡卡號、認證編號、PIN、一次性密碼OTP、網路銀行密碼等，避免遭盜用。

不點擊來路不明的連結

收到要求提供個人資料的私訊或電子郵件時請格外小心。確認寄件者的帳號名稱或電子郵件地址，檢查是否合理正當或包含拼寫錯誤。

不輕易相信可疑帳號

先瀏覽用戶的個人資料，例如檢查該帳戶是否已通過驗證及帳號加入日期，或查看用戶評論，以了解其他用戶的交易體驗。

“安全是銀行與客戶的共同責任
黑客永遠尋找最弱一環, 別讓自己成為漏洞”