
# 「守網聯盟遊戲卡」延伸教材

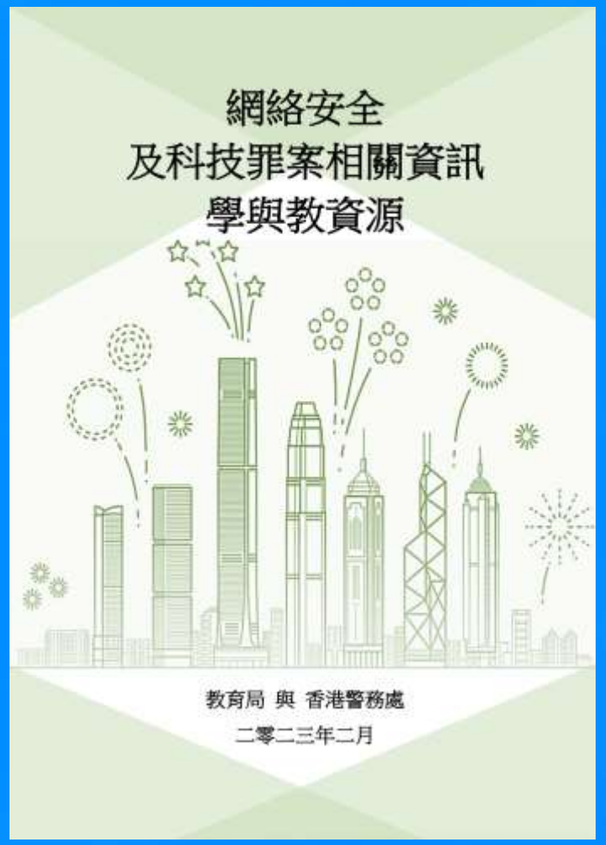
# 引言

為提升青少年對網絡安全的認識，網絡安全及科技罪案調查科於2025年10月推出「守網聯盟」遊戲卡。這套遊戲卡以本地高小及中學生為主要對象，透過輕鬆有趣的遊戲方式，讓學生在互動中學習防騙知識，加強對科技罪案及網絡威脅的警覺性。

「守網聯盟遊戲卡」結合多個深受歡迎的政府部門吉祥物，每張卡片均印有實用的網絡安全資訊，寓教於樂，讓學生在收集與遊玩的過程中，掌握自我保護的技巧。是次活動更獲得教育局及數字政策辦公室的全力支持，共同推動網絡安全及數碼素養教育，共建更安全的網絡環境。

# 學與教建議

適合中小學使用
建議與《網絡安全及科技罪案相關資訊》學與教資源冊一同使用






請瀏覽網址：
https://www.edb.gov.hk/cybersecurity

# 騙案類型

- 網上購物騙案
- 網上投資騙案
- 網上求職騙案
- 釣魚騙案
- 網上戶口盜用
- 裸聊勒索騙案
- 網上援交騙案
- 網上情緣騙案
- 信用咭盜用
- 電郵騙案

# 網上購物騙案

「在社交平台購物，
付款後卻收不到貨品。」

# 騙徒欺騙消費者之手法

1

## 假扮賣家

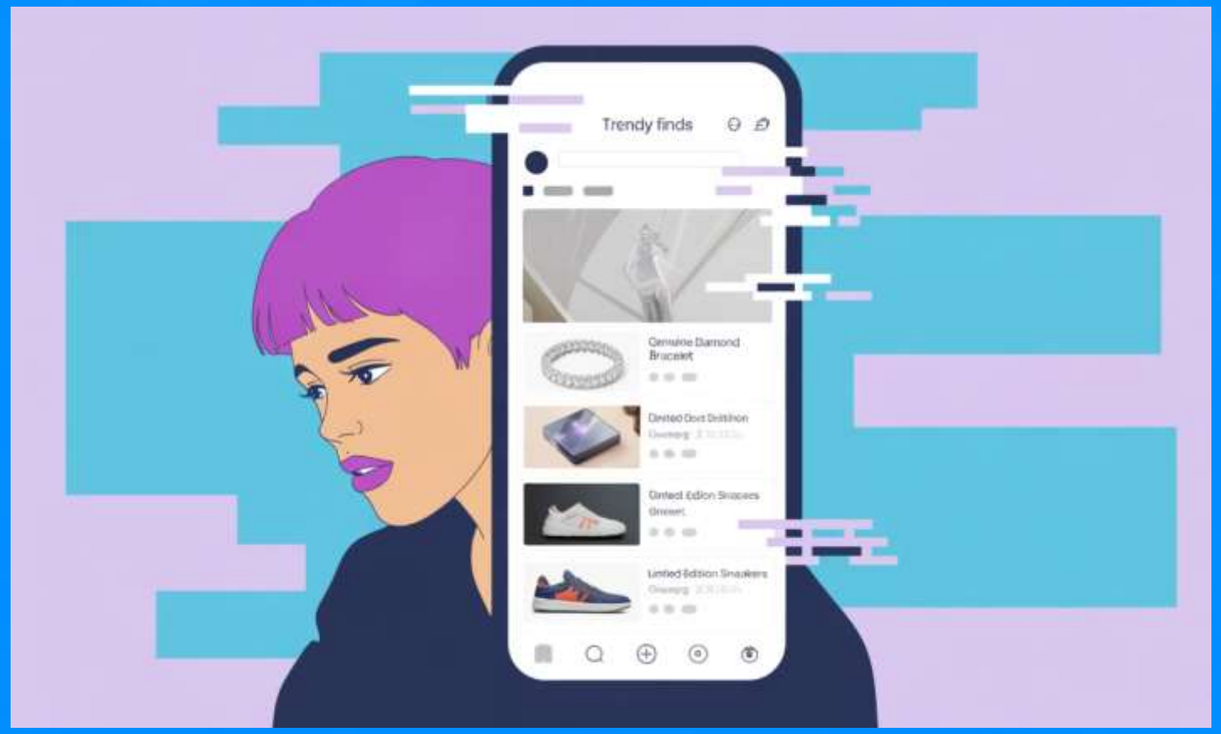
- 特別優惠 - 以限購、減價、外地代購等作招徠，吸引買家
- 先收錢後失聯 - 要求買家先匯款至指定戶口，拒絕當面交收。收款後失去聯絡

2

## 假扮買家

- 虛假收據 - 以虛假入數收據作匯款證明
- 無效支票 - 將未能兌現的支票存入賣家戶口，營造虛假的入賬記錄
- 收貨後失聯 - 騙徒收取貨品後便會失去聯絡，賣方其後發現未能入賬方知被騙

# 可疑特徵




## 買家留意：可疑社交平台網店之特徵

- 專頁一般只經營了數天或數星期，無實體店地址或辦公室電話（提示：在「專頁透明度」能看到專頁建立日期）
- 專頁或會刊登廣告以提升知名度
- 專頁內售賣的貨品種類不一，大多是一些近期受歡迎貨品
- 聘用打手給予好評或留言，製造多人光顧假象
- 專頁內只有少量貼文
- 貼文內的相片多從其他網店擷取

# 如何分辨假網購專頁

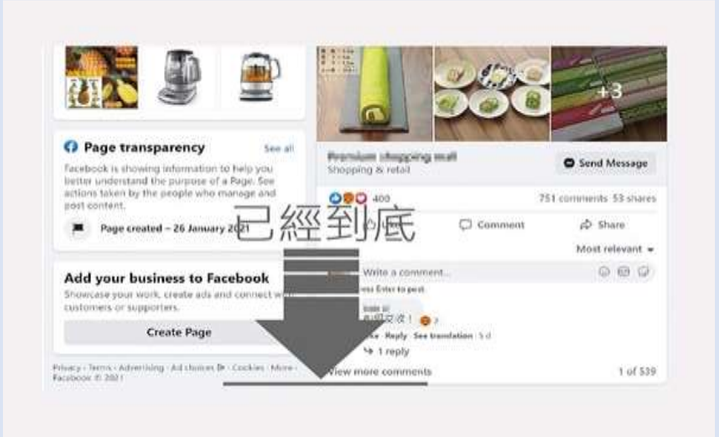
## 識別網上平台假專頁特徵


只經營了短時間
無實體店地址或辦公室電話


管理人員來自不同國家及刊登廣告以提升知名度


聘用打手給予好評或留言
製造多人光顧假象


出售近期受歡迎的產品




專頁內只有少量貼文


貼文相片多從其他網店擷取

# 防騙建議

1

光顧信譽良好的賣家，儘量選擇當面交收

2

應盡量透過官方銷售渠道購買貨品

3

出售貨品時，不應單憑入數收據便相信付款完成

4

付款前應先搜尋賣家的電話號碼、銀行戶口號碼、專頁名稱等，並留意負評

5

如有任何懷疑，應立即終止交易

6

如有懷疑，可在「防騙視伏器」輸入電話號碼、社交媒體帳號等評估風險，或致電18222查詢

# 思考問題

**消費模式：**

1. 你有在網上購物的經驗嗎？
2. 你日常的消費模式是怎樣的？
3. 你認為怎樣才是正確的消費態度？

**網上購物騙案：**

1. 一般人為何會成為「網上購物騙案」的苦主？
2. 應如何保護自己，防範騙徒？
3. 如果不幸受騙應如何處理及應持守怎樣的態度？


# 網上投資騙案

騙徒在網上社交平台、討論區貼文或在即時通訊軟件發放訊息，以低風險、高回報作招徠，吸引素未謀面的網民參與投資。然而，這些投資大多是不存在或充滿陷阱。有騙徒會偽造獲利的交易記錄，誘使受害人投放更多資金後，便會失去聯絡。

# 騙案手法

1

## 網上尋找獵物

漁翁撒網地識新朋友，經常上載「生活照」炫富，提高可信性

2

## 假扮投資顧問或基金經理

訛稱有豐富投資虛擬資產、貴金屬或外匯的經驗

3

## 唱高散貨

推介受害人購買「仙股」。實際上騙徒早在低位大量入貨，當受害人買入股票被推股價，騙徒隨即沽貨離場

4

## 虛假投資應用程式

誘使受害人安裝虛假投資應用程式，當中顯示虛假交易和回報

5

## 套現時被要求繳交手續費/出現系統故障

受害人如欲套現，騙徒會以須繳交高昂手續費，或聲稱系統故障拖延付款

6

## 建立曖昧關係(又稱「殺豬盤」)

與受害人建立曖昧或網戀關係，以獲取受害人信任，繼而誘騙投資

# 虛假投資網站或軟件的特點

1. 假網站的網址一般不能在搜尋器找到，假app也不會在官方軟件商店上架。假平台顯示的股票或商品價格、用戶的資產組合等均為偽造

2. 當受害人欲套現獲利，「假客服」會以各不同藉口拖延，例如戶口被凍結，投資涉及違規操作需交罰款，或者充值到某金額才可套現等，誘騙受害人再投放資金。受害人最終蒙受巨額損失

# 防騙建議

1. 提防網上認識的「高富帥」或「白富美」推介投資項目。如有懷疑，可利用搜尋器搜尋對方社交帳戶的照片、查看對方帳戶的朋友圈是否有異常或要求與對方視像通話
2. 不要隨便簽署任何投資授權書
3. 提防回報高得不切實際的投資計劃
4. 切勿下載不明來歷的應用程式
5. 切勿輕信在社交平台上發放的「內幕消息」
6. 切勿將本金轉賬至個人名義的戶口。如透過加密貨幣轉賬更應審慎
7. 在投資虛擬資產前，應充分了解相關產品特性和資訊安全風險

# 思考問題

**理財模式：**

1. 你如何管理個人財務？
2. 你是否有為個人的收入與支出作記錄？

**網上投資騙案：**

1. 「投資」是甚麼？市面上有哪些流通的投資工具？
2. 「投資」有甚麼風險？投資者應持甚麼投資態度？
3. 一般人為何會成為「網上投資騙案」的苦主？
4. 應如何保護自己，防範騙徒？
5. 如果不幸受騙應如何處理及應持守怎樣的態度？


# 網上求職騙案

騙徒透過不同網上社交平台、討論區或即時通訊軟件，刊登招聘貼文吸引應徵人士，並以不同藉口誘騙他們繳交費用、保證金或其他款項，其後失去聯絡。

# 騙徒的招聘廣告一般有的特點

- 聲稱高人工、即日出糧或在家工作
- 對應徵者年齡及學歷要求低
- 聲稱無需工作經驗及不用提供履歷
- 不會提及公司名稱或地址，只提供即時通訊軟件或手機號碼聯絡方法
- 會強調不涉及犯法或色情活動，以減低應徵者戒心
- 不會提及實際職位及工作內容

# 常見「刷單」騙案手法


1

## 聲稱招聘「訂單處理員」

與一般虛假招聘廣告類同，騙徒聲稱招聘「訂單處理員」、「跟單助理」、「落單員」等，以低門檻和優厚待遇吸引應徵者。騙徒也會以SMS和iMessage等大量發出招聘訊息

2

## 假冒真實商店

騙徒會假冒真實的網購平台貼文，並製作假網站或假app

# 「刷單」流程

## ① 白撞訊息介紹職位空缺

唔好意思 打攪喇！我系 Cherry 目前我哋有幾個職位空缺，可以同你分享資料睇吓？ 15:12

好丫 15:12

呢排我哋幫緊幾家公司招人，免費提供各類職位空缺及發展機會 福利同待遇 良好。
（長期 / 臨時工 / 周末散工) 早晚間都有，合作公司包括大小型企業。
地點：香港各地區 ✅
條件：要求系成年者/銀行戶口出糧/履歷表 (CV) 列出工作經歷/知識/技能
歡迎任何人/新手/退休人士 ✅

我安排雇主 send 詳細工種資料,薪資待遇畀你參考，可以了解睇睇吓有咩適合你嘅工作。Ok? 15:13

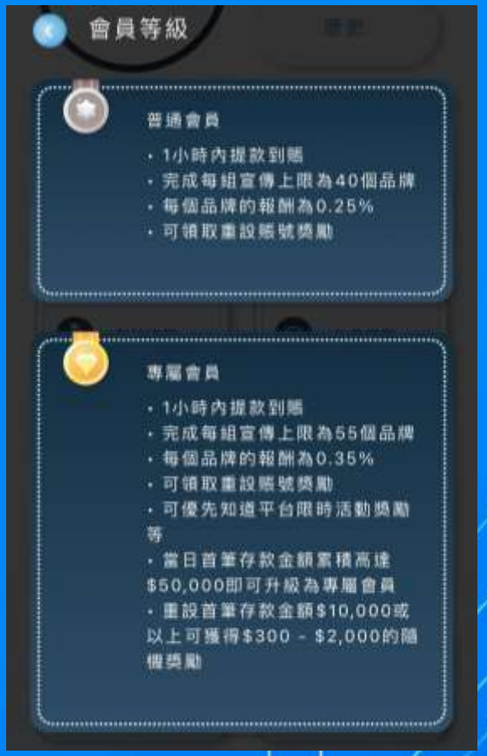
## ② 介紹網上宣傳工作並強調即時出糧

公司名：InitiativeIQ
呢间公司主要做嘅就係幫助啲同公司合作嘅品牌方做宣傳，主要係利用線上宣傳（SMM技術）幫助提高品牌嘅知名度同时都可以刺激到品牌嘅價值 17:46

好 工作內容? 17:46

人工方面計日，一日400蚊-1300蚊，工作時間同地點自己定，每日喺平台運營時間完成就得，完成工作後公司會通過 FPS 或者網銀出糧 17:46

## ③ 虛假網站完成任務後收取「報酬」，存款愈多， 比率愈高



# 其他騙案手法


## 代客轉資

借出戶口代公司客戶轉資，以賺取佣金，但先要以個人名義向財務公司申請貸款，或以信用咭透支購買金飾，並交出財物作抵押。有騙徒甚至藉詞要求受聘人交出提款咭及密碼，及後將其戶口存款偷走

## 境外代購

招聘人士到境外代購奢侈品如名牌手袋，並要求受聘人墊支機票及酒店住宿等費用


## 採購墊支貨款

招聘人士進行採購智能電話等貨品，並要求受聘人墊支貨款或以高價購買平價原材料

## 買LIKE

以「俾Like」賺佣金做招徠，甚至推出月費套餐，月費套餐越貴，每次「俾LIKE」賺佣越多

# 其他騙案手法 要求預先支付學費


# 防騙建議


使用可靠的
求職平台


提防無須經驗
及報酬優厚的
招徠

了解聘方公司背
景及業務性質


切勿隨便透露
個人資料

被要求付費時應
提高警惕

# 防騙建議


一招避免陌生人
加你入WhatsApp群組
1
設定
CyberDefenderHK
虛擬替身
清單
群發訊息
已標上星號
已連結裝置
帳戶
私隱
對話
通知
儲存空間及數據
2
私隱
最後上線時間及在線狀態
個人頭像
關於我
連結
群組
虛擬替身貼圖
動態
目前位置
通話
聯絡人
變更群組私隱設定
3
群組
誰可將我新增至群組
所有人
我的聯絡人
我的聯絡人，除了...

# 思考問題

**生涯規劃：**

1. 你會如何規劃你未來？
2. 你會如何選擇適合自己的工作？
3. 你認為求職時有什麼地方需要注意？

**網上求職騙案：**

1. 一般人為何會成為「網上求職騙案」的苦主？
2. 應如何保護自己，防範騙徒？
3. 如果不幸受騙應如何處理及應持守怎樣的態度？

# 釣魚騙案

騙徒透過發放短訊、電郵、語音、二維碼等作餌，騙取受害人帳戶憑證、信用卡及個人資料。

# 騙案流程

① 騙徒發送釣魚短訊，內附連結至假網站

② 網站要求輸入帳戶資料、個人資料、信用咭資料等

③ 套取帳戶資料後盜用積分換取禮品，信用卡資料用於海外網站購買無實物的貨品轉售圖利或個人資料作不法用途

# 其他騙案手法


發送釣魚訊息開展對話，以套取對方個人資料


假扮政府部門或的私人公司，誘騙聯絡假冒客服


假扮證券公司，以套對方的證券公司資料，並以高買低放其股票的方法套現

# 防騙建議

1. 切勿隨意回撥來歷不明短訊內的電話號碼
2. 鼓勵更多行業積極參與登記制，以有效提升短訊的安全性和可信度
3. 定期將短訊收件箱內存舊記錄清除
4. 當收到任何短訊都應提高警惕，切勿開啟或點擊來歷不明電郵或訊息內的超連結
5. 在任何情況下，不要向身分未經核實的短訊發送人披露任何個人或敏感資料
6. 應透過官方渠道查證

# 思考問題

**釣魚攻擊：**
1. 甚麼是釣魚攻擊？
2. 日常生活中你有遇過嗎？試舉一例子說明。

**釣魚攻擊的影響：**
1. 釣魚攻擊對個人有何影響？
2. 一般人為何會成為「釣魚攻擊」的苦主？
3. 應如何保護自己，防範騙徒？
4. 如果不幸受騙應如何處理及應持守怎樣的態度？


# 網上戶口盜用

騙徒利用釣魚短訊或搜尋器優化中毒攻擊，騎劫受害人網上帳戶，繼而向其親友索取金錢。


# 網上戶口盜用手法

1

## 手法一：釣魚短訊

- 騙徒發送釣魚短訊，內附連結至假網站
- 假網站套取用戶電話號碼，並要求平台向用戶發放轉移代碼
- 騙徒再向用戶套取轉移代碼
- 騙徒用另一裝置登入用戶的帳戶
- 騙徒向用戶的親友以轉賬或借貸為名騙財

2

## 手法二：搜尋器優化中毒攻擊

- 騙徒製作假WhatsApp網頁登入版面網站
- 騙徒在搜尋器以「WhatsApp」作為關鍵字投放廣告
- 用戶在搜尋器輸入關鍵「WhatsApp」，假網站便會以置頂廣告形式出現
- 用戶點擊置頂廣告進入虛假網站，然後掃描惡意二維碼，騙徒隨即取得用戶連線資料
- 騙徒經網上版WhatsApp同時登入用戶的帳戶，並向親友騙財

# 其他網上戶口盜用手法

1


受害人收到假冒「WhatsApp」發送的釣魚訊息，並在假網站中輸入騙徒所提供的「八字代碼」，導致其 WhatsApp 帳戶被騎劫。

2


複製受害人女兒早前發送的語音短訊。

3


刪除受害人與其女兒所有對話記錄。

4


在受害人 WhatsApp 中新增假冒「女兒」為聯絡人，盜用其頭像及暱稱。

5


以假冒「女兒」的 WhatsApp 帳戶向受害人提出轉賬要求。


# 網上帳戶入侵的原因

例如曾在公用電腦上登入網頁版的即時通訊軟件而忘記登出、使用了惡意的多帳戶登入工具、電子裝置遭到惡意軟件入侵等。

騙徒通常以網上銀行轉賬超出限額為由，要求通訊錄的聯絡人幫忙轉錢，並且承諾翌日還錢，要求轉錢的數目也是由數千至數萬元不等。當然偶爾也有巨額轉賬要求。

# 防騙建議

1. 啟用雙重認證功能
2. 定期檢視帳戶所連結的裝置，並且登出所有不明的已連結裝置
3. 於留言信箱設定強密碼，避免一次性語音密碼被盜取
4. 不要盡信搜尋器的結果，建議將常用網頁加入書籤
5. 留意短訊內容和網頁是否有異樣，例如域名串錯字、繁簡字夾雜等
6. 如收到親友透過訊息要求幫忙過數或匯款，應致電對方確認其身份及有關要求
7. 避免連接公共WiFi或在公共電腦上登入網上帳號
8. 切勿隨便透露密碼、驗證碼或掃描二維碼

# 思考問題

**網上戶口及個人資料：**

1. 你有網上開設戶口嗎（社交平台/遊戲平台/電郵……）？
2. 你應為網上戶口資料會被洩露嗎？
3. 你會如何保護你的個人資料私隱呢？

**網上戶口盜用：**

1. 一般人為何會被騙徒盜用戶口？
2. 應如何保護自己，防範騙徒？
3. 如果不幸受騙應如何處理及應持守怎樣的態度？


# 裸聊勒索騙案

騙徒在社交媒體假扮妙齡少女結識男受害人，誘使其進行裸聊，期間錄製整個過程。亦有騙徒事先向受害人發出超連結，誘使受害人下載能夠偷取電話內通訊錄的惡意程式，再進行裸聊。最後，騙徒會威脅將受害人的裸露片段發佈於網上或轉發受害人親友，從而向對方索取點數卡、加密資產或要求轉賬到外地戶口。

# 犯案三步曲

## 拍攝裸露影片

騙徒利用預先錄製的性感「罐頭片」以假亂真，讓受害人降低戒心，再誘使受害人在鏡頭前裸露甚至作出猥褻動作。其實騙徒已拍下受害人裸露片段

## 偷取通訊錄資料

部分騙徒會以轉用其他通訊平台為藉口，誘使受害人以下載惡意程式，偷取受害人電話通訊錄

## 購買點數卡/加密資產/海外銀行轉賬

騙徒會指示受害人購買點數卡、加密資產或轉賬到海外銀行，以換取受害人的裸露影片不被外泄予親友


# 防騙建議

切勿在視像聊天期間裸露身體

切勿點擊不明來歷的超連結或下載程式

切勿輕信對方是以「真面目」示人，可要求對方做出指定動作

# 思考問題

**網上交友及聊天：**

1. 你有網上聊天及交友嗎？你認為當中有風險嗎？
2. 你會如何選擇「朋友」呢？
3. 你會如何保障個人私隱及自我保護？

**裸聊勒索騙案：**

1. 一般人為何會成為「裸聊勒索」的對象？
2. 應如何保護自己，防範騙徒？
3. 如果不幸受騙應如何處理及應持守怎樣的態度？

# 網上援交騙案

「騙徒於社交媒體結識受害人，聲稱提供援交或性服務，並約會受害人。但在見面前，會要求受害人購買遊戲點數卡或比特幣作服務之按金，並在行騙後失聯。受害人與騙徒從未真正見面。」

# 犯案三步曲

1

## 假扮妙齡少女尋找目標

騙徒透過社交平台、約會軟件或援交網站等假扮妙齡少女尋找目標(以男性為主)，在交談過程中套取事主個人資料，以便搜尋其社交圈子。騙徒聲稱提供援交服務，或假裝急需事主的金錢協助。

2

## 要求購買點數卡/禮物卡/支付虛擬資產

騙徒假稱擔心警察「放蛇」，要求事主見面前先購買遊戲點數卡 / 禮物卡、支付虛擬資產（如比特幣）或以銀行轉賬作服務按金，甚至提供身分證明文件影像。當完成「課金」後，「少女」當然不會現身。

3

## 進一步勒索

騙徒假扮「少女」的「經理人」，聯絡事主並要求加碼「課金」。由於騙徒已掌握事主的個人和社交圈子的資料，如事主拒絕跟從，騙徒便會威脅傷害受害人及其家人為名進行勒索。受害人往往擔心自身安全，惟有跟從騙徒指示，最終蒙受巨大損失。

# 防騙建議

網上交友時，請認清對方身份

不要向陌生人提供個人資料

若在見面前被要求繳付保證金，絕大部分都是騙案

如接獲恐嚇應報警求助

# 思考問題

**誘惑：**

1. 你平常活躍於社交/影片平台嗎？
2. 你會因為想得到物品或優惠上載個人相片或影片嗎？
3. 你在面對誘惑時應如何加強自我保護意識，作出合理的判斷及負責任的決定？

**網上援交騙案：**

1. 一般人為何會成為「網上援交騙案」的苦主？
2. 騙徒可以通過什麼方式或途徑得知受害人的資料？
3. 應如何保護自己，防範騙徒？
4. 如果不幸受騙應如何處理及應持守怎樣的態度？

# 網上情緣騙案

「騙徒在社交平台找尋目標，認識受害人後向對方展開追求攻勢，以迅速建立網上的戀人關係，繼而用不同藉口去騙取金錢。騙徒與受害人之間卻從未真正見過面。」

# 傳統騙案的手法

## 扮專業人士

騙徒多在網上自稱來自歐美、或於東南亞地區工作的專業人士，如工程師和跨國企業管理層等，以英語與受害人溝通，並以各種籍口向受害人要求金錢

## 藉口多多

訛稱需支付巨額醫療費用或急需現金週轉；或訛稱有貴重禮物從海外寄給受害人，但被扣查，需清關費 / 手續費

## 100%未見面

受害人100%從未見過騙徒(無論親身或視像通話)，騙徒騙取金錢後，便會取消社交媒體戶口、電話號碼或電郵地址等，和受害人斷絕聯絡

# 「殺豬盤」手法


## 「搵豬」

騙徒在社交平台、約會軟件等以「高富帥」或「白富美」的身分尋找目標，並投其所好，迅速建立曖昧或網戀關係

## 「養豬」

誘騙受害人在虛假投資平台 / 下載假軟件進行投資，例如買賣證券、外匯或虛擬資產。騙徒起初會讓受害人賺取少許回報，以吸引對方進行大額投資

## 「殺豬」

當受害人投入大額資金，帳面獲利甚豐，欲套現離場時，平台「客戶服務員」便會以各不同藉口拖延，並誘騙受害人再投放資金。受害人最終蒙受巨額損失

# 虛假投資網站或軟件的特點

- 假網站的網址一般不能在搜尋器找到；假app也不會在官方軟件商店上架，只能透過非官方途徑下載。假平台顯示的股票或商品價格、用戶的資產組合等均為偽造

- 當受害人想套現獲利，「假客服」會以不同藉口拖延，例如戶口被凍結，投資涉及違規操作需交罰款，或者充值到某金額才可套現等，誘騙受害人再投放資金。受害人最終蒙受巨額損失

# 防騙建議

利用搜尋器搜尋對方社交帳戶的照片

查看對方帳戶的朋友圈是否有異常

如對對方身份有懷疑，可嘗試與對方視像通話

切勿下載不明來歷的應用程式

提防回報高得不切實際的投資計劃

# 思考問題

**兩性關係：**

1. 你平常活躍於社交/影片平台嗎？
2. 你會接受於通訊軟件與陌生人交談嗎？
3. 你認為網上/以通訊軟件交友會面對什麼風險？
4. 你如何面對與異性的關係？

**網上情緣騙案：**

1. 一般人為何會成為「網上情緣騙案」的苦主？
2. 應如何保護自己，防範騙徒？
3. 如果不幸受騙應如何處理及應持守怎樣的態度？

# 信用咭盜用

「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。」

# 信用咭資料有什麼失竊途徑

## 信用咭遺失或被盜

賊人可直接使用你遺失或被盜的信用咭進行消費，直至信用額用盡為止

## 實體商戶盜用咭資料

立心不良的店員可能會複製信用咭資料以作轉售或其他非法用途

## 釣魚攻擊

黑客設置虛假網站，並發放釣魚電郵，以不同借口(如戶口更新、被凍結等)誘使用戶輸入信用卡資料

## 零售系統(POS)終端機

零售系統伺服器如受到POS惡意程式感染，連接伺服器的電腦便會被黑客控制並盜取信用咭資料

## 非法盜取個人資料以申請信用咭

騙徒假冒咭主向銀行報失信用咭，其後從咭主信箱偷取銀行補發的新信用咭。騙徒或會利用非法盜取個人資料向銀行提供偽造住址證明，以便新咭寄到騙徒指定信箱

# 防騙建議

- 收到新咭時，應盡快更改預設帳戶名稱及密碼
- 應在可靠及商譽良好的網店購物
- 只在有https加密保護的官方網站進行網上付款
- 切勿以公共電腦登入網上銀行或輸入咭資料
- 切勿向任何人披露自己的咭資料
- 提防釣魚網站或電郵，不要隨意點擊電郵內含的超連結或附件

# 思考問題

**咭類資付工具：**

1. 你有信用咭/扣賬咭/個人八達通嗎？
2. 你一般用來做什麼？
3. 你認為當中有什麼風險？

**信用咭盜用：**

1. 信用咭在什麼情況下會較易被盜用？
2. 應如何保護自己，防範騙徒？
3. 如果不幸受騙應如何處理及應持守怎樣的態度？

# 電郵騙案

「騙徒利用黑客技術入侵目標公司或其商業夥伴電郵系統，窺看有關的商業電郵往來，繼而透過電郵假冒該公司高層或商業夥伴，欺騙公司員工匯款至騙徒戶口。」

# 騙案手法

### 假冒伙伴

假冒公司商業夥伴/供應商，要求受害人將貨款轉賬至「新戶口」

### 假冒高層

假冒公司高層，指示員工匯款至不明戶口

## 如何識別詐騙電郵

- 騙徒會以極相似域名製作虛假電郵魚目混珠
- 查看電郵標頭，可得知郵件的真實來源地址、回覆地址，以判斷電郵的真偽

# 防騙建議

- 查看電郵標頭，判斷電郵真偽
- 匯款到新帳戶前要核實對方身分
- 不要輕信突然改變的匯款要求
- 向公司職員 / 商業伙伴傳遞以上資訊

# 思考問題

**電郵：**

1. 你有用電子郵件嗎？
2. 你會用什麼方式下載及閱讀郵件（網上平台/本機軟件）？
3. 你會開啟電郵及相關連結嗎？為什麼？

**電郵騙案：**

1. 一般人為何會成為「電郵騙案」的苦主？
2. 應如何保護自己，防範騙徒？
3. 如果不幸受騙應如何處理及應持守怎樣的態度？

# 謝謝