

# Common scams you need to avoid

## 常見詐騙可疑交易樣態

### Purchase Scam

In a purchase scam, the victim pays in advance for goods or services that are never received, which they advertise at a low price to attract buyers. These scams usually involve the victim using an online platform such as an auction website or social media.

#### 購物詐騙

騙徒會在社群平臺或拍賣網站散布虛假售物訊息。歹徒通常會以低廉的價格吸引買家。被害人預先繳付貨款，但最終不會收到貨物。

### Investment Scam

In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. The criminal will usually promise a high return to entice their victim into making the transfer.

Adverts on social media usually offering unrealistic returns, and letters are also used heavily in investment scams.

#### 投資詐騙

騙徒透過交友軟件、在社交平台刊登假冒名人教投資的廣告，又或透過白撞訊息結識事主；取得信任後，便向事主透露有“穩賺必贏”的“內幕投資消息”，並傳送虛假投資網站連結或要求下載第三方虛假投資APP進行投資；初期事主確能小額獲利及成功提現，一旦事主加大投資金額，有關平台或APP便會以不同藉口拒絕事主提取金錢；及後，事

主繼續不斷被威逼利誘要求支付金錢，最終仍無法取款始知被騙

## **Romance Scam**

In a romance scam, the victim is persuaded to make a payment to a person they have met, often online through social media or dating websites and with whom they believe they are in a relationship.

Fraudsters will use fake profiles to target their victims to start a relationship, which they will try to develop over a longer period. Once they have established their victim's trust, the criminal will then claim to be experiencing a problem, such as an issue with a visa, health issues or flight tickets and ask for money to help.

### **網戀詐騙**

“戀人”透過網絡社交平台主動結識事主；“戀人”自稱專業人士，例如工程師、飛機師、軍人、甚至皇室貴族；以甜言蜜語博取事主歡心，繼而發展成網戀關係；各種藉口表示未能與事主親身見面，但又不斷強調希望將來一同生活；其後“戀人”以生病、周轉困難等理由向事主借錢；又或聲稱郵寄貴重禮物，而隨後有自稱海關、物流公司之職員徵收關稅或運費；最終被騙去金錢，“戀人”失去聯絡，才醒覺被騙

## **Advance Fee Scam**

In an advance scam, the fraudster tells the victims that a fee must be paid to release the funds or goods, however, when the payment is made, the promised goods or money never materialise. These scams often begin on social media or with an email, or a letter sent by the criminal to the victim.

### 預付款詐騙

騙徒在網上不同社交平台出售商品(例如“一票難求”的演唱會門票)、預訂或提供服務;並要求買家“先預付款、後寄貨”的方式交易;最終買家無法收到商品或服務

### Invoice & Mandate Scam

In an invoice or mandate scam, the victim attempts to pay an invoice to a legitimate payee, but the criminal intercepts emails, claiming that the bank account details have changed, and convince the victim to redirect the payments to an account they control.

### 發票詐騙

在這類詐騙中，當被害人嘗試匯款給他們的正式收款人時，歹徒截取被害人的電郵，聲稱銀行戶口資料有所變更，誘導被害人匯款至歹徒控制的銀行戶口。

### Impersonation: Police/Bank Staff/Others

In this scam, the criminal contacts the victim purporting to be from the police or the victim's bank and convinces the victim to make a payment to an account they control.

These scams often begin with a phone call or text message, with the fraudster claiming there has been fraud on the victim's account, and they need to transfer the money to a 'safe account' to protect their fund. However, the criminal controls the recipient account. Criminals may pose as the police and ask the individual to take part in an undercover operation to investigate 'fraudulent' activity at a branch.

假冒公檢法詐騙: 騙徒假扮不同身份(公安、快遞、電訊公司等...)來電，報上事主身份資料後，訛稱事主身份資料被

盜用或涉及犯罪，繼而將電話轉線到另一名假冒公安的騙徒，以進行“視頻辦案”；騙徒展示印有事主相片及身份資料的拘捕令、保密協議等偽造的文件；其後，以“資金審查”或“取保候審”為由，要求事主匯款到“安全帳戶”或繳交“保證金”，藉此騙取事主款項；又或者利用偽冒政府機關網頁或應用程式的“共享屏幕功能”，騙取事主銀行帳號資料、密碼及驗證碼；而沒有經濟能力的事主，騙徒則改為“教唆其欺騙父母轉賬”，或被騙徒利用進行各種“戴罪立功的任務”。騙徒或假扮公安人員與事主通話，騙徒偽造法律文件令事主信以為真