提高安全「智」識　慎防受騙

我有可能成為騙徒的目標嗎？

社會上任何人都有機會遇上形形式式的騙案。根據香港警務處資料顯示，長者通常較易成為街頭及電話騙案騙徒的目標。騙徒手法層出不窮，我們要提高防騙意識，及早認清騙徒手法，方能免卻不必要的損失。透過推出「樂齡理財」，滙豐致力協助年長客戶提高警覺以應對金融罪案，保障財產安全。雖然我們擁有行業領先的欺詐偵測系統以保障客戶財產，但我們仍希望加強客戶對詐騙的認知和了解如何防範詐騙陷阱。本指南將介紹各種常見騙局、騙徒和銀行與您聯繫時的分別，以及如何獲取更多相關資訊和舉報懷疑騙案的途徑。敬請仔細閱讀。

有哪些常見騙局？

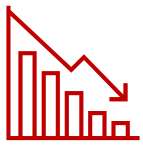
大部分騙徒會主動出擊，行騙手法亦有一些共通點，例如要求您提供個人資料或保安資料，並試圖製造事態緊迫的錯覺。若您透露了重要的戶口資料，騙徒就會以此竊取您的財產。以下部分將列出一些常見騙局。

電話詐騙｜「語音釣魚」

騙徒會致電您或留下語音訊息，並自稱銀行職員、某間知名機構、政府部門職員，甚至是內地公安。他們可能已經掌握您一些個人資料，試圖藉此取得您的信任。他們會脅逼您馬上採取某些行動，而且不給予您足夠時間考慮。

	騙徒會…	*銀行職員會…*
例子一 您收到自稱是銀行防詐騙部門的來電，要求您協助調查一宗騙案。	要求您匯款至另一戶口以作安全保管。他們亦可能會要求您提供自動櫃員機密碼，或網上理財密碼和保安資料。	向您解釋戶口出現異常活動，並要求您確認是否有進行有關匯款。銀行職員也可能會在通話過程間向您詢問一些問題，以識別和驗證您的身分。
例子二 您收到自稱是銀行職員的來電，邀請您申請私人貸款或信用卡。	催逼您透露個人資料以申請低息信貸產品，例如私人貸款或加按套現。他們並不會向您提供任何可供追查或確認的資料。	以您的全名稱呼您，並向您提供姓名和內線號碼以供核實，和表明是從哪一渠道獲取您的電話號碼和戶口資料。如您有任何懷疑，銀行職員將歡迎您透過致電銀行客戶服務熱線的方式回電。

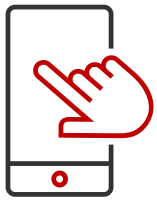
投資詐騙



騙徒會向您介紹一個具吸引力的投資機遇，並利用偽冒客戶推薦或虛構營銷資料企圖令您信以為真。

	騙徒會…	*銀行職員會…*
例子 有人主動向您推薦一個投資機遇。	聲稱有一個高回報、低風險，但需在有限時間內進行的投資機遇。他們會向您施壓，迫使您盡快作出決定。	保持專業操守，並向您提供可透過銀行客戶服務熱線驗證的產品資料。

「社交工程」詐騙



「社交工程」詐騙是一個結合電話和社交媒體的詐騙手法。騙徒會偽冒可信賴機構的員工、政府官員或執法部門人員，並對您某些生活瑣事和習慣有一定了解，例如購物紀錄、外遊歷史、親友名稱等。但事實上，他們是透過您的社交媒體貼文猜測或取得這些資訊。騙徒將企圖說服或威逼您採取某些行動，例如提供銀行戶口登入資料和敏感個人資料、進行轉賬等，令您蒙受損失。

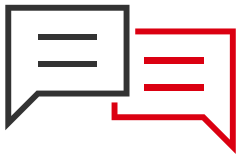
	騙徒會…	*可信賴機構會…*
例子 您收到自稱是內地公安人員的來電。他們表示您的銀行戶口已被駭客入侵，或您涉嫌逃稅，因此需要承擔嚴重法律責任。	以「監察可疑活動」為由，要求您提供銀行戶口資料，並表示假如您在提供個人資料前掛斷電話，將招致嚴重後果。他們也可能會向您查問您過去往返中國內地和香港兩地的事宜，並對您曾經在社交媒體分享的個人資料有一定了解。	邀請您以官方客戶諮詢渠道聯絡他們。同時，他們不會在未能提供容許您透過客戶熱線等官方渠道加以確認的資料下，強迫您分享任何個人資料。

電郵詐騙｜「網絡釣魚」

騙徒會向您發送電郵，誘使您提供個人資料、點擊偽冒網站連結、掃瞄二維碼或開啟電郵附件，以趁機在您的電腦安裝惡意軟件並竊取您的資料。

	騙徒會…	*銀行會…*
例子 您收到一封看似由銀行發出的電郵。	要求您提供戶口號碼、自動櫃員機密碼、網上或電話理財密碼，或進行轉賬。	只透過電郵推廣對您可能有用的服務資訊，或向香港客戶發送跟進電郵，以了解其理財體驗。

短訊詐騙｜「短訊釣魚」



騙徒會向您發送看似來自銀行或其他可信賴機構的短訊。

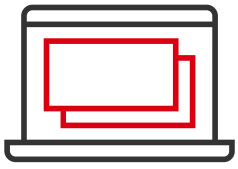
	騙徒會…	*銀行會…*
例子一 您收到短訊，要求您儘快致電某個電話號碼與銀行聯絡。	於您撥通電話後向您查問您戶口的一筆可疑付款，並要求您提供銀行戶口登入資料，訛稱需要有關資料方能中止交易。	馬上中止交易並停用您的銀行卡。
例子二 您收到短訊提示有一個新的收款人加到您的戶口，並要求您點擊網頁連結以作確認。	當您點擊連結後會把您帶到一個與您銀行網頁相似的頁面，並要求你輸入戶口登入資料及密碼。	不會向您發送任何需要輸入戶口登入資料的網頁連結。

網絡情緣詐騙

一個在現實中與您素未謀面的人與您展開網絡情緣，其後以各種原因向您索取金錢。

	騙徒會…	*銀行職員會…*
例子一 您的網絡情人表示家人病重，需要緊急醫藥費，並向您借錢，承諾會於日後歸還。	先向您表達愛意，並於一段時間後表示他們自己或家人遇上生死攸關的緊急狀況，急需金錢解決問題。	只會與您進行公事往來，不會就私人事務聯絡您，或向您詢問私人問題。
例子二 您的網友表示有意探訪您、或想送贈珠寶等名貴禮物給您。	表示您需先代為支付旅費，方能前來探訪；或需先墊付稅項或其他費用，才能向您送贈有關名貴禮物。	
例子三 您的網友表示繼承了一筆巨額遺產，但需要您先提供資金才能取得。	向您借錢，並承諾於日後歸還。	

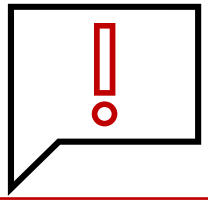
網購詐騙



騙徒會透過偽冒的購物網站或在網上假裝出售商品，試圖騙取您的付款資料。

	騙徒會…	*可信賴機構會…*
例子 您有意從網上購買某件產品，而您並不知悉賣家的身分。	將惡意網站設計成真實購物網站一樣，在您網購過程中（如在網站開立帳戶時）趁機竊取您的個人資料或付款資料。	建議您查看網址欄左方是否有一個鎖頭圖示，確保網站安全。

戶口接管騙局



騙徒會假冒您的網絡供應商，並表示您的網絡連線出現問題，誘使您下載某個惡意軟件、網上理財或電子銀包應用程式，從而盜取您的銀行資料。

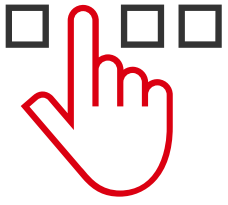
	騙徒會…	*可信賴機構會…*
例子 您收到自稱是您的網絡供應商的電話，並要求您下載一個軟件，讓他們可以查看您的電腦畫面。然後他們要求您登入網上理財戶口作「測試」。	要求您前往網址與真實機構網頁非常相似的偽冒網站，以打開或下載惡意軟件或流動應用程式。其後騙徒會要求您授權他們全面控制或「遠端遙控」您的電腦，以「解決問題」。	只建議您前往銀行官方網頁或到app store下載所需軟件或應用程式。職員只會在您主動致電時，才會提出分享電腦屏幕的請求。

WhatsApp | 通訊軟件詐騙

騙徒或會入侵您密切聯絡人的戶口並冒充其身分，然後向您發送訊息，要求您代為購買某物品、點擊某相片、GIF圖或連結，或下載某些東西等，從而盜取您的個人敏感資料。

	騙徒會…	*真實聯絡人會…*
例子 親友向您發送訊息，要求您代為購買網絡遊戲點數卡，讓他們能以較高價錢轉售。	要求您點擊某連結或前往某網站分享您的銀行戶口資料和自動櫃員機密碼。他們或會接二連三向您發送訊息加以催促，並要求您以 WhatsApp 或其他通訊軟件傳送載有您敏感個人資料的圖片。	致電或親身向您講解要求。

自動櫃員機騙局



騙徒或會在自動櫃員機的卡槽上偷裝讀卡器或在附近暗藏針孔攝錄機進行偷錄，盜取您的個人戶口資料。他們也可能在自動櫃員機附近等待，試圖窺視您的密碼，或走近您並聲稱您掉下了現金或個人物品。

	騙徒會…	*普通人會…*
例子 在您使用提款卡過程中，有人提醒您拾回某些物件。	試圖分散您的注意力，伺機以假卡換走您插在自動櫃員機的提款卡或信用卡。	等待您完成交易，並與您保持適當距離。

我可如何保障自己，慎防受騙？

請採取以下重要預防措施，保障自己免墜詐騙陷阱：

時刻保持警覺

- 如您獲得某個好得有點不可思議的優惠，例如一個超值禮遇、服務或獎品，但您必須先預支一筆款項，這可能是一個騙局。
- 對主動接洽您的不明來歷人士保持警惕。使用自動櫃員機時，不要接受陌生人提供的任何幫助。
- 當您懷疑自己遇上騙案時，請保持冷靜。您可聯絡我們，或致電相關機構的官方聯絡電話號碼，以確認有關通話或訊息的真偽。

建立良好習慣

- 定期檢查您的銀行結單。如察覺任何異常，應立刻聯絡我們。
- 定期使用您的銀行戶口，以提醒自己您的登入密碼及自動櫃員機密碼，並定期更新密碼。
- 為不同網站和理財平台（如自動櫃員機、電話理財、網上及流動理財）戶口設置不同密碼。
- 定期更新您的流動應用程式。

謹慎分享資料

- 切勿與未經核實身分的人士分享個人資料或相片。
- 在網上尤其是社交媒體平台進行分享時，要保持審慎。
- 妥善銷毀載有個人資料的重要文件和紙張。

加強安全措施

- 登記及善用生物認證功能，即 iOS Face ID、iOS Touch ID、Android™指紋認證和語音認證[1]。
- 在WhatsApp或其他通訊軟件啟用雙步驟驗證功能，加強帳號安全性。
- 使用網上及流動理財服務時，確保您正使用可靠的Wi-Fi無線網絡和服務供應商。不使用藍牙時，可將功能關閉。
- 如不確定發送者是否可信，切勿點擊訊息中的圖片或連結。在您的通訊錄中尋找發送者以核實其身分。

您可瀏覽 www.hsbc.com.hk/zh-hk/help/cybersecurity-and-fraud 以了解更多安全資訊和指引。

我可如何獲得更多相關支援，或舉報可疑行為或騙案？

香港警務處反詐騙協調中心

提供最新的騙案警示、短片和有用連結，助您保障財務安全和在有需要時尋求協助。

- 您可致電「防騙易18222」熱線舉報懷疑騙案。
- 詳情請瀏覽 www.police.gov.hk/ppp_tc/04_crime_matters/adcc。

投資者及理財教育委員會

載有不同防範詐騙建議、指引、短片和有用連結。

- 詳情請瀏覽 www.ifec.org.hk/web/tc/moneyessentials/scams/index.page。

[1] Touch ID及Face ID均是Apple Inc.在美國及其他國家和地區的商標或註冊商標。iOS是Cisco在美國及其他國家和地區的商標或註冊商標，且由 Apple Inc. 經過授權使用。Android是Google LLC的商標。指紋認證只適用於兼容Android系統版本8.0或以上的Android™裝置。如欲了解更多資訊，請前往 www.hsbc.com.hk/zh-hk/ways-to-bank/internet/security-key/#activation 或 www.hsbc.com.hk/zh-hk/help/cybersecurity-and-fraud/safeguard。

聯絡我們 | 我們樂意為您提供支援

如欲了解如何妥善制定未來財務規劃，請瀏覽 www.hsbc.com.hk/zh-hk/age-friendly-banking。

如欲了解如何應對及舉報懷疑騙案，請瀏覽 www.hsbc.com.hk/zh-hk/help/cybersecurity-and-fraud/how-to-report-fraud。

您亦可透過以下途徑聯絡我們：

- 親臨任何一間滙豐分行
- 致電客戶服務熱線
  - 滙豐卓越理財尊尚 (852) 2233 3033
  - 滙豐卓越理財 (852) 2233 3322
  - 其他客戶 (852) 2233 3000
- 電郵向我們舉報問題 csv@hsbc.com.hk