

# 滙豐防騙資訊手冊

緊貼最新資訊 識破百變騙術  
善用「防騙視伏App」辨真偽





# 釣魚短訊、電郵

釣魚短訊同電郵係騙徒慣用手段，一不留神隨時誤墮詐騙陷阱。



## 常用手法



### 1 扮知名及公共機構

騙徒會假扮政府機構、銀行、支付平台或保險公司，用「積分即將過期」、「自動轉賬失敗」、「保險到期」，甚至訛稱你可獲退稅等藉口，催促你登入假網站，騙取敏感個人資料。



### 2 通訊軟件假認證

騙徒或會聲稱你嘅賬戶尚未認證，誘使你輸入個人資料，包括驗證碼，然後盜用其通訊賬戶向親友要求轉賬。

## 防騙貼士

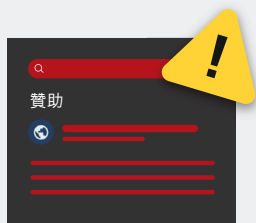
- 💡 你絕不會收到由銀行發出要求你輸入任何敏感個人資料或登入嘅連結，使用滙豐網上服務時，請用你嘅流動理財應用程式或自行輸入銀行網址
- 💡 留意已登記短訊發送人名稱係會以「#」開頭（唔適用於雙向交易短訊）
- 💡 收到親友要求轉賬，記得致電驗證
- 💡 切勿透露驗證碼、一次性密碼、銀行戶口等敏感資料

# 釣魚網站

面對幾可亂真嘅假網站，你又能否分辨真偽？



## 常用手法



### 1 落廣告置頂假網站

騙徒會於搜索引擎投放廣告將假網站置頂，令受害人誤以為真網頁，繼而留下敏感個人資料。

### 2 扮滙豐網站

透過假冒滙豐網站，假裝提供投資、定期存款等銀行服務，誘使大家轉賬，從中盜取銀行戶口、信用卡等重要資料。



## 防騙貼士

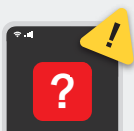
- 💡 切勿向未知人士或機構轉賬
- 💡 如你見到銀行提供好到難以置信嘅優惠，你可以透過熱線、流動或網上理財嘅線上對話聯絡我哋或前往分行確認
- 💡 使用滙豐網上服務時，請確保域名正確，建議手動輸入 <https://www.hsbc.com.hk/zh-hk>

# 網購詐騙

網購係一件開心事，但一時貪平而誤中騙徒陷阱，就隨時得不償失！



## 常用手法



提防來歷不明應用程式

### 1 網購騙案

利用虛假社交媒體專頁及交易平台，以各種理由吸引事主下載含惡意軟件嘅app，從中駭入手機盜取資料，甚至控制你嘅應用程式，令騙徒可以登入銀行戶口偷走你嘅財產。



### 2 旅行預訂騙案

冒充大型旅行社推廣機票及酒店優惠，再透過假客服主任誘使大眾過數；甚至用假相嘅預訂平台扮出租房間，實情酒店或民宿並不存在。



### 3 網上買賣平台

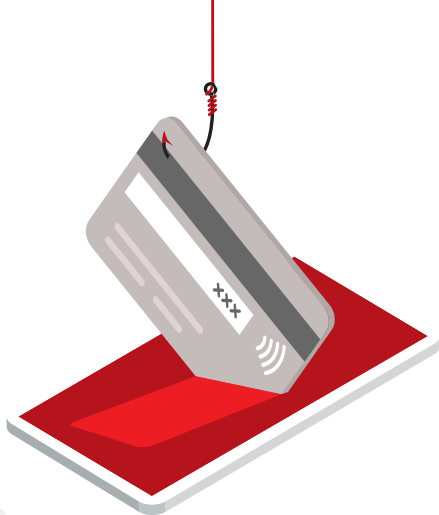
騙徒會喺買賣平台發布優惠帖文，要求買家先付款再出貨，收款後就消失；亦會化身假買家，偽冒買賣平台寄送「收款」通知電郵，引導你去假銀行網站騙取個人資料，甚至操控銀行戶口。

## 防騙貼士

- 提防抵到難以置信嘅優惠
- 在交易平台購買商品時，盡量不要預付貨款。如賣家不必要地催促付款，請考慮取消購買
- 避免於非官方網站進行付款，並檢查是否正在使用正確嘅網站
- 核實商戶身份及個人檔案（註冊年資、正評數目、聯絡資料等）
- 網上放售物品謹記使用可靠收款渠道，例如現金及快速支付系統（轉數快）

# 信用卡詐騙

你嘅信用卡號碼、到期日同安全碼，一旦落入不法分子手上，資料隨時會被盜用，最終令你蒙受損失。



## 常用手法



### 1 假網上優惠

騙徒會以優惠套票、門票作誘餌，將受害人誘導至假網頁並騙取信用卡資料。



### 2 小心指定快遞公司

騙徒會冒充「買家」並要求選用特定嘅快遞公司，再發送虛假訊息表示「買家」已付款，指示事主到虛假網站輸入銀行戶口、密碼、流動保安編碼等重要資料以完成「交易」。

## 防騙貼士

- 💡 懷疑信用卡被盜用應盡快透過HSBC HK App鎖卡
- 💡 喺有需要時暫停信用卡 / 扣賬卡網上交易功能
- 💡 設置每月網上消費限額，以防騙徒進行大額未經授權交易
- 💡 如發現可疑交易，可於HSBC HK App內提出爭議
- 💡 保管好實體信用卡，切勿隨便輸入一次性密碼，並啟用HSBC HK App網上交易認證服務認證網上交易
- 💡 如收到你沒有授權嘅交易通知，請立即聯絡銀行

# 假冒詐騙 – 執法人員篇

扮公安、扮法官、扮檢察官……騙徒搞咁多大龍鳳，無非都係想利用你嘅情感脆弱面，配合不同藉口同心理技巧，令你墮入騙局！



## 常用手法



### ① 假扮內地公安 / 執法機構

指控你涉嫌洗黑錢、發布虛假資訊或者觸犯內地法律等等，要求你提供戶口資料同繳交巨額保證金，否則將起訴或禁止你(或你嘅家人)返回內地，甚至會以網絡電話 (VoIP) 嘅改號技術更改來電顯示號碼，騙你入局！

## 防騙貼士

- 💡 提防可疑來電，切勿向陌生人透露銀行或個人資料
- 💡 內地執法人員絕不會透過來電向你索取個人資料或要求轉賬
- 💡 騙徒可用不法手段取得你嘅個人資料，就算對方講得出你嘅資料，亦唔代表佢嘅身份屬實

# 假冒詐騙 - 客服篇

有疑問，你會搵客服幫手，但對於主動聯絡你嘅「客服」，你又有冇遇過？騙徒會化身成不同客服職員，隨時由「客服」秒變「中伏」。



## 常用手法



### 1 假扮網購 / 支付平台客服

騙徒會致電受害人，聲稱事主申請咗付費服務或VIP會籍，如需取消服務，需要提供銀行資料，否則會被自動收費。當事主要求取消服務時，電話就會轉駁到同樣係假冒嘅銀行職員，並要求事主交出銀行卡及信用卡資料，訛稱會將存款轉賬至指定戶口。



### 2 假扮銀行客服

騙徒假冒銀行職員，聲稱客戶嘅戶口出現異常或將會被凍結，要求客戶提供個人網上銀行密碼，甚至發送具有密碼重置連結嘅電郵，以盜用銀行戶口。

## 防騙貼士

- 切勿點擊可疑短訊、電郵或網頁中嘅連結，避免進入可疑網站並下載不明軟件
- 一旦發現密碼或敏感個人資料被盜取，應立即聯絡銀行，同時檢查有冇可疑交易紀錄，並更改戶口密碼
- 使用銀行官方網站、應用程式提供嘅資訊，或銀行卡背面嘅熱線



# 假冒詐騙 - 技術支援及深度偽造(Deepfake)

助人為快樂之本？對騙徒嚟講，助人背後原來係詐騙之本！唔想受對方嘅「熱心」而受騙，就要提防假支援、真詐騙！



## 常用手法



### 1 假扮技術支援人員

騙徒會透過彈出視窗訊息、詐騙電話或釣魚電郵，以服務暫停、偵測到非法活動等理由，誘使受害者致電熱線或安裝指定軟件程式，從而遙距駭入裝置，盜取敏感個人資料或操控網上銀行。



### 2 假企業高層、政府官員

不法份子會利用深度偽造新型換面技術製作影片，偽裝成企業高層或政府官員，並透過電郵或即時通訊要求受害者進行轉賬。

## 防騙貼士

- 切勿點擊彈出視窗嘅網址或撥打裡面嘅電話號碼
- 切勿將資金轉賬至陌生戶口，或將個人資料及電腦遙距存取權限分享至陌生人
- 切勿從非官方應用程式商店下載應用程式
- 定期為裝置掃描惡意軟體和病毒，以尋找任何潛在保安漏洞
- 除非你確信檔案或附件的來源安全可靠，否則不要開啟或下載
- 即使你認識發件人，也要提防深度偽造，留意片中人物聲線、語氣、表情有冇異常、模糊或經過剪接

# 加密貨幣投資騙案

心急便輸了！騙徒就係睇準投資者著急嘅心態而設下騙局，一不小心隨時未投資先「輸」錢！



## 常用手法



### 1 「低風險、高回報」投資平台

騙徒會喺社交平台或群組冒充名人分享內幕貼士，或假扮「交友筍盤」，遊說受害人於虛假投資平台「開戶」及匯款，甚至為盈利效果而偽造交易紀錄，最終呢走資金、個人資料及操控網上銀行。

## 防騙貼士

- 💡 應在已註冊或可信賴機構進行投資
- 💡 投資前應諮詢專業人士並了解投資產品嘅相關內容
- 💡 只從裝置嘅官方商店下載應用程式
- 💡 避免下載可疑應用程式或於可疑投資平台透露敏感個人資料

# 網上情緣騙案

網上交友，身份可以係假，  
感情都可以係假，可能只有  
詐騙企圖先係真！

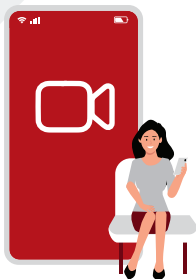


## 常用手法



### 1 急需現金周轉

透過社交或交友平台吹噓自己背景及職業，又可能加入特殊群組去接近情感脆弱嘅人士，同受害者建立網戀關係後，會訛稱因生活或海外物流被扣查而急需現金周轉，繼而要求轉賬至騙徒戶口。



### 2 裸聊勒索

騙徒會遊說受害人進行視像聊天，甚至會說服受害者進行裸聊，繼而勒索對方。

## 防騙貼士

- 💡 與陌生網友保持適當距離，亦應善用搜尋器驗證身份
- 💡 避免於社交平台上透露個人資料及切勿透露銀行戶口資料
- 💡 面對過於「完美」的交友對象應加緊提防

# 通訊軟件及社交平台騙案

今時今日，通訊同社交平台軟件已經係大家日常必備嘅app，但亦係騙徒「速食」詐騙嘅手法之一。



## 常用手法



### 1 扮親友借錢

一句「忙緊嗎？」，表面係關心，其實背後暗藏目的。騙徒會藉著各種不法手段盜取大眾嘅通訊軟件或社交平台賬戶，並訛稱各種理由向受害人嘅親友借錢。

## 防騙貼士

- 💡 於即時通訊軟件啟用雙重認證，增加賬戶安全性
- 💡 當收到親友要求銀行轉賬或匯款嘅訊息，記得致電對方驗證真偽
- 💡 切勿於未經核實嘅情況下透露驗證碼、一次性密碼、銀行戶口等資料

# 支票騙案

網上購物，一般會以網上過數，但部分騙徒卻化身成「彈票黨」，利用無效支票行騙。



## 常用手法



### 1 先「入票」後出貨

騙徒普遍會冒充學校、老人院、慈善機構職員，甚至交易平台買家，以無效支票進行交易，此時賣家銀行戶口嘅「賬面結餘」會增加，製造成已付款嘅假象，令受害人誤以為支票已入賬並出貨，造成財物損失。

## 防騙貼士

- 💡「賬面結餘」包括存入但未結算以供提取嘅支票，呢個金額只供參考
- 💡「可用結餘」係指戶口內實際可供提取嘅款項
- 💡存入支票後需1至2個工作天才完成結算，收款時留意戶口嘅「可用結餘」，「賬面結餘」不能作準

# 求職騙案

機會，係要由自己爭取，但有時主動送上門嘅機會，背後隨時係個精心設計嘅騙局，例如係「筍工」！



## 常用手法



### 1 假招聘 真呃錢

有騙徒透過社交平台刊登招聘廣告，以人工高、福利好、要求低作為賣點，過程中要求應徵者提供個人及銀行戶口資料，同時施加壓力，迫使受害者匆忙做出決定。



### 2 網購平台刷單賺佣

騙徒會將市民加至虛假刷單通訊群組，聲稱只要完成簡單任務即可獲得酬勞，從中騙取敏感個人資料，或者要求受害人墊支及存款。

## 防騙貼士

- 💡 求職時若對方要求你即時提供敏感個人資料，務必小心提防
- 💡 切勿透露你嘅銀行登入資料、一次性密碼，甚至借出個人名義申請任何貸款
- 💡 對海外工作機會保持高度警惕
- 💡 切勿授權他人使用你的戶口
- 💡 潛在僱主或招聘人員絕不會要求你支付費用



以上情況只供參考。如對本行之有關服務有任何疑問，歡迎致電滙豐熱線2233 3000，或親臨分行向職員查詢。

若懷疑自己遭遇詐騙，請致電香港警方的「防騙易熱線18222」，或下載升級版「防騙視伏App」進行識別。

