台灣首府大學圖資處
110 學年資訊安全暨
智慧財產權宣導

什麼是假交友假投資

假交友　假投資　真詐騙流程圖

詐騙集團

透過社群網站、通訊軟體，散播假投資訊息；或透過交友軟體結合「假交友」方式，認識並取信被害人

LINE

YouTube

「高獲利」、「零風險」利誘吸引被害人加入施詐標的物平台

比特幣

代操外匯期貨

網路博弈

錢進詐騙集團

1. 買入投標的：引導被害人以買入虛擬貨幣、外幣等方式，要求被害人匯入詐騙集團提供的個人匯款帳戶

2. 繳納保證金：以匯款金額過大已遭金管會等政府機關注意，需繳納保證金始能取回為由，再要求被害人匯款保證金

受害人：領不出錢，聯絡不到人，荷包都空了

資料整理：Mr. Market市場先生

常見的詐欺模式分析一

資料來源：新北市警察局提供　　資料整理：Mr.Market市場先生

- **案例1：被害人在臉書認識一位「哈先生」，並推薦使用「HEKX香港聯合交易所平台」（行動應用程式APP）投資，致使損失高達三千餘萬**
- **步驟一）取信被害人：**
- **步驟二）購買虛擬貨幣作為投資資金：**
- 首先在「MAX交易所」（臺灣合法的虛擬貨幣交易所）購買虛擬貨幣，再將虛擬貨幣轉至「HEKX香港聯合交易所平台」，
- 然後讓被害人**取回獲利一次，利用實際感受到獲利，又再次取信被害人**。

常見的詐欺模式分析一

•步驟三）繳納保證金：

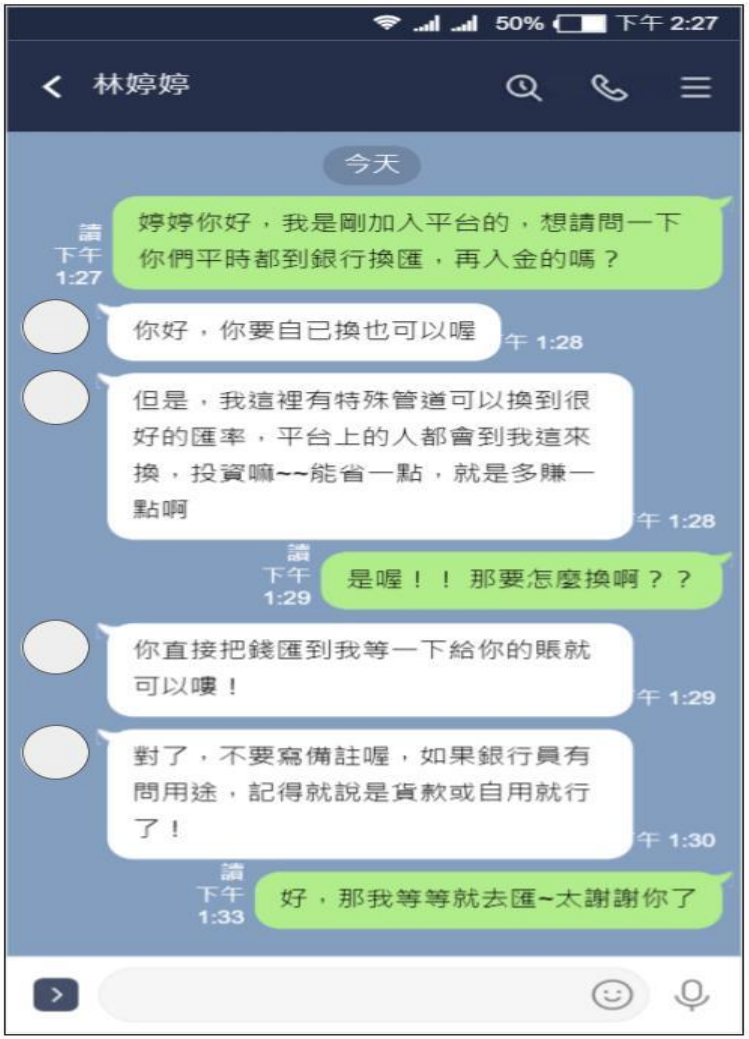
•接下來，被害人想要再取回獲利，平台客服（詐騙集團）以匯款金額過高，被香港金管會列為可疑帳戶，

•須先繳納保證金（以人民幣繳納）為由，要求被害人至臨櫃匯款至指定換匯賬戶（人頭帳戶），始能換匯並繳納保證金，

•最後，被害人連絡不上平台客服（詐騙集團），也無領出平台上的錢，此時才明白被騙，損失總金額高達三千萬。

常見的詐欺模式分析二

只要把錢匯入指定的個人帳戶
就可以拿到很好的換匯匯率

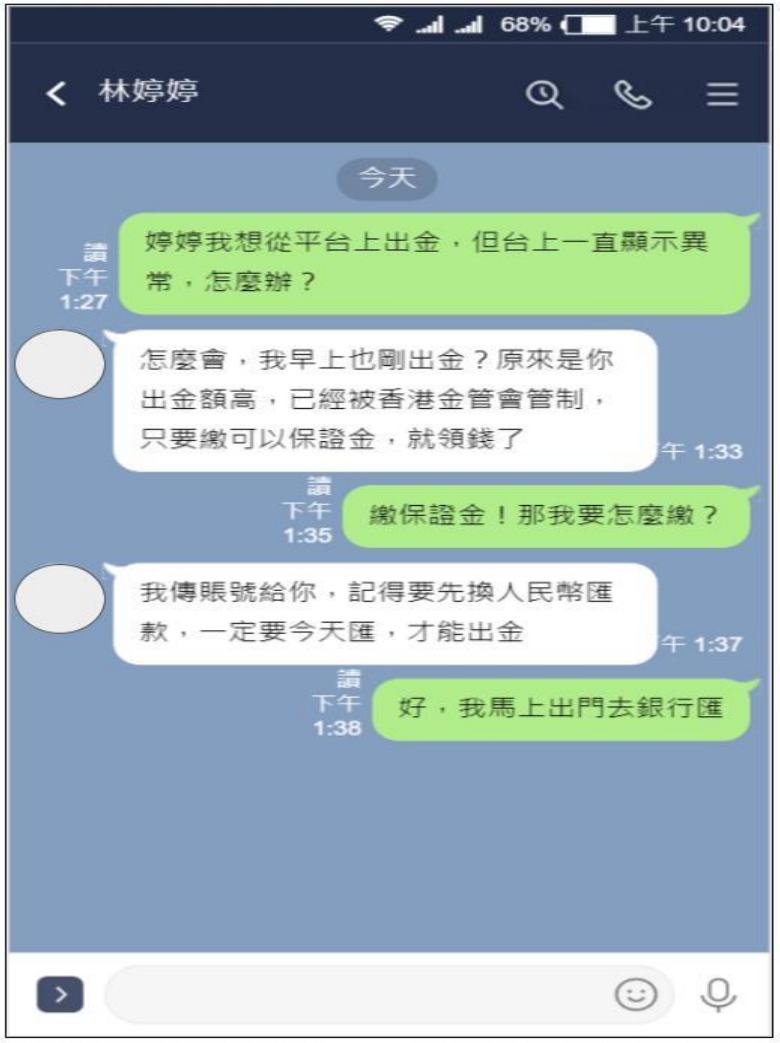


資料來源:新北市警察局提供　　資料整理:Mr.Market市場先生

- **案例2：被害人受邀加入LINE群組「股票期貨技術分析」，在群組助理暱稱「林婷婷」指導，下載投資平台「GLENBER及「MT4」（行動應用程式APP）**
- **步驟一）換匯（美金）作為投資資金：**
- 林婷婷以**提供較佳匯率的換匯帳戶（人頭帳戶）**，引導被害人直接匯款至換匯帳戶（人頭帳戶），並在**金融機構行員詢問資金用途時，必須說貨款或自用。**
- 在來自於「GLENBER平台」投資的獲利後，林婷婷便慫恿被害人加大本金以獲得更多獲利。

常見的詐欺模式分析二

領不出錢，怎麼辦?
只要再繳保證金，就可以領錢了



資料來源:新北市警察局提供　　資料整理:Mr.Market市場先生

•步驟二）繳納保證金：

•接下來，被害人要取回獲利，平台客服（詐騙集團）以匯款金額過高，被香港金管會列為可疑帳戶，須先繳納保證金（以人民幣繳納）為由，然後，要求被害人至臨櫃匯款至指定換匯賬戶（人頭帳戶），換匯並繳納保證金之後詐騙集團切斷聯絡管道，被害人無法登入「GLENBER平台」，才明白被詐騙，損失總金額超過一千萬。

常見的網路釣魚方式一

如果你的朋友用臉書私訊你,還附上一個來自”即時新聞”社團的影片 連結,問:「這是你嗎？」你會不會不假思索的點入連結,看看自己是不是成了醜聞中的主角?
這就是最近流傳,讓許多人卸下心防的臉書網路釣魚手法。

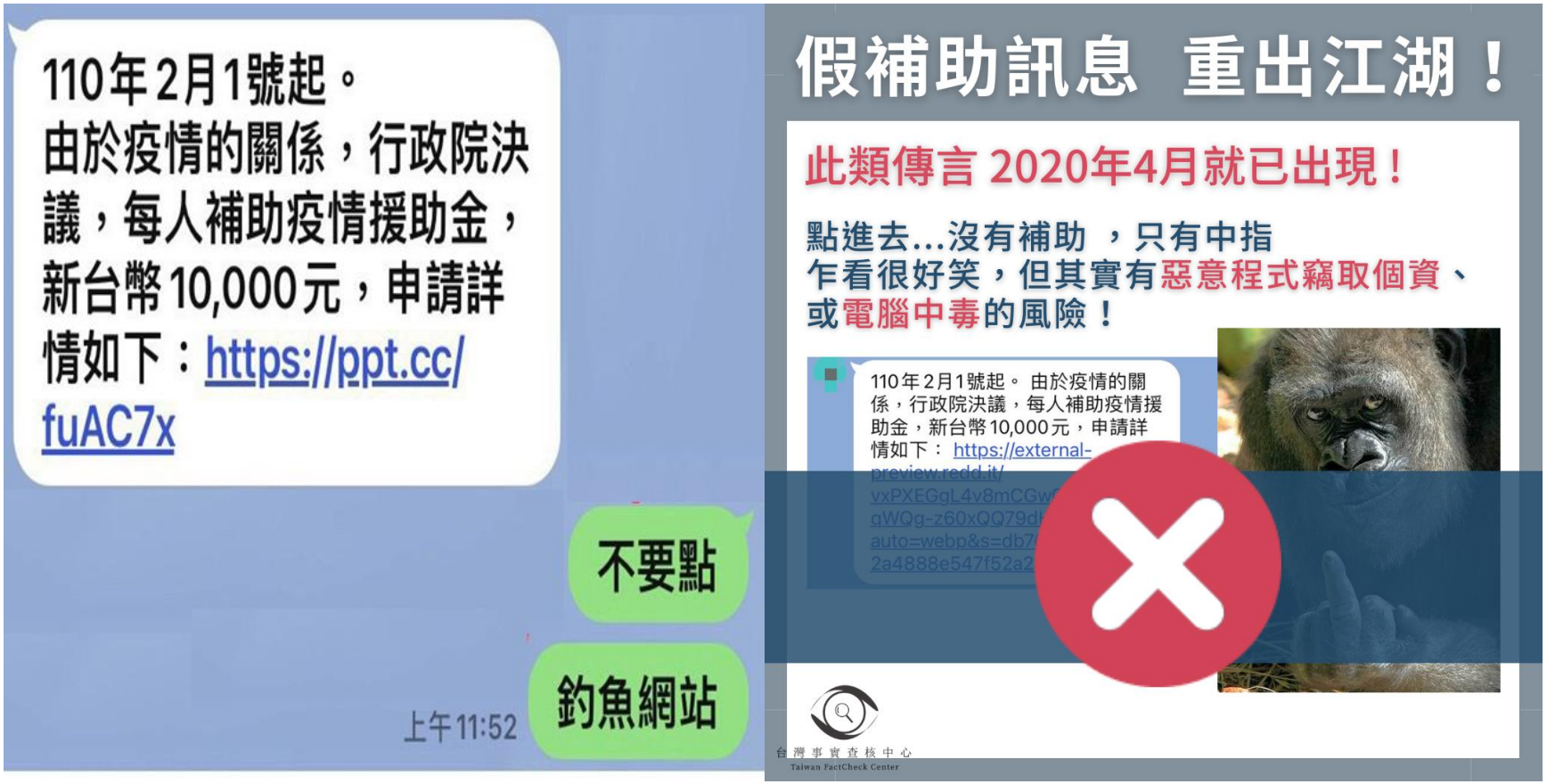
常見的網路釣魚方式二

透過好友分享的訊息會進入到一個 **FB** 社團中的某篇文章裡，而底下的留言是一個網址，它就是傳說中的臉書釣魚網站啦！！

常見的網路釣魚方式二(續)

點進留言中的臉書釣魚連結後，會進入到FB登入頁面，這是詐騙集團用來搜集你帳號密碼的方式，如果把你真實的帳號密碼輸入，他們就會竊取你的帳戶，並且用你的帳號繼續發臉書釣魚連結給其他人喔！

常見的網路釣魚方式三



「網址連.gov都沒有，一定是假的」。行政院下午表示，經查證這是假訊息，去年很早就在傳，行政院並沒有所謂2月1日起每人發放10000元疫情援助金的政策。

常見的網路釣魚方式四

接到惡意簡訊
並點擊連結

1、點擊後下載惡意程式

下載惡意程式
至裝置

常見的網路釣魚方式四

(一)遭歹徒利用向電信業者進行小額付費交易詐騙。

(二)手機為歹徒所控制，用來濫發惡意簡訊，除了使更多人誤觸連結並下載惡意程式外，更讓使用者簡訊費用暴增。

可以在家/在公司下載破解版/
盜版軟體來用嗎

案例說明

- 案例1：如果我自己在家中下載破解版（俗稱盜版）的軟體使用，我的行為有犯法嗎？

- 案例2：如果我上班的公司讓我和其他員工使用盜版軟體，公司和我會觸犯什麼法律嗎？

資料來源：鴻安法律事務所(https://www.honganlaw.com.tw/copyright-infringement-2/)

個人使用盜版軟體的法律責任

- 案例1：如果我自己在家中下載破解版（俗稱盜版）的軟體使用，我這樣的行為有犯法嗎？

  答案是有的。

  這樣子的行為已經構成經由擅自重製的方法侵害他人著作財產權。可依《著作權法》第91條：處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。

  除了上述的刑事責任，還有可能要負擔民事責任，依照《著作權法》第88條第1項規定：因故意或過失不法侵害他人之著作財產權或製版權者，負損害賠償責任。

  民事責任就是金錢的賠償，所以個人下載、安裝或使用盜版軟體，一旦被檢舉或查獲，不但有可能要賠償超過當初花錢買正版軟體的金額，還有可能面臨被關的下場，這樣子得不償失的行為，還是少做為妙。

資料來源：鴻安法律事務所(https://www.honganlaw.com.tw/copyright-infringement-2/)

公司使用盜版軟體的法律責任

- 案例2：公司讓我和其他員工使用盜版軟體，公司和我會面臨什麼法律責任呢？

答案是公司老闆、我跟其他有使用的員工都有可能犯法。

如果公司使用盜版軟體，除了公司負責人（或雇主）可能成為被起訴的對象以外，使用軟體的員工也有可能得視其使用行為來負擔刑責及民事責任（金錢賠償）。

因此，如果今天我們是受雇者，明知公司沒有預算或其他原因，不願意花錢購買正版軟體，被雇主要求使用盜版軟體即可的時候，應該要了解到自己的立場，這樣的行為不只老闆有可能被告，連員工都會是一起求償的對象，所以為了保護我們自身權益，安裝及使用盜版軟體的這些行為，一定要適時反應且不該照做。

反過來說，若今天的情形是員工「擅自」安裝及使用盜版軟體，即使雇主真的不知情，還是有可能會因為未盡到管理監督的責任，要一起負擔連帶責任。所以並不是單方面只有員工要注意，身為雇主的一方也應該善盡義務管理責任。

※如侵害電腦程式著作財產是作為「營業」使用的話，其刑事責任會依最終法院判決條文為主，但基本上一樣會是刑事責任及民事責任皆可求償。

資料來源：鴻安法律事務所(https://www.honganlaw.com.tw/copyright-infringement-2/)

使用開源P2P檔案分享軟體（BT、eMule）也有可能構成犯罪？

很多人會覺得使用P2P軟體的話，會找不到來源者，所以也就不會找到使用者（下載的人），但這樣的想法是不對的，因為只要有IP位址，在我國境內都可以查，何況使用P2P分享的種類繁雜，舉凡電影、音樂、動畫、漫畫、小說.....等等，只要「下載」或「分享」，就有可能會侵害到他人的著作財產權。

實務上也有很多案例，是個人透過這些非官方管道下載不明來源的檔案，而收到警察局的調查通知單，有些甚至是起訴至法院的例子，所以千萬不要僥倖以為只要自己沒有商業行為（營利），只是自己要收藏就可以擅自下載這些受著作權保護的檔案。

所以，你發現了嗎，千萬不要為了省小錢來下載盜版軟體，到時候因而吃上官司就虧大了！

除了「下載」之外，「分享」的行為也有可能會侵害到他人著作財產權，有時候只是一個簡單轉發或轉貼的動作，就有可能會為自己帶來麻煩。

資料來源：鴻安法律事務所(https://www.honganlaw.com.tw/copyright-infringement-2/)

如何在熱門網站上啟用雙重認證功能

Twitter

- 登入您的 Twitter 帳號，然後到「**設定**」。
- 在左側選單上，按一下「**設定和隱私**」。
- 在「**登入認證**」的地方，勾選「**認證登入請求**」。接下來網站會請你新增一個電話號碼。
- 請依照步驟進行，然後您的手機會收到一組六位數代碼，以後您每次登入 Twitter 都會收到一組像這樣的代碼。

手機使用者：

- 點一下 Twitter 應用程式上的**個人頭像**。
- 點一下「**設定和隱私**」來開啟設定。
- 點一下「**帳號**」。
- 然後點一下「**安全性**」來啟用「**登入認證**」選項。

Facebook

- 登入 Facebook 然後前往「**帳號設定**」。
- 按一下「**帳號安全和登入**」，往下捲到「**設定額外的安全措施**」，並找到「**使用雙重認證**」。
- 按一下「**編輯**」
- 看一下它的運作說明，然後選擇「**啟用**」。
- 系統會請您設定「已知的瀏覽器」，也就是您信賴而不需輸入認證碼的瀏覽器。
- 輸入您的電話號碼。
- 您的手機會收到一組確認碼。在畫面上輸入這組確認碼，就完成設定程序。

如果您不想透過手機簡訊來收到認證碼，您可以回到「**設定額外的安全措施**」，然後選擇「 **代碼產生器**」。遵照指示安裝可產生認證代碼的應用程式。

LinkedIn

- 在您的個人首頁上，按一下右上角的「**我**」，然後選擇「**隱私和設定**」。
- 按一下「**隱私權**」標籤，然後往下捲到「**安全**」來開啟兩步驟驗證，您需要提供手機號碼。

Amazon

- 登入您的 Amazon 帳號，然後前往「Your Account」(您的帳戶)。
- 按一下「Change Account Settings」(變更帳號設定)。
- 往下捲到「Advanced Security Settings> Edit」(進階安全設定 > 編輯)，就會進入兩階段驗證的開始頁面。
- 按一下「Get Started 」(開始使用) 按鈕。您必須選擇接收代碼的方式：簡訊或驗證器程式 (該程式可用來直接產生代碼，手機沒訊號時也能使用)。
- 輸入您手機接收到的代碼 (透過簡訊或應用程式) 來完成設定。
- 按一下「Verify code and continue」(確認代碼並繼續)。
- 設定完成之後，Amazon 會要求您提供備用電話號碼 (以防萬一您的主要電話無法使用)，或者下載驗證器應用程式到您的手機上，這樣就算手機沒訊號也能使用。

Instagram

- 開啟您的應用程式，然後到您個人檔案，選擇螢幕右上角的「...」(帳號設定選項)。
- 在「帳號」下方，點一下「雙重驗證」。
- 啟用「索取安全驗證碼」。
- 當您從新的裝置存取你的帳號時，您就會收到安全驗證碼，您必須輸入這個碼才能登入。

Apple ID

- 只有使用 iOS9 和 OS X El Capitan 或更新版本的 Apple 使用者才能使用雙重認證。
- 到蘋果選單當中選擇「系統偏好設定」。
- 按一下「iCloud」。
- 找到「帳號詳細資訊」，然後按一下「安全性」就會看到開啟雙重認證的選項。

Google

- 手機簡訊代碼
- 安全金鑰

手機簡訊代碼

- 請至 Google 的兩步驟驗證網頁，登入您的帳號。
- 點一下螢幕右上角的「**開始使用**」，然後照著指示進行。
- 選擇您要接收代碼的方式：簡訊或電話。

此外，您也可以安裝「Google Authenticator」(驗證器) 程式來取得驗證碼，就算沒有手機訊號也能使用。

安全金鑰

使用一個安全金鑰裝置插入電腦的 USB 連接埠來進行驗證。您的電腦必須使用 Google Chrome 40 或更新版本，您可使用任何符合「FIDO 通用第二要素」(U2F) 規格的金鑰裝置。

- 請至 Google 的新增安全金鑰網頁。
- 將您的安全金鑰裝置插入 USB 連接埠，然後按「註冊」。
- 視您的安全金鑰類型而定，請依步驟完成您的註冊。