

高發詐欺手法解析

刑事警察局預防科

釣魚連結詐騙流程

發送帶有「釣魚連結」訊息

點入「釣魚」網頁

騙取輸入「個資」

偽冒開立「電子支付」會員

帳戶款項遭「盜轉」

訊息來源:

iMessage



RCS(即時通訊)



電子郵件



簡訊

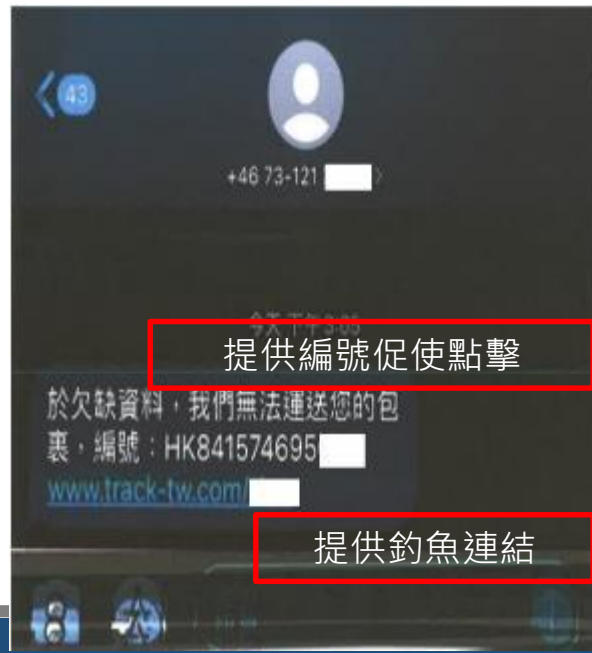
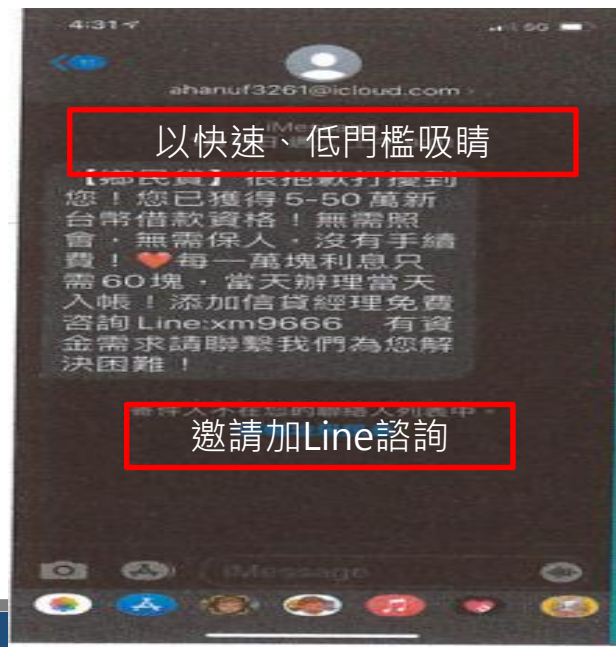


釣魚連結防範方法:

- ◆ IOS開啟「未知與垃圾訊息」過濾功能，阻絕可疑訊息
- ◆ 於設定中關閉RCS(即時通訊)功能，避免收到詐騙訊息
- ◆ 不輕易點擊不明連結，境外來訊(開頭顯示+886、+44)應多加注意



案例：
簡訊通知「通行費」未繳
點擊連結輸入個資信用卡秒
遭盜刷



案例：
「恭喜獲得貸款額度！」詐釣
魚簡訊誘上鉤 詐團海撈19
萬

假投資詐騙流程



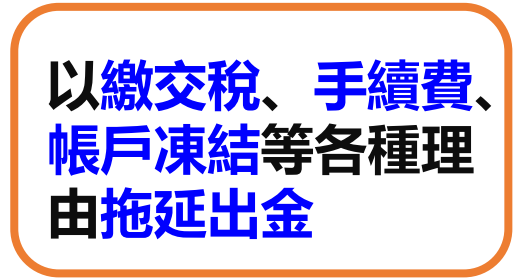
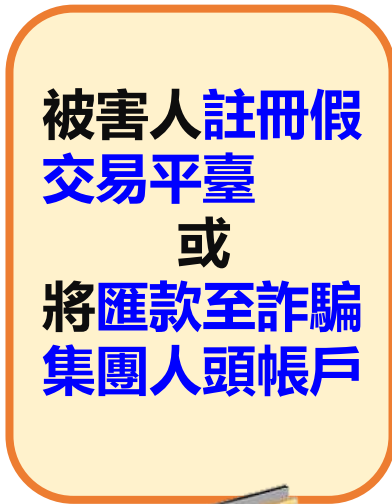
詐騙集團



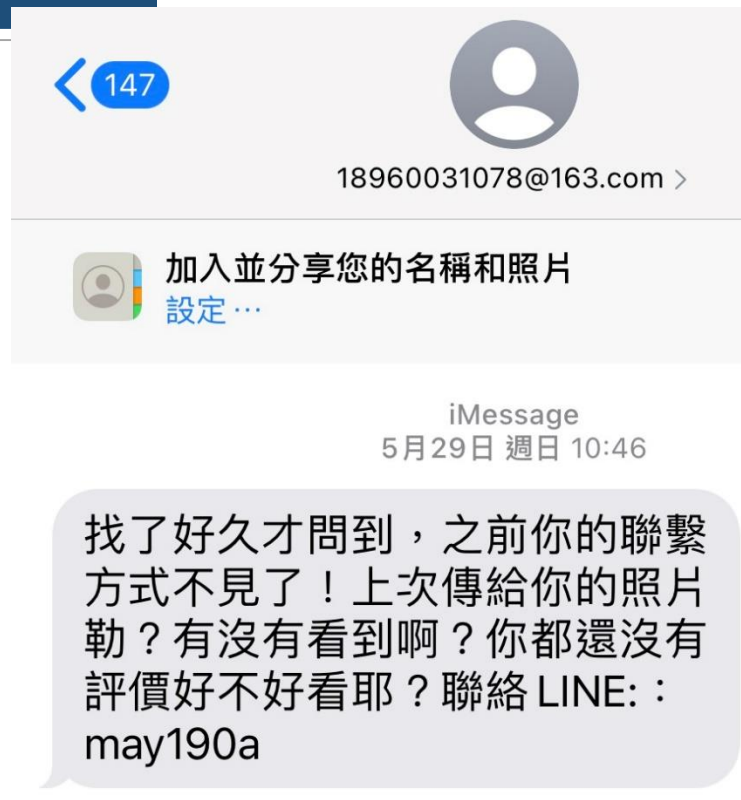
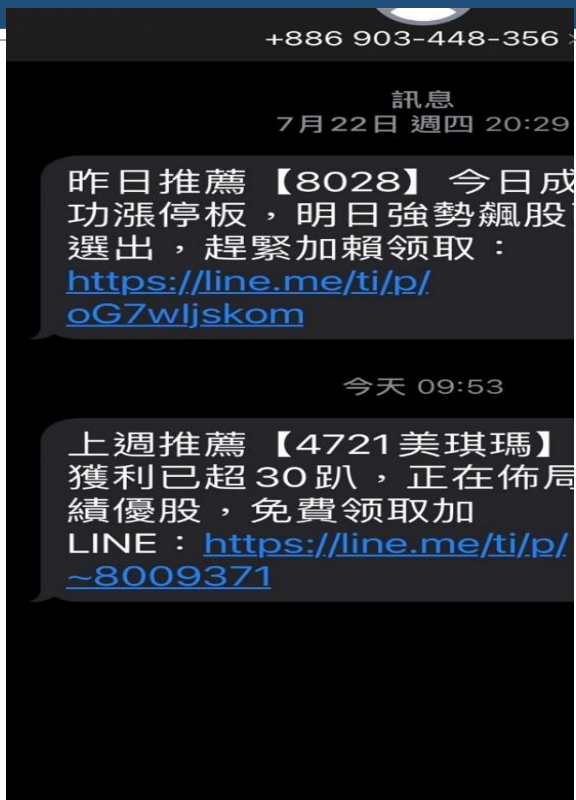
假扮名人、投資顧問等，透過網路接觸被害人



以高獲利、穩賺不賠話術，慫恿被害人投資股票、虛擬貨幣等



被害人血本無歸



假投資防範方法:

- ◆ **不聽信來源不明的投資信息，如網友推薦、非正規投資顧問等**
- ◆ **選擇良好交易平台，不依他人指示註冊或使用不明交易網站或APP**
- ◆ **勿貪小便宜，聽到穩賺不賠、高獲利零風險等關鍵字應提高警覺**



假網拍防範方法:

- ◆ 使用有優良信譽、第三方支付之購物平台
- ◆ 避免使用通訊軟體或社群網站與賣家私下交易
- ◆ 以面交或貨到付款方式交易，於確認商品後再支付款項

假分期付款詐騙案常見 2 階段轉接手法

1 線 假冒賣場服務人員

假冒賣場
謊稱員工
誤設分期
付款。

詢問民衆金融卡
或信用卡客服電
話，表示金融機
構人員會聯絡
民衆。

2 線 假冒銀行或郵局客服

要求民衆
至提款機
(ATM)操作
解除分期付
款設定。

提供錯誤帳
戶，致民衆
操作失敗(
卸除民衆心
防)。

指示於轉入帳
號畫面輸入商
品編碼或銷帳
編號，指示輸
入密碼。

謊稱與遊戲
點數公司合作
，幫民衆做強
制性退款，要
求至超商購買
遊戲點數。

手機接到國外
來電(開頭有
帶+號)請先掛
掉，歹徒會竄改
電話顯號。

來電顯號市話開
頭出現002、009，
手機開頭出現
+02、+2等顯號，
應提高警覺。

銀行或郵局
客服不會要
求操作提款
機(ATM)。

防騙專家 怎麼說



提款機(ATM)
只有提款或轉
帳功能，不能
解除分期付款
或退款。

遊戲點數僅
供遊戲使用，
無解除分期
付款功能。

如有疑問，請直
撥165反詐騙諮
詢專線查詢。

3 招教您別上當

1 要求至ATM解除
分期付款並詢問金融
機構客服電話即是詐
騙。

2 要求在ATM轉帳
畫面輸入商品(銷帳)編
號、密碼即是詐騙。

3 電話中要求購買
遊戲點數，詢問序號、
密碼即是
詐騙。



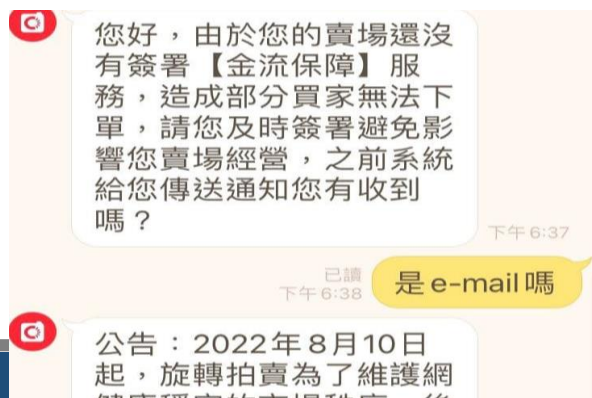
解除分期(假買家)詐騙流程

假冒買家

假賣場客服

假冒銀行員

私訊或偽裝成官方平台訊息，稱賣場連結無法下單，轉而提供假客服連結、QR CODE或LINE ID



以「賣家未簽署金流服務協議或帳戶認證」等名義要求賣家提供個人資料進行身分驗證

要求賣家依指示操作ATM、網銀APP匯款或遊戲點數

解除分期(假買家)防範方法:

- ◆ 使用經認證的合法交易平台，避免使用通訊軟體與買家聯繫
- ◆ 勿點擊買家提供之客服、銀行網站連結
- ◆ 看到未簽署金流服務協議、帳戶認證等關鍵字，應中止交易、立即查證
- ◆ 不依指示操作ATM或網路銀行

假愛情交友詐騙

STEP 01



歹徒用帥哥、美女圖
於交友APP、社群軟體
隨機搭訕、加好友

STEP 03



以各種理由說要將
積蓄、退休金等貴重
物品以包裹寄給你，
拜託你代收、代保管

STEP 05



收到匯款後便人間
蒸發、再也聯繫不上

STEP 02



自稱戰地軍官(醫)、駐外
工程師等成功人士
每天噓寒問暖、喊你寶貝、
親愛的、老公老婆

STEP 04



以包裹卡在機場、港口需
繳納關稅、手續費等理由
陸續要求民眾於短時間內
儘速前往匯款

詐

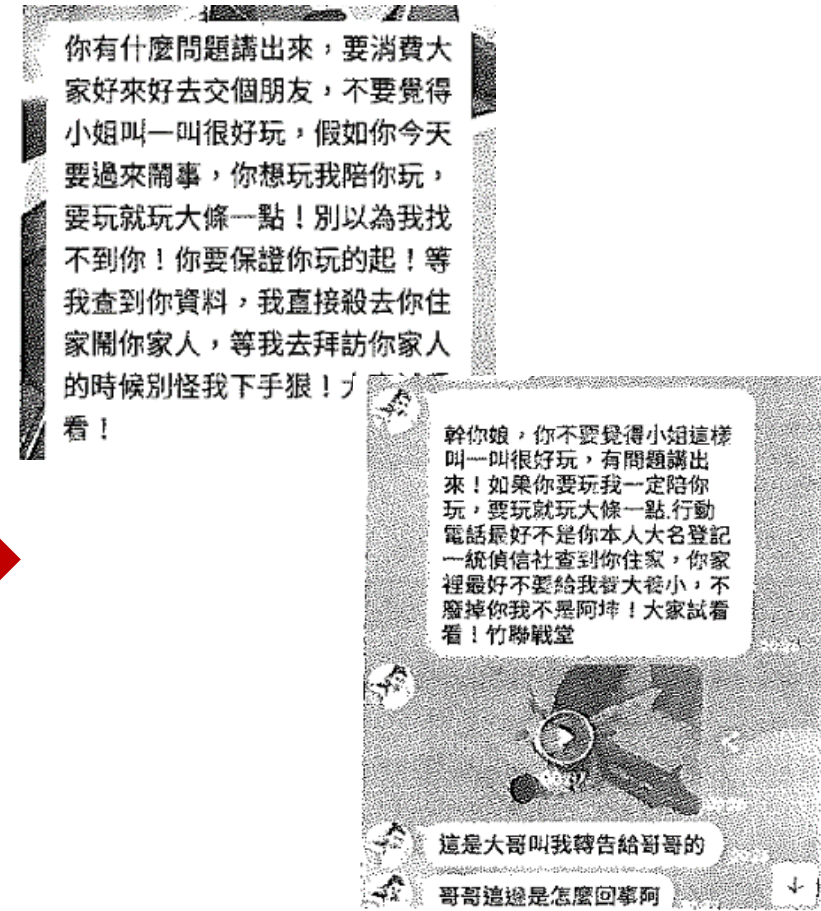
根本沒有包裹



假愛情交友防範方法:

- ◆ 不輕信網友說法，應確實查證網友身分是否屬實
- ◆ 不輕易接受對方要求，特別是代收包裹或要求金錢
- ◆ 不可提供個人隱私資訊，如身分證字號、銀行帳戶等

色情應召詐騙手法



詐騙集團假冒年輕貌美女生，透過社群網站、交友軟體尋找被害人並加入LINE好友

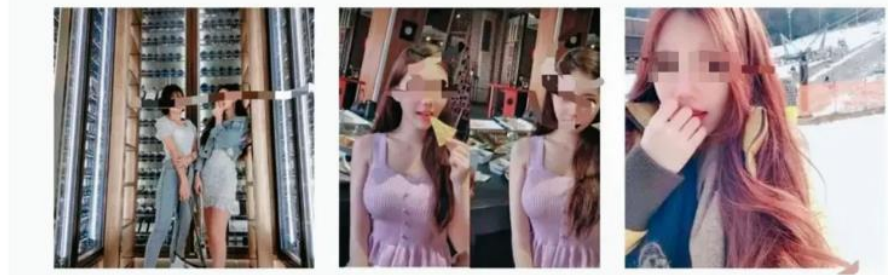
透過LINE向被害人透露有兼職援交，並要求被害人購買遊戲點數當保證金及付款

被害人如不從，則由另一自稱黑道男子恐嚇要對被害人不利，要求買點數或匯款

• 色情應召詐騙手法

33.3k 人追蹤 ☆ 追蹤

【逾萬詐欺都輕判3】騷妹舔舌清涼照誘上鉤 先詐欺後恐嚇
受害人被扒兩層皮



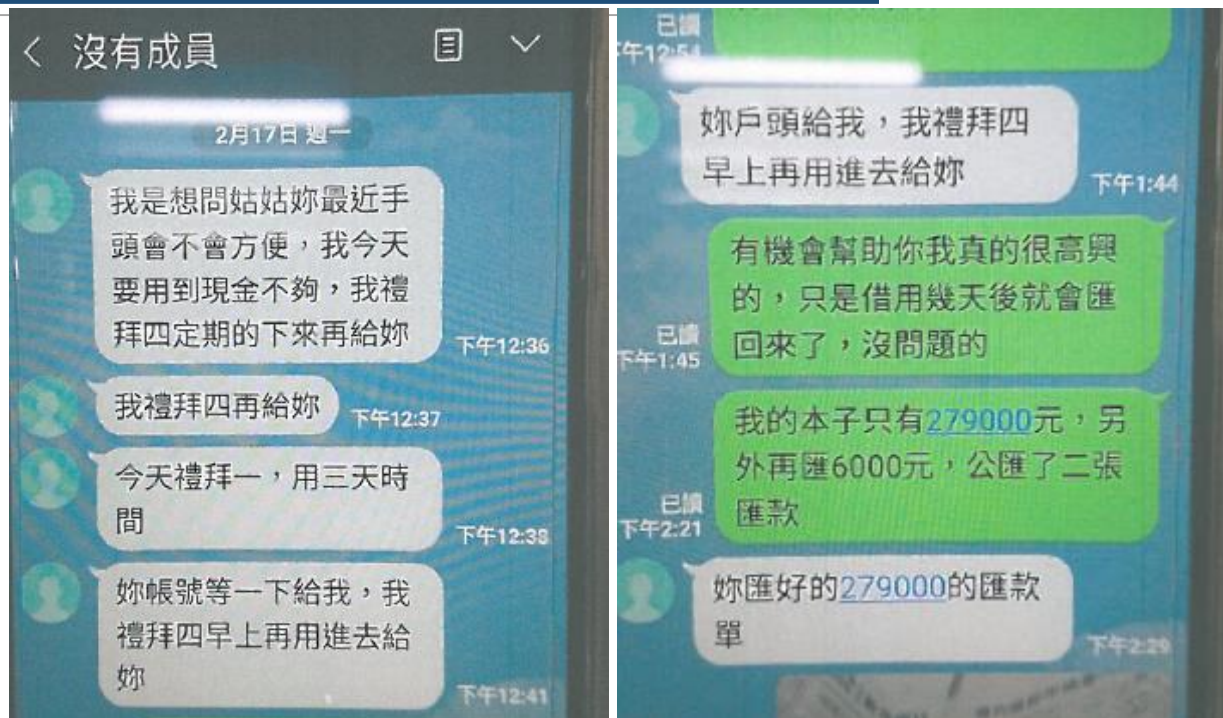
檢警發現，詐騙集團最新手法是盜用美女或帥哥照，透過IG等社群誘騙被害人上鉤，再以投資等各種名義詐財。（翻攝畫面）



檢警發現，詐騙集團最新手法是盜用美女或帥哥照，透過IG等社群誘騙被害人上鉤，再以投資等各種名義詐財。（翻攝畫面）

刑事局掌握，宜蘭一名洪姓男子上月初在IG追蹤身材火辣的美女網友「小茹」，與對方聊天過程中，小茹不時私傳吐舌舔嘴的爆乳曖昧照，並向洪男推薦投資虛擬貨幣網站，表示該網站會有專業人員帶領操作，誇口穩賺不賠、低成本、高利率。

洪男信以為真，陸續匯款21萬元至該虛擬貨幣平台交易所人員指定的帳戶，後來想從該網站平台提領款項時，該平台人員告知密碼錯誤，一下子說需要繳交平台錢包內的15%金額做為押金才能提領，後來又改口需要25%代辦費，洪男此時驚覺醒悟遭詐騙報警。



猜猜我是誰防範方法:

- ◆ **小心提防不明來電**，特別是境外電話(開頭顯示+886)
- ◆ **聽到對方要求金錢時**，應掛掉電話向本人查證
- ◆ **不可於對話中提供個人隱私資訊**，如身分證字號、銀行帳戶等



妳是麗美嗎?

妳聲音怎麼怪怪的?

舅媽~

對啊!我是麗美

我感冒了啦~



手法介紹



假檢警防範方法:

- ◆ 接到聲稱為檢警或公務機關電話時，應要求對方提供單位、職稱、姓名，並掛掉電話向該單位查證
- ◆ 聽到聲稱「身分遭冒用」、「偵查不公開」、「監管帳戶」等關鍵字時，應提高警覺、向原單位或165查證

詐騙關鍵語

假醫護人員通話

您的身分遭冒用申領醫療補助證明，我將為您向該醫院所在縣（市）政府警察局報案，等一下會有警官打電話給您。

假警察通話

您涉及洗錢等重大案件，需製作電話筆錄，本案偵查不公開，向他人洩漏任何案情為重罪，我將電話轉接地檢署偵辦本案檢察官。

假檢察官通話

為證明您的清白，請清空您的所有帳戶，如果不配合，只好將您收押；我將會派書記官監管您的帳戶，請您將錢用銀行匯款或面交給公署保管，等案子結束再發還。

防詐五不 做好防護

跨境來電 不接

✓ 詐騙關鍵字：+886+市話號碼、+886+9偽手機號碼

防詐方法

不接不明跨境來電、務必確認對方身分

不明連結 不點

✓ 詐騙關鍵字：限時限量販售、賣場金流協議認證、假冒商家或政府發送簡訊

防詐方法

不點選不明連結、不載來路不明APP、官方網站查詢

穩賺不賠 不聽

✓ 詐騙關鍵字：飆股、穩賺不賠、高獲利零風險、領錢須繳交保證金或扣稅

防詐方法

不信網友教投資、不載來路不明APP、不加不明投資群組

個資卡號 不傳

✓ 詐騙關鍵字：提供金融帳戶安全碼、填輸個人身分資料、發送網路個人資料

防詐方法

不點選不明連結、不填輸個人資料、不發送個人資料

聲稱檢警 不信

✓ 詐騙關鍵字：偵查不公開、繳交保證金、監管帳戶

防詐方法

先詢問單位姓名、掛斷電話求證、撥打165反詐專線查證

有疑義請撥打
反詐騙專線165



防禦面思維

安全智慧防詐-保護個資隱私

不要輕易在電話、簡訊或
網路上提供個人資訊。



避免使用公用WIFI傳輸資料

防禦面思維

安全智慧防詐-保護個資隱私

定期檢查銀行和信用卡帳戶，確保沒有未經授權的交易。

112/09/02	IB81206	-1,000	✓
跨行提款	543		
112/09/04	IB00406	-500	✓
跨行提款	453000		
112/09/05	0130030	-73	✓
V S 購貨	363		
112/09/05	0133301	-140	✓
V S 購貨	378		
112/09/05	0133301	-120	✓
V S 購貨	308		
112/09/05	IB81206		
跨行提款	373		
112/09/07	0130030		
V S 購貨	363		

112/09/05	IB81206	-1,000	✓
跨行提款	373		

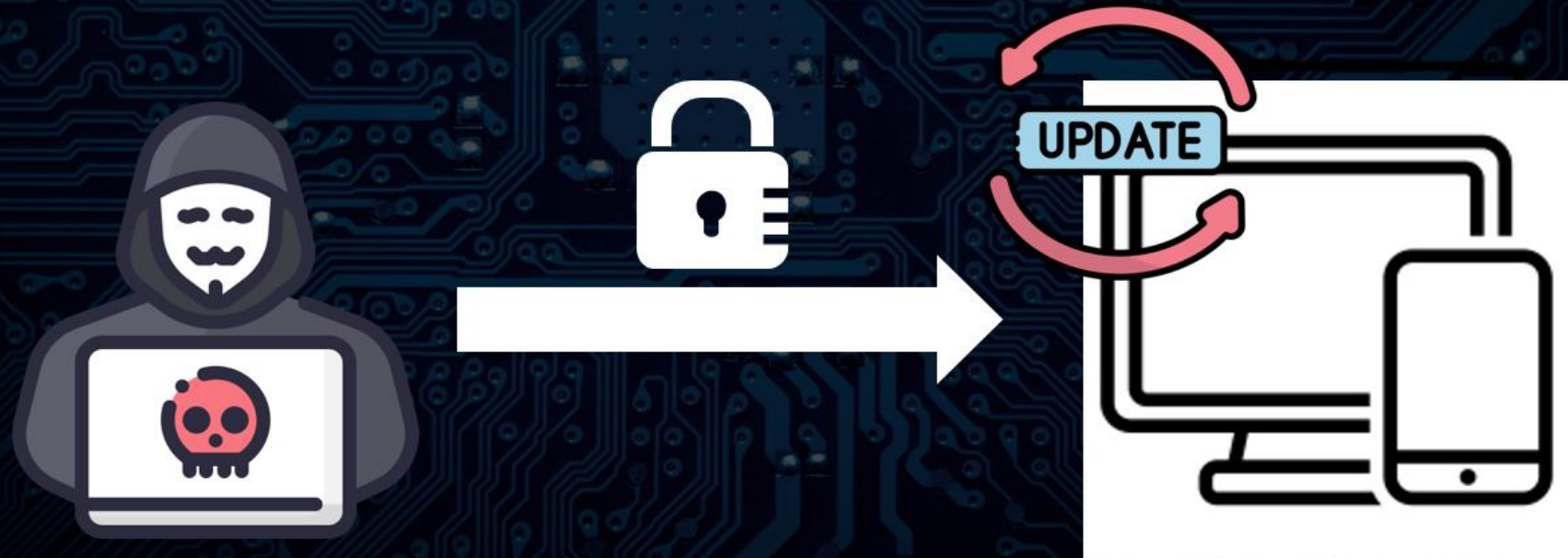
發現不明交易，立即確認



防禦面思維

安全智慧防詐-保護個資隱私

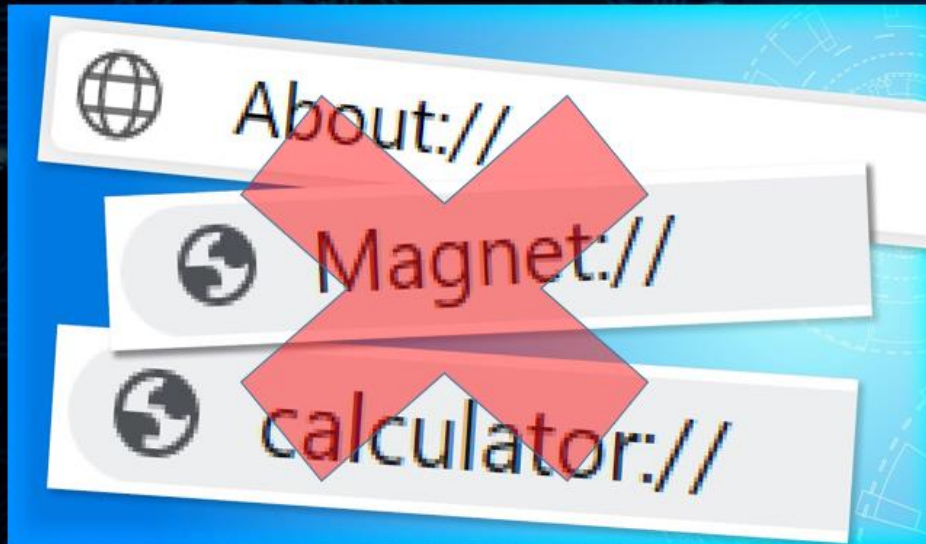
定期更新電腦、手機中的軟體至最新版本。



防禦面思維

安全智慧防詐-加強身分認證

不要隨意點擊來自不明來源的連結，特別是通過電子郵件或簡訊發送的連結。



<https://www.twsgov.me>



<https://www.twffgov.com>



<https://www.mohw.gov.tw>



防禦面思維

安全智慧防詐-加強身分認證

接到要求提供個人資訊的電話，要求對方提供相關證明。



防禦面思維

安全智慧防詐-加強身分認證

登入網站時，使用多重要素驗證(MFA)。

Multi-factor Authentication (MFA)



簡報完畢 敬請指導