永遠走在最前面
Always Ahead

防範社交工程
網路釣魚防範與假新聞識別

中華電信資訊技術分公司

中華電信
Chunghwa Telecom

大綱

- **網路釣魚分析與防範**
  - 釣魚網站、社交工程郵件
  - Line、Facebook社群詐騙
  - BEC變臉詐騙(商業電子郵件詐騙)
- **假新聞分析與防範**
  - 假新聞主要戰場與動機
  - 假新聞案例
  - 事實查核

社交工程演練通知

113 年度教育部電子郵件社交工程演練通知，請各位長官、同仁勿點選不明之電子郵件。

1. 依臺教資通字第1132700735 號辦理。
2. 演練對象：本校行政人員（含主管人員、約用人員、技工工友）。
3. 演練時程：**自本(113)年4 月至12 月止，期間辦理2 次演練**。
4. 社交工程演練郵件型態：以偽冒公務、個人或公司行號等名義，發送社交工程演練郵件給受測人員，郵件主題分為八卦、休閒、保健、財經、新奇、時事、模擬實際社交工程樣本等類型，郵件內容包含連結網址或附檔。
5. 特別提醒：
   A. 社交工程演練失敗教育部將來函要求本校提出改善方式與稽核成效。
   B. 本中心提供電子郵件安全設定重點，請確實完成設定將“郵件預覽”功能關閉；防範網路詐騙與電子信箱攻擊相關文件參閱網址: **https://net.nthu.edu.tw/netsys/security:social_engineering**。
   C. 本校公務電子郵件信箱請勿用於收取私人郵件，私人郵件惠請同仁以自身私人信箱收取，並落實電子郵件安全性設定。
   D. 勿開啟並立即刪除任何不明寄件人、主旨聳動或欲誘使點擊之可疑郵件。且因轉寄郵件與設定為垃圾郵件視同開啟行為，因此，切勿將可疑郵件轉寄至自身私人信箱或他人信箱。

收信軟體設定建議

https://net.nthu.edu.tw/netsys/security:email_setup

防止電子郵件社交工程攻擊 收信軟體設定建議

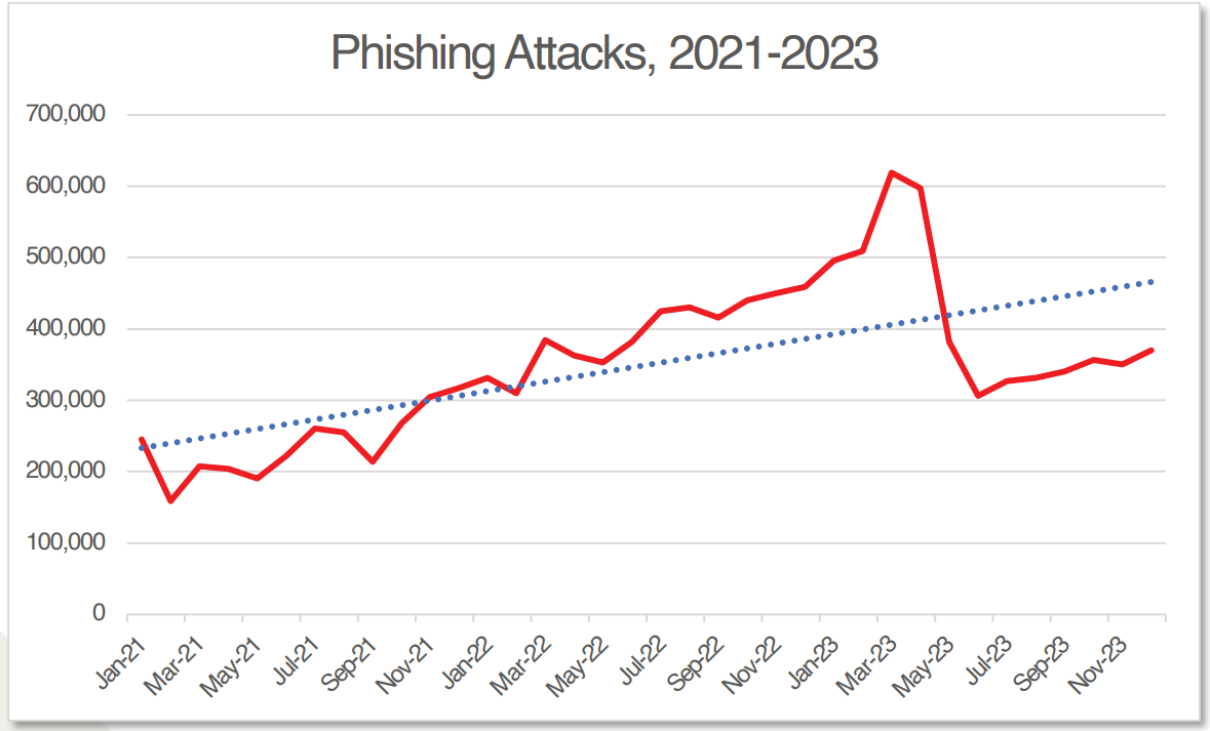
電子郵件社交工程攻擊常利用好奇心、興趣來吸引使用者開啟信件，為避免不小心或是誤開啟此類信件，而被植入惡意或後門程式，**為讓自己的電腦遠離危險，須調整自己的收信軟體設定，以增加安全性，「不自動下載圖片」、「不開啟預覽視窗」、「以純文字開啟信件」，可有效避免電子郵件社交工程型的攻擊**，常見收信軟體之設定建議如下：

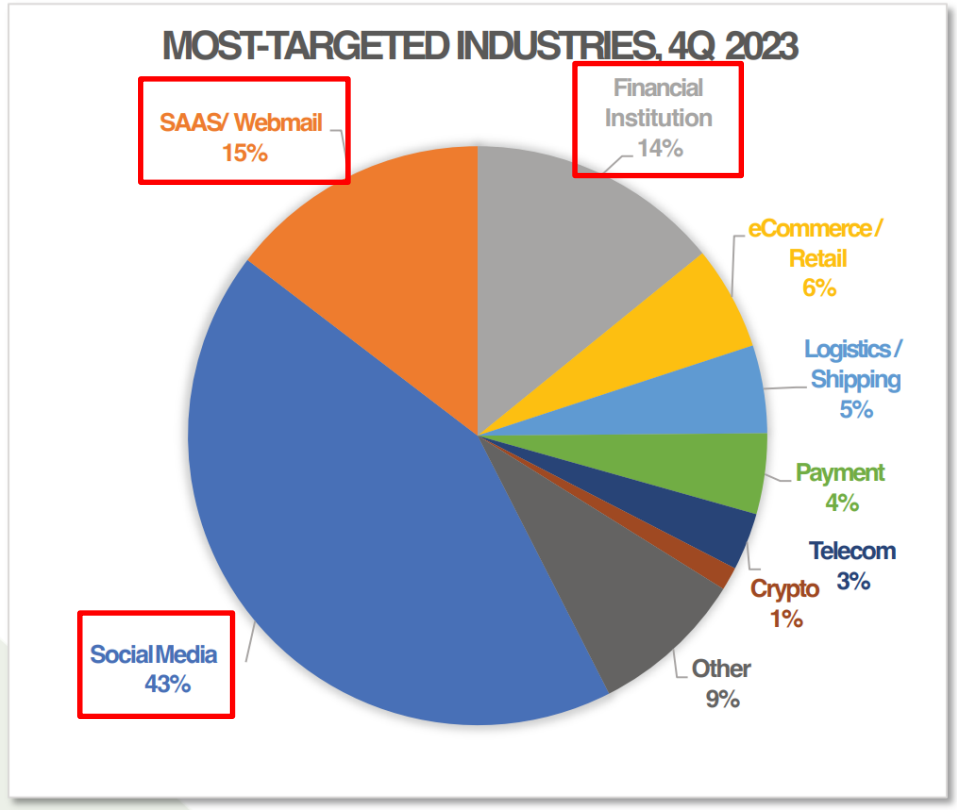
- **Apple iOS** NEW
- **Android Gmail app** NEW
- Outlook 2007
- Outlook Express
- Live mail

參考資料：

- 98年08月12日防範惡意電子郵件社交工程教育訓練 PDF 投影片
- 教育部98上半年度電子郵件社交工程演練結果說明

釣魚網站趨勢統計





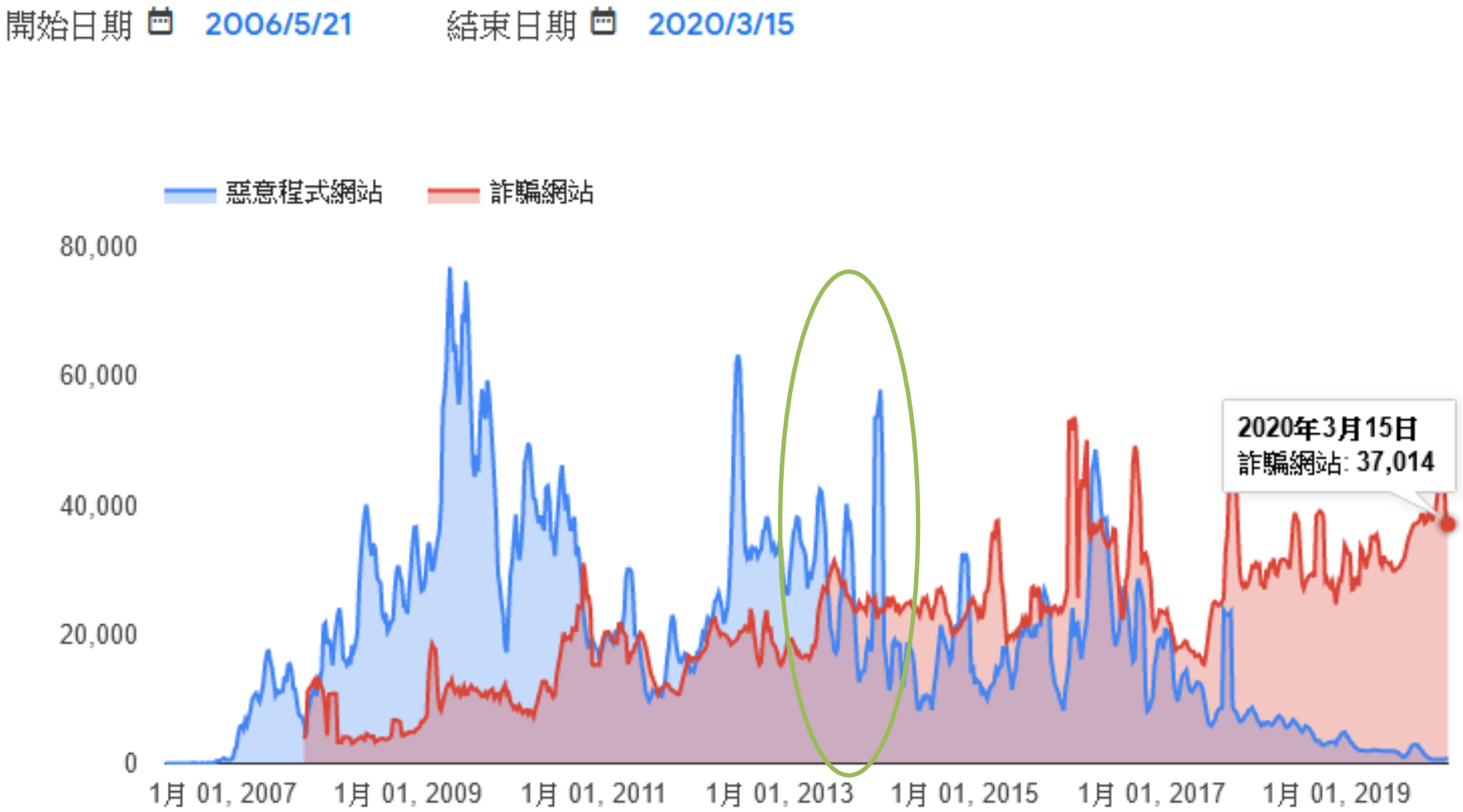
釣魚攻擊數量持續增長，2023 Q4共有**1,077,501次**
2023年釣魚攻擊達史上新高，次數接近**5百萬次**

針對**社群網站**的網路釣魚數量為最大宗，其次為**SaaS及網路郵件**、**金融業**，共佔所有網路釣魚攻擊**72%**

中華電信 Chunghwa Telecom

Ref: APWG Q4 2023 Phishing Activity Trends Report

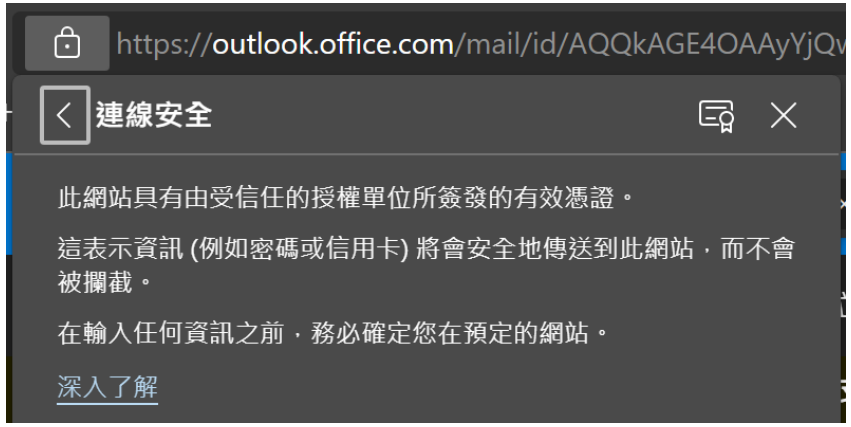
釣魚網站與惡意程式網站黃金交叉

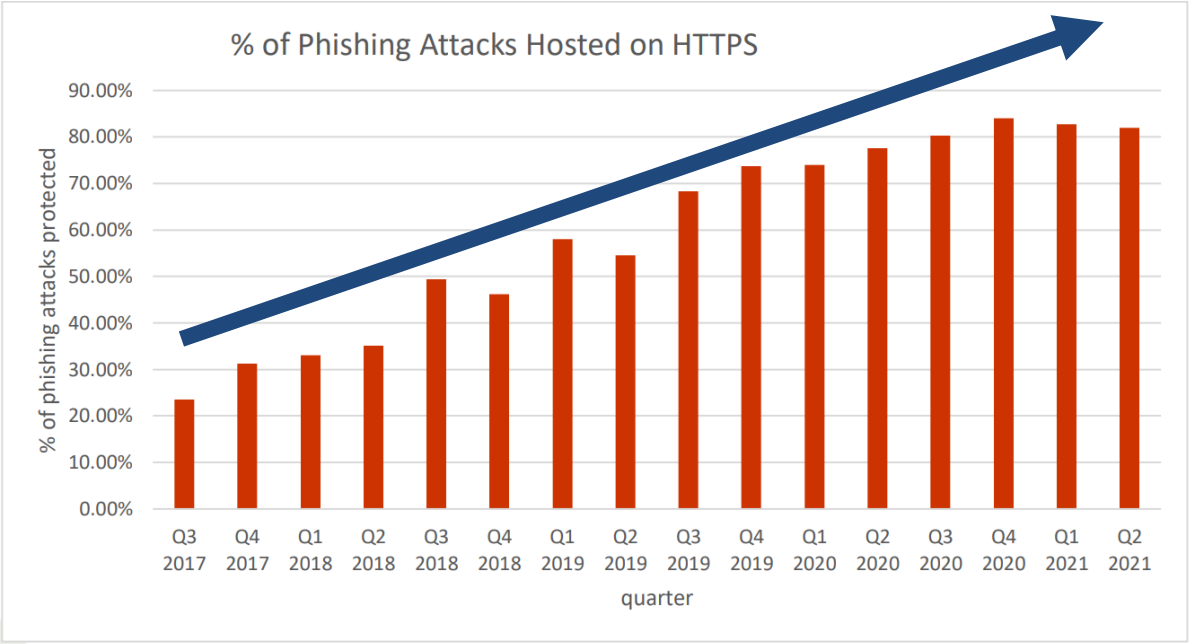


Ref: https://transparencyreport.google.com/safe-browsing/overview

釣魚網站也搭上HTTPS的熱潮

- HTTPS用於通過加密使用者的瀏覽器與其所訪問的網站的數據資料來保護通訊內容
- HTTPS在提供電子商務、購物網站或受密碼保護的帳戶的網站上尤為重要
  - **網站使用HTTPS更能使消費者安心**
- 2017年初，有使用HTTPS的釣魚網站僅約10%
- 但是，到2020年的Q3時已經有超過**80%的釣魚網站都有加上HTTPS和SSL憑證!**



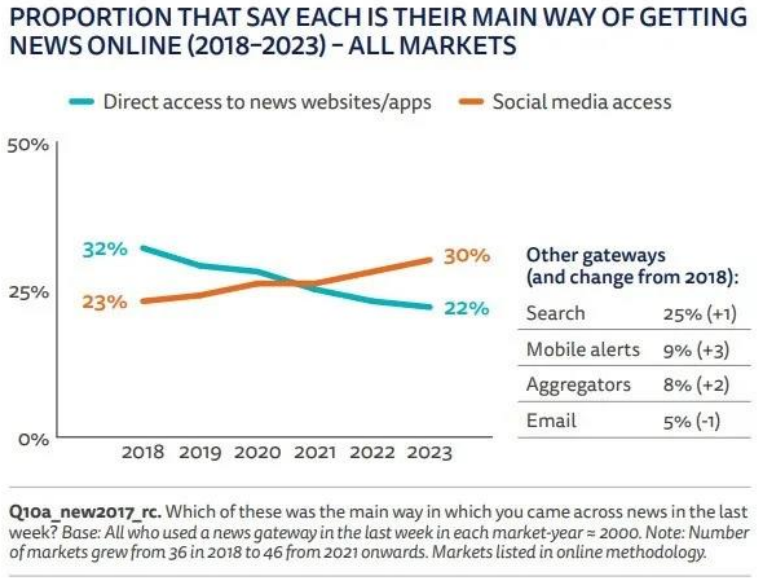


Ref: APWG Q2 2021 Phishing Activity Trends Report [p. 9]

假新聞撲朔迷離，真假難辨

- 台灣網路資訊中心(TWNIC) (2023年台灣網路報告)
  1. 台灣民眾查證新聞真假的能力有信心者占40.94% < 沒有信心者48.3%
  2. 差距拉大，代表民眾對自己查證新聞真假能力信心下降
  3. 有69.55%社群媒體使用者同意「社群媒體上的訊息不太可信」的敘述
  4. 有47.07%社群媒體使用者表示從未在平台上見過不實訊息的警示機制
  5. 有20.17%民眾在網路上接觸到假新聞、假訊息、不實訊息時，願意主動採取更正行為

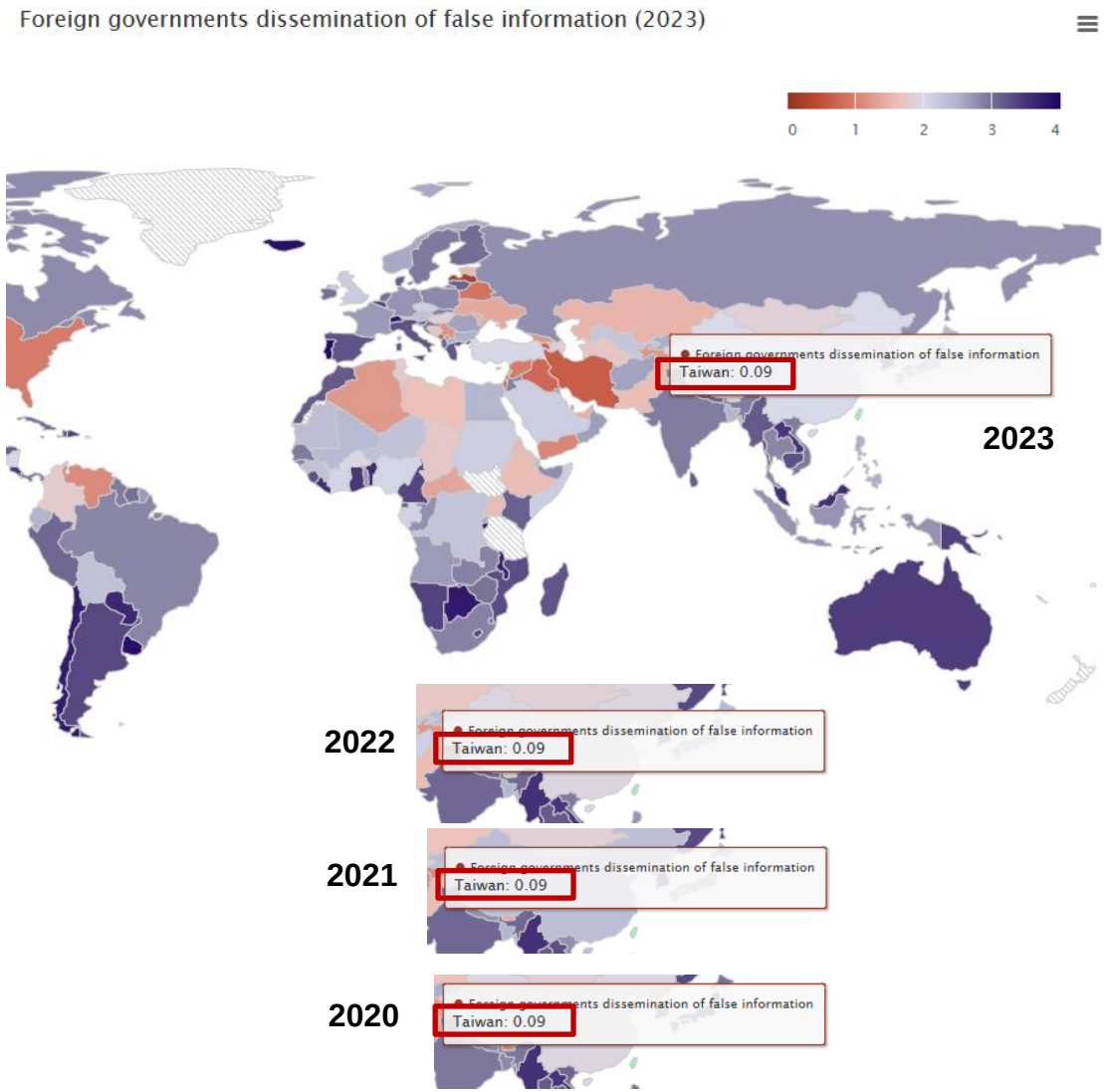
- 牛津大學路透新聞學研究所 (2023數位新聞產業報告)
  1. 傾向從新聞網站/App取得新聞資訊僅有22%
  2. 使用社群媒體取得新聞資訊的受訪者升至30%
  3. 擔憂網路假新聞的人有56%



Ref:
1. https://report.twnic.tw/2023/
2. https://tw.stock.yahoo.com/news/%E8%B7%AF%E9%80%8F-2023-%E6%95%B8%E4%BD%8D%E6%96%B0%E8%81%9E%E5%A0%B1%E5%91%8A-%E9%87%8D%E9%BB%9E%E6%91%98%E9%8C%84-facebook-014500002.html

臺灣連續多年受境外假消息影響程度最重

- 據Varieties of Democracy的資料，臺灣自2013年來，受到外國假消息散播的情形就已是全球第一，且日趨嚴重
- 該機構對全球各國遭受外國假消息散播(Foreign Dissemination of False Information)的程度做調查
  - 評分介於0-4分，0分最嚴重，4分最輕微
  - 台灣：**僅有0.09分，為全球最低**
  - 其他國家：美1.16、中1.93、德1.97、英2.06、日2.97、澳3.41
- 此現象顯示即使在民主自由、網路發達的時代，思想、言論仍然會被操弄
  - 事實查證、思辨能力很重要！



https://www.v-dem.net/data_analysis/MapGraph/

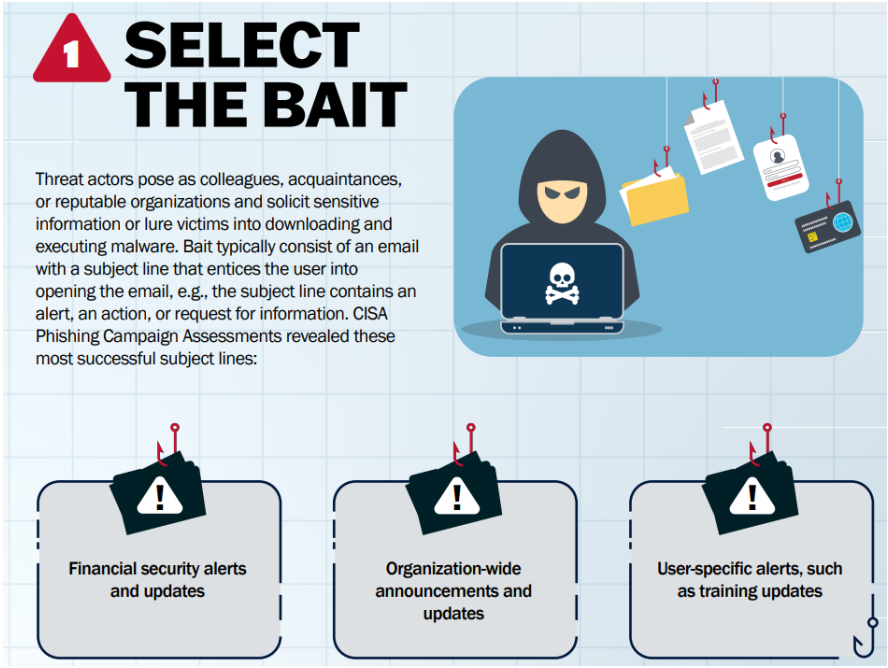
Ref. iThome, V-Dem

網路釣魚(Phishing) - 釣魚網站、社交工程郵件

中華電信 Chunghwa Telecom

什麼是網路釣魚?! (1/2)

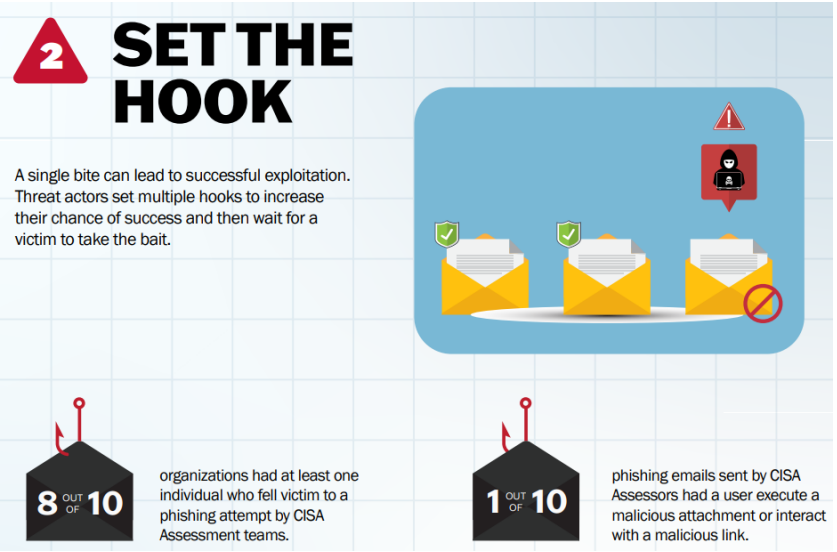
- 網路釣魚是一種**社交工程(Social Engineering)**的手法
- 冒充**信賴的同事與組織**，企圖引誘受害者上當
- 常將用戶導引至**URL與介面外觀與真正網站幾無二致的假冒網站**輸入個人資料
- 可利用的**管道多元**，包含電子郵件、通訊軟體或SMS簡訊，以及電話等
- 攻擊者常使用的題材
  - 財務相關安全通知與最新消息
  - 全公司公告與最新消息
  - 針對受害人的通知，例如員工訓練消息

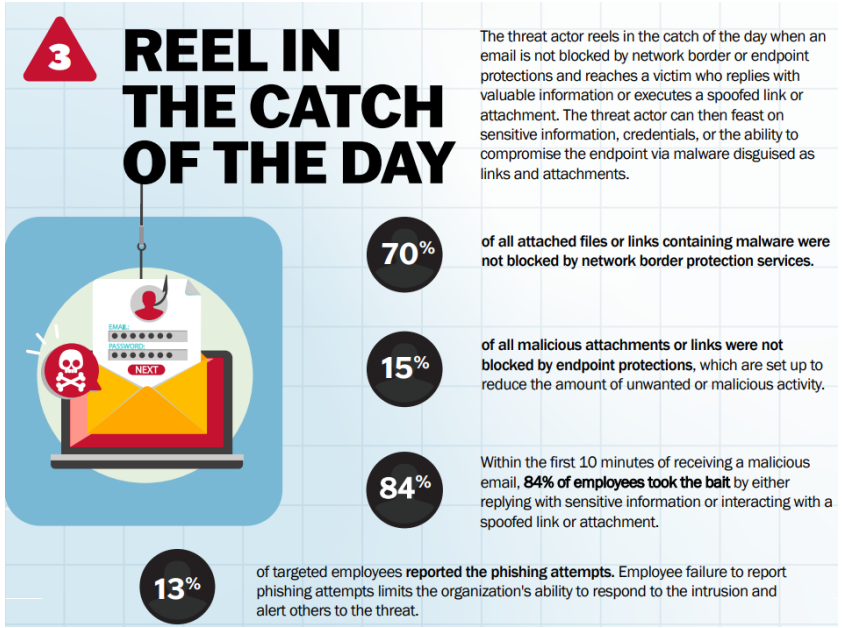


Ref: https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf

什麼是網路釣魚?! (2/2)

- 2023/2美國CISA Phishing Infographic報告
  - 每10個接受模擬網釣測試人員，就有**1人**點擊連結或下載附件
  - 每10間企業組織就有**8間至少有1人**淪為模擬網釣測試的受害者
  - 有**70%**的惡意程式或惡意連結未被網路邊界防護服務阻擋
  - 有**15%**的惡意程式未被端點防護產品阻擋
  - 有**84%**的員工在收到惡意郵件的前10分鐘內，就逕自回覆敏感資訊或是點擊連結與附件
  - 僅**13%**的目標鎖定員工回報自己遭遇網路釣魚事件





Ref: https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf

反網路釣魚工作小組(APWG)

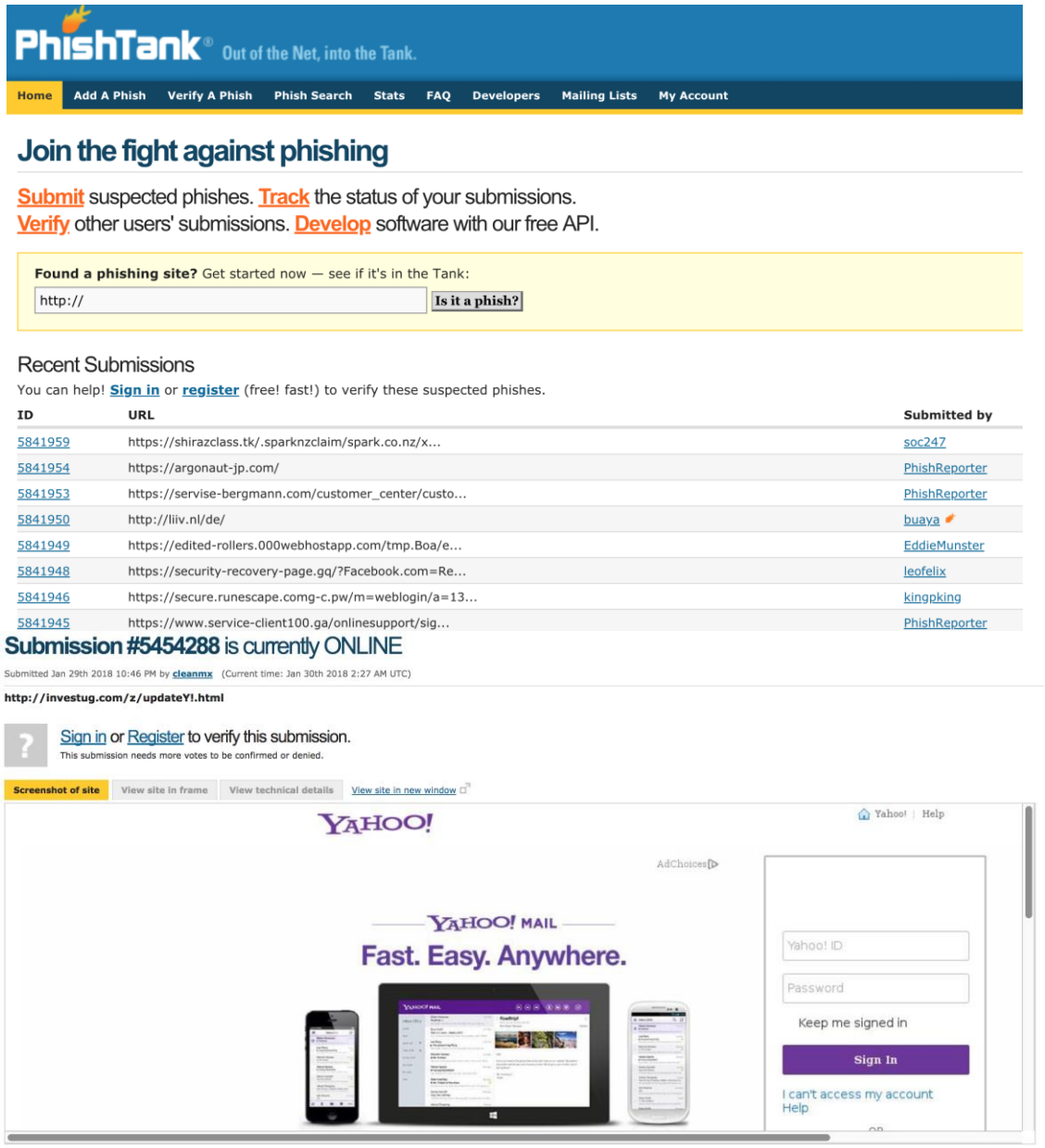
- https://apwg.org/
- 反網路釣魚工作小組（APWG）是一個國際聯盟，匯集了受網路釣魚攻擊影響的企業，安全產品和服務公司，執法機構，政府機構，行業協會，區域性國際條約組織和通信公司
- 專注於**詐騙電子郵件**、**釣魚網站**、**網址嫁接**和**電子犯罪**的研究與情資，近年也開始研究**加密貨幣**
- APWG由David Jevans於2003年創立，擁有來自全球1700多家公司和代理商的超過3200多名會員
  - 成員公司包括BitDefender，Symantec，McAfee，VeriSign，IronKey和Internet Identity等領先的資安公司
  - 金融業成員包括ING集團，VISA，萬事達卡和美國銀行家協會

已知釣魚網站清單

- http://www.phishtank.com/

PhishTank® Out of the Net, into the Tank.

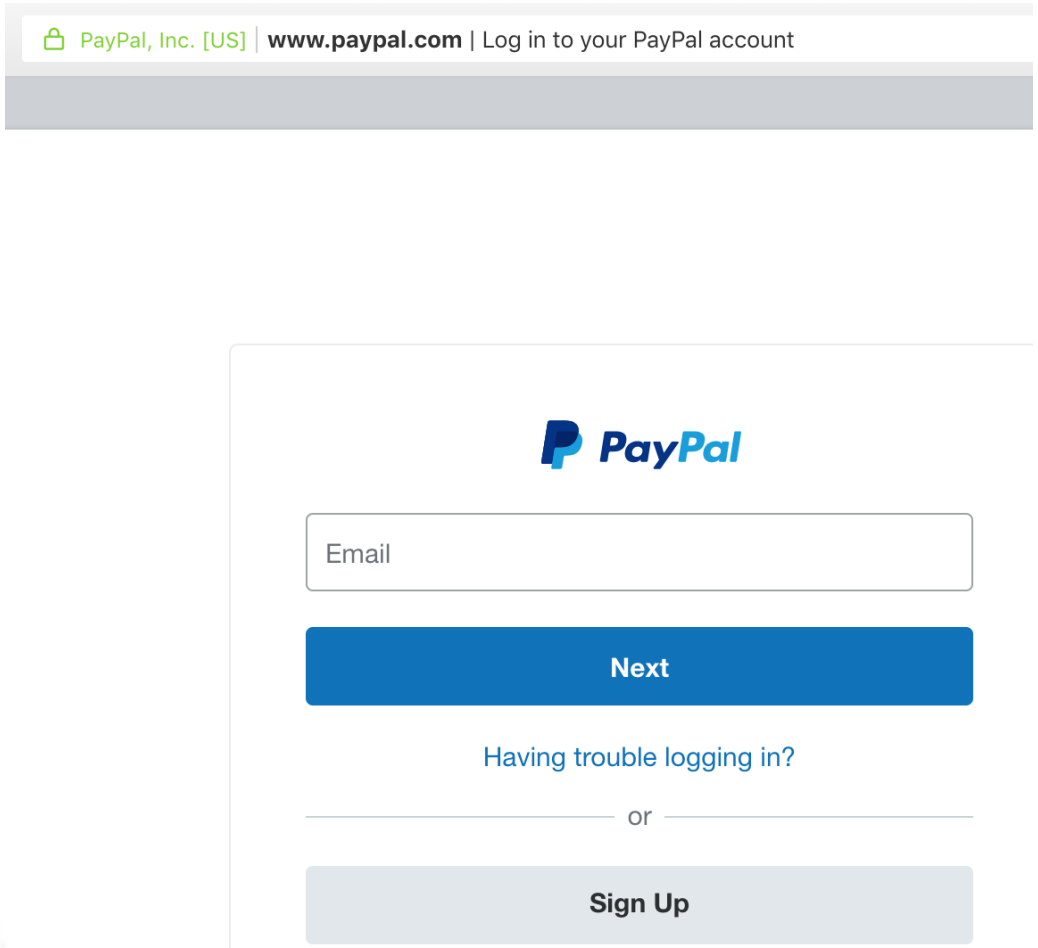
- PhishTank是基於社群的反釣魚攻擊服務
- PhishTank於2006年10月2日作為OpenDNS的子公司建立，用戶可以從世界各地向其匯報釣魚網站，經其他用戶以投票的形式認證後，即通過公開的API共享給所有使用PhishTank服務的機構和個人



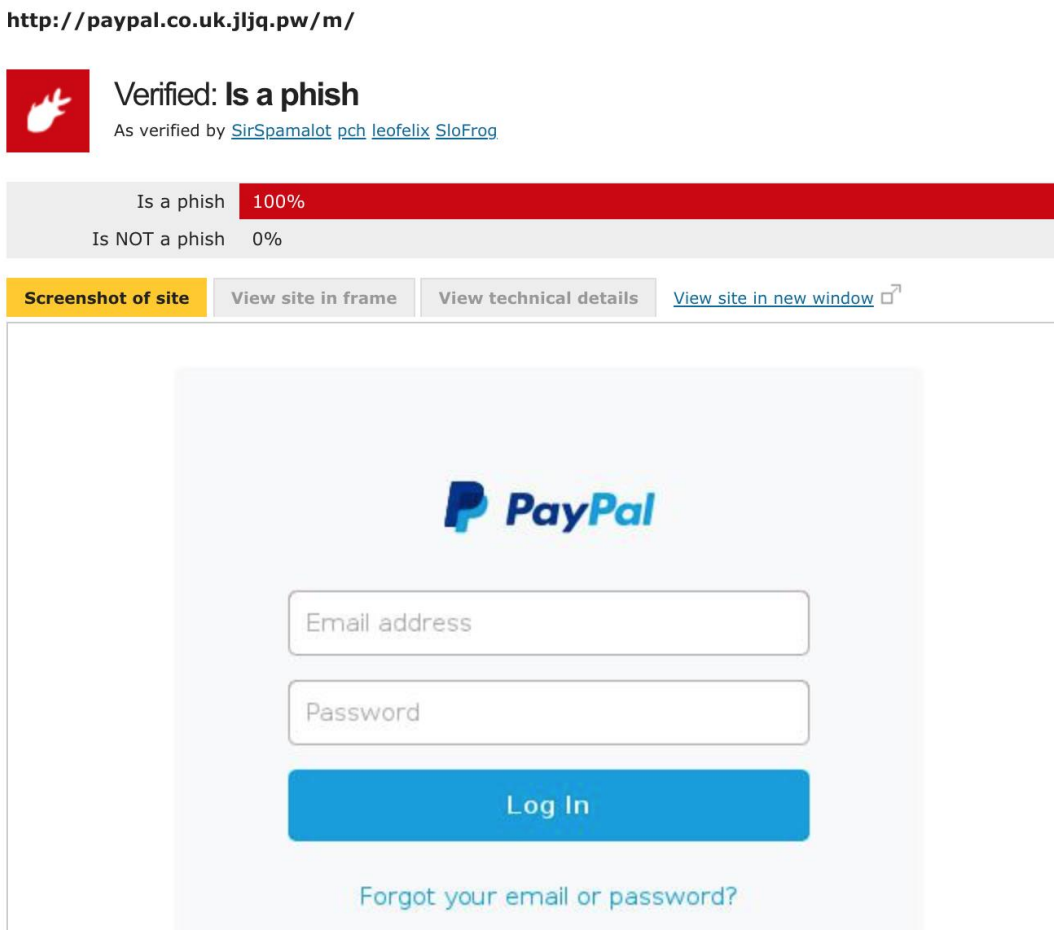
Ref: https://zh.wikipedia.org/wiki/PhishTank

★釣魚網站 (1/2) – 與真實網站相似

- 模仿官方網站的登入頁面，誘導使用者輸入帳號密碼



正確的網站



釣魚網站

釣魚網站 (2/2) – 單頁式網站

一頁式廣告詐騙 今年已逾千人受害

2023/09/16 05:30

〔記者邱俊福／台北報導〕刑事警察局統計，網拍一頁式廣告詐欺案件，去年受理六二一件，財損四百多萬元，今年一至八月，已受理達一一六七件，財損高達一千五百多萬元，有明顯倍增的趨勢。刑事局提醒，詐騙集團利用這類連鎖速食餐廳一頁式詐欺廣告結合釣魚網站，以騙取民眾輸登個人信用卡資料假連結，遂行盜刷行騙，因此民眾網購時應提高警覺，勿擊點不明網址，避免受騙造成財損。

財損一千五百多萬 有增溫趨勢

刑事局表示，網拍一頁式廣告詐欺，通常是詐團於臉書、Line及各大網路平台購買廣告版面，假冒明星專家代言加持、截取正版廠商圖片或竄改新聞報導圖片等，以低於市場行情價格促銷，吸引民眾透過廣告連結至購物網頁，再以「貨到付款」廣告字眼取信民眾，當民眾收貨付款後才發現商品和廣告不符，或商品品質低劣、有明顯瑕疵，這時才發現遭到詐騙。

這類詐騙具有的特徵，包括網頁沒有公司地址、客服電話，僅留下電子信箱或通訊軟體帳號；售價明顯低於市場行情，常以限時或倒數方式吸引消費者；號稱免運費、七天鑑賞期、可拆箱驗貨、不滿意包退；廣告底下留言都是正評，沒有負評；僅能使用「貨到付款」或信用卡刷卡付款；網頁大多粗糙不精美或夾雜簡體字等等。

刑事局呼籲，民眾如果有網路購物需求，應選擇具第三方支付功能且商譽良好的正規網購平台，並使用平台提供的安全交易機制，不要跟賣家透過通訊軟體私下交易，更不要擊點不明連結。

Ref:
https://news.ltn.com.tw/news/society/paper/1605045
https://www.ettoday.net/news/20230915/2582982.htm

烏克蘭商人單頁詐騙

社會

2022.03.24 11:54 臺北時間

自稱在烏克蘭老闆「賣完音響才能回台」　遭打臉詐騙中國腔全露餡

文 | 陳凱俊

網路上驚見有自稱是在烏台灣老闆的求助文，遭打臉擺係假。（翻攝自臉書）

↑ ↑ ↑
除了音響以外
還有其他產品

烏克蘭遭俄羅斯入侵今（24日）滿一個月，戰爭開打以來不少外國僑民紛紛撤離當地以求自保，但卻也發生有「吃人血饅頭」的情況，有不肖份子自稱人在烏克蘭，對外求助金援，其實全是騙局一場。事實查核中心近日查證指出，有一個自稱是「在烏台灣老闆的求助」，請大家幫忙購買其所販售的音響，好讓他能趕快賣完回台灣，然而其內容疑點重重，根本就是常見的「一頁式詐騙」手法。

近日在社群平台流傳一則廣告連結，文案中宣稱自己是台灣人，在烏克蘭經營音響店，但因為戰爭導致店鋪被毀損、無法營業，音響賣不出去，希望大家幫忙購買，「賣完就連夜回台灣！」

該網站打出悲情牌，希望引起眾人同情，更表示「原價近萬的哈曼卡頓音响！原裝未拆、質量保證」「哈曼卡頓音箱烏克蘭直郵」等語，試圖以低價為號召吸引消費者。但就有網友發現，他的內文和一般台灣人習慣用語不同，反倒像是中國用法，例如「質量保證」「直郵」等，更不用說把音響寫作「音响」等情況，引發部分網友質疑。未料「老闆」留言掛保證：「那肯定是真的，我拿命給你發的，你還懷疑我。」這句語氣反而更讓人覺得可疑。

台灣事實查核中心昨（23日）公開調查結果，指出該網站所呈現的音響倉庫照片可已在多家中國店家網站找到，至少2018年起就流傳在網路上，可確認所謂的倉庫照不是近期照片。

Ref: https://www.mirrormedia.mg/story/20220324edi026/

★ 單頁式網站詐騙特徵

NT$849 ~~NT$4699~~ 限時優惠 免運費 貨到付款

價格遠低於市價

【Apple官方】日本大丸百貨心齋橋店重修開幕 AirPods無線藍牙耳機2組1699，日本原裝正品，限時3天

七天鑒賞期

永遠倒數不完的時間

8時29分30秒

已搶購 81 件 98%

【爆款特賣】【Apple官方】日本大丸百貨心齋橋店重修開幕 AirPods無線藍牙耳機2組1699，日本原裝正品，限時3天

商品介紹 | 商品參數 | 評價 (63)

Apple日本大丸百貨心齋橋店6月重新裝修隆重開幕

新店開業 低至一折

限量99件藍牙

AirPods 無線

7天鑒賞 貨到付款

但卻沒有公司地址和客服電話

2.退換貨流程:

確認收貨—申請退換貨—客服審核通過—用戶寄回商品—倉庫簽收驗貨—退換貨審核—退款/換貨；

退換貨請註明：訂單號、姓名、電話。

·如何取消訂單

取消訂單需要向售後服務中心發送郵件並註明相關原因，郵件內容應註明您的訂單號、姓名、電話。

最新評價

匿名用戶 滿意度：★★★★★

掛在耳上運動也沒有掉，比想象中好很多啦，打折果然很便宜

虛假的評論

匿名用戶 滿意度：★★★★★

打折很便宜啦，就是客服會不會太忙，很久才回我

匿名用戶 滿意度：★★★★★

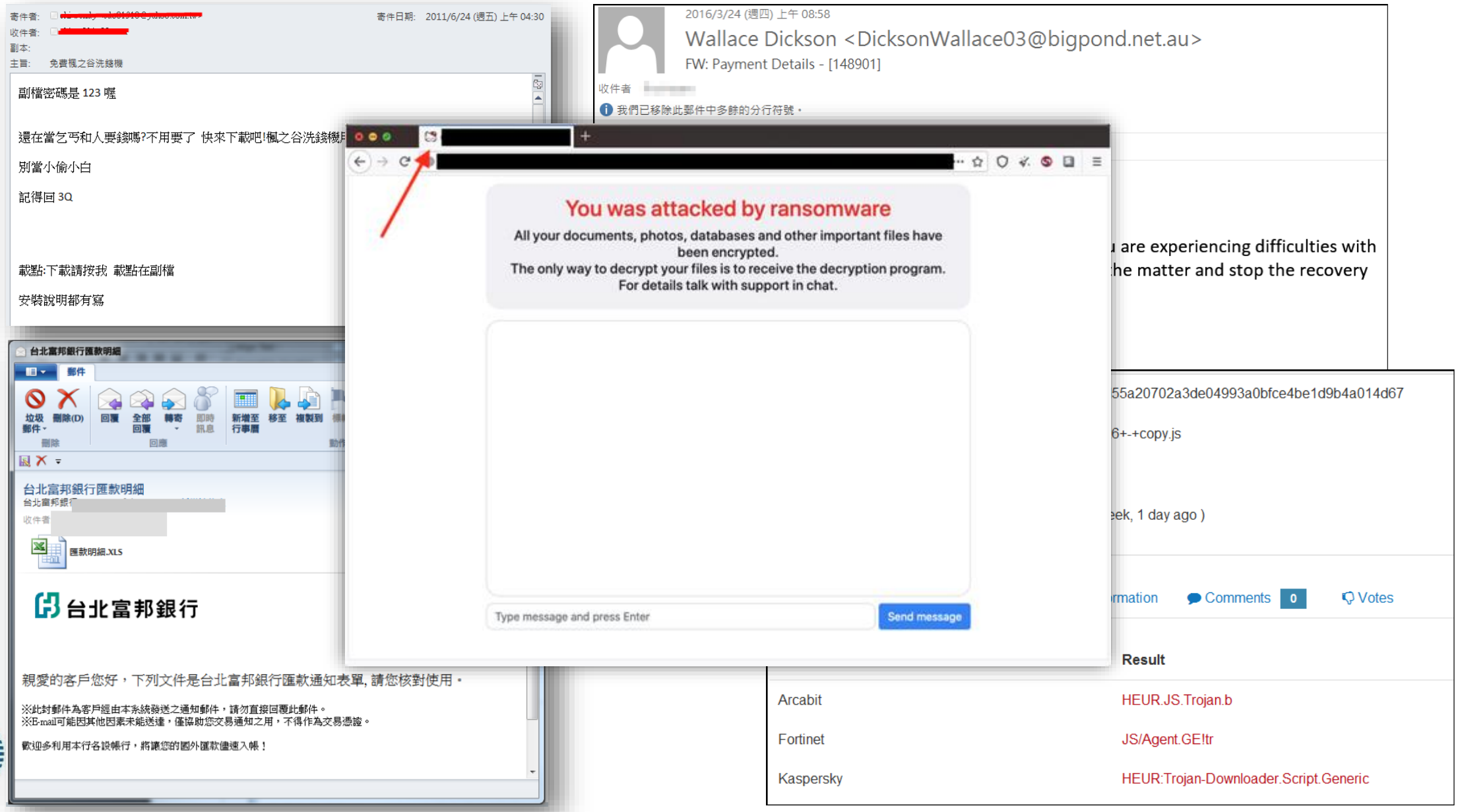
便宜就敗咯，正品無疑，跟我的智慧型手機連上沒有問題

匿名用戶 滿意度：★★★★★

還是日貨好用，原價太貴，竟然被我搶到了，很便宜

我要評價

避免點擊可疑社交工程郵件比以往重要



個資外洩時會發生什麼事

當你個資外洩時會發生什麼事？

2020 年 10 月 14 日　Trend Labs 趨勢科技全球技術支援與研發中心　資料外洩/個資外洩

> 當您的姓名、出生年月日、照片、聯絡方式、信用卡號、銀行帳戶資料，以及用於各種網路服務認證上的帳號與密碼在網路上外洩，會發生什麼事呢？

如果這些資訊落到惡意的第三方手中，可能會發生隱私受到侵害、財物損失、被他人假冒、被跟蹤或脅迫等情況。因此，我們必須在平時就小心運用及管理自己和家人朋友的個人資料。

BBC 報導指出一個叫做「Maktub」的勒索病毒 在 2016 年大量散發網路釣魚郵件,警告收件人積欠某企業機構數百英鎊，要求他們點郵件中的連結列印發票，而這個連結會讓電腦感染勒索軟體。有些網路釣魚郵件還冒名專門輔導更生人或監獄受刑人的慈善機構。值得注意的一點是，網路釣魚（Phishing）郵件內容當中不僅寫出了收件人的姓名，還附上了受害人的地址。包含 BBC 的工作人員在內，都發現這些地址的正確性頗高。據推測這些資料很可能來自一些外洩事件中失竊的資料庫。

犯罪分子可能會拿你的個資做的八件事

一旦你的個人身份資訊（PII）被盜，通常會在暗網上賣給那些會將其用於惡意用途的人。它可以被用來：

1. 破解其他使用相同帳密的帳號（透過憑據填充）。2018年有300億次這樣的攻擊。
2. 登入你的網路銀行帳號來取走資金。
3. 以你的名義辦理銀行帳號/信用貸款（這可能會影響你的信用評等）。
4. 以你的名義訂手機或將你的SIM卡轉到新裝置（每月影響7,000名美國行動網路運營商Verizon客戶）。
5. 以你的名義購買昂貴物品（如新手錶或電視機）用於犯罪轉賣。這通常是透過劫持你在電子零售商的網路帳號進行。據說電子商務詐騙每年大約造成約120億美元的損失。
6. 提交虛假的退稅單，以你的名義收取退稅。
   (美國曾發生駭客蒐集民眾個資騙過了稅單申請服務的身份驗證程序，盜領退稅恐達15億的事件)
7. 利用你的保險詳細資料進行醫療服務。
8. 可能會入侵工作帳號來攻擊你的雇主。

七個造成資料外洩的原因

我們在日常生活中使用電腦或智慧型手機時，個人資料究竟是如何外洩出去的呢？我們一起來確認其主要外洩途徑和原因。

1.網路釣魚攻擊

盜取網路使用者個資的手法中，最具代表性的方式就是網路釣魚(Phishing)詐騙。舉例來說，其手法之一就是以釣魚郵件將使用者引導至偽裝成真實購物網站、銀行、信用卡公司或網路服務等之合法登入頁面的假網站（釣魚網站），藉以竊取使用者在該網站所輸入的個資。除了引導至釣魚網站外，其他還有各種形式的巧妙手法，例如誘導使用者安裝惡意應用程式或要求回覆釣魚郵件。

從你購物的網站偷偷收集信用卡資訊。因為新冠狀病毒(COVID-19,俗稱武漢肺炎)封城期間有更多使用者湧向電子商務網站，使得網頁卡號側錄相關的事件在三月增加了26%。

中華電信 Chunghwa Telecom

Ref: https://blog.trendmicro.com.tw/?p=63237

亞洲詐騙調查報告

亞洲防詐高峰會登場，最多臺灣人認為上當原因竟是「不確定詐騙但願意冒險」！ 面對真偽難辨AI詐騙，需從更多管道更多方式去確認

臺廠Gogolook與全球防詐聯盟合作舉辦首屆「亞洲防詐高峰會」，強調推動防詐與發展信任科技是挑戰也是機會，希望促進更多公私協力，並呼籲大家認清一件事：AI詐騙已是現在進行式

文/ 羅正漢 | 2023-11-29 發表

讚 94 分享

身為全球防詐聯盟GASA創始會員的Gogolook，該公司執行長郭建甫，也與Jorij Abraham同臺，共同揭露《亞洲詐騙調查報告》，分析他們觀察到的詐騙態勢。

這些年來，詐騙事件屢見不鮮，幾乎每天的新聞都會報導，但到底有多氾濫？在這次揭露內容中，有幾項數據我們認為需要特別重視。

郭建甫指出，亞洲地區有超過6成民眾表示，每週至少會接觸到一次詐騙事件，並且有超過15%的人每天遭遇詐騙，而在臺灣，有4成民眾每週都會遭遇數次詐騙。

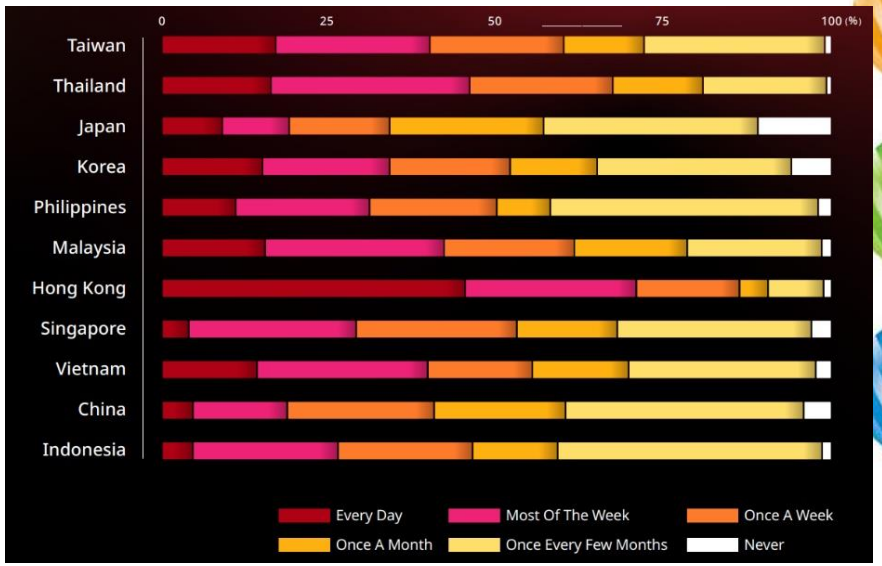
在這樣的「詐騙新常態」之下，我們認為，民眾更需要確認各種資訊，才能彼此信任。

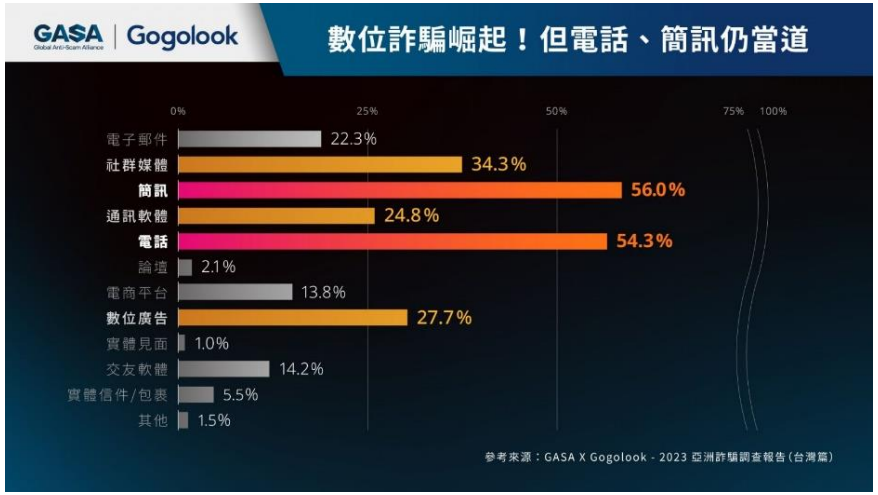
GASA還提到另一個更令人憂心的數據，Jorij Abraham指出，全球只有4成受害者回報自身的詐騙經歷，但是，有機會將損失金錢要回的人僅有4%。

至於哪些國家遭受詐騙金錢損失最多？肯亞居首，其次為巴西、南非、阿根廷、馬來西亞、中國、印尼。

身分冒用最常見，臺灣「帳單繳款詐騙」高於亞洲各國

關於詐騙方利用的途徑，遍及電話、簡訊、即時通訊、社群平臺、電子郵件，以及數位廣告。電話、簡訊的詐騙是最嚴重的管道，而在即時通訊與社群平臺方面，主要是各國最受歡迎的應用為主，如臺灣、泰國，大多數詐騙都是使用Facebook、Line，而在馬來西亞、香港、新加坡，詐騙的首選平臺是WhatsApp、Facebook。





Ref: https://www.ithome.com.tw/news/160062

品牌網路釣魚報告

首頁 > 雲端/資訊安全

Check Point《2023年第三季品牌網路釣魚報告》：AI加劇釣魚郵件辨別難度

ycr 發表於 2023年11月26日 11:00 | 收藏此文

讚 1

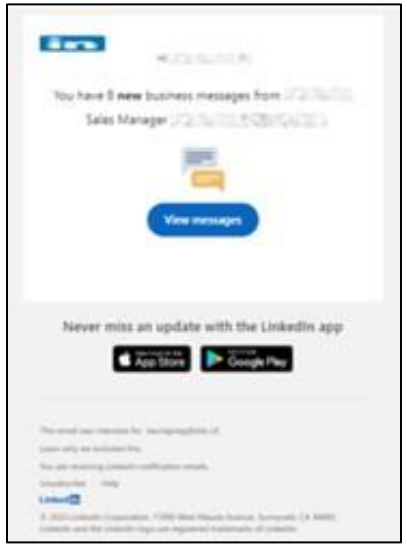
全球網路安全解決方案領導廠商 Check Point Software Technologies的威脅情報部門 Check Point Research 發佈了《2023 年第三季品牌網路釣魚報告》，羅列 2023 年第三季最常被用於網路釣魚攻擊的品牌。其中跨國零售巨頭沃爾瑪是最常遭冒充的品牌榜首（39%），其次為科技巨擘微軟（14%）、跨國金融服務商富國銀行則名列第三（8%）。

值得注意的是，全球第二大支付處理商萬事達卡首次進入前十大最常遭冒充品牌排行，位居第九。假冒亞馬遜的網路釣魚攻擊數量也居高不下，這與該公司的秋季大型促銷活動— 訂於 10 月第二周的「Prime 會員大促」— 密切相關。

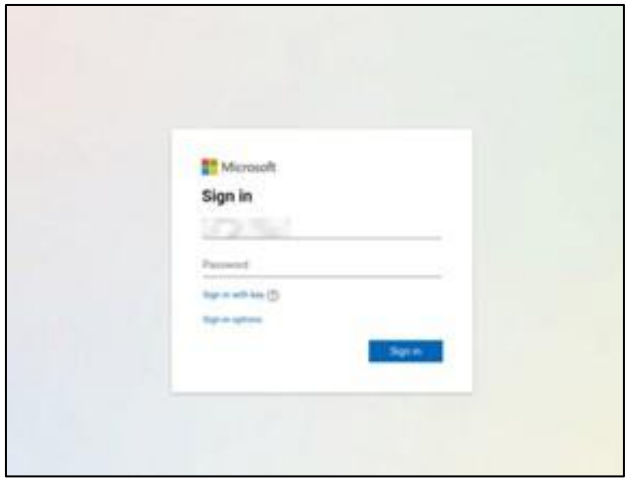
Check Point Software 數據研究經理 Omer Dembinsky 表示：「網路釣魚仍是最常見的攻擊手法之一，許多零售、科技和銀行業品牌都遭到假冒。人工智慧的廣泛應用增加了辨別合法和詐騙電子郵件難度，不過這也並非無計可施。在開啟來自知名公司的電子郵件時，必須保持警惕，且務必檢查寄件者的電子郵件地址和消息正確性，並經由安全網站交易，而非透過電子郵件中的連結。若企業察覺其品牌遭假冒，應透過經驗證的管道通知客戶，同時針對潛在威脅發出警告。」

在品牌網路釣魚攻擊中，犯罪分子會試圖使用與真實網站相似的網域名稱、URL 及網頁設計，來模仿知名品牌的官方網站。導向詐騙網頁的連結可透過電子郵件或簡訊發送給目標對象，並在瀏覽網頁期間被重新導向，也可能經由詐騙應用程式觸發；其中，詐騙網站通常會設計一個用於竊取用戶憑證、付款明細或其他個人資料的表單。

排名	品牌	出現率
1	沃爾瑪（Walmart）	39%
2	微軟（Microsoft）	14%
3	富國銀行（Wells Fargo）	8%
4	谷歌（Google）	4%
5	亞馬遜（Amazon）	4%
6	蘋果（Apple）	2%
7	家得寶（Home Depot）	2%
8	領英（LinkedIn）	2%
9	萬事達卡（MasterCard）	1%
10	網飛（Netflix）	1%



LinkedIn未讀訊息詐騙電郵



Amazon購物詐騙電郵

中華電信 Chunghwa Telecom

Ref: https://www.techbang.com/posts/111216

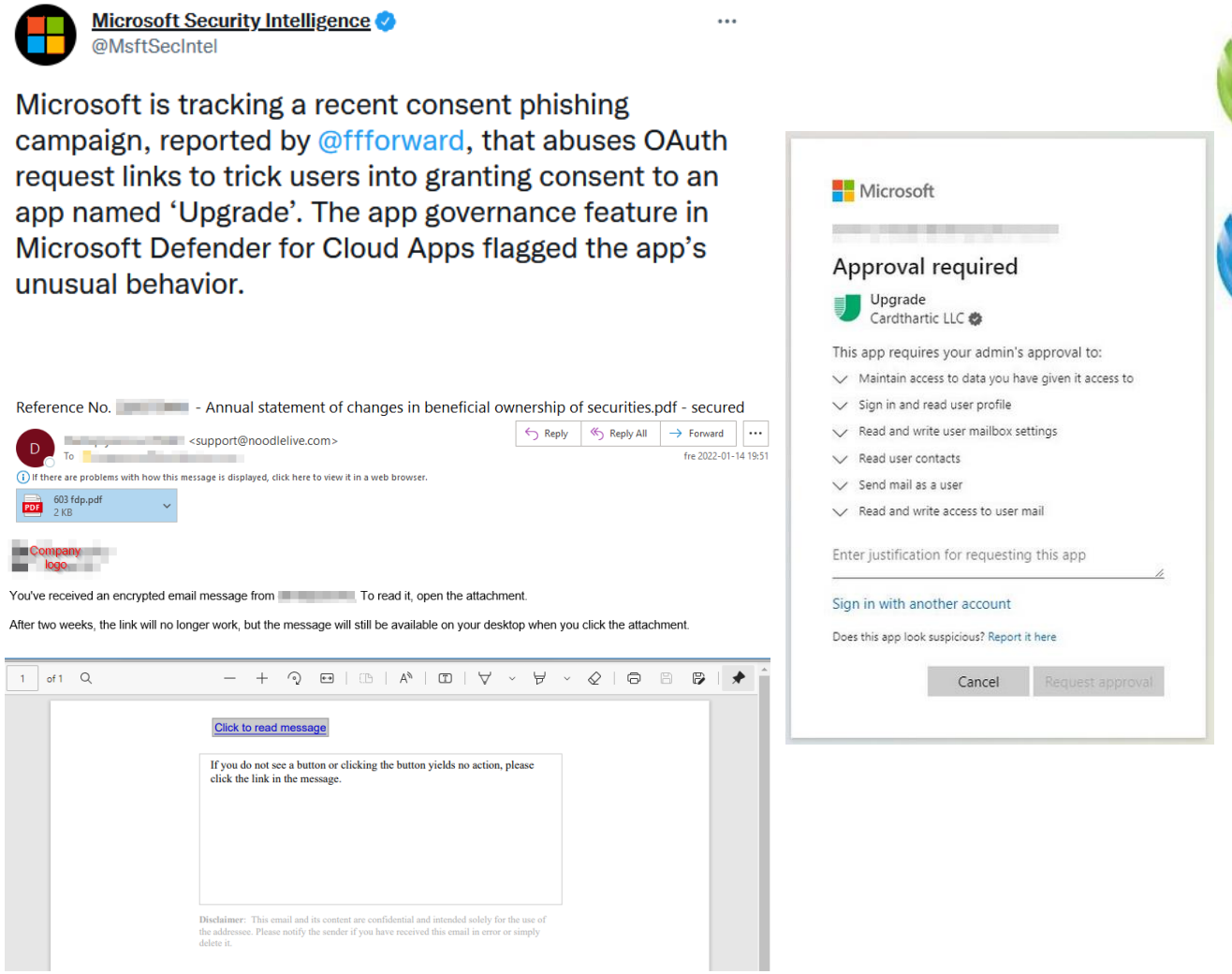
Microsoft 提醒 Office 365 用戶提防釣魚

嚴防 Office 365 網絡釣魚　Microsoft 向客戶發出警告

2022-01-29

Microsoft 日前在 Twitter 披露，一款名叫 Upgrade 的惡意程式正嚴重威脅 Microsoft 365 用戶的網絡安全，該惡意程式透過針對 Office 365 用戶的網絡釣魚電郵散播。Microsoft 表示電郵要求用戶開放 OAuth 權限，去新增收件箱規則、撰寫和閱讀電郵、新增日曆項目，同時要求讀取聯絡人資料的權限。

Microsoft 保安團隊提醒 Office 365 用戶小心網絡釣魚，指電郵哄騙用戶交出權限，不法份子藉此可以控制用戶的帳號，繼而進行其他惡意活動。這類網絡釣魚活動開宗明義向用戶要求取得權限，但用戶往往不清楚請求並非來自官方或合法的途徑，一旦用戶授權予不法份子，就有機會馬上或在未來被利用去攻擊其他網站。



Ref: https://unwire.hk/2022/01/29/microsoft-issues-office-365-phishing-warning/tech-secure/
@ffforward, @MsftSecIntel

假冒DHL包裹追蹤釣魚簡訊

MyGoPen

【詐騙】欠缺資料？假的DHL追蹤貨件包裹簡訊！騙信用卡釣魚網站，切勿輸入個資！

2022年2月14日 週一 下午3:31 · 2 分鐘 (閱讀時間)

當心山寨的 DHL 簡訊和詐騙假網站！最近民眾收到內容為「欠缺資料，我們無法運送您的包裹」的簡訊，並附上一個設計得一模一樣的追蹤貨件包裹網址連結。這是要誘騙你進去填信用卡卡號、驗證碼等資料，若不小心輸入的話信用卡恐遭盜刷！平常除了當心不明的簡訊連結外，務必一定要確認官方網址是否正確，更不要隨便填寫個資！

查證說明：

偽裝成 DHL 追蹤包裹網址的詐騙手法

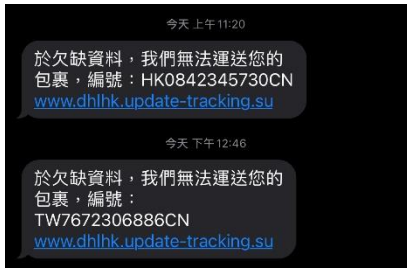
過去 MyGoPen 提醒宣導過冒用官方網站的案例，近期民眾回報收到假裝 DHL 官方通知的詐騙簡訊，該手法主要誘導你逐步輸入個人信用卡資訊與驗證碼，後續恐因此被盜刷信用卡而受害。

實際上 DHL 的正確追蹤與追查貨件的官方網站網址為：

https://www.dhl.com/tw-zh/home/tracking.html

這樣的手法主要透過簡訊中的連結誘騙點擊，民眾依此連到看似 DHL 的偽造國際快遞服務網站，接著根據要求輸入信用卡持有人姓名、卡號、有效日期以及安全碼等個資，說是來支付郵資安排遞送。

根據 MyGoPen 實際測試，除了是錯誤的網址之外，山寨網站多個站內連結也是無效的，且無法有其他的選擇項目，都會引導民眾到信用卡資訊填寫頁面。



Ref: https://www.mygopen.com/2022/02/dhl.html

花旗銀行客戶被網路釣魚攻擊鎖定

花旗銀行用戶被網釣攻擊鎖定

駭客鎖定花旗銀行（CitiBank）用戶，以帳號遭停權、詐騙損害賠償為主旨，吸引用戶連至釣魚網站輸入網銀帳密

文/ 林妍溱 | 2022-02-25 發表

讚 6.8萬 按讚加入iThome粉絲團 讚 60 分享

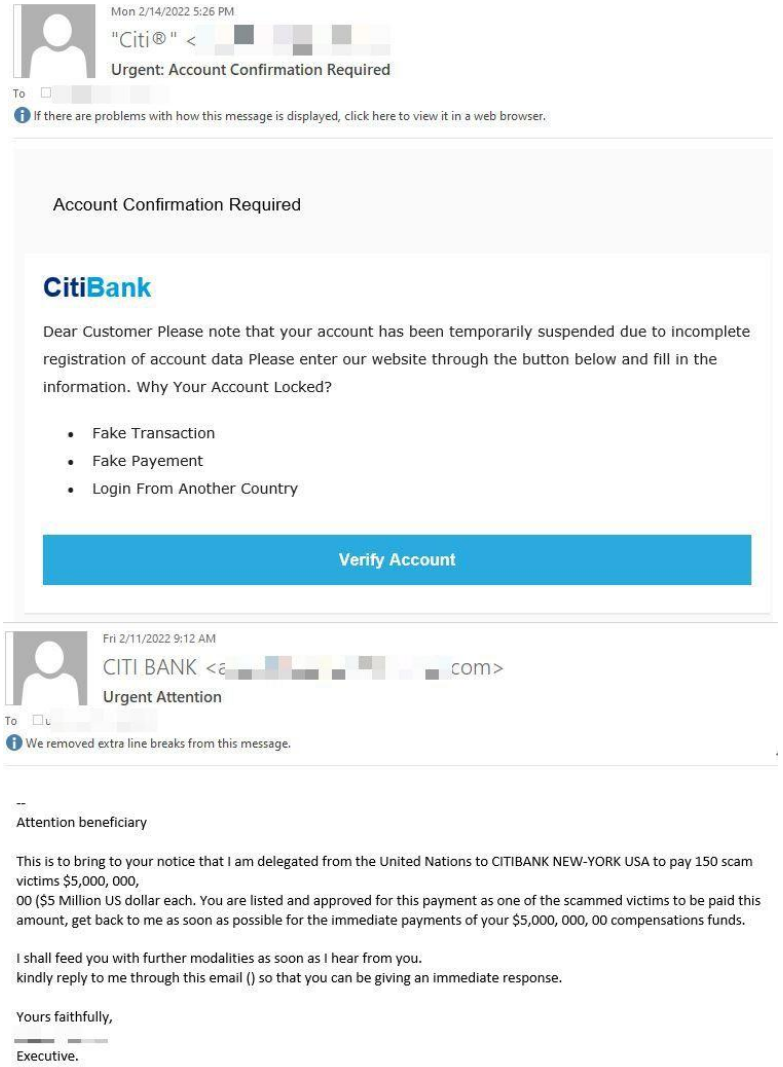
安全廠商Bitdefender警告近日一波釣魚郵件攻擊鎖定花旗銀行（CitiBank）用戶，以騙取網銀帳密等資訊。

針對花旗銀行用戶的攻擊是以以假亂真的信件，誘使用戶連到釣魚網站輸入帳密或其他個資。主要有2波攻擊。第一波發生於上周，駭客假冒寄自花旗財富管理窗口的帳號安全確認信件，信中包含花旗相同的官網圖示及版型設計，宣稱註冊不全或其他因素遭到停權，要求用戶經由信中所附連結前往花旗網站輸入帳號、密碼、電子郵件等資料以完成驗證。

第二波則類似樂透詐騙信，宣稱用戶被選中獲得聯合國財務賠償5百或千萬美元，將匯入花旗銀行帳戶，要求用戶輸入個資包括姓名、地址、年齡、電話及身份證相片以完成轉帳。這波釣魚信件40%來自美國，13%寄自墨西哥。以信件目的地來看，美國居絕大多數（81%）、英國和韓國（7%）居次，以及加拿大、愛爾蘭、印度及德國。

第二波攻擊發生在2月11日到15日間。安全公司分析，釣魚信件發出的IP位址以印度、挪威及荷蘭為主。釣魚信件目的地以美國佔最大宗，約34%，其次分別寄往丹麥、瑞典、英國、愛爾蘭及南非等地。

一如所有釣魚信件的防範方法，安全廠商呼籲用戶對宣稱銀行服務窗口主動發送的信件一概不予回應，且留心信件網域或信箱是否有不正常拼法等元素。



Mon 2/14/2022 5:26 PM
"Citi® " <
Urgent: Account Confirmation Required
To
If there are problems with how this message is displayed, click here to view it in a web browser.

Account Confirmation Required

CitiBank

Dear Customer Please note that your account has been temporarily suspended due to incomplete registration of account data Please enter our website through the button below and fill in the information. Why Your Account Locked?

- Fake Transaction
- Fake Payement
- Login From Another Country

Verify Account

Fri 2/11/2022 9:12 AM
CITI BANK <a com>
Urgent Attention
To
We removed extra line breaks from this message.

--
Attention beneficiary

This is to bring to your notice that I am delegated from the United Nations to CITIBANK NEW-YORK USA to pay 150 scam victims $5,000, 000,
00 ($5 Million US dollar each. You are listed and approved for this payment as one of the scammed victims to be paid this amount, get back to me as soon as possible for the immediate payments of your $5,000, 000, 00 compensations funds.

I shall feed you with further modalities as soon as I hear from you.
kindly reply to me through this email () so that you can be giving an immediate response.

Yours faithfully,

Executive.

Ref: https://www.ithome.com.tw/news/149558

Zendesk員工被駭致用戶個資外洩

Zendesk員工被駭致用戶個資外洩

駭客去年9~10月間以釣魚簡訊攻擊手法，取得雲端客服軟體業者Zendesk員工帳號存取憑證，Zendesk直到今年1月中旬，才私下通知客戶資料可能因此外洩

文/ 林妍溱 | 2023-01-30 發表

讚 17 分享

知名雲端客服軟體業者Zendesk兩周前通知客戶，數名員工遭到釣魚簡訊攻擊被竊取資料，導致客戶個資外洩。

Zendesk提供整合郵件、留言板、即時通訊的雲端客服平臺。該公司似乎未公告安全外洩事件，而是私下以郵件通知客戶。加密貨幣交易暨電子錢包平臺商Coinigy於兩周前（1/13）接獲Zendesk的通知後，決定在本月19日向其客戶公開此事。

根據Coinigy張貼的Zendesk客戶通知信件，Zendesk 2022年10月25日遭到鎖定該公司員工的進階簡訊釣魚攻擊，「少數」員工的帳號存取憑證遭駭入一段時間，使其紀錄平臺2022年9月25日到10月26日的非結構資料被非授權存取。Zendesk說該公司一發現此事即立刻解決，並聯絡外部鑑識廠商檢視後果。根據截至今年1月12日的調查，Zendesk判斷外洩的資料包含屬於客戶的服務資料。

但Zendesk表示，通知信件是示警作用，目前沒有證據顯示其客戶的Zendesk執行個體遭到存取。Zendesk也沒有說明可能受影響的資料型態。

Zendesk表示已經採取的行動包括：封鎖發現的釣魚信件網域、關閉受影響的帳號、並聯絡其他單位關閉該惡意網域、聯絡FBI及調查所有受影響資料。此外Zendesk也建議用戶留意其網域的可疑或非授權活動。

這是這家雲端CRM業者近年第二次通知客戶資料外洩。2016年Zendesk也曾遭駭，致其Zendesk線上支援及聊天服務近萬家企業客戶個資，包括電子郵件、姓名、電話等遭存取，但Zendesk直到2019年才發現並通知客戶。

zendesk

This ticket (#11140787) has been created on your behalf.

Lisa Core (Zendesk Support)
Jan 13, 2023, 8:51 PM CST

Hello,

We are writing to provide you with information about a security incident that recently impacted your account.**What happened?**On October 25, 2022, Zendesk became aware of a sophisticated SMS phishing campaign targeting several Zendesk employees. A limited number of those employees' account credentials were temporarily compromised, and unstructured data from a logging platform from September 25, 2022 to October 26, 2022 was accessed. The last identified instance of unauthorized access activity occurred on October 26, 2022.Upon learning of this incident, Zendesk promptly

Ref: https://www.ithome.com.tw/news/155283

Coinbase員工密碼被竊致駭客存取系統

Coinbase員工密碼被竊致駭客存取系統

今年2月間有駭客針對Coinbase員工發動釣魚簡訊攻擊，甚至假冒公司IT來電而成功取得Coinbase部份員工聯絡資訊，但Coinbase強調客戶資料或加密資產未受影響

文/ 林妍溱 | 2023-02-22 發表

讚 65 分享

全美最大加密貨幣交易平臺Coinbase上周公告因員工遭釣魚及詐騙電話騙走登入密碼，使駭客得以存取部份系統資料，但強調未影響客戶加密貨幣或個資。

今年2月5日數名Coinbase員工接到冒充緊急事件的手機簡訊，要求員工點入釣魚連結。大部份員工都沒有理會，但有一名員工點入且輸入了用戶名稱及密碼。駭客取得了合法用戶名稱和密碼後，多次企圖遠端存取Coinbase系統。雖然駭客一開始無法通過多因素驗證（Multi-Factor Authentication，MFA）的把關，但駭客之後冒充Coinbase IT員工打電話給該員工，誘騙其按照指示登入公司系統，導致成功的駭入事件。

Coinbase表示，攻擊者取得了部份員工聯絡資訊，包括姓名、電子郵件信箱和一些電話號碼，但未竊得或存取任何客戶資訊或加密貨幣資產。

SecurityWeek引述Coinbase的調查，判定這次攻擊是由0ktapus的組織所為。0ktapus又名Scattered Spider，去年曾以類似手法駭入Twilio及Cloudflare等130多家企業。此外，今年一月安全廠商Crowdstrike也發現該組織利用9年前的Intel驅動程式漏洞，攻擊Windows PC用戶。

Coinbase並提醒客戶，為免社交工程攻擊，切勿將登入憑證分享他人，或讓他人遠端存取個人裝置，並且應使用強驗證，像是實體安全金鑰。針對非經常交易的客戶，Coinbase建議使用其儲存庫（vault）解決方案，可透過共同簽章或取消未許可提款等功能確保資產安全。

Social Engineering - A Coinbase Case Study

Tl;dr - Coinbase recently experienced a cybersecurity attack that targeted one of its employees. Fortunately, Coinbase's cyber controls prevented the attacker from gaining direct system access and prevented any loss of funds or compromise of customer information. Only a limited amount of data from our corporate directory was exposed. Coinbase believes in transparency, and we want our employees, customers, and the community to hear the details of this attack and to share the Tactics, Techniques, and Procedures (TTPs) used by this adversary so everyone can better protect themselves.

By Jeff Lunglhofer Engineering, 2023年2月17日, 4min read time

中華電信 Chunghwa Telecom

Ref: https://www.ithome.com.tw/news/155630
https://www.coinbase.com/blog/social-engineering-a-coinbase-case-study

惡意雲端應用程式存取信箱內容

微軟已驗證發布者狀態遭濫用，誘使被害者授權惡意雲端應用程式

Proofpoint發現一個新的同意網路釣魚（Consent Phishing）攻擊行動，惡意攻擊者濫用微軟已驗證發布者（Verified Publisher）狀態，誘使受害者授予惡意雲端應用程式權限

文/ 李建興 | 2023-02-01 發表

讚 56 分享

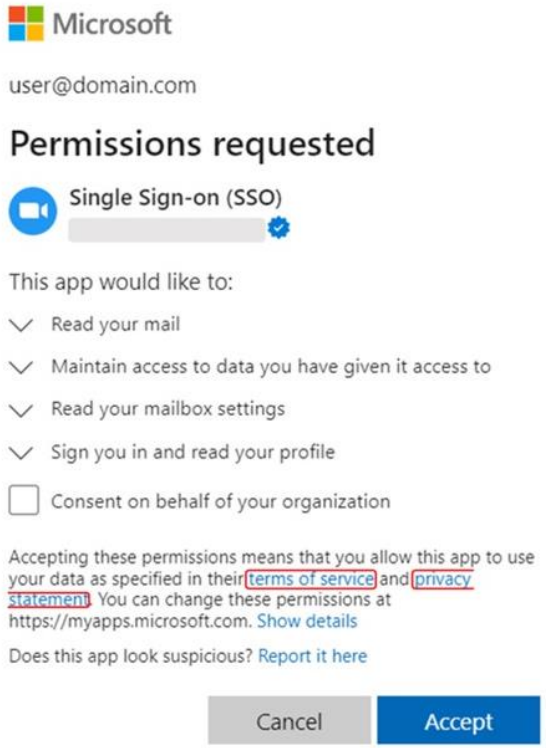
資安公司Proofpoint研究人員發現一個新的同意網路釣魚（Consent Phishing）攻擊行動，惡意攻擊者濫用微軟已驗證發布者（Verified Publisher）狀態，誘使受害者授予惡意雲端應用程式權限，使攻擊者能夠存取用戶資料，並取得電子郵件信箱、日曆和會議邀請委派權限。

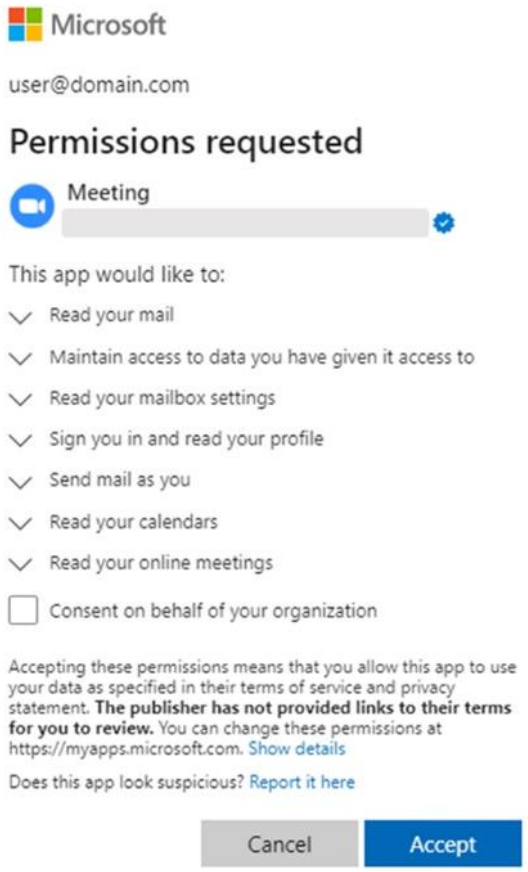
在這個新的同意網路釣魚攻擊活動中，由於攻擊者使用微軟已驗證發布者狀態，因此當惡意第三方OAuth應用程式，請求透過使用者帳戶存取資料時，增加了用戶被誘騙同意的可能性，研究人員發現惡意程式所取得的委派權限（Delegated Permissions）影響極廣，能夠瀏覽使用者的電子郵件、調整信箱配置，以及存取和帳戶相關連的檔案和資料（下圖）。

微軟已驗證發布者是指，一個應用程式發布者經由MCPP驗證身份，並將該MCPP帳戶和應用程式註冊相關聯，所獲得的狀態。當應用程式發布者經過驗證時，在應用程式Azure AD同意提示和網頁中，變會出現藍色的已驗證徽章。微軟提到，攻擊者透過冒充合法公司註冊MCPP帳戶。攻擊者將詐欺取得的合作夥伴帳戶，添加到他們在Azure AD所創建的OAuth應用程式註冊中，誘使用戶授予惡意應用程式權限。

該網路釣魚攻擊主要影響英國和愛爾蘭的部分用戶，Proofpoint研究人員總共發現了三個不同的惡意程式發布者，以及他們所創建的三個惡意應用程式，這些惡意應用程式鎖定相同的組織，並且與相同的惡意基礎設施關聯，已有多個用戶上鉤授權惡意應用程式。

在獲得受害者同意後，惡意雲端應用程式預設取得委派權限，使攻擊者可以存取和操縱受感染用戶關聯的電子郵件信箱、日曆和會議邀請，而且因為受害者同意的權限中，還包括離線存取，因此在同意權限後不需使用者的互動，便能夠存取受感染帳戶的資料，受害者的組織品牌也可能遭到濫用。





微軟在收到Proofpoint通報後，已經下架惡意應用程式，停用攻擊者擁有的帳戶，並且主動通知受影響用戶，同時也增加MCPP審查流程的安全措施，避免之後發生類似的詐欺活動。Proofpoint研究人員則建議，使用者不應該僅根據經驗證發布者狀態就信任OAuth應用程式，應該仔細評估授予第三方應用程式存取權限的風險。

Ref: https://www.ithome.com.tw/news/155325
https://www.proofpoint.com/us/blog/cloud-security/dangerous-consequences-threat-actors-abusing-microsofts-verified-publisher

QR Code網路釣魚攻擊

新聞

您現在位置：首頁 > 新聞

美國主要能源組織遭QR Code網路釣魚攻擊

2023 / 08 / 20 - 編輯部

據外媒報導，近日美國著名能源公司遭遇了大規模QR Code網路釣魚攻擊，攻擊者向目標發送大量包含惡意QR Code的電子郵件並成功繞過安全措施。

此次攻擊總共發送超過1000封電子郵件，其中大約有三分之一(29%)針對一家大型美國能源公司，而其餘的目標分佈於製造業(15%)、保險業(9%)、技術(7%)、和金融服務（6%）。

據發現該活動的Cofense公司表示，這是業界首次監測到如此大規模的QR Code網路釣魚攻擊，這表明更多的網路釣魚攻擊者可能正在測試QR Code作為攻擊媒介的有效性。

Cofense透露，攻擊開始於一封網路釣魚電子郵件，聲稱收件人必須採取行動更新其Microsoft365帳戶設置。這些電子郵件帶有包含QR Code的PNG或PDF附件，系統會提示收件人掃描以驗證其帳戶。電子郵件還要求收件人必須在2-3天內完成此步驟，以增加緊迫感。

攻擊者使用圖像中嵌入的QR Code來繞過掃描郵件中惡意連結的電子郵件安全工具，從而使網路釣魚郵件能夠順利到達目標的收件箱。

為了逃避安全檢測，該攻擊活動中的QR Code還使用Bing、Salesforce和Cloudflare的Web3服務中的重定向功能，將目標重定向到Microsoft365網路釣魚頁面。

攻擊者透過在QR Code中隱藏重定向URL、濫用合法服務以及對網路釣魚連結使用Base64編碼，大大增加了逃避檢測和通過電子郵件安全閘道的成功率。

QR Code網路釣魚是去年才逐漸開始流行的攻擊手段，2022年1月，FBI曾警告稱，網路犯罪分子越來越多地使用QR Code竊取憑證和財務資訊。

最後，儘管QR Code釣魚郵件往往能夠繞過郵件安全檢測，但依然需要受害者採取行動才能攻擊成功，因此有針對性的網路安全意識培訓能夠有效緩解此類威脅。

透過QR Code隱藏URL重新導向

Ref: https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10640

釣魚信件會跟上時事更新題材(矽谷銀行倒閉)

利用矽谷銀行事件的網釣與詐騙如雨後春筍般地湧現

根據SANS網路風暴中心觀察，在矽谷銀行（SVB）關閉隔天，駭客為了誘騙SVB關係人、合作夥伴或客戶，開始大量註冊SVB相關網站

文/ 陳曉莉 | 2023-03-16 發表

任何重大新聞事件都會惹來駭客的覬覦，不管是ChatGPT或者是上周發生擠兌的矽谷銀行（Silicon Valley Bank，SVB），SANS網路風暴中心（SANS Internet Storm Center）與資安業者Cyble明顯看到以SVB相關字眼註冊的網域名稱數量大增，另有駭客假冒為穩定幣USDC發行商Circle，企圖危害使用者的加密貨幣錢包。

駭客大量註冊SVB相關網站是為了利用它們來展開網釣攻擊。根據SANS網路風暴中心的統計，原本平日僅有不到10筆使用SVB文字的相關註冊，但在SVB關閉（3/10）的隔天，單日註冊量即超過20筆，3月12日更達到50筆。

這些新的網域名稱都是用來誘騙SVB關係人，或許是合作夥伴、投資人或存款人，SVB的官網網址為svb.com，各方駭客則註冊了login-svb、svbclaim、svbdebt、svb-usdc或svbank。駭客利用這些以假亂真的網址來進行商業電子郵件詐騙，寄送郵件要求SVB存款人變更帳戶資訊。

Cash4SVB

Are you a company or individual with frozen customer balances at Silicon Valley Bank?

Are you owed money by Silicon Valley Bank as a trade creditor or lender?

We will buy your verified claim for CASH and pay you within 24 hours.

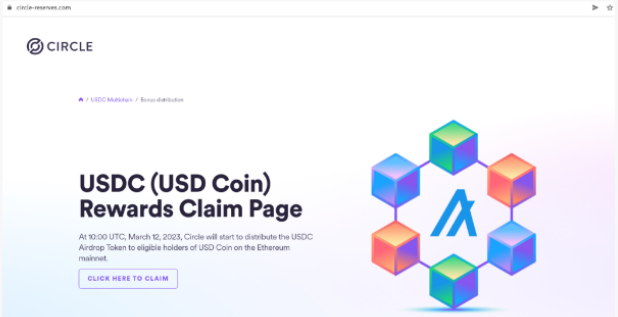
If approved, most claims are paid out at 65-85% of the claim value, depending on terms.

We are not affiliated with Silicon Valley Bank. We are a private investment group based out of Stanford, California

Enter your contact information below to get the process started.

因應SVB事件出現的網釣網站不僅假冒為SVB，也偽裝成USDC發行商Circle。

USDC用戶遭到駭客鎖定的主要原因，為其發行商Circle存放了33億美元的USDC現金儲備於SVB，使得SVB的擠兌事件一度造成USDC與美元脫鉤，也讓USDC用戶急著贖回，一直到Circle宣布，將在SVB於3月13日重新開張時，開放用戶以1:1贖回美元。隨後Circle也已安全地將所有現金儲備移轉至其它銀行。



Ref: https://www.ithome.com.tw/news/155967

Linkedin私訊詐騙鎖定人資行銷

寄發假PDF檔蒐集帳號登入憑證　提防不明連結避免上鉤

Ducktail網路釣魚再起　私訊詐騙鎖定人資行銷

2023-09-28　趨勢科技威脅研究中心

駭客利用LinkedIn私訊發動了一波瞄準行銷和人力資源專業人才的魚叉式網路釣魚攻擊。Ducktail駭客集團這波攻擊的目的是為了控制受害的Facebook商業帳戶並濫用廣告功能來刊登惡意廣告。隨著LinkedIn的不斷成長與日漸受到歡迎，它也成了駭客發動社交工程詐騙與其他犯罪所偏愛的工具之一。

去（2022）年7月，資安研究人員發現一起名為「Ducktail」的攻擊，在這起攻擊當中，駭客利用資訊竊取程式來攻擊具備Facebook商業帳戶存取權限的個人使用者或企業員工。駭客利用LinkedIn私訊發動了一波瞄準行銷和人力資源專業人才的魚叉式網路釣魚攻擊。Ducktail駭客集團這波攻擊的目的是為了控制受害的Facebook商業帳戶並濫用廣告功能來刊登惡意廣告。隨著LinkedIn的不斷成長與日漸受到歡迎，它也成了駭客發動社交工程詐騙與其他犯罪所偏愛的工具之一。

2023年3月，趨勢科技Managed XDR團隊調查了多起涉及不同客戶的Ducktail網頁瀏覽器登入憑證竊盜事件。發現了一個會蒐集使用者資料的程式，蒐集的資料包括瀏覽器資訊、IP位址、定位資訊，而且還會連線到Facebook和Telegram網域。本文說明趨勢科技的研究發現，以及針對該攻擊所做的技術分析。

Ducktail攻擊事件的技術層面分析

從這個樣本的檔案名稱看來，這波攻擊顯然是衝著行銷專業人才而來，因為檔名提到了行銷總監這個職務（圖1）。此外，它還提到另一個更高階的主管職缺來引誘受害者點選壓縮檔。這裡請注意，由於只有拿到下載連結，因此無法斷定這些連結如何發送到受害者手中，不過有可能是經由LinkedIn訊息，因為Ducktail過去就曾經使用過該平台。

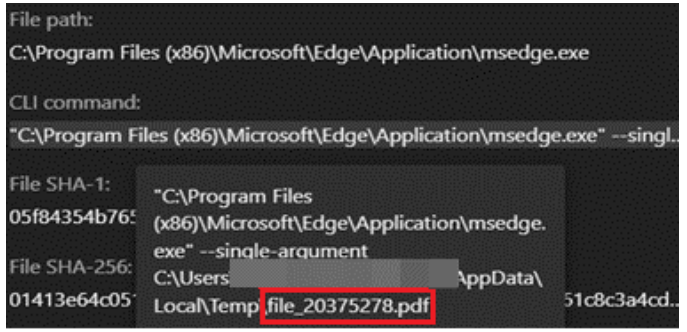
.....

當受害者忙著閱讀Ducktail產生的PDF檔案時，惡意程式就在背後偷偷蒐集瀏覽器儲存的帳號登入憑證（圖8），同時連上Facebook網域來蒐集帳號的Facebook相關資訊（圖9）。資料蒐集到之後，惡意程式會將資料儲存成一個文字檔「%User.Temp%\temp_update_data_8.txt」（圖10），接著利用Telegram將資料外傳。也觀察到，惡意程式每10分鐘就會更新並傳送一次資料（圖11）。

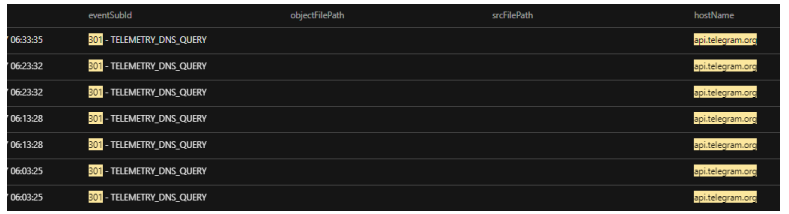
附件包含行銷總監職缺相關內容

Name	Date	Type	Size
GAP _ Spring 23 Denim.mp4	3/18/2023 6:22 PM	MP4 Video	3,405 KB
GAP 2023 Campaign Products (2).png	3/18/2023 6:03 PM	PNG image	1,163 KB
GAP 2023 Campaign Products (3).png	3/18/2023 6:03 PM	PNG image	572 KB
GAP 2023 Campaign Products (4).png	3/18/2023 6:03 PM	PNG image	783 KB
GAP 2023 Campaign Products (5).png	3/18/2023 6:04 PM	PNG image	565 KB
GAP 2023 Campaign Products (6).png	3/18/2023 6:04 PM	PNG image	1,139 KB
GAP 2023 Campaign Products.png	3/18/2023 6:03 PM	PNG image	490 KB
Job JD for the position of Marketing Director at GAP.exe	3/19/2023 3:30 PM	Application	75,898 KB
Role of Marketing Director Manager GAP 2023.exe	3/19/2023 3:29 PM	Application	75,453 KB
The plan describes the salary and requirements GAP 2023 - Copy.exe	3/19/2023 3:30 PM	Application	75,898 KB

開啟PDF檔掩護背景惡意活動



竊取瀏覽器儲存密碼，透過Telegram外傳



Ref: https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/14E0316BBCC34FF4BE44F6156771C5D4

針對密碼管理工具LastPass的攻擊 (1/2)

駭客正鎖定LastPass用戶發動釣魚信件攻擊

近期一波釣魚郵件攻擊以LastPass官方技術支援的名義發送，導致LastPass用戶的密碼及個資外洩，資安業者Malwarebytes則建議民眾使用密碼管理器，登入線上服務時也應採用基於實體金鑰的雙因素驗證措施，才能避免淪為這類攻擊的受害者

文/ 林妍溱 | 2023-09-27 發表

讚 51 分享

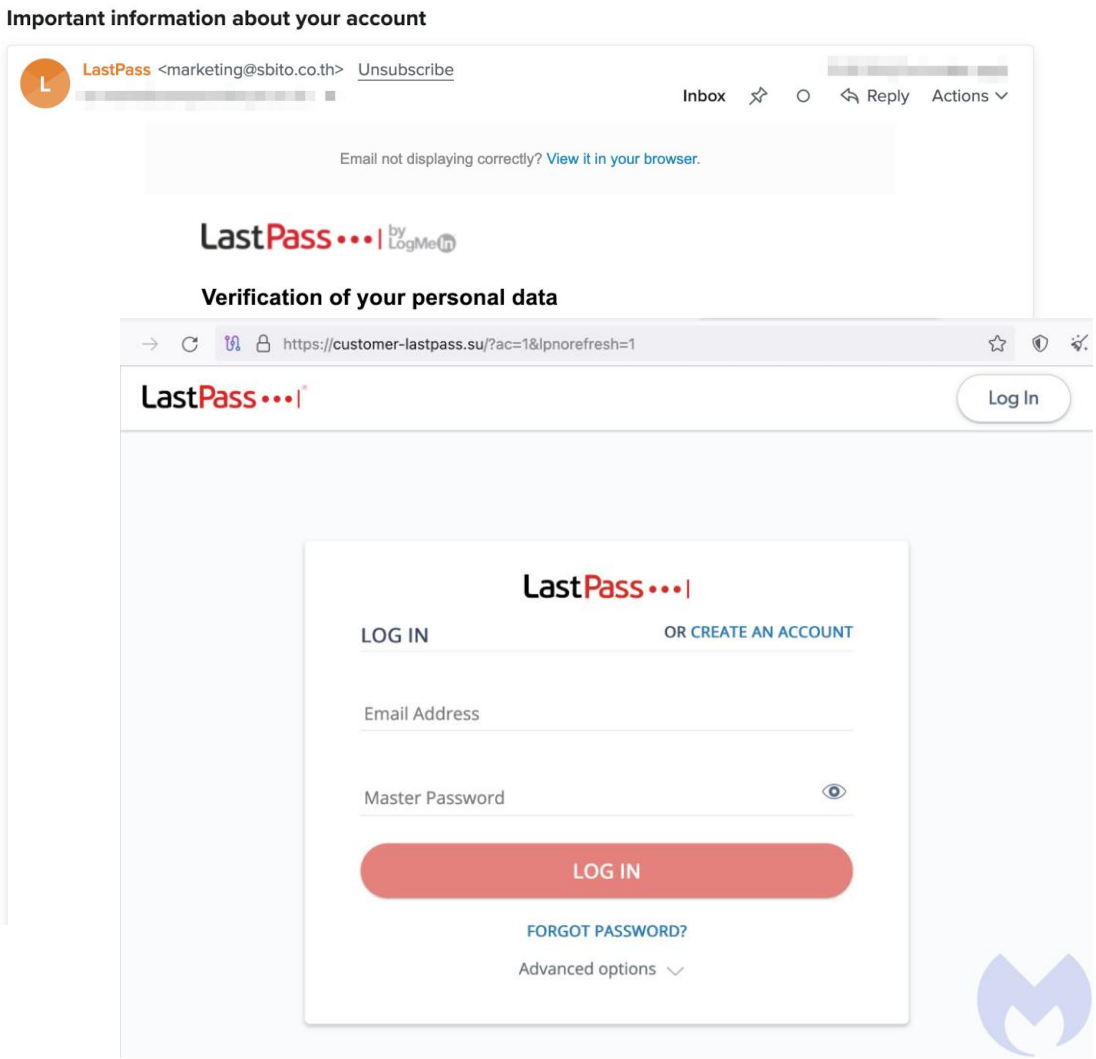
近日有不知名駭客鎖定LastPass用戶發動釣魚信件攻擊，導致LastPass用戶的密碼及個資外洩，連LastPass員工也受害。

本月13日LastPass接獲用戶通報遭到釣魚信件攻擊，安全廠商Malwarebytes也取得信件樣本進行分析。這波攻擊中，用戶接到貌似LastPass技術支援單位寄來的信件，表示用戶某項功能遭到封鎖，用戶需在9月26日前輸入個資完成身分確認以便重啟該功能。為數不詳的用戶點入信中所附連結連進釣魚網站後，讓駭客取得了個資。

被騙走的用戶個資包括電子郵件、公司名稱、用戶姓名、住家地址、電話號碼、IP位置，駭客並用這些資訊竊取了用戶的密碼庫（password vaults）。不過LastPass聲稱，如果用戶有遵循密碼最佳實作的話（例如主密碼使用強密碼），要暴力破解取得密碼庫儲存的密碼並不容易。

釣魚網站是代管在本月才設立在斯洛維尼亞的網域。LastPass指出，儘管9月上旬該公司聯同安全廠商關閉了該網域，到了9月下旬又死灰復燃，再度發動攻擊。受害者有多少不得而知，LastPass指出，這波攻擊是全球性，受害者遍及不同產業，也包括該公司87名員工。

安全廠商提醒，要防止被網釣攻擊，除了提高警覺外，最好使用密碼管理器，此類工具不會將用戶憑證輸入假網站。此外業者說，雙因素驗證（2FA）也有分，有的只是密碼而已，使用者應該選用搭配FIDO2裝置（例如USB硬體式）的2FA。



Ref: https://www.ithome.com.tw/news/158995
https://www.malwarebytes.com/blog/news/2023/09/nasty-lastpass-phish

針對密碼管理工具LastPass的攻擊 (2/2)

小心語音網路釣魚！ 駭客冒充LastPass客服誘騙用戶密碼庫資料

密碼管理業者LastPass指出，有人搶註看似該公司客服的網域名稱，並打算對其用戶透過語音網釣攻擊，騙取他們的主控密碼

文/ 周峻佑 | 2024-04-19 發表

讚 4 分享

資安業者LastPass針對網路釣魚套件CryptoChameleon的攻擊行動提出警告，他們接獲資安業者Lookout的通報，並得知新的停放網域（Parked Domain）help-lastpass[.]com，然後著手進行監控，並表明一旦該網域出現可疑活動且針對該公司客戶從事網路釣魚，他們就會採取行動。

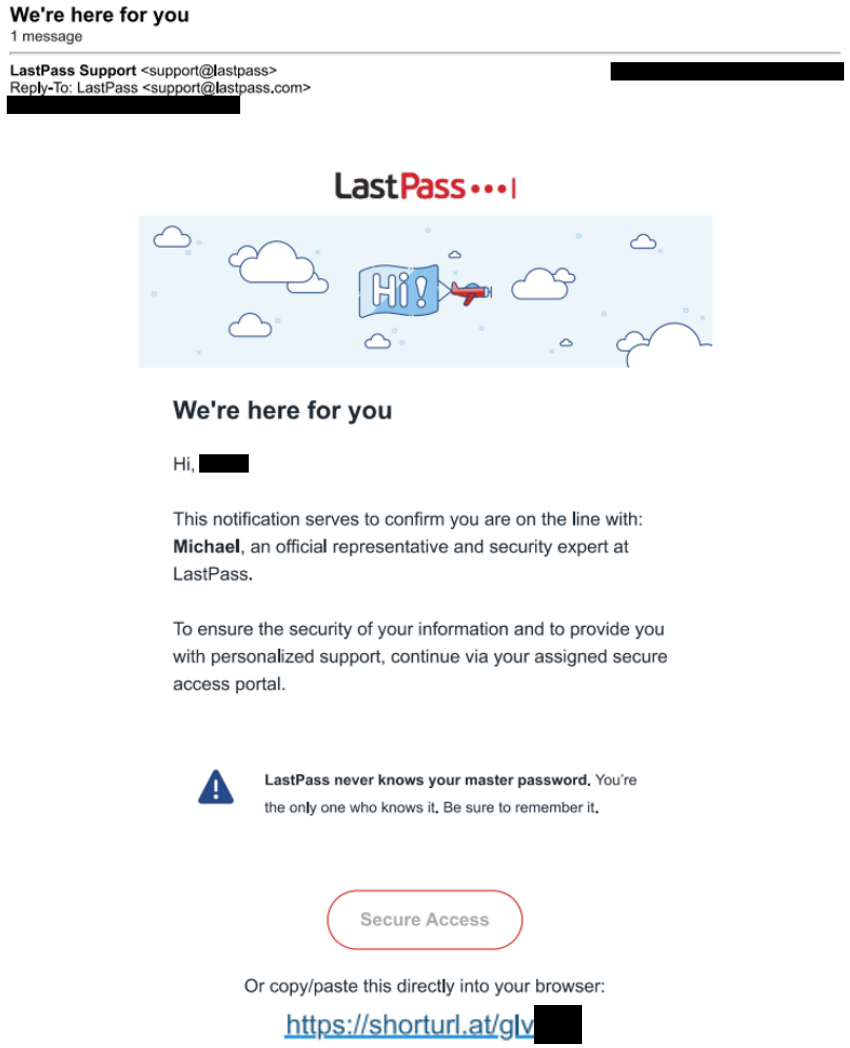
所謂的停放網域，就是有人付費登記網域後，即將其閒置，並未與網站、電子郵件服務等網路服務連結。一般而言，這麼做的目的通常是要保留特定網域名稱，並防止遭到他人買走。但如今也有駭客利用這樣的方法，以便未來從事攻擊行動。

而對於攻擊者利用上述網域的方式，LastPass表示對方很可能會透過語音網釣從事攻擊行動。

攻擊者先透過888的電話號碼打電話給LastPass用戶，聲稱他們的帳號有新裝置存取，要求按1允許或是按2禁止。假若使用者按下2，對方就會表明接下會來有客戶代表致電，要將事故結案。

接著，用戶就會接到佯稱是LastPass員工的電話，對方將會寄出重設帳號存取權限的電子郵件，若是用戶依照指示操作，並在help-lastpass[.]com網站輸入LastPass的主控密碼（此密碼可用來登入用戶的LassPass帳號，並查看存放的所有密碼），攻擊者就有可能嘗試存取LastPass帳號並竄改設定，以便進行完全控制。

對此，LastPass提供網路釣魚攻擊的相關特徵，呼籲用戶提高警覺，並強調他們不會向用戶詢問主控密碼。



We're here for you
1 message

LastPass Support <support@lastpass>
Reply-To: LastPass <support@lastpass.com>
[redacted]

LastPass

We're here for you

Hi, [redacted]

This notification serves to confirm you are on the line with: **Michael**, an official representative and security expert at LastPass.

To ensure the security of your information and to provide you with personalized support, continue via your assigned secure access portal.

LastPass never knows your master password. You're the only one who knows it. Be sure to remember it.

Secure Access

Or copy/paste this directly into your browser:

https://shorturl.at/glv[redacted]

中華電信 Chunghwa Telecom

Ref: https://www.ithome.com.tw/news/162411
https://blog.lastpass.com/posts/2024/04/advanced-phishing-kit-adds-lastpass-branding-for-use-in-phishing-campaigns

釣魚信件導致公司機密資訊外洩

友訊1.2GB產品原始碼、客戶、員工資料在駭客論壇上兜售

友訊坦承因網釣攻擊導致資料外洩，但否認駭客說法以及攻擊時間點，表示外洩的資料屬於過時零碎資訊，不至於對現有客戶造成影響

文/ 林妍溱 | 2023-10-18 發表

讚 176 分享

《Bleeping Computer》報導，網路設備商友訊（D-Link）產品原始碼及客戶、員工個資等資料遭駭客在地下論壇上兜售，友訊坦承此事，但表示是員工誤點網釣信件才讓駭客存取系統，不過存取的也是過時的資料。

報導指出，一名地下論壇用戶張貼公告，指其曾駭入友訊的內部網路，取得300萬行客戶及員工客製以及網路管理軟體D-View的程式碼。

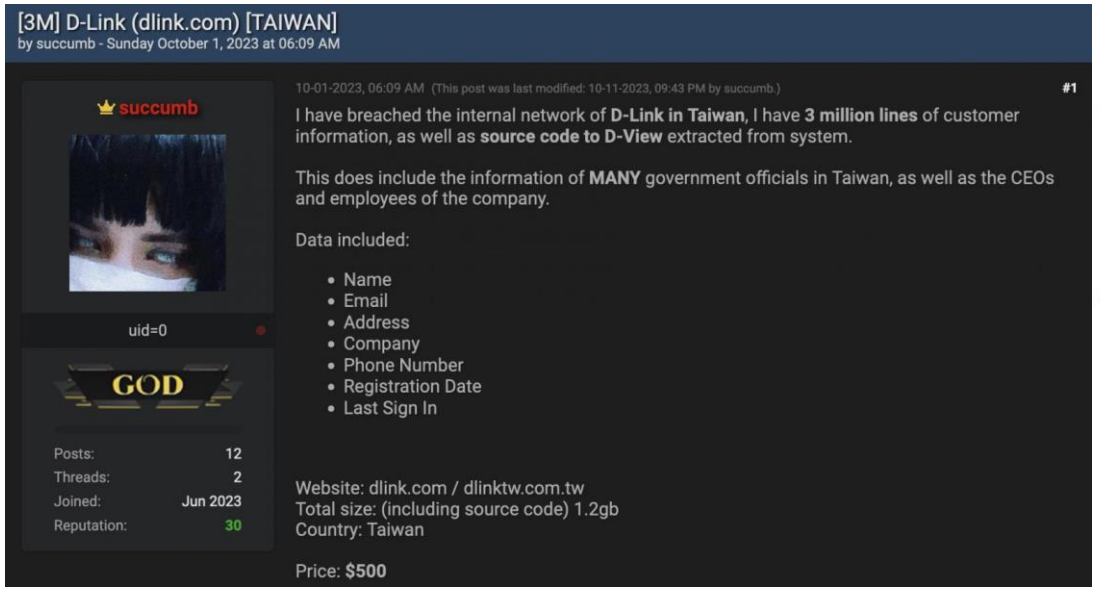
這批1.2GB的資料包含客戶及員工姓名、電子郵件、住家地址、公司、電話、帳號註冊及最後登入日期，要價僅500美元。值得注意的是，兜售者宣稱名單上還有「許多」政府官員，以及友訊CEO的個資。

友訊已經向媒體證實此事，表示原因是一名員工不慎點入網釣信件，而讓攻擊者取得公司網路系統的登入憑證。該公司說已立即關閉受影響的伺服器，及封鎖用戶帳號，除了2個正在調查的帳號外。

這家網路設備商聲稱，駭客是存取了測試實驗室中的產品註冊系統取得了這批資料。但外洩的產品程式碼是屬於舊版D-View 6，後者已在2015年終止支援。友訊也否認外洩的資料量及機密性，聲稱經過調查顯示只有700筆過時、零碎的資訊，並說大部分資料都是低敏感性，且半公開可取得的資訊。

友訊並表示，這起事件是舊安全事件了，只是駭客刻意竄改存取時戳，以假造駭入事件是最近所為，因此現有客戶不太可能受影響。

友訊常因其生產網路設備、網路攝影機安全漏洞遭濫用而登上資安新聞。2017年美國聯邦貿易委員會（FTC）因網路路由器及攝影機軟體安全性不足控告友訊，雙方於2019年達成和解。



Ref: https://www.ithome.com.tw/news/159336
https://www.bleepingcomputer.com/news/security/d-link-confirms-data-breach-after-employee-phishing-attack/

其他近期網路釣魚案例

Instagram詐騙傳出以提供時裝購物商城Shein禮物卡為誘餌的事故

2023/3/29

防毒業者Avast揭露近期的Instagram詐騙攻擊行動，駭客針對英國、澳洲、法國、西班牙、波蘭用戶下手，對方發文聲稱是2023年時裝購物商城Shein禮物卡的幸運兒，並標記一長串的Instragram使用者。

若用戶依照指示存取駭客提供的URL，就會被帶往釣魚網站，而該網站會對用戶發出通知訊息，表示時限內完成問卷，就有機會贏得禮物卡，且無論使用者輸入有效答案與否，都會通過審核並要求填寫個人資料，支付些許費用取得禮物卡，然而，受害者最終非但不會拿到禮物卡，還會「被訂閱」來路不明的服務。

臺灣民眾網路詐騙抵抗力有待加強，透過錯誤資訊來確認資訊真偽的比例高達8成

2023/3/29

金融服務業者Visa針對全球18個市場、6千個成年人進行詐騙話術（Fraudulese）有關的調查，結果發現，一般人大多會擔心親友受騙，但忽略自己也是歹徒行騙的目標，再者，有81%受訪者透過錯誤資訊來確認資訊真偽──有46%主要依據公司名稱與標誌來判斷。此外，對於釣魚郵件橫行的現象，他們發現僅有6成受訪者會檢查是否來自寄件者的電子郵件信箱，且只有47%會確認郵件是否有錯字。

而針對臺灣的部分，該公司表示，我國消費者最容易受到「限定期間回應」、「免費贈禮」等關鍵字的引誘。

歐洲刑警組織警告網路罪犯濫用ChatGPT

2023/3/29

機器學習模型ChatGPT被用於攻擊行動的現象日益頻繁，這樣的情況也引起警方的高度重視。歐洲刑警組織（Europol）於3月27日提出警告，他們呼籲大家注意，網路罪犯正在濫用ChatGPT與其他的大型語言模型（LLM），例如，他們很可能在詐欺與社交工程領域，利用這種語言模型來模仿特定人士的書寫、說話方式，來產生網路釣魚誘餌，而且，攻擊者也可能將其拿來產生假訊息。

再者，也有人將其用於製作惡意程式，在這樣的狀況下，攻擊者即便自身無開發能力，也有機會製作相關工具。

美國警告駭客假借採購名義進行商業郵件詐騙

2023/3/29

美國聯邦調查局（FBI）針對近期的商業郵件詐騙（BEC）態勢提出警告，指出駭客假借當地商家的名義，向目標公司「批發」各式商品，包含了建材、農業器具、電腦硬體、太陽能產品等。

為了取信攻擊目標，駭客會冒用真實員工或前員工的姓名犯案，而且，這些駭客也採用了延遲付款的方式，如Net-30或Net-60短期融資的方式，指定在交貨後的30天或60天才付款，並付上偽造的推薦函與W-9貸款表單，從而讓受害公司收不到貨款、察覺上當為時已晚。

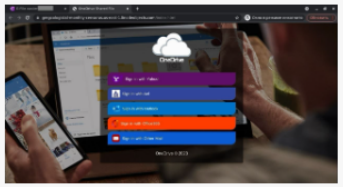
【3月20日】政府全民普發6千元在即，傳出有詐騙集團架設冒牌網站行騙

2023/3/20

臺灣政府2022年稅收超徵4,500億元，行政院宣布2023年將提撥1,400億元，當中將對全國民眾普發6千元現金。消息一出，駭客也開始架設假網站來行騙。3月中財政部宣布將在22日開放登記，但也出現新的假網站，民眾要提高警覺。

駭客假冒企業SharePoint檔案共用通知郵件，對攻擊目標所屬的員工進行網路釣魚

2023/3/27

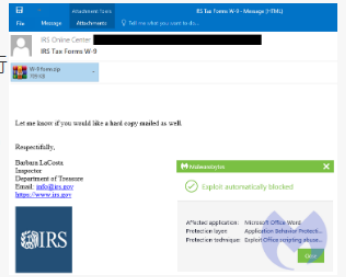


不少企業採用微軟SharePoint讓員工能共用文件檔案，但有駭客看上這點來發動網路釣魚攻擊。資安業者卡巴斯基揭露濫用SharePoint的攻擊行動，駭客寄送SharePoint檔案共用的通知郵件，表示要分享OneNote筆記檔案，一旦收信人依照指示點選，就會存取SharePoint伺服器上的OneNote檔案，但該檔案內容卻是另一個PDF文件的「檔案共用」，若是點選連結就會被帶往偽冒OneDrive的釣魚網站，而有可能導致Yahoo!、AOL、微軟帳號資料被騙走。

研究人員指出，攻擊者發動相關攻擊之前的準備工作，就是取得可存取SharePoint伺服器的權限，之後再上傳檔案並開放共用的連結。由於這種檔案共享的通知信來自SharePoint服務，使得大部分的網路安全系統都會放行。

適逢美國報稅季，殭屍網路病毒Emotet假借IRS寄出申報單名義進行網路釣魚攻擊

2023/3/28



資安業者Malwarebytes、Palo Alto Networks針對殭屍網路病毒Emotet的攻擊行動提出警告，這次駭客鎖定即將到來的美國報稅季，假冒國稅局（IRS）提供W-9表單的名義寄送釣魚郵件。

Malwarebytes看到駭客寄送了含有ZIP檔案、檔案大小為709 KB的附件，但裡面的W-9表單Word文件解壓縮卻高達548 MB，攻擊者這麼做的目的是為了規避防毒軟體偵測。一旦收信人開啟，就會出現文件受到保護，必須啟用巨集的內容才能瀏覽內容，然而一旦照做，電腦就會被植入Emotet。

Ref: https://www.ithome.com.tw/news/156193
https://www.ithome.com.tw/news/156121
https://www.ithome.com.tw/news/156142
https://www.ithome.com.tw/news/156172

利用AI生成釣魚信件 (1/2)

AI生成釣魚信件攻擊比例逐漸上升，研究人員建議以AI對抗AI

攻擊者開始運用生成式人工智慧，產生更具針對性且攻擊有效性更高的釣魚信件，Abnormal資安研究人員建議組織應該以人工智慧對抗人工智慧，以發現傳統安全解決方案所無法偵測的釣魚信件

文/ 李建興 | 2023-12-27 發表

讚 147 分享

隨著生成式人工智慧技術的普及，攻擊者已經將其用於網路釣魚攻擊中，資安公司Abnormal收集由人工智慧所生成的電子郵件並且進行分析，資安研究人員認為，攻擊者已經將生成式人工智慧融入到攻擊策略中，而組織也必須以相同的方式反應，運用人工智慧阻擋這些釣魚攻擊。

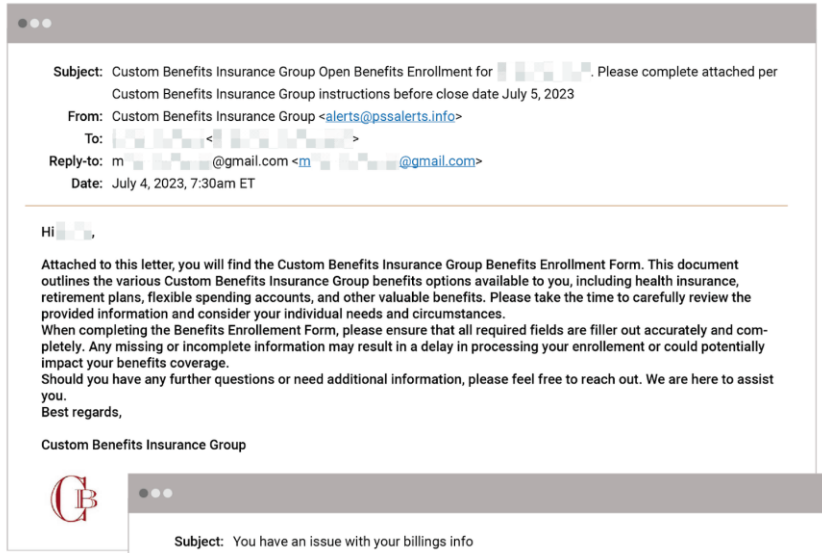
傳統釣魚郵件通常仰賴固定的模板和格式，同時也會使用共同的網域或是連結，整體郵件內容和風格較統一缺乏客製，因此相當容易被安全軟體標記和攔截。但是研究人員指出，攻擊者運用生成式人工智慧，便可以非常快速地創建獨特且具針對性的內容，每封釣魚郵件都可以針對特定的收信人特別設計，不只看起來更真實，而且因為這些郵件不具有共同的惡意指標，因此也就更難被安全解決方案辨識出來。

雖然像是ChatGPT等產品都存在限制避免被濫用，但是攻擊者也可以開發攻擊專用的生成式人工智慧模型，研究人員舉例，像是WormGPT便可以製造具說服力的釣魚郵件，而專為網路攻擊所開發的生成式人工智慧工具FraudGPT，也能夠生成欺騙性內容。

研究人員分析了生成式人工智慧被濫用於釣魚攻擊的案例，像是攻擊者偽裝成保險業務，透過電子郵件試圖散布惡意軟體。信件中使用看似真實的名稱和電子郵件地址增加可信度，但附件卻是惡意軟體檔案。

經過開源軟體Giant Language Model Test Room（GLTR）的偵測，發現郵件文字多數由人工智慧生成，研究人員提到，這個案例是因為信件內容大多使用人工智慧預測高機率單詞，因此大部分人工智慧所產生的內容都可以被辨識出來。

另一個釣魚信件案例則是偽裝Netflix信件的釣魚攻擊，攻擊者冒充客服人員，並稱受害者的訂閱即將到期，需要點擊連結續訂。信件內使用線上玩具購物網站Teeela相關網域，以及使用客服平臺Zendesk，讓整封信看起來更可信，進而增加了攻擊的有效性，但同樣整封信大部分內容，也被人工智慧發現可能不是由人類編寫。

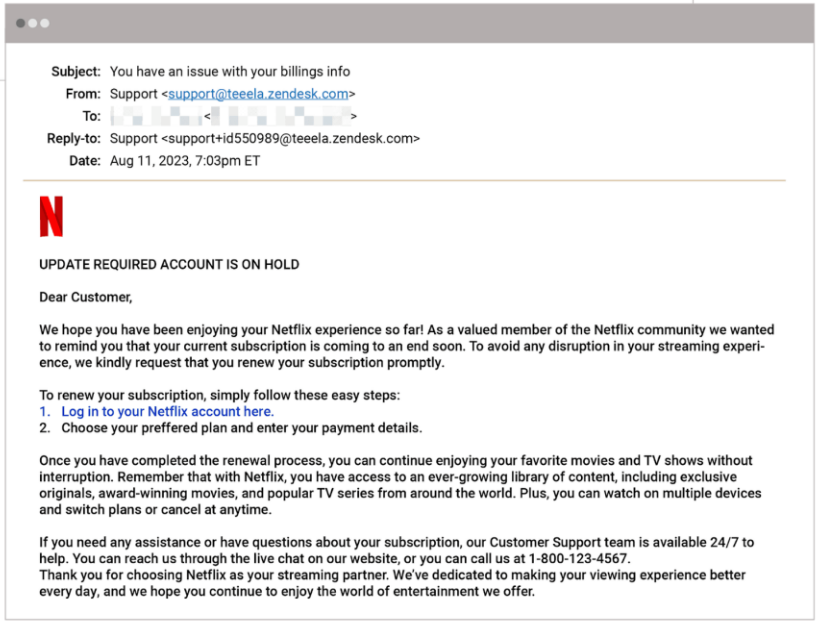


Subject: Custom Benefits Insurance Group Open Benefits Enrollment for [redacted]. Please complete attached per Custom Benefits Insurance Group instructions before close date July 5, 2023
From: Custom Benefits Insurance Group <alerts@pssalerts.info>
To: [redacted]
Reply-to: m[redacted]@gmail.com <m[redacted]@gmail.com>
Date: July 4, 2023, 7:30am ET

Hi [redacted],

Attached to this letter, you will find the Custom Benefits Insurance Group Benefits Enrollment Form. This document outlines the various Custom Benefits Insurance Group benefits options available to you, including health insurance, retirement plans, flexible spending accounts, and other valuable benefits. Please take the time to carefully review the provided information and consider your individual needs and circumstances.
When completing the Benefits Enrollement Form, please ensure that all required fields are filler out accurately and completely. Any missing or incomplete information may result in a delay in processing your enrollement or could potentially impact your benefits coverage.
Should you have any further questions or need additional information, please feel free to reach out. We are here to assist you.
Best regards,

Custom Benefits Insurance Group



Subject: You have an issue with your billings info
From: Support <support@teeela.zendesk.com>
To: [redacted]
Reply-to: Support <support+id550989@teeela.zendesk.com>
Date: Aug 11, 2023, 7:03pm ET

UPDATE REQUIRED ACCOUNT IS ON HOLD

Dear Customer,

We hope you have been enjoying your Netflix experience so far! As a valued member of the Netflix community we wanted to remind you that your current subscription is coming to an end soon. To avoid any disruption in your streaming experience, we kindly request that you renew your subscription promptly.

To renew your subscription, simply follow these easy steps:
1. Log in to your Netflix account here.
2. Choose your preffered plan and enter your payment details.

Once you have completed the renewal process, you can continue enjoying your favorite movies and TV shows without interruption. Remember that with Netflix, you have access to an ever-growing library of content, including exclusive originals, award-winning movies, and popular TV series from around the world. Plus, you can watch on multiple devices and switch plans or cancel at anytime.

If you need any assistance or have questions about your subscription, our Customer Support team is available 24/7 to help. You can reach us through the live chat on our website, or you can call us at 1-800-123-4567.
Thank you for choosing Netflix as your streaming partner. We've dedicated to making your viewing experience better every day, and we hope you continue to enjoy the world of entertainment we offer.

Ref: https://www.ithome.com.tw/news/160551
https://abnormalsecurity.com/blog/2023-ai-generated-email-attacks

利用AI生成釣魚信件 (2/2)

- 根據網路安全公司 Darktrace 最新研究報告，**攻擊者使用 ChatGPT 等生成式 AI，通過增加文字描述、標點符號和句子長度，讓社交工程攻擊量增加 135%**
- 研究英、美、法、德、澳、荷 6700 多名員工，82% 的人擔心駭客可以使用生成式 AI 來建立與真實通訊無法區分的詐騙電子郵件
- 全球 30% 的員工過去曾因欺詐性電子郵件或簡訊而上當受騙。此外，87% 的人擔心線上有關他們的個人資訊可能會被用於網路釣魚和其他電子郵件詐騙
- 過去 6 個月中，**詐騙電子郵件和簡訊的頻率增加了 70%**

- 電子郵件可能是網路釣魚攻擊的前三大特徵
  - 郵件中需要使用者點選連結或者打開附件（68%）
  - 來自未知發件人或意外內容（61%）
  - 拼寫和語法使用不當（61%）

Ref: https://www.techbang.com/posts/105183-generative-ai-such-as-chatgpt-led-to-a-135-increase-in

★釣魚郵件三大手法 (1/2)

1. 寄件人偽裝

- 寄件人的電子信箱被入侵
- 使用相似的電子郵件位址
  - 如將l改成1，m改成rn，順序調換，加上後(前)綴詞
  - G00GLE、App1e、 Adrnin 、Faecbook、dropbox-admin
- 偽造電子郵件寄件者資訊
  - SMTP 通訊協定，允許自訂寄件者資訊
- 假扮使用者所以信任的人
  - 如主管、系統管理員、法院、廠商等

釣魚郵件三大手法 (2/2)

2. 網址/超連結混淆偽裝

- 透過收件人感興趣的議題誘使收件人點擊連結
  - 其中超連結顯示文字和實際網址可能不同或暗藏惡意程式碼
- 利用短(縮)網址暗藏惡意網址
- 關鍵字廣告

3. 附加檔案偽裝

- 將惡意程式偽裝成一般文件如Word(.docx)、PDF(.pdf)為大宗
- 利用加密壓縮檔案使防毒軟體不能掃描

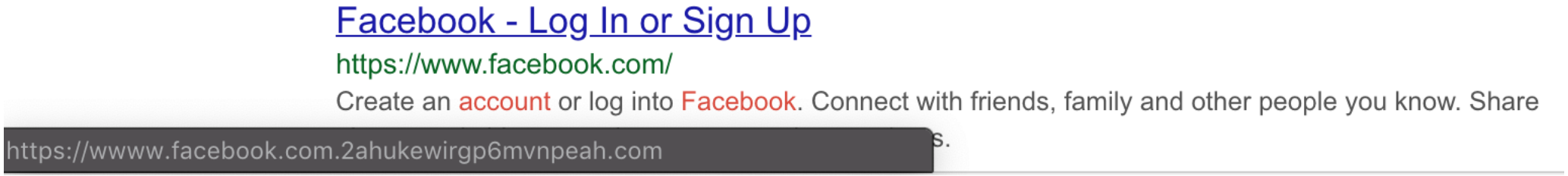
網址/超連結混淆偽裝 (1/2)

- 頂級網域混淆：
  - 釣魚網站：https://www.cht.xyz
- 子網域混淆
  - 釣魚網站：https://www.cht.com.tw.fakesite.com
- 文字數字混淆:
  - 釣魚網站： https://www.g00gle.com
- 相似域名混淆：
  - 釣魚網站：https://www.dropbox-filex.com

網址/超連結混淆偽裝 (2/2)

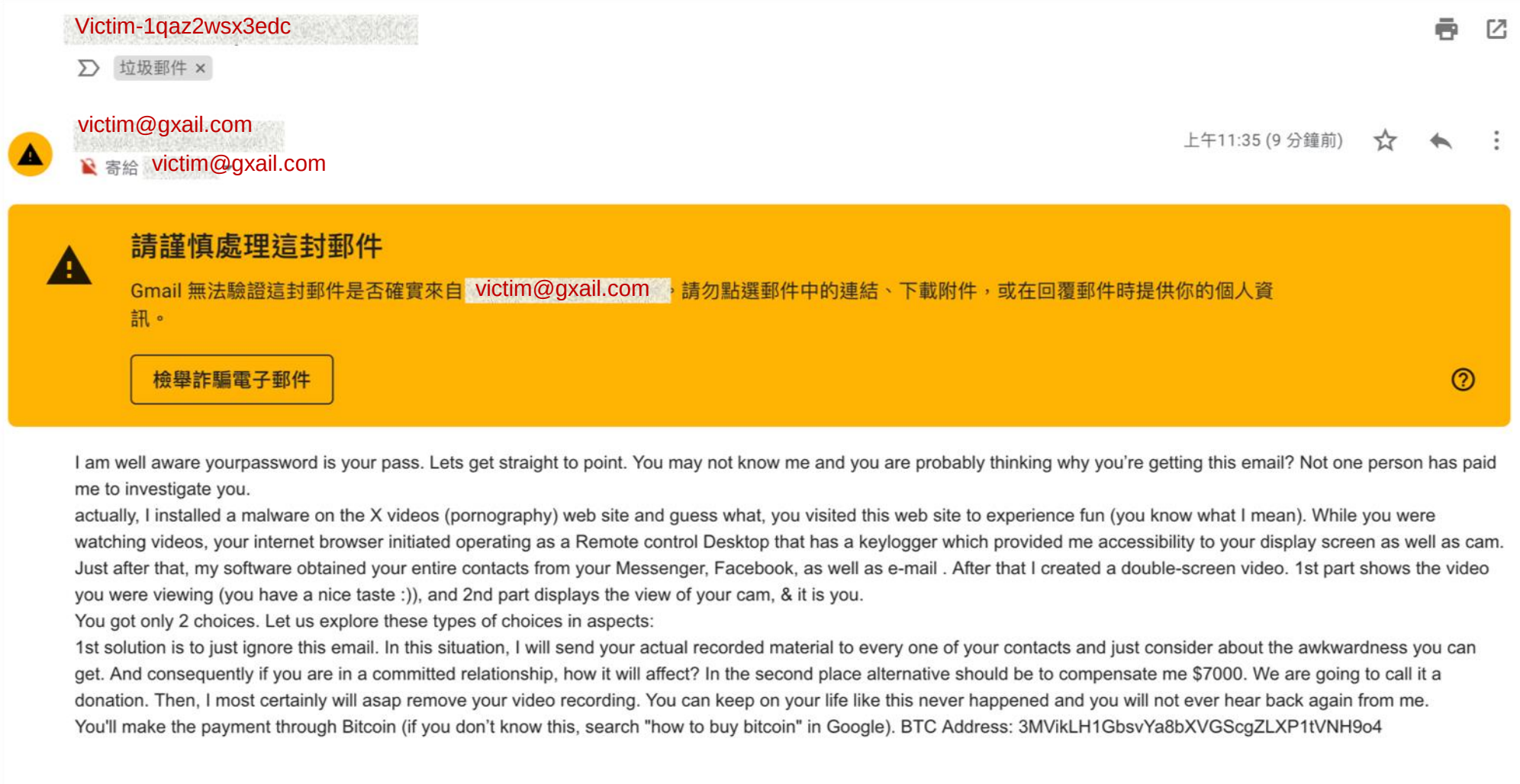
- 超連結顯示與實際連結網址不同
  - www.facebook.com

實際連結網址　　顯示的網址

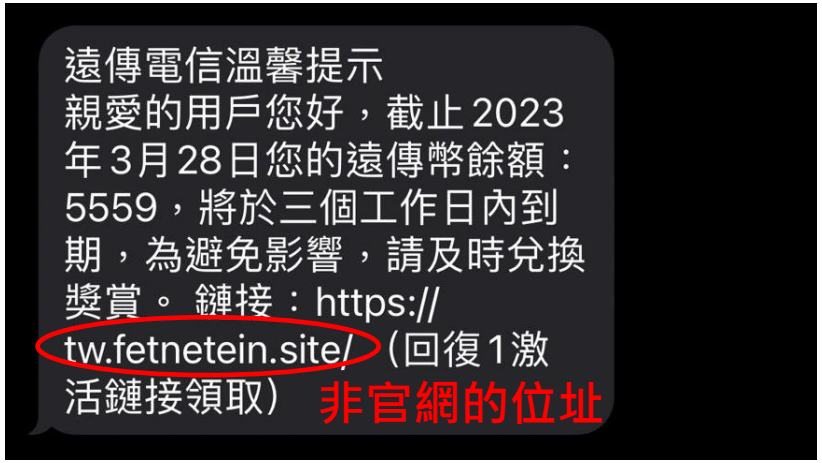


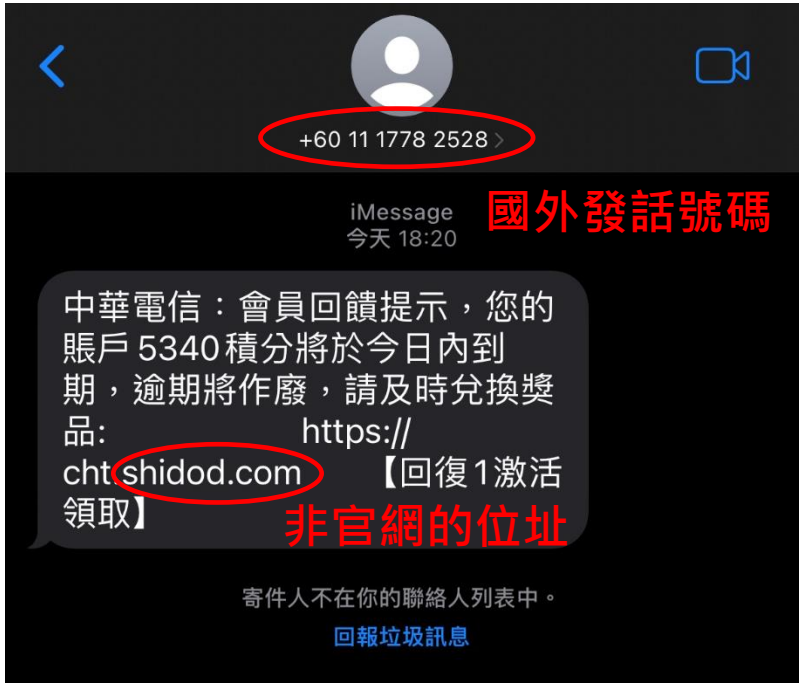
- 網址重新導向或短網址
  - https://www.example.com/login.html?redir=https://www.fake.site
  - https://goo.gl/wbJJxL
  - https://ppt.cc/flhXKx

信箱容易偽造，不可輕信


Victim-1qaz2wsx3edc
垃圾郵件 ×
victim@gxail.com
寄給 victim@gxail.com
上午11:35 (9 分鐘前)
請謹慎處理這封郵件
Gmail 無法驗證這封郵件是否確實來自 victim@gxail.com，請勿點選郵件中的連結、下載附件，或在回覆郵件時提供你的個人資訊。
檢舉詐騙電子郵件
I am well aware yourpassword is your pass. Lets get straight to point. You may not know me and you are probably thinking why you're getting this email? Not one person has paid me to investigate you.
actually, I installed a malware on the X videos (pornography) web site and guess what, you visited this web site to experience fun (you know what I mean). While you were watching videos, your internet browser initiated operating as a Remote control Desktop that has a keylogger which provided me accessibility to your display screen as well as cam. Just after that, my software obtained your entire contacts from your Messenger, Facebook, as well as e-mail . After that I created a double-screen video. 1st part shows the video you were viewing (you have a nice taste :)), and 2nd part displays the view of your cam, & it is you.
You got only 2 choices. Let us explore these types of choices in aspects:
1st solution is to just ignore this email. In this situation, I will send your actual recorded material to every one of your contacts and just consider about the awkwardness you can get. And consequently if you are in a committed relationship, how it will affect? In the second place alternative should be to compensate me $7000. We are going to call it a donation. Then, I most certainly will asap remove your video recording. You can keep on your life like this never happened and you will not ever hear back again from me.
You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in Google). BTC Address: 3MVikLH1GbsvYa8bXVGScgZLXP1tVNH9o4

行動裝置上的惡意釣魚訊息 (1/4)





請各位用戶務必留意：

1. 勿點擊不明網域連結(如：chtcoonm-vip、cutt.ly、chttrad.top)，且留意詐騙簡訊內容經常包含錯字("賬"戶)、簡體字(回"复")或大陸用語(激活、鏈接)。
2. 勿直接留下個人資料或輸入帳戶、密碼，Hami Point服務皆採中華電信會員(網址https://member.cht.com.tw/)認證，完成會員認證或使用Hami Pay APP登入後才能使用點數。

刑事局會請電信業者配合阻擋對釣魚網站的DNS解析

中華電信 Chunghwa Telecom

Ref: https://www.mygopen.com/2023/03/fake-msg.html
https://news.ltn.com.tw/news/society/breakingnews/4489318
https://hamipoint.cht.com.tw/news/77/view

行動裝置上的惡意釣魚訊息 (2/4)

Your code is 852537.Goods is on hold
s.id/1KNuc
Keep it safe

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

經 Google 技術強化 進階搜尋 A

首頁 / 公告訊息 / 公告事項

XML JSON

公告事項

發布日期：112-06-02 更新日期：112-06-02 發布單位：刑事警察局公共關係室

「配送地址有誤」！全民小心落入「釣魚簡訊詐騙圈套」

刑事局發現近期有大量「偽冒驗證碼及包裹追蹤連結」之釣魚短網址，內容：「Your code is 852537.Goods is on hold s.id/1KNuc Keep it safe」，誘使被害人點擊後以為包裹配送地址有誤，而至包裹追蹤頁面輸入自身之信用卡資料，詐騙集團即同步取得相關資訊盜刷信用卡，造成民眾財物損失。

釣魚簡訊往往會附帶來路不明的網站連結，點擊後可能誘導民眾前往詐欺集團所製作的偽冒網站頁面，如民眾信以為真，依該網站頁面填輸自身資料，歹徒將同步蒐集相關資訊以進行犯罪，刑事局提醒當接收附帶短網址連結之訊息，如不慎點擊進入頁面，應詳加查證所引導之網站是否與該公司公布之官方網站相同，亦可透過網域名稱來分辨真偽；如信用卡資料不慎外洩而遭盜刷，可先電話撥打信用卡客服申請止付，並立即向警方報案以確保自身權益。

刑事局呼籲，如民眾發現釣魚網站或可疑訊息，可前往「165全民防騙官網或警政服務APP」，填入基本資料(姓名、連絡電話)後，並於註解說明欄位中提供發訊者資訊、簡訊內容等資訊，再將訊息截圖後上傳送出，即可由165專線查處，如有任何疑問亦可撥打165反詐騙諮詢專線即時查證。

正牌網頁

冒牌網頁及
詐騙簡訊

Ref: https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1887&serno=bed71cfe-be00-424d-9e1d-fa4ce127a191

行動裝置上的惡意釣魚訊息 (3/4)

您未繳費？Google RCS釣魚簡訊增加 男點網址遭盜刷8萬

2023-11-05 14:48 聯合報／記者李奕昕／台北即時報導

＋詐騙集團

讚 22 分享 分享

政府加強防堵釣魚簡訊，今年手機簡訊、蘋果手機iMessage訊息的釣魚簡訊下降，詐騙集團上月起轉移至Google RCS發送釣魚簡訊，黃姓男子收到誤以為忘記繳交國道通行費，輸入信用卡資料遭盜刷8萬元。

上班族30歲黃姓男子近期收到Google RCS訊息，內容為「尊敬的用戶，您好！請您注意，您的ETC費用尚未繳納，請儘快完成繳費以避免影響您的ETC服務使用。如有任何疑問，請登錄我們的官方網站。」他誤以為忘記繳交國道通行費，點擊訊息中網址輸入信用卡資料，遭盜刷8萬元。

詐騙集團透過Google RCS發送釣魚簡訊，謊稱積分即將到期、罰款尚未繳納等，誘使民眾點擊網址輸入個人資料、金融帳戶帳號、信用卡號等，盜刷或盜轉款項。

刑事局說，建議Android手機用戶關閉RCS功能，避免收到釣魚簡訊，若接到夾帶網址的可疑簡訊，勿點擊網址及輸入資料，可至165全民防騙網檢舉，填寫發訊者資訊、簡訊內容等資料，並截圖簡訊內容上傳。

Ref: https://udn.com/news/story/7320/7552899 & 刑事警察局

行動裝置上的惡意釣魚訊息 (4/4)

兩岸詐團冒充公家機關簡訊釣魚 盜刷精品轉售得手逾600萬

#簡訊 #釣魚 #Burberry #10月 ...

發布時間：2023-12-05 19:31 更新時間：2023-12-05 20:42

陳冠勳 陳立峰 / 台北報導

結論先講

國內爆出詐騙盜刷案件，兩岸的不法集團共謀冒充台灣公家機關寄送欠費的釣魚簡訊，包含自來水費、ETC等費用，騙國人在夾帶網址中填寫個資，並使用騙來的信用卡號等資料，從電子票券平台買禮券，或在外國官網刷精品，再從臉書等社團轉賣變現。警方清查，今（2023）年6到10月，不法集團發送超過8000則簡訊，超過百人受害，盜刷金額達600萬。

從超商到百貨，品牌包羅萬象，這家電商平台專賣各類禮券，現在爆出慘遭不法集團盯上，淪為犯罪管道。

員警兵分多路帶回17人到案，涉嫌廣發釣魚簡訊拐騙國人填個資，信用卡號到手後，盜刷大量禮券，透過社群平台半價折扣轉賣，也跑家樂福、全國電子等賣場，用禮券買3C在網路脫手變現。

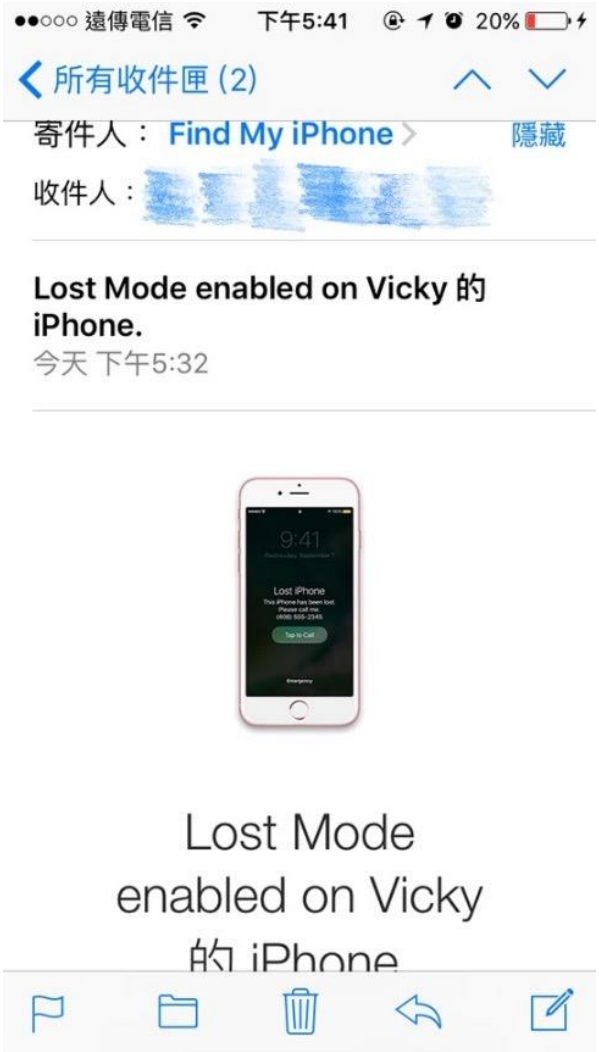
典型釣魚套路，簡訊一寄來就說台水未繳清、停車費逾期，冒充公家機關，要求即刻處理，警方清查今年6到10月發出超過8000則，多達百人受騙，追查還發現中國集團在背後主導。

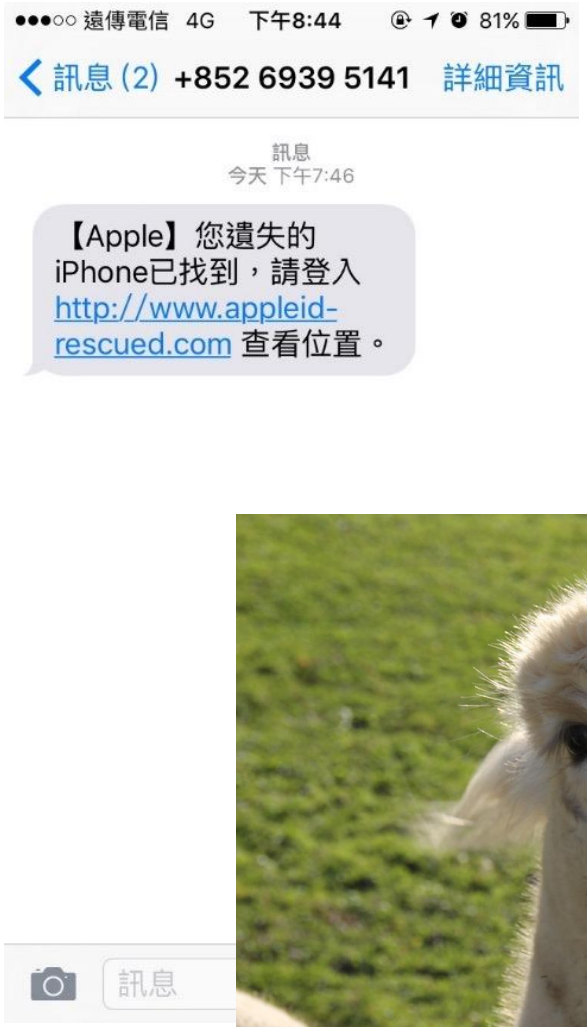
刑事局偵九大隊第三隊長邱承迪說：「境外有主嫌，他是負責架設釣魚簡訊的網站，以及建立釣魚簡訊的範本。」

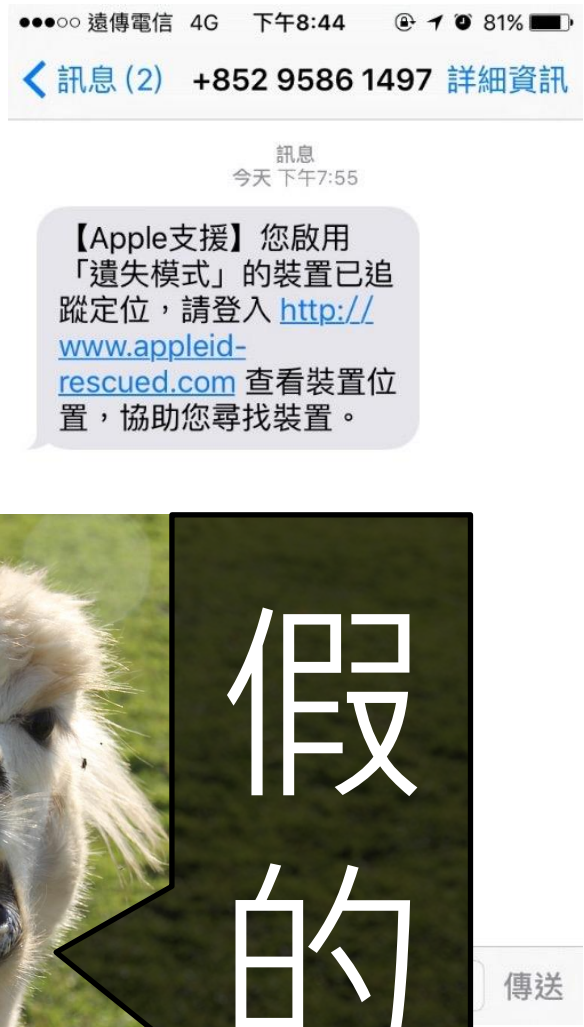
LV背包、LOEWE香水、Burberry服飾通通擺上桌，嫌犯不僅買禮券，精品也刷好刷滿，官網購買後，從臉書等社團將正品原價打1折，轉手找下家，更趁電商平台祭出滿千送百活動，把犯案用的手機門號大量辦會員，扮演買家與賣家用假交易賺價差。

Ref: https://news.pts.org.tw/article/670006

Case: Find My iPhone釣魚郵件

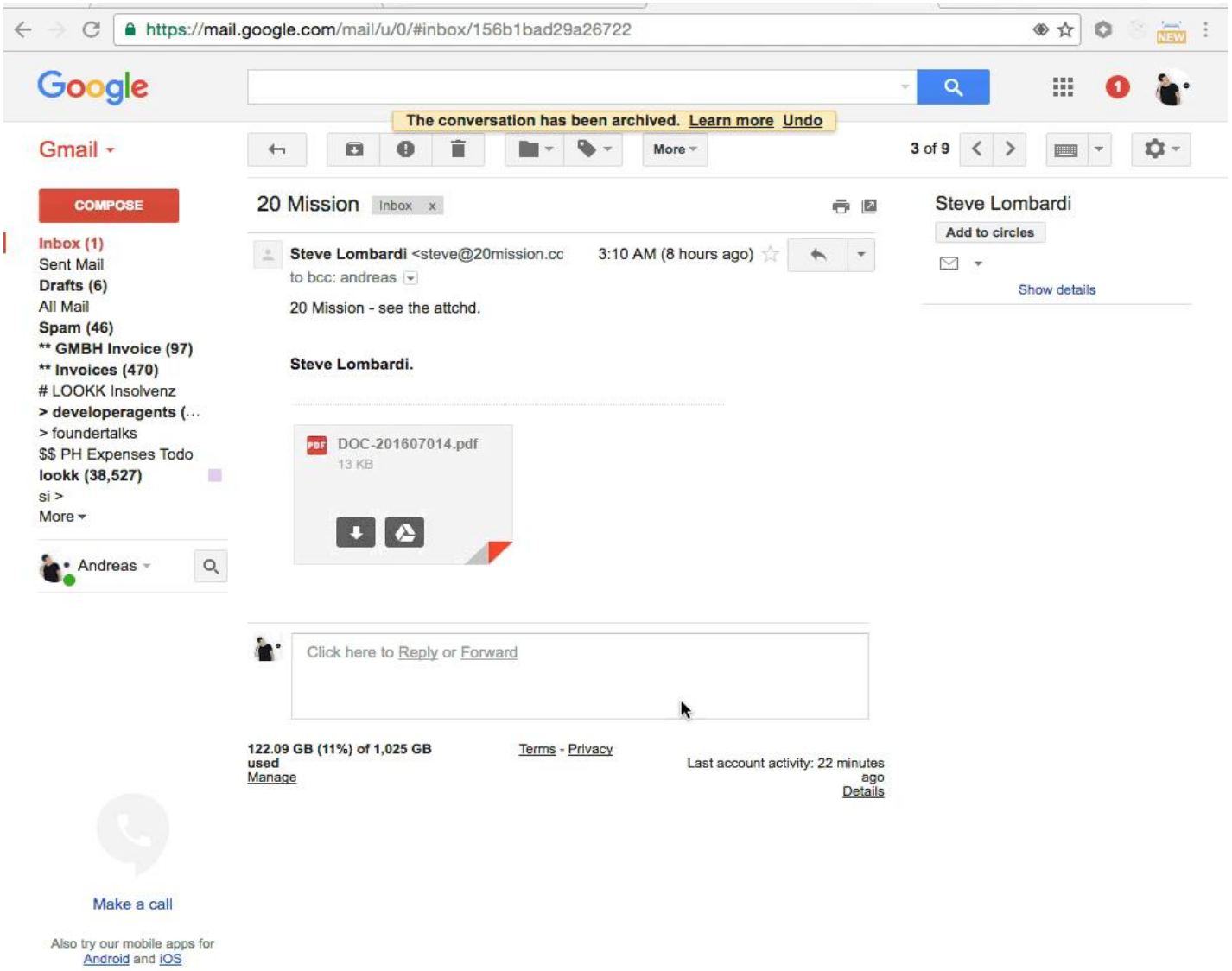






中華電信 Chunghwa Telecom

Case: 附加檔案偽裝-圖片+超連結



- 透過圖片與超連結偽裝成附件，誘使人點擊下載
- 偽造官網登入畫面誘騙受害人輸入帳號密碼

Demo: Fake365 釣魚網站

Office 365

Sign in with your organizational account

someone@example.com

Password

Sign In

Keep me signed in

Most Common Passwords of 2023

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	123456	< 1 Second	4,524,867
2	admin	< 1 Second	4,008,850
3	12345678	< 1 Second	1,371,152
4	123456789	< 1 Second	1,213,047
5	1234	< 1 Second	969,811
6	12345	< 1 Second	728,414
7	password	< 1 Second	710,321
8	123	< 1 Second	528,086
9	Aa123456	< 1 Second	319,725
10	1234567890	< 1 Second	302,709
11	1234567	< 1 Second	234,187
12	123123	< 1 Second	224,261
13	111111	< 1 Second	191,392
14	Password	< 1 Second	177,725
15	12345678910	< 1 Second	172,502
16	000000	< 1 Second	168,653
17	admin123	11 Seconds	159,354
18	1111	< 1 Second	144,262

RANK	PASSWORD	TIME TO CRACK IT	COUNT
19	P@ssw0rd	< 1 Second	135,424
20	root	1 Second	122,834
21	654321	< 1 Second	109,908
22	qwerty	< 1 Second	109,836
23	Pass@123	5 Minutes	105,505
24	112233	< 1 Second	100,920
25	102030	< 1 Second	99,612
26	ubnt	1 Second	98,743
27	abc123	< 1 Second	94,698
28	Aa@123456	11 Seconds	90,414
29	abcd1234	< 1 Second	86,921
30	1q2w3e4r	< 1 Second	86,486
31	123321	< 1 Second	83,206
32	qwertyuiop	< 1 Second	79,434
33	87654321	< 1 Second	79,310
34	987654321	< 1 Second	78,452
35	Eliska81	3 Hours	75,755
36	123123123	< 1 Second	73,033

不安全的密碼：

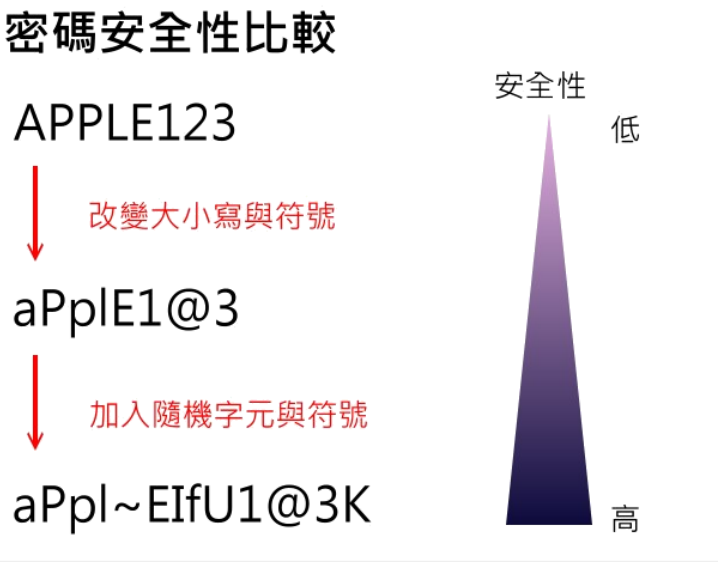
- 數字/字母順序
- 鍵盤排列
- 英文單字
- 缺乏複雜度

Ref: https://nordpass.com/most-common-passwords-list/

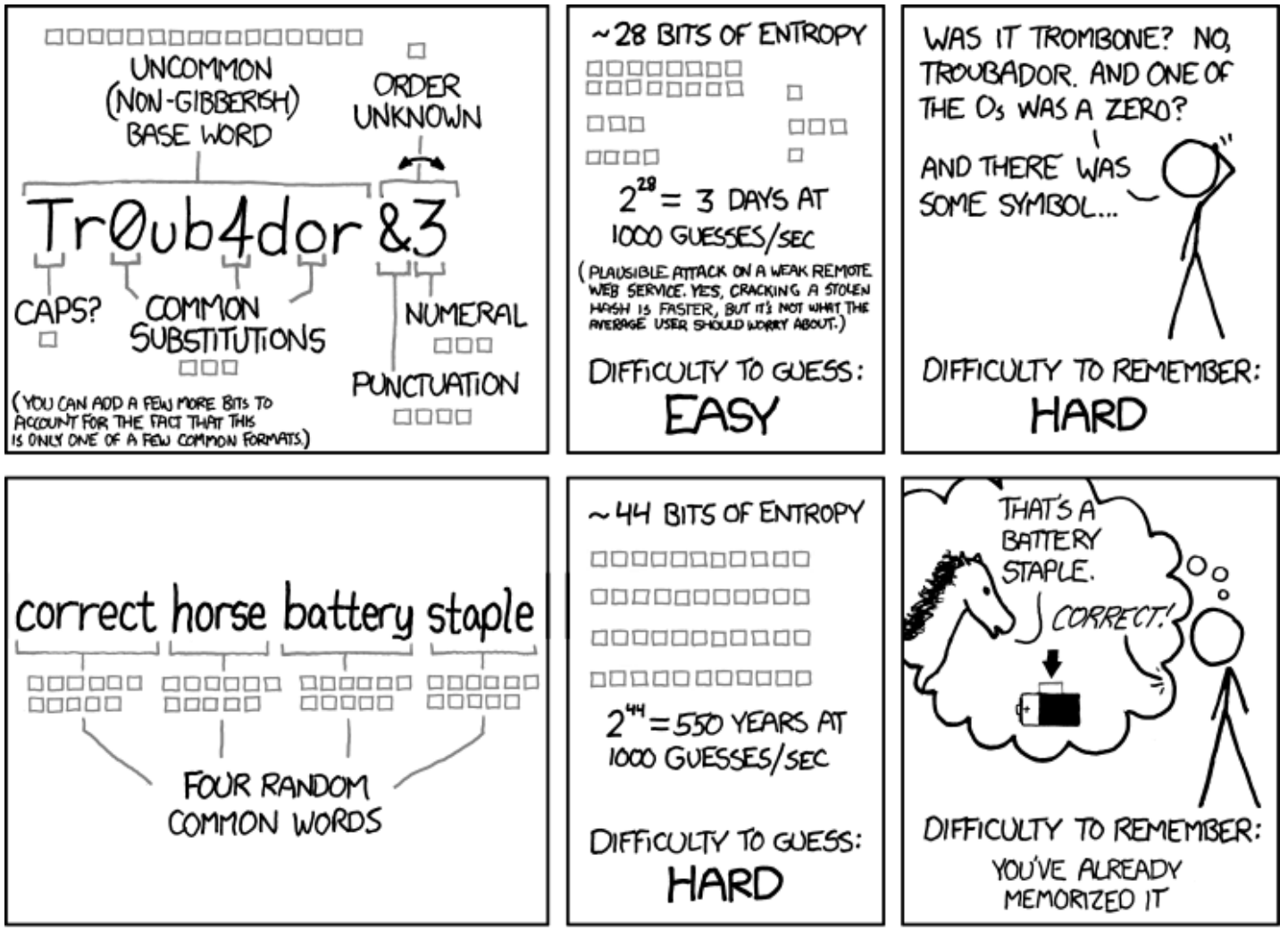
密碼強化策略

- 避免使用駭客易猜的密碼
- 不要跨服務重複使用
- 定期更換
- 提高密碼複雜度

1.重複或者順序數字密碼
2.英文單字密碼
3.鍵盤排列密碼 (駭客知道鍵盤排列會符合密碼規則)
4.生日密碼 (實際上變動位數只有六位19xx xx xx)
5.中文姓名拼音/注音密碼 (對岸駭客也懂)



★密碼長度是重點



Ref: https://xkcd.com/936/

密碼安全最重要的一件事情

- 2FA (Two Factor Authentication)，兩步驟驗證機制
  - ✓除了傳統帳號密碼外，使用如：OTP(一次性密碼)、晶片卡、生物因子認證器等方式進行第二重身分驗證
- Google、Microsoft、Facebook、Yahoo等各大服務幾乎都有支援，請一定要啟用
- 好處：
  - ✓假使密碼真的外洩了，2FA是另一道防線
  - ✓可以協助偵測到有人在嘗試登入你的帳號...等
  - ✓但絕對不是意味著我們可以~~使用懶人密碼~~

Google

Microsoft

Passkey無密碼成未來趨勢

Passkey 登入免密碼將取代傳統方式，可抵擋網路釣魚威脅

作者 陳 冠榮 | 發布日期 2023 年 02 月 14 日 16:10 | 分類 app , 網路 , 資訊安全 分享 分享 Follow 讚 40 分享

相較於傳統密碼輸入的登入方式，由 FIDO 聯盟和 W3C 聯手蘋果、Google、微軟等共同推動的「Passkey」標準更加安全，不必輸入密碼，愈來愈多服務和裝置將支援 Passkey。

「Passkey 是未來保護網路安全的基本做法，本質上更加安全，更能抵禦網路釣魚等威脅」，網際網路安全中心（Center for Internet Security，CIS）技術長 Kathleen Moriarty 指出，Passkey 是由 FIDO 聯盟（Fast IDentity Online Alliance）和全球資訊網聯盟（World Wide Web Consortium，W3C），與蘋果、Google、微軟等指標性公司合作建立的無密碼登入標準，這些公司的平台支援 Passkey，以 Passkey 取代密碼輸入的服務和組織也不斷增加。

當一項服務採用 Passkey 標準時，無需輸入密碼，用戶只要在信任裝置同意登入，就能獲得帳號使用權限。若他人試圖使用密碼登入服務，系統因向用戶持有的手機等裝置發送通知，必須輸入 PIN 碼或通過臉部、指紋辨識等生物辨識方式才能登入帳號，多了一道重要的身分驗證關卡。

密碼安全有個存在已久的問題是，為了易於記住密碼，人們傾向在不同平台上使用相同或非常相似的字串當做密碼，通常包含個人資訊如英文名字、生日、電話號碼等，密碼強度不高。還有更糟糕的是，選用簡單易猜的密碼（如「abc123」或「password」），如同為駭客創造絕佳的攻擊機會。這也意味著駭客只要取得單一網站或 App 的密碼，有機會入侵用戶多個帳號。

Passkey 則解決這個問題，它為每位用戶使用網站或 App 提供單獨的身分驗證，每次加密都不相同。從安全的角度來看，Passkey 比密碼輸入安全得多。

Passkey 因有蘋果、Google、微軟三大廠撐腰，像是適用於 iPhone 的 iOS 16 以及 Mac 電腦的 macOS Ventura 已支援 Passkey，Google 自 2022 年 12 月起也對 Android、Windows、macOS 上的 Chrome 瀏覽器給予支援。

三大廠各自已有雙重驗證、多重要素驗證等機制，通常以原本帳號密碼伴隨信任裝置來驗證身分。驗證程序也不盡相同，像是登入蘋果需要輸入 Apple ID 驗證碼，Google 則是要求用戶開啟特定 App 來允許 / 拒絕登入。而 Passkey 強調不需輸入密碼就能跨平台和裝置使用，並為用戶提供一致的登入體驗。

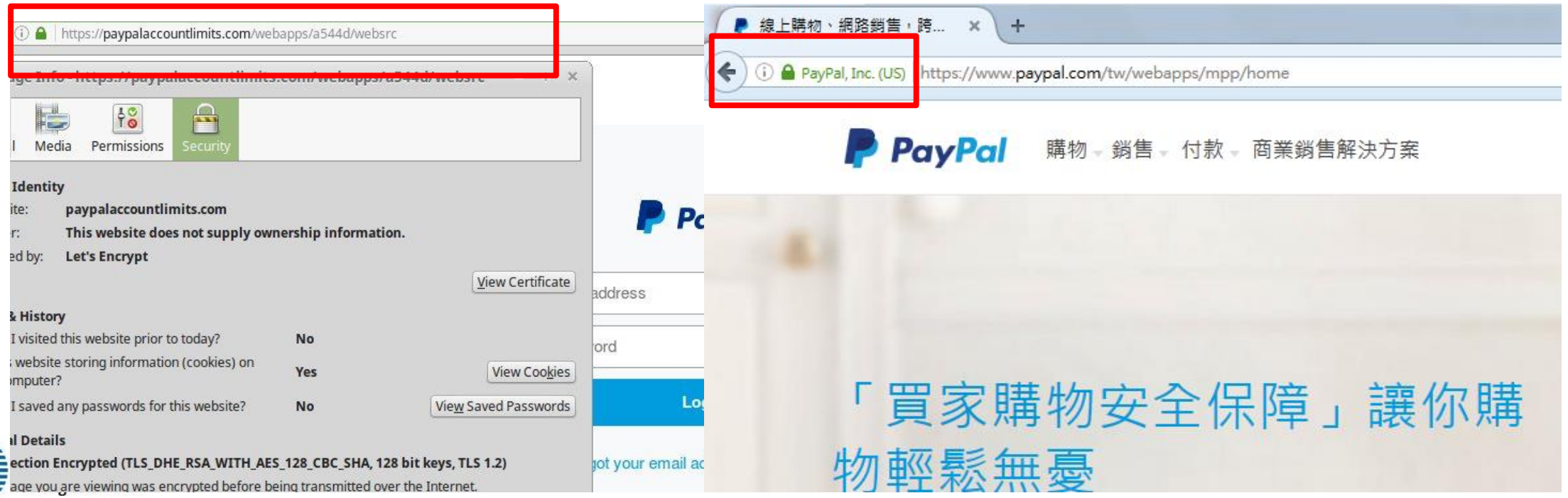
儘管 Passkey 正在加速普及，仍是一種相對較新的登入方式。Passkey 的潛在缺點是，一旦用戶遺失用於登入驗證的信任裝置時，必須立即重置 Passkey，以防遭到他人冒用。建議手邊要有備用機，防範這類狀況發生。

微軟數位防禦報告指出，現今網路犯罪不停增加，密碼攻擊次數飆升至平均每秒約 921 次攻擊，一年內成長 74% 相當驚人。無論如何，用戶應採取如 Passkey 等安全登入措施，或使用密碼管理工具以及高強度的密碼，好好保護自己的帳號以及個人資料。

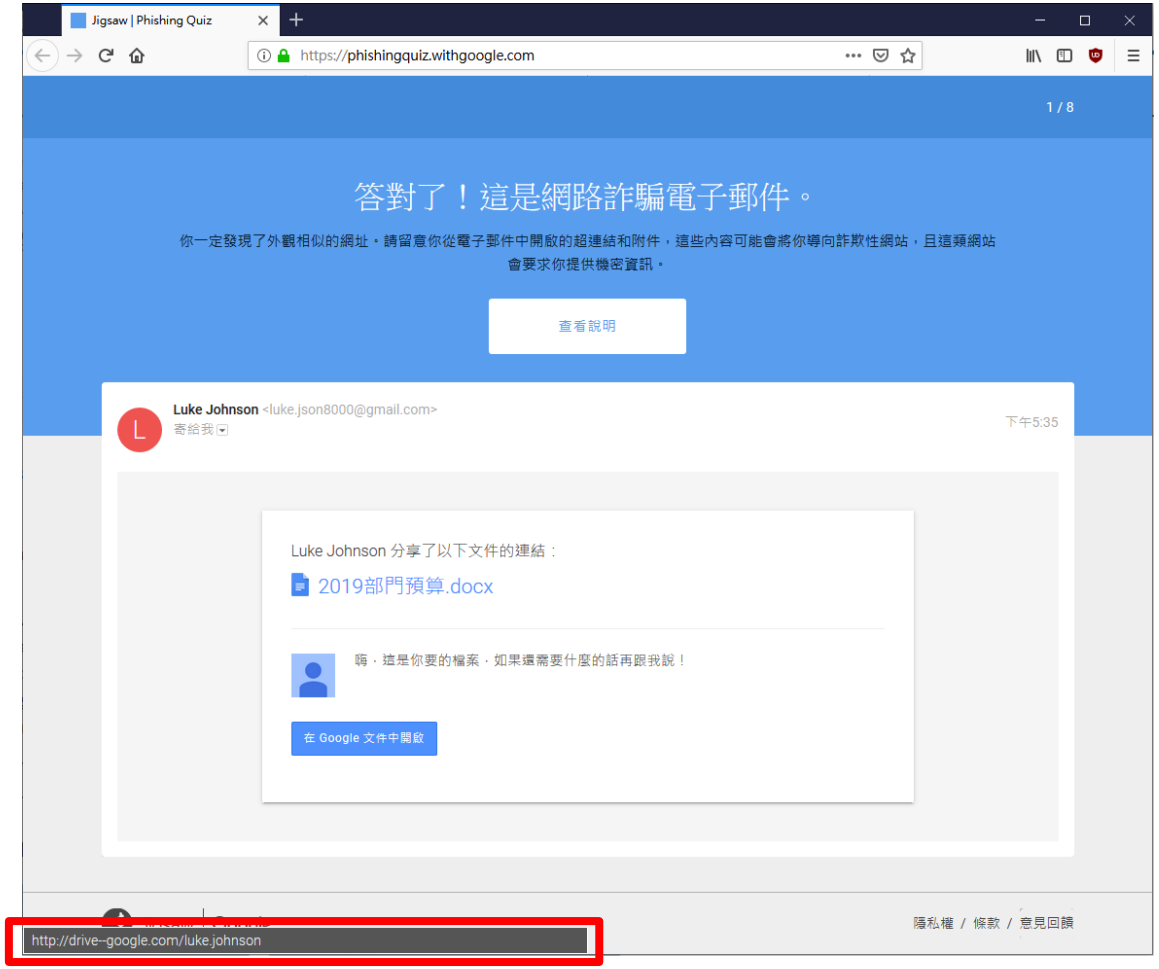
Ref: https://technews.tw/2023/02/14/apple-google-microsoft-are-pushing-more-users-towards-using-passkeys-over-passwords/

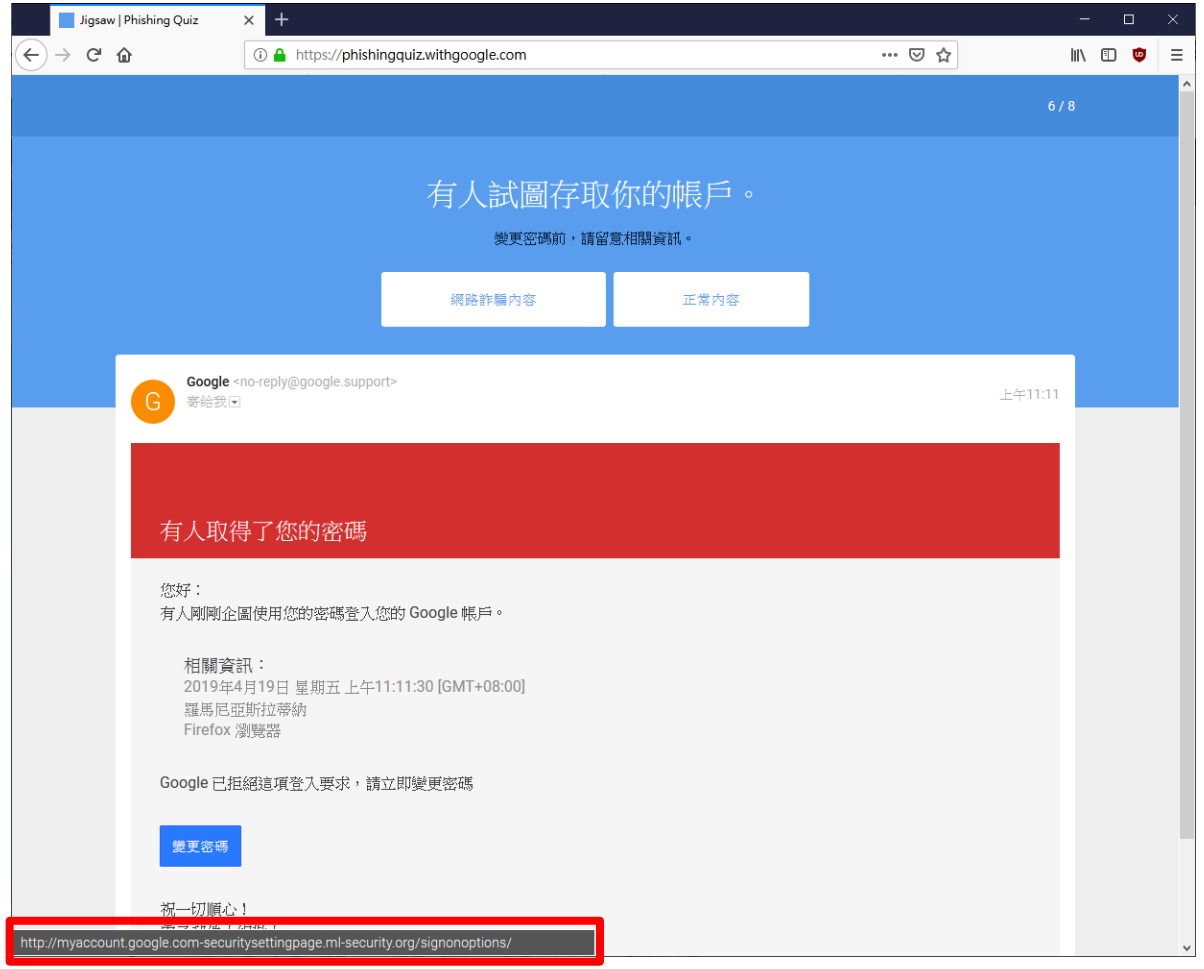
網站信譽與網址正確性檢查

- 確認網址列的網址
  - 重要的網站如網路銀行，網址的起頭是否是https開頭
  - 通常都會有EV憑證驗證其身分
  - 以Paypal為例:



Google釣魚網站小測驗





中華電信 Chunghwa Telecom

Ref: https://phishingquiz.withgoogle.com/

卡巴斯基對於防範釣魚攻擊的建議

- 對付這類攻擊沒有萬靈丹
  - 調整服務設定(例如關閉自動接受行事曆)雖然有效但也會影響到正常的
- 攻擊者永遠會找到新的手法
- 我們可以怎麼做降低受害機會？
  - 不要開啟**來源不明的訊息**
  - 不要接受**不認識人員發送的邀請**
  - 不要點擊你**並未預期會收到的訊息內的連結**
    (Do not tap or click links in messages you weren’ t expecting)
  - 安裝有Antispam模組的**網路安全/防毒軟體**可再擋掉一些網路服務(如微軟、Google)未能過濾掉的釣魚或垃圾訊息

Ref: https://www.kaspersky.com/blog/spam-through-google-services/27228/

美國CISA對於防範釣魚攻擊的建議

- 阻擋誘餌：**網路邊界強化**，如驗證郵件合法性、將封鎖清單或威脅情資匯入資安設備(如防火牆)攔阻
- 不被誘騙：增進員工對釣魚郵件識別能力、在**所有通訊平臺**都應保持警惕
- 回報：將可疑郵件**回報公司資安團隊**、**不要轉寄給其他人**、組織要有應變團隊確認事件及防範入侵範圍擴大
- 保護：遵循最小權限原則、審查並減少可存取關鍵資料與設備的帳號數量，對密碼共享與重複使用做出限制，防止權限提升、取消用戶不必要的高權限、執行釣魚演練、做好安全更新、增加端點與EDR防護，以及實施軟體限制政策等

Ref: https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf

其他可以注意的地方

- 從自己做起，前面防的再多**終究還是會有漏網之魚**
- 郵件
  - 不隨意點擊**不認識的寄件人**提供的附件與連結
  - 如果網址是使用**短網址**或**註冊相似網域**則更要小心
  - 不要被對方的「緊急需求」帶著走，該怎麼做就還是怎麼做
- 手機
  - 政府或是公用事業通告會透過**專有識別短碼**以降低詐騙冒用，如111、165、1922
  - 看到簡訊發話號碼有**國碼(+86、+886)**要提高警覺
  - 不要隨意點掃**不認識的寄件人**發送簡訊內的連結、QR Code
  - 如果網址是使用**短網址**或**註冊相似網域**則更要小心
  - 公用事業**欠費**、**罰單**、**法院文書**、**快遞未投遞**等都是近期常見題材

Photo: https://captainverify.com/blog/phishing.html

網路釣魚(Phishing) - Line、Facebook社群詐騙

中華電信 Chunghwa Telecom

Line、Facebook社群詐騙 (1/7)

Line、Facebook社群詐騙 (2/7)

Ref:

1. https://www.ettoday.net/news/20180626/1199371.htm
2. https://news.tvbs.com.tw/life/973677

Line、Facebook社群詐騙 (3/7)

領飆股先加LINE？小心陷入詐騙三部曲

2021-10-13 10:35 經濟日報 / 記者孫靖媛、黃靖文、蔣明倫、邱力行/即時報導

近來許多民眾反應在手機簡訊、臉書，或其他的**社群媒體**上，收到類似的 「加賴送飆股」訊息，不論是出於好奇或是想進一步了解的心態，一旦加賴，可能就已落入有心人的詐騙套路三部曲了。

根據刑事局提供資料顯示，近三年台灣的投資詐欺案，以及受害者財物損失逐年攀升，去年被害人受騙財損金額就突破10.2億元，今年1-7月，詐騙案件數亦突破2,500件、損失金額直逼9億元。

這些看似簡單又無害的加賴手法，是怎麼搬走民眾口袋裡的錢呢？

投資有風險 心態正確慎選合法平台

時代在走，詐騙集團的數位技術也不斷進化。證券商公會及投信投顧公會再三提醒投資民眾，切記三不三要，不要讓手機變詐機。投資心態要正確，若有穩賺不賠的飆股就要小心是詐騙，另外也提醒民眾一定要有資安意識，只要出現要求匯款、轉帳，就要提高警覺。

投資詐騙首部曲：拉入群組

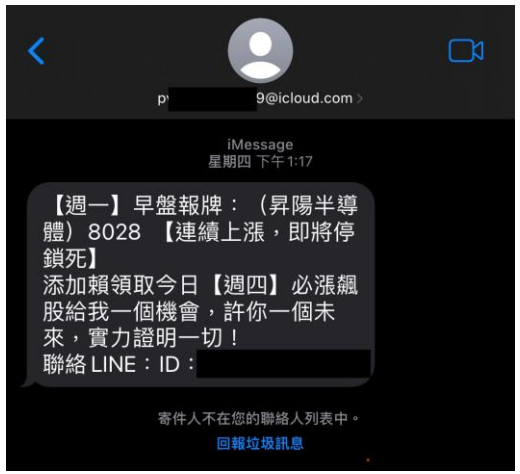
- 透過簡訊、社群網站要受害人加Line進入投資群組

二部曲：暗樁洗腦貼對帳單給你看

- 推薦飆股、港股、美股、未上市股票、加密貨幣
- 群內有暗樁跟老師一搭一唱

三部曲：收割後人間蒸發

- 設法誘使受害人加入假投資、博弈網站，讓受害人嘗甜頭
- 當受害人投入金額多了之後人間蒸發



Ref: https://udn.com/news/story/7320/5812735

Line、Facebook社群詐騙 (4/7)

【詐騙】臉書社團買二手商品，要求私訊並用LINE Pay先付款？詐騙得手就封鎖！

2021/12/3

臉書上有許多販賣商品、二手貨的社團或是粉絲專頁，提供民眾簡便的平台撿便宜、輕鬆找到想要買賣的貨品。不過，最近 MyGoPen 收到不少民眾的詢問，發現很多買家在透過「電子支付」，如 LINE Pay 先付款後，賣家就「人去樓空」！不止商品拿不到，還損失了錢財。MyGoPen 為您解析相關詐騙手法，遇到這些疑點都要提高警覺！

通常會在社團看到這樣的貼文版本：

因搬家 閒置大量全新物品 銅板價 需要私訊
哈曼卡頓3代音響一個
小米S5掃地機器人一個
LV包包一个
氣炸鍋一個
Dyson吹風機一個
DJ無人機一個
三代藍牙耳機一個
鞋子穿著有點小，一次沒穿過，一雙
大同電鍋一個
任天堂遊戲機一個
縫紉機一組
樂高玩具一組
蘋果手錶一個
滑板車一個
需要私訊

如何判斷賣家是否為詐騙?

- 張貼販售多樣商品，標榜分手、搬家便宜出售
- 藉此吸引民眾私訊或是留言

各種推託就是不願意面交

- 告知距離很遠不方便
- 即使表示可以面交仍會表示無法確定時間、不是詐騙、可以先去警局備案，來取信被害人

要求使用電子支付

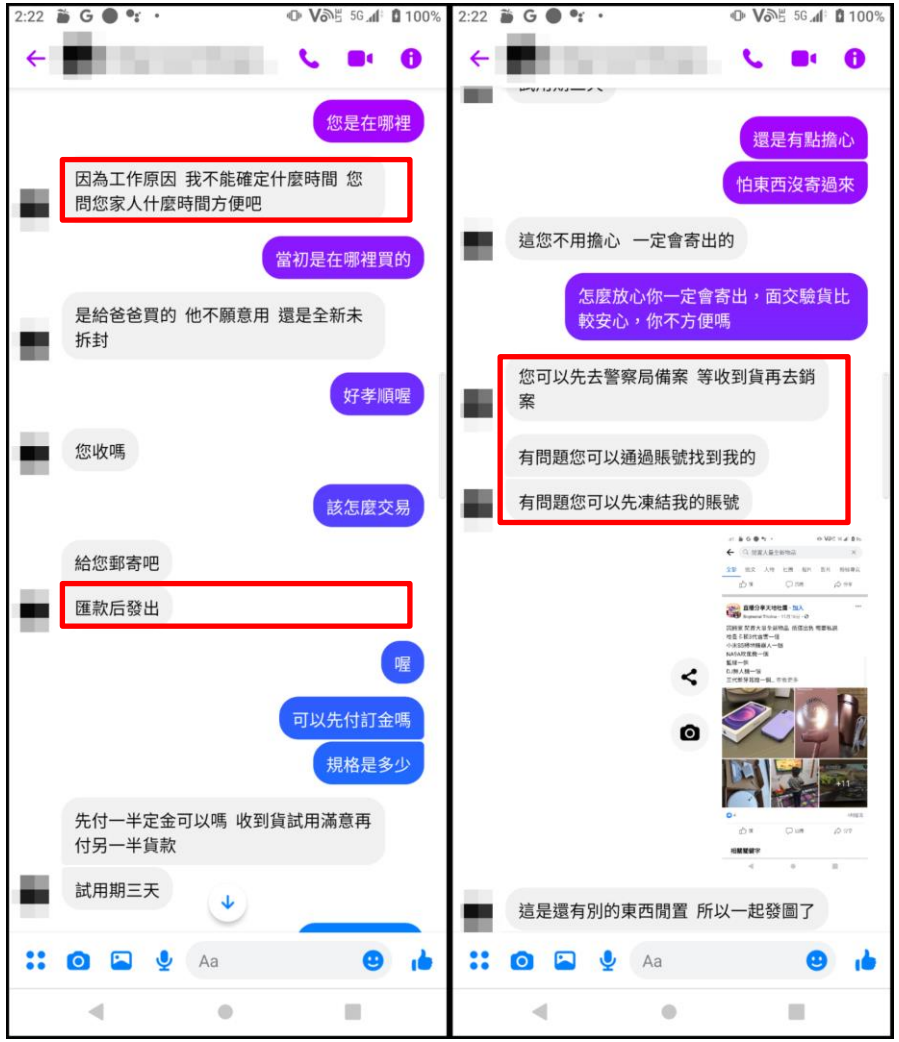
- 例如Line Pay
- 收款之後封鎖被害人，人間蒸發

在FB購買東西應注意什麼?

- 警政署 165 反詐騙專線表示，確實有民眾諮詢，在臉書購買東西，使用電子支付付款後，對方就把他封鎖，後續找不到人
- 如果民眾驚覺自己受騙了，建議應直接去派出所報警處理
- 由於臉書的詐騙案件很多，因此建議民眾盡量少在臉書上購買商品，因為很多賣家資訊並不完整
- 不然盡量以面交或貨到付款，雙方協調後續應如何付款保障雙方權益。如果遇到要先付款才能領貨等情況，建議先不要購買

Ref: https://www.mygopen.com/2021/12/fraud-pay.html

Line、Facebook社群詐騙 (5/7)



中華電信 Chunghwa Telecom

Ref: https://www.mygopen.com/2021/12/fraud-pay.html

Line、Facebook社群詐騙 (6/7)

首頁 > 社會

FB買賣陷阱多 不只買家被騙、連賣家也是目標

2023/10/08 14:50

〔記者姚岳宏 / 台北報導〕正值國慶連假及百貨周年慶期間，也是網購詐欺的高發期，刑事警察局今提醒，不只買東西會被騙，連賣東西也成為詐團鎖定目標，網購時千萬要小心，避免使用臉書、LINE、IG等社群與對方聯繫，而當對方要求操作ATM或網路銀行時，應提高警覺。

刑事局指出，一名洪姓女子在FACEBOOK交易社團向賣家購買二手iPhone，並透過Messenger私訊談交易細節，洪女聽從賣家指示匯款數萬元新台幣後，卻遲遲未收到商品，欲私訊賣家詢問時發現已遭對方封鎖，交易社團貼文也被刪除，洪女求償無門才知遭到詐騙。

警方表示，不只買家遭詐騙，連賣家也是詐騙目標，日前一名邱姓男子在FACEBOOK經營個人賣場，遇到歹徒自稱欲購買商品，但希望以7-11賣貨便交易，請邱男開設7-11賣貨便賣場，待邱男照做後，歹徒又稱邱男「未開通簽署金流服務」無法下單，將假的客服連結傳給邱男，由歹徒同夥假冒客服人員要求邱男依指示操作ATM以完成「帳戶驗證」，邱男依指示操作而遭騙，損失近3萬元。

警方提醒，買家方面應使用安全、有第三方支付及提供退貨、退款服務的購物平台，避免使用FACEBOOK、LINE、Instagram等社群與賣家聯繫，同時也應避免購買價格遠低於市價或是標榜限量、限時搶購等噱頭的商品。

賣家方面，因把自己的訊息公開於網路上，更容易成為歹徒直接下手詐騙目標，網路「賣家」常與陌生「買家」接觸聯絡，每次都是歹徒施展詐騙攻勢的機會，當買家聲稱「無法下單」、「未開通金流服務」、「需帳戶驗證」等話術，並要求依指示操作ATM或網路銀行時，應提高警覺，立即掛斷並撥打110或165反詐騙諮詢專線查證。

☆自由時報電子報提醒您，防詐騙專線：165，報案專線：110☆

Ref: https://news.ltn.com.tw/news/society/breakingnews/4452466

Line、Facebook社群詐騙 (7/7)

Home › LINE › 詐騙

【詐騙】LINE Pay 紅包？查看紅包狀態的連結？山寨活動網站！會騙個資

2024/2/9

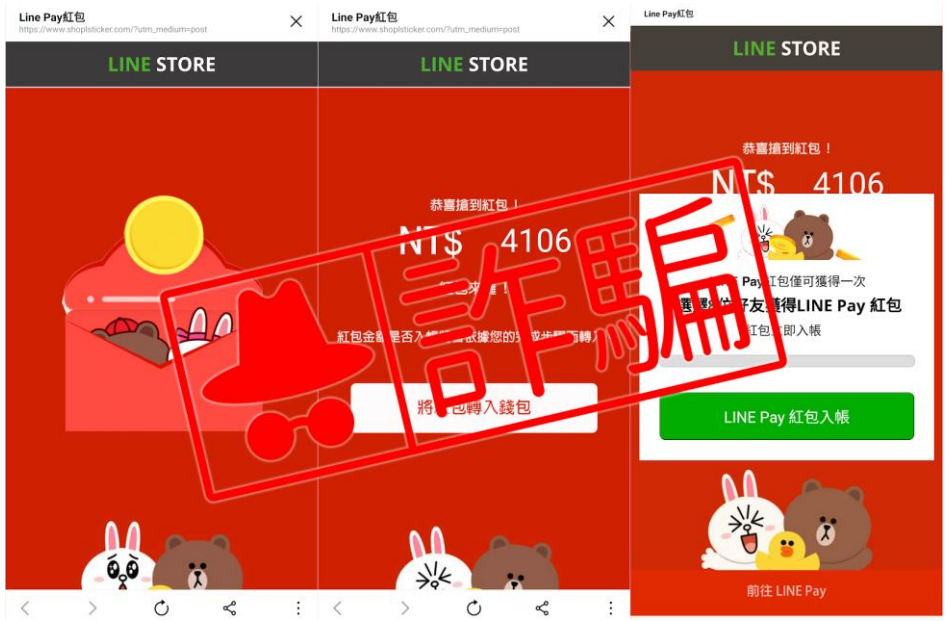
你可以先知道：

（1）LINE 官方並沒有類型的 LINE Pay 領紅包的活動，進入的網址為詐騙網站。

（2）點擊詐騙連結後會誘導分享，後續可能被盜取個資或帳號。

（3）刑事警察局提醒切勿點選連結，務必到官方網站查驗活動真偽。

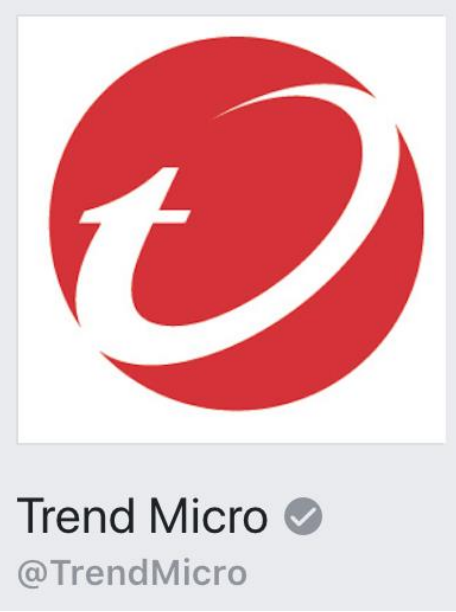
網傳「查看紅包狀態」的 LINE 訊息連結，並要求你邀請多位好友或群組一起領紅包。事實上這是常見騙個資的詐騙手法，是冒用 LINE Pay 的名義設計的假網站。對此警方也提醒民眾切勿點擊可疑連結，務必透過官方網站前往並查證活動真偽，以免遭受詐騙、信用卡盜刷、帳號被盜等風險。



Ref: https://www.mygopen.com/2024/02/red-envelope.html

★Facebook 認明驗證標章(藍勾勾、灰勾勾)

- 藍色標章 表示 Facebook 已經確認那是屬於該公眾人物、媒體公司或品牌的真實粉絲專頁或個人檔案
  - 請注意，某些公眾人物、名人、品牌的 Facebook 專頁可能沒有藍色標章。
- 灰色標章 表示那是屬於該企業或組織的真實專頁



Ref: https://www.facebook.com/help/196050490547892?helpref=faq_content

Line 認明認證帳號(綠盾牌、藍盾牌)

Q：如何辨別帳號？

用戶若要辨識此帳號是否為認證帳號，可至該帳號主頁看左邊之盾牌顏色。管理員若要辨識可至LINE@ App中檢查帳號狀態為承認/一般帳號。

★**藍色盾牌**－認證帳號

★灰色盾牌－一般帳號

★**綠色盾牌**－**官方帳號**

認證帳號　一般帳號　官方帳號

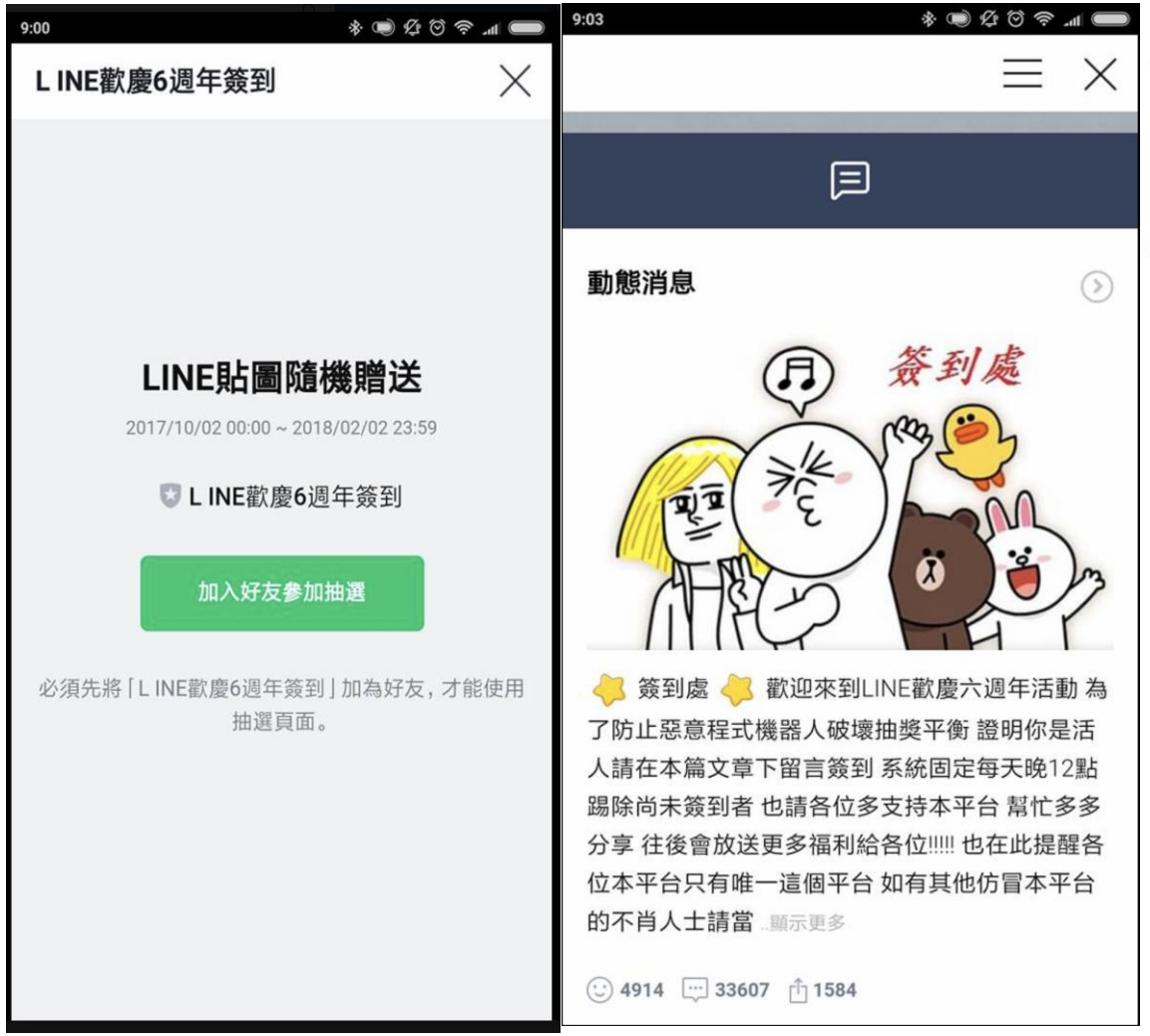
官方帳號

↓

認證帳號

↓

一般帳號



中華電信 Chunghwa Telecom

Line 官方資安宣導

1

知名品牌卻是灰色盾牌

LINE帳號盾牌分為官方帳號的綠色、認證帳號的藍色與灰色的一般帳號

若是知名企業大品牌、卻是灰色盾牌！？要留意

2

以假亂真的假網站

製作假網站、竊取商家影片與圖片讓你誤以為真！先別急著點選網頁，檢查網址、搜尋正版的官方網站比對。

3

分享才能拿貼圖、優惠

求你分享給越多人才能拿貼圖或優惠券？！小心有詐

4

要求加陌生帳號好友

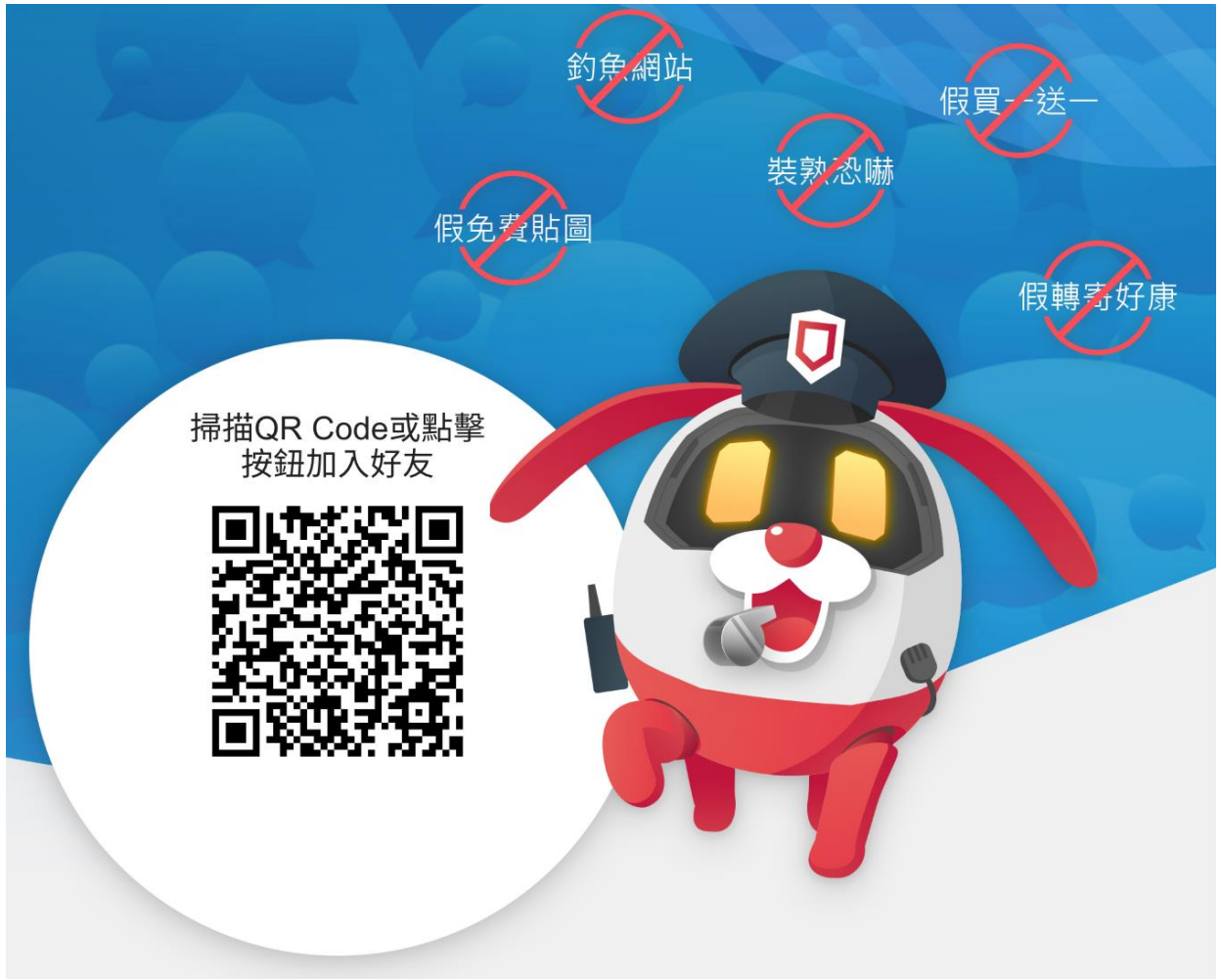
假帳號特徵之一就是希望你加入更多假帳號。

要你加入客服帳號、驗證帳號、詢問主辦單位，點擊後若跳出加好友畫面，這些都要小心！

165 反詐騙宣導

中華電信 Chunghwa Telecom

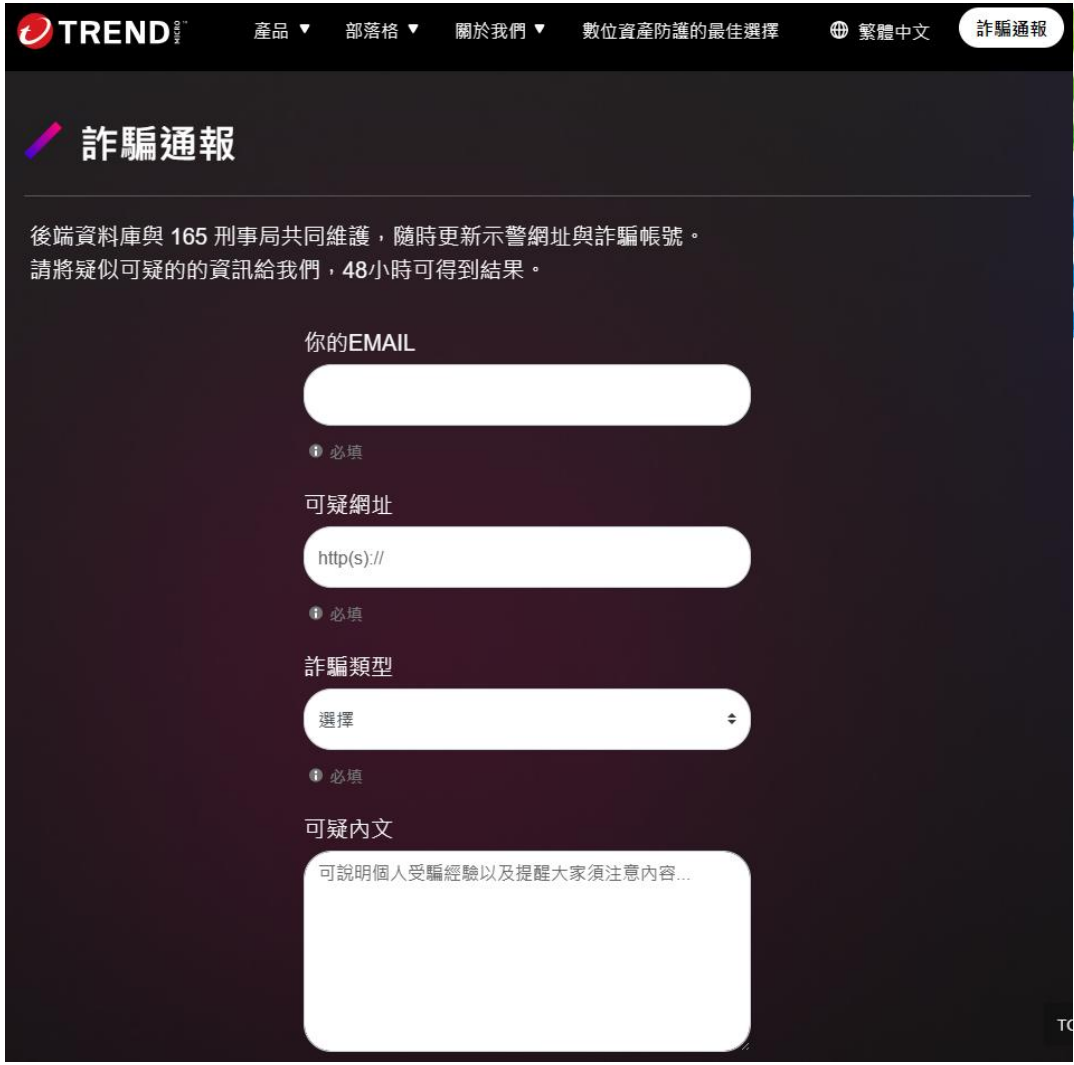
趨勢科技防詐達人(1/2)


釣魚網站
假買一送一
裝熟恐嚇
假免費貼圖
假轉寄好康
掃描QR Code或點擊
按鈕加入好友


113
趨勢科技防詐達人
到Line
貼上網址
【日本進口】高...
NO!
汪！危險！訊息或
網頁內有不安全連
結。
使用說明 | 分享給好友


趨勢科技防詐達人
如果您覺得這不是安全連結，請
回報給防詐達人。
感謝您，汪!
立即回報
點選立即回報
汪，您回報了:
感謝您 汪!
臉書廣告 退貨...
使用說明 | 分享給好友

趨勢科技防詐達人(2/2)



Ref: https://getdr.com/category/recent-new/

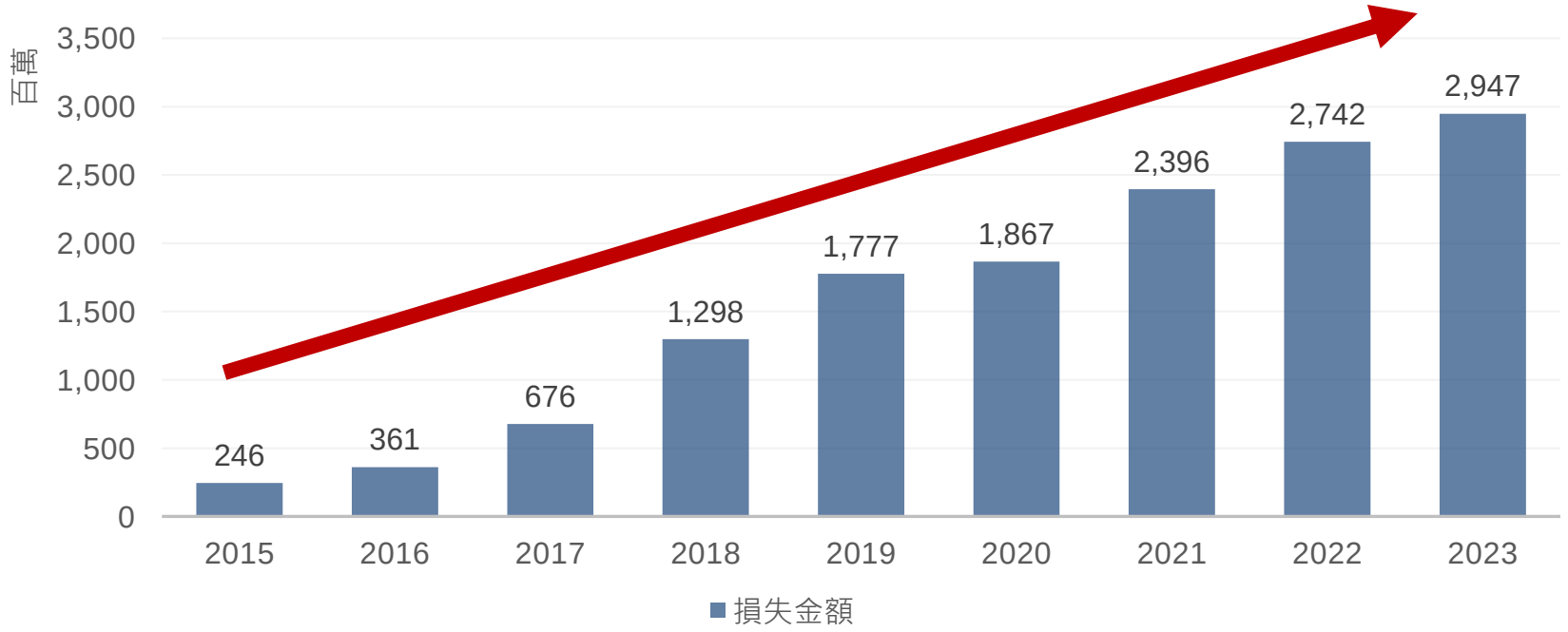
網路釣魚(Phishing) - BEC變臉詐騙

(商業電子郵件詐騙)

中華電信
Chunghwa Telecom

BEC商業電子郵件詐騙簡介

- 商業電子郵件詐騙(Business Email Compromise，亦稱變臉詐騙)，利用**電子郵件假造身分**(跨國公司、高階主管)，取得被害人的信任，藉此進行**詐欺性轉帳**及**騙取財物**
- 美國聯邦調查局統計2023年損失金額來到$2,946,830,270 (29.4億)



Ref: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

BEC數量大幅上升

新聞

您現在位置：首頁 > 新聞

研究：利用企業電子郵件詐騙數量大幅上升

2023 / 05 / 29 - 編輯部

微軟發佈了第四版 Cyber Signals，數據顯示利用企業電子郵件詐騙（business email compromise, BEC）在近期大幅上升，根據微軟觀察，2019 年至 2022 年期間，針對企業電子郵件的網路犯罪即服務（CaaS）增加了 38%。

企業電子郵件詐騙案件正在成長，詐騙成功將使組織每年損失數億美元。根據美國聯邦調查局（FBI）調查報告，有超過 21,000 件企業電子郵件詐騙的投訴，調整後的損失仍超過 27 億美元。2022 年，美國聯邦調查局（FBI）的資產追回小組就針對 2,838 起涉及美國國內交易且潛在損失超過 5.9 億美元的 BEC 投訴啟動了金融詐騙攻擊鏈（Financial Fraud Kill Chain, FFKC）。由此可見 BEC 詐騙對於企業組織的運作已經造成嚴重的衝擊。

BEC 攻擊在網路犯罪產業中之所以能夠脫穎而出，主要來自於其對社交工程與詐騙的了解。在 2022 年 4 月至 2023 年 4 月期間，微軟威脅情報數位犯罪機構偵測並調查了 3,500 萬次 BEC 嘗試攻擊，平均每天嘗試 15.6 萬次。並在 2022 年 5 月至 2023 年 4 月成功下架 417,678 個釣魚網站連結。

常見的 BEC 攻擊手法

威脅攻擊者使用 BEC 詐騙會採取多種形式，包括透過電話、簡訊、電子郵件或社群媒體。偽造身份驗證請求的訊息以及冒充個人或公司身份也是常見的攻擊手法。

BEC 詐騙並不是利用未修補裝置中的漏洞進行攻擊，而是利用每天大量的電子郵件和其他訊息來誘騙受害者提供財務資訊或採取某些行動，如引導受害者在不知情的情況下將資金匯入幫助犯罪分子進行詐欺性資金轉移的洗錢帳戶。

與具有破壞性勒索訊息嘈雜的勒索軟體攻擊不同，BEC 的攻擊者採取一種低調的信任遊戲，利用虛構的截止日期來引誘可能分心或習慣於此類緊急請求的收件者上鉤。BEC 攻擊者沒有使用新穎的惡意軟體，而是將他們的手法與重點放在提高惡意訊息的規模、可信度和提高收件者開信率的工具上。

雖然已經發生了幾次利用住家 IP 位址的攻擊並引發關注，但微軟與執法部門和其他組織一樣擔心這種趨勢可能會迅速擴展，使傳統警報或通知難以偵測到此類活動。

儘管威脅攻擊者已經建立了專門的工具來強化 BEC 詐騙，包括網路釣魚套件和針對領導階層、應付帳款負責人和其他特定角色等已經通過驗證的電子郵件清單，但企業可以採取一些方法來預防攻擊並降低風險。

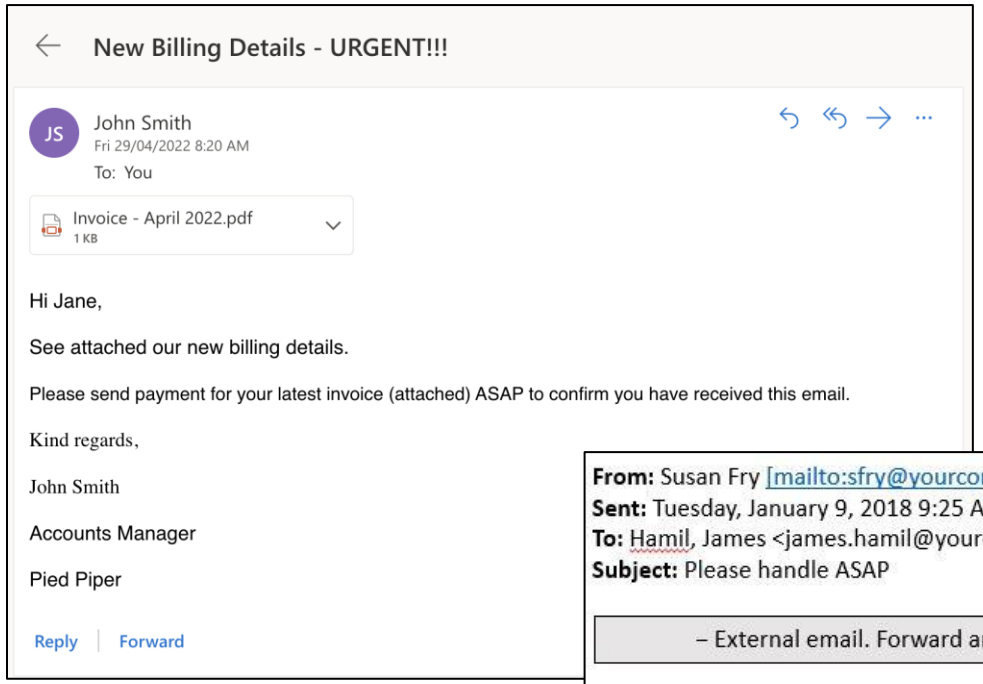
降低網路風險需要透過包含 IT、合規、網路風險管理人員、執行長、領導者、財務人員、人力資源主管以及其他有權存取員工記錄（如身份證字號、稅務報表、聯絡資訊和行事曆）的人員等跨部門一起參與討論並提供解決方案，BEC 的攻擊凸顯跨部門合作的重要性。

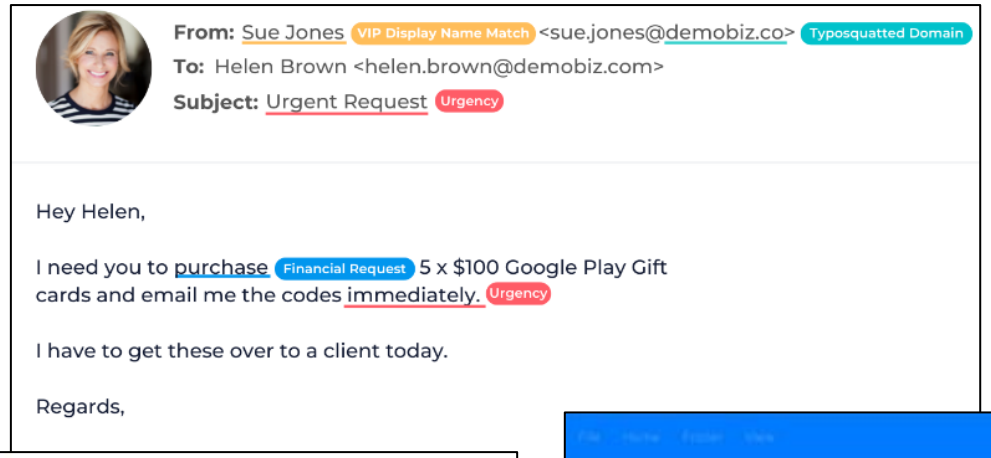
打擊BEC詐騙的建議

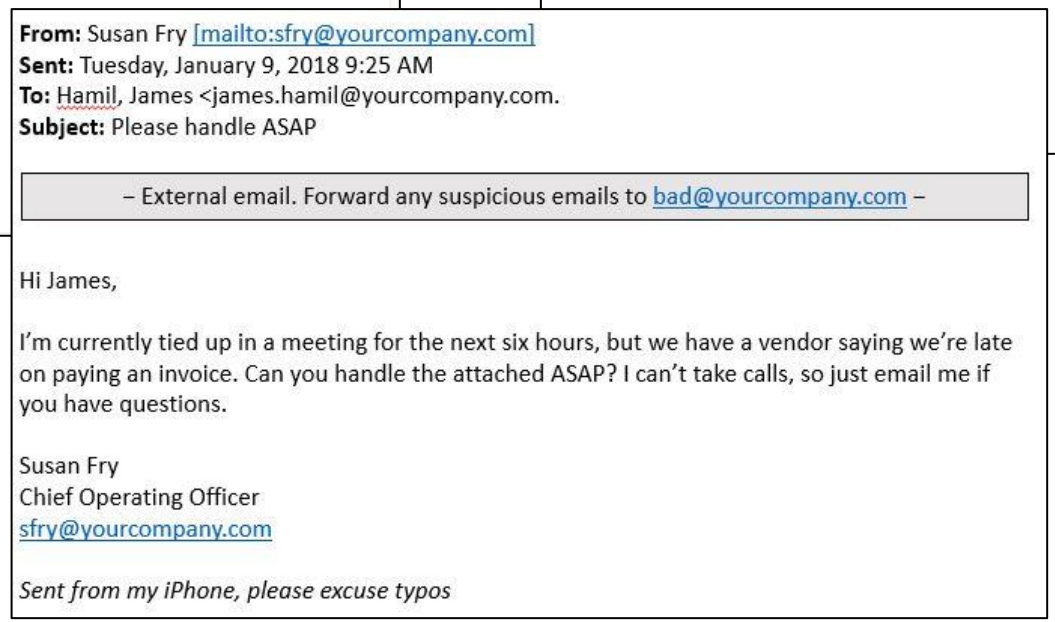
- 使用安全的電子郵件解決方案：現今雲端平臺的電子郵件服務使用如機器學習的 AI 功能來強化防禦，增加進階網路釣魚防護和可疑信件轉發偵測。其中，用於電子郵件和生產力相關的雲端應用還提供持續並自動的軟體更新以及安全政策集中化管理的優勢。
- 保護身份以禁止橫向移動：進行身份識別的保護是打擊 BEC 詐騙的關鍵要點。透過零信任和自動化識別管理來控制對應用程式以及資料的存取權。
- 採用安全的支付平台：建議將透過電子郵件寄送發票的模式轉換成使用專門為驗證付款設計的系統。
- 加強員工對不安全訊號警惕性的教育訓練：持續教育員工如何辨識詐騙和其他惡意的電子郵件，例如網域和電子郵件位址不符，以及了解成功的BEC攻擊所帶來的風險和成本。

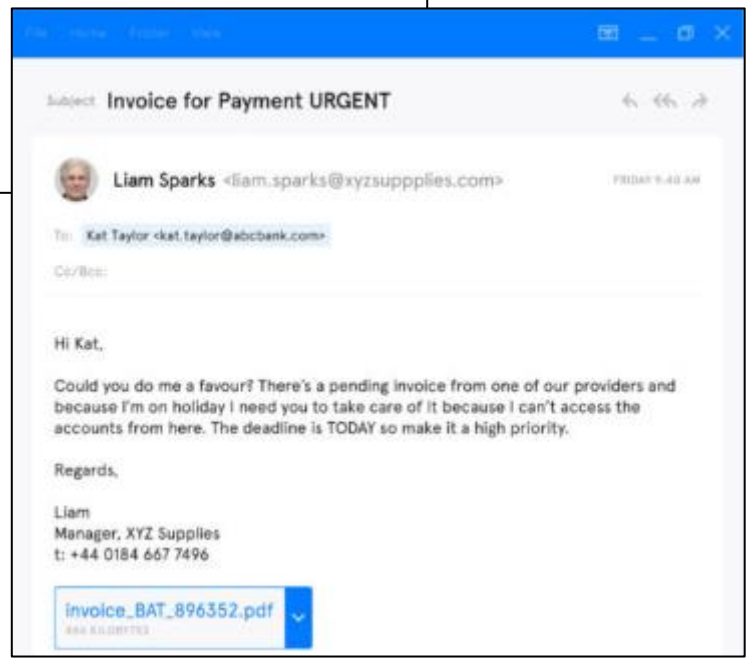
Ref: https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10492

BEC詐騙範例









可能的特徵：

- 偽裝**寄件者身份**
- 但是用**外部信箱**
- 標示**緊急**
- 需要**處理轉帳**，或要求**購買禮物卡**

Ref: https://www.upguard.com/blog/business-email-compromise
https://www.tessian.com/blog/business-email-compromise-bec-examples/
https://www.terranovasecurity.com/blog/examples-business-email-compromise
https://www.terranovasecurity.com/blog/examples-business-email-compromise

BEC佔比不大，但金錢損失最為慘重

2023 CRIME TYPES

By Complaint Count

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		

*Descriptors**			
Cryptocurrency	43,653	Cryptocurrency Wallet	25,815

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

2023 CRIME TYPES continued

By Complaint Loss

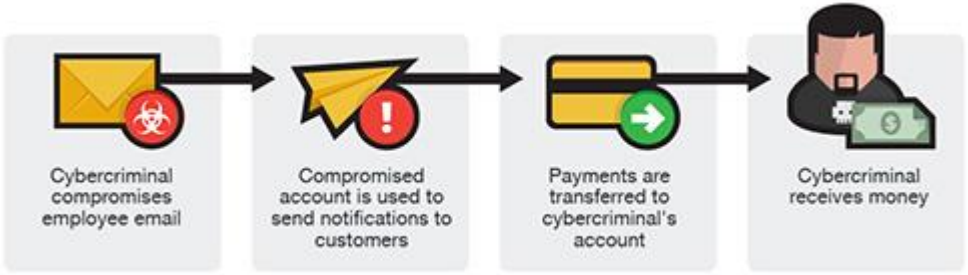
Crime Type	Loss	Crime Type	Loss
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

*Descriptors**			
Cryptocurrency	$3,809,090,856	Cryptocurrency Wallet	$1,778,399,729

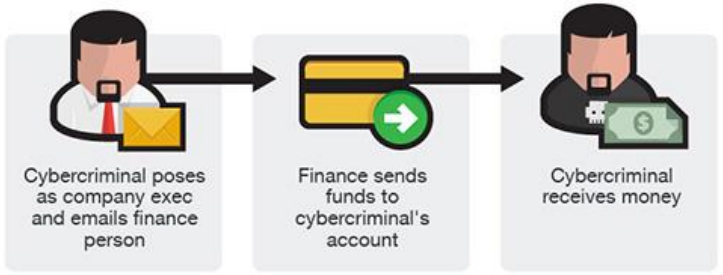
資料來源: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

★BEC五大手法

- 趨勢科技也整理出五大常見BEC手法
- **Case 1: 假發票、收據**

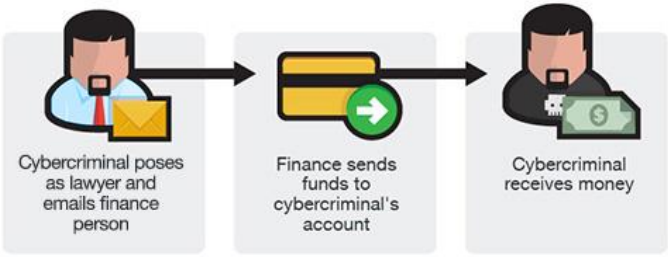


- **Case 2: 偽造身份(CEO、CFO、CTO)**

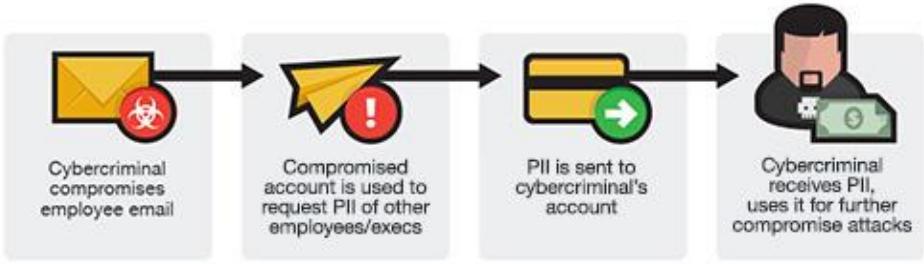


- **Case 3:入侵員工的電子郵件信箱**

- **Case 4: 扮演律師**



- **Case 5: 盜取資料**



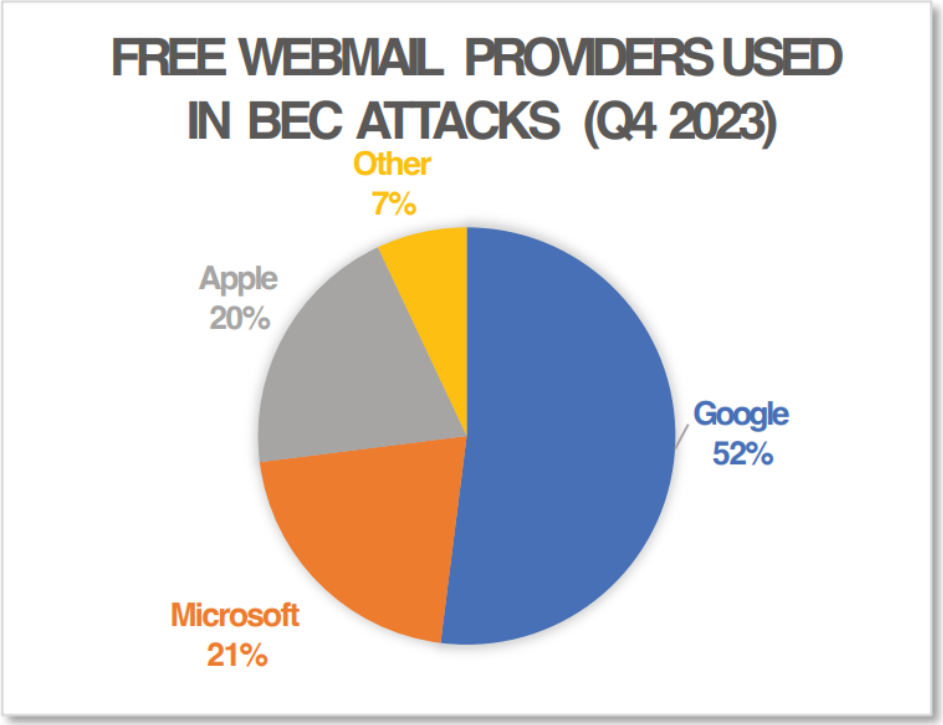
Ref: https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes/

APWG 2023 BEC 調查結果

- 據APWG成員Fortra調查指出，透過檢視 BEC 郵件內容統計(Q4 2023)
  - **37.6%** 要求以禮品卡支付
  - **30.6%** 預付款詐騙
  - **9.2%** 要求將款項改付至其他帳戶

- 直接轉帳詐騙次數上升、金額下滑
  - 2023 Q4 較 Q3 攻擊次數增加 **24%**
  - 2023 Q4 較 Q3 詐騙金額減少 **64%**
  - 2023 Q3 平均 **USD $157,422**
  - 2023 Q4 平均 **USD $56,195**

- 透過郵件發送詐騙信件需要信箱
  - 有**52%** BEC郵件從Google信箱服務發出
  - 有**21%** BEC郵件從微軟信箱服務發出



Ref: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf

BEC郵件成因

本身郵件信箱被駭

- **自建Mail Server**
  - 暴力破解(弱密碼)
  - 釣魚郵件
  - APT攻擊
  - 共用帳號
- **使用服務提供商**
  - 暴力破解
  - 釣魚郵件
  - APT攻擊
  - 共用帳號(就無法雙因子認證)
- **使用免費信箱**
  - domain較難以辨認是否為該公司
  - 駭客可以申請很像的帳號

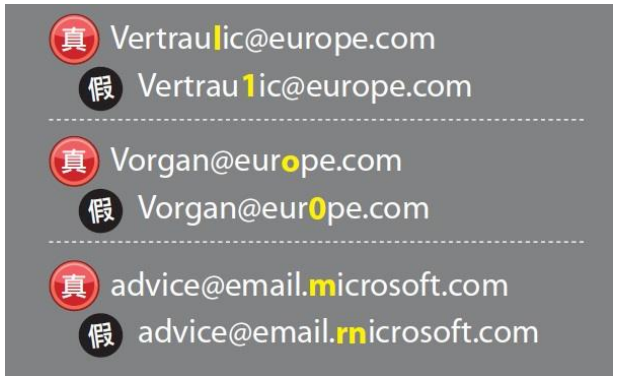
本身郵件信箱沒被駭

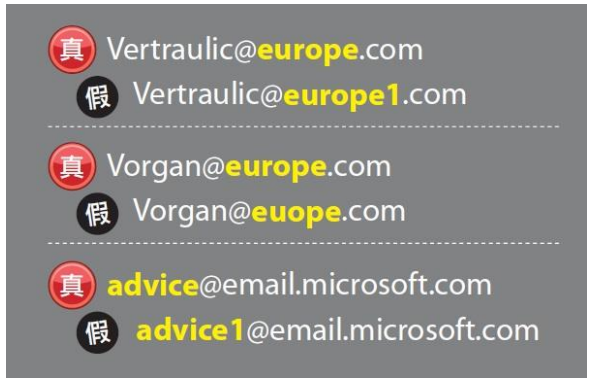
- **駭客直接用相似domain信箱**
  - 註冊類似供應鏈之公司名稱 (小寫L改成數字1，或是m改成rn，又或者是增減一個字母等作法)
  - 駭客可以透過偽造信箱跟使用者互動
- **駭客偽造己方/對方公司信箱**
  - 駭客偽冒信箱名稱直接對SMTP送出
- **供應鏈的信箱被駭**
  - 暴力破解(**弱密碼**)
  - 釣魚郵件
  - APT攻擊

BEC詐騙之防範機制

- **自身郵箱之防護**
  - 開啟**雙因子**認證
  - 提高密碼強度
  - 郵件登入告警 (異地登入偵測)
  - 郵件加密(需解密才能讀取)
  - BEC郵件偵測機制
- **自身裝置的防護**
  - APT防護(郵件沙箱、NGFW、防毒軟體)
  - **社交工程教育訓練**
    - 防範釣魚郵件竊取密碼
  - 行動裝置安全防護

- **針對供應鏈信箱的防護**
  - 透過**第二管道**確認匯款
  - 匯款流程由多人確認，不進行緊急匯款
  - 郵件簽章或PKI方式(但須雙方配合)
  - SPF、DKIM、DMARC 的郵件驗證機制





假新聞(Fake News)

中華電信
Chunghwa Telecom

★假新聞（Fake news）

- 假新聞（Fake news）是以不實資訊誤導大眾，以帶來政治、經濟、市場利益或心理得到成就感的新聞或宣傳
  - 包括通過**傳統新聞媒體**（印刷和廣播）或**線上社群媒體**傳播故意錯誤資訊
  - 假新聞為了增加讀者或網路分享，常會配合**吸引人的標題**或是**完全假造的新聞故事**，也有基於事實**斷章取義**或是**主觀誘導**的假新聞
  - 假新聞類似**標題殺人**，主要都是靠所產生的**廣告收入，不管內容正確與否**
  - 假新聞容易取得**廣告收入**、增加**政治上的兩極分化**，因著社群媒體的無所不在，Facebook與假新聞的散布也有相當的關係
  - 一些**沒有標示維護者或編輯者的匿名網站**，由於很難針對製造假新聞的作者起訴，也會成為假新聞的媒介之一

Ref: https://zh.wikipedia.org/wiki/%E5%81%87%E6%96%B0%E8%81%9E

假新聞相關罰則

- 社會秩序維護法第三編第一章妨害安寧秩序第六十三條第一項第五款
  - https://law.moj.gov.tw/LawClass/LawSingle.aspx?Pcode=D0080067&FLNO=63

第 三 編 分則

第 一 章 妨害安寧秩序

第 63 條

有左列各款行為之一者，處三日以下拘留或新臺幣三萬元以下罰鍰：
一、無正當理由攜帶具有殺傷力之器械、化學製劑或其他危險物品者。
二、無正當理由鳴槍者。
三、無正當理由，攜帶用於開啟或破壞門、窗、鎖或其他安全設備之工具者。
四、放置、投擲或發射有殺傷力之物品而有危害他人身體或財物之虞者。
五、散佈謠言，足以影響公共之安寧者。
六、蒙面偽裝或以其他方法驚嚇他人有危害安全之虞者。
七、關於製造、運輸、販賣、貯存易燃、易爆或其他危險物品之營業，未經主管機關許可；或其營業設備及方法，違反法令規定者。
八、製造、運輸、販賣、攜帶或公然陳列經主管機關公告查禁之器械者。
前項第七款、第八款，其情節重大或再次違反者，處或併處停止營業或勒令歇業。

假新聞相關刑責

- 刑法第二編第七章第151、153條，第二十七章第309、310條
  - https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=C0000001

第 151 條　以加害生命、身體、財產之事恐嚇公眾，致生危害於公安者，處二年以下有期徒刑。

第 153 條　以文字、圖畫、演說或他法，公然為下列行為之一者，處二年以下有期徒刑、拘役或三萬元以下罰金：

一、煽惑他人犯罪者。

二、煽惑他人違背法令，或抗拒合法之命令者。

第 309 條　1　公然侮辱人者，處拘役或九千元以下罰金。

2　以強暴犯前項之罪者，處一年以下有期徒刑、拘役或一萬五千元以下罰金。

第 310 條　1　意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或一萬五千元以下罰金。

2　散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或三萬元以下罰金。

3　對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。

如何識別假新聞?

- Facebook提出識別假新聞的方法
  - **對標題持懷疑態度**：如果標題裡有誇張成分，那就可能是假新聞
  - **仔細檢視網址**：把網站和已經儲存的可信來源網站進行對比
  - **確認新聞來源**：確認所有的新聞都是由可信賴的新聞機構或記者撰寫
  - **留意排版**：許多假新聞網站都會有詞語的拼寫錯誤和奇怪的排版，仔細閱讀你就可以看到這些問題
  - **留意圖片**：把圖片放在搜尋引擎上尋找確認它的來源
  - **檢查日期**：假新聞可能包括沒有任何意義的時間訊息，或者相關事件的日期已被更改
  - **尋找資料來源**：檢查作者使用的資料來源是否準確真實，缺乏證據或援引不具名人士的訊息就表示這是一則假新聞
  - **尋找相關新聞**：一個新聞事件往往會有多個相關報導，如果相關訊息能查到多個新聞報導，且有多個可信任的機構報導，那這新聞可能是真實的
  - **判斷新聞是否是個笑話**：仔細檢視新聞細節和文風，看看是否為了開玩笑而寫
  - **只分享自己相信的訊息**：沒有確認新聞的真實性之前，不應在網路上分享

Ref: https://zh.wikipedia.org/wiki/%E5%81%87%E6%96%B0%E8%81%9E

Infographic *How to spot fake news*published by the International Federation of Library Associations and Institutions

社群網站與假新聞

Facebook 又被另一前員工指控放任假新聞、仇恨言論傳播，以利增加廣告營收

by Mash Yang | 2021.10.24 12:54AM

傳送 推文 讚 37 https://www.cool3c.com/article/167425

科技應用 # Facebook # 仇恨言論內容 # 公民誠信

依照這名前員工指稱說法，Facebook內部刻意讓產生對立內容傳播，一方面藉此產生更多流量，同時也能避免激怒當時擔任美國總統的川普，以及其支持者，減少本身服務發展受限風險，甚至可能影響使用人數成長表現。

在過去於Facebook任內負責公民誠信問題的前員工Frances Haugen提出指控，表示Facebook內部實際上放任假新聞、仇恨言論內容傳播，藉此增加流量與廣告內容營收之後，稍早又有另一名同樣曾負責Facebook公民誠信的前員工也出面指證，甚至指出內部主管經常下指導棋，避免過度的內容限制影響使用流量增長。

華盛頓郵報指出，另一名曾負責Facebook公民誠信的前員工出面指證，說明Facebook內部並非像對外說明般，會妥善處理倍受爭議的假新聞、仇恨言論內容，反而會刻意放任此類內容流傳，僅以消極態度處理被檢舉、反應內容，為的就是增加使用流量與廣告內容營收。

依照這名前員工指稱說法，Facebook內部刻意讓產生對立內容傳播，一方面藉此產生更多流量，同時也能避免激怒當時擔任美國總統的川普，以及其支持者，減少本身服務發展受限風險，甚至可能影響使用人數成長表現。

這名前員工指證說法，恰好呼應先前Frances Haugen提出指控，強調Facebook明知其服務平台被用於傳播仇恨、暴力與假新聞等錯誤訊息，卻依然以自身廣告、流量等利益為優先，進而影響更多用戶感受。

不過，Facebook後續則反駁表示Frances Haugen陳述內容造成誤導，強調本身在確保用戶發表言論自由之餘，更積極確保隱私安全之間平衡，同時更持續改善錯誤訊息與有害內容產生影響。而在後續說明中，Facebook發言人Nick Clegg透露Facebook與Instagram兩大社群平台將作調整，讓使用者能有「更多朋友、更少政治」的互動體驗。

Ref: https://www.cool3c.com/article/167425

仇恨言論與假消息充斥印度網路社群，外媒揭 Facebook 未有足夠資源應對

作者 陳 冠榮 | 發布日期 2021 年 10 月 24 日 16:25 | 分類 Facebook, 國際觀察, 社群 分享 分享 Follow

華爾街日報、紐約時報在內的新聞媒體取得大量的 Facebook 內部文件，這些是由 Facebook 前產品經理 Frances Haugen 收集，並向媒體舉報。新聞媒體不斷從這些內部文件挖掘，其中更發現印度做為 Facebook 最大的市場，但過去這些年卻充斥了仇恨言論、錯誤訊息以及暴力活動，而 Facebook 卻未針對印度部署足夠資源加以應對。

紐約時報報導舉出其一案例，Facebook 研究人員在 2019 年 2 月建立新的帳號，以了解做為居住在印度喀拉拉（Kerala）的民眾體驗 Facebook 的感受；在接下來的 3 週內，這個帳號遵循一個簡單規則，即是按照 Facebook 演算法產生的所有推薦來加入群組、觀看影片以及前往網站瀏覽頁面。

然而結果卻是動態消息（News Feed）充斥了仇恨言論、錯誤訊息以及暴力活動，這些全都記錄在 Facebook 內部報告裡，測試體驗的動態消息幾乎不斷出現極端分化的民族主義內容、虛假消息、暴力和血腥內容，Facebook 研究人員甚至寫道「我在過去 3 週內看到的死者圖片比這一生所看過的還要多」。

這份內部報告是 Facebook 員工撰寫的數十項研究與備忘錄的其中之一，反映這個社群平台對印度的影響，在沒有充分了解當地文化與政治的潛在影響下進入這個市場，並且未能部署足夠資源以防一旦問題發生立即採取行動。根據一份描述 Facebook 資源分配的內部文件顯示，Facebook 用於對虛假消息進行分類的全球預算中，有多達 87% 是用於美國，所以只有 13% 用於其他國家，然而北美用戶僅占 Facebook 的 10% 比例。

印度擁有超過 13 億人口，有著很深的社會與宗教分歧，並且屢屢為此爆發衝突傷亡。此外，印度用戶使用多達 22 種語言，這也對 Facebook 進行內容審查帶來極大的挑戰；而且許多人民的數位素養有限，缺乏面對網路社群應有的同理心、思辨力以及相互尊重的觀念。

Facebook 發言人 Andy Stone 指出媒體取得的一些報告內容是包含提供討論的調查線索，並非完整的調查，也不包括個別政策建議。他表示 Facebook 為找出跨越多種語言的仇恨言論，在技術上已進行大量投資，且在自家這樣的全球性平台上這類內容正在減少。

Ref: https://technews.tw/2021/10/24/facebook-internal-documents-show-a-struggle-with-misinformation-hate-speech-and-celebrations-of-violence-in-india/

AI讓假新聞更難辨識

【烏俄戰爭】深偽影片首在烏俄資訊戰現身 冒充澤倫斯基要求烏軍投降

更新日期：2022-03-17

記者何蕙安／編譯

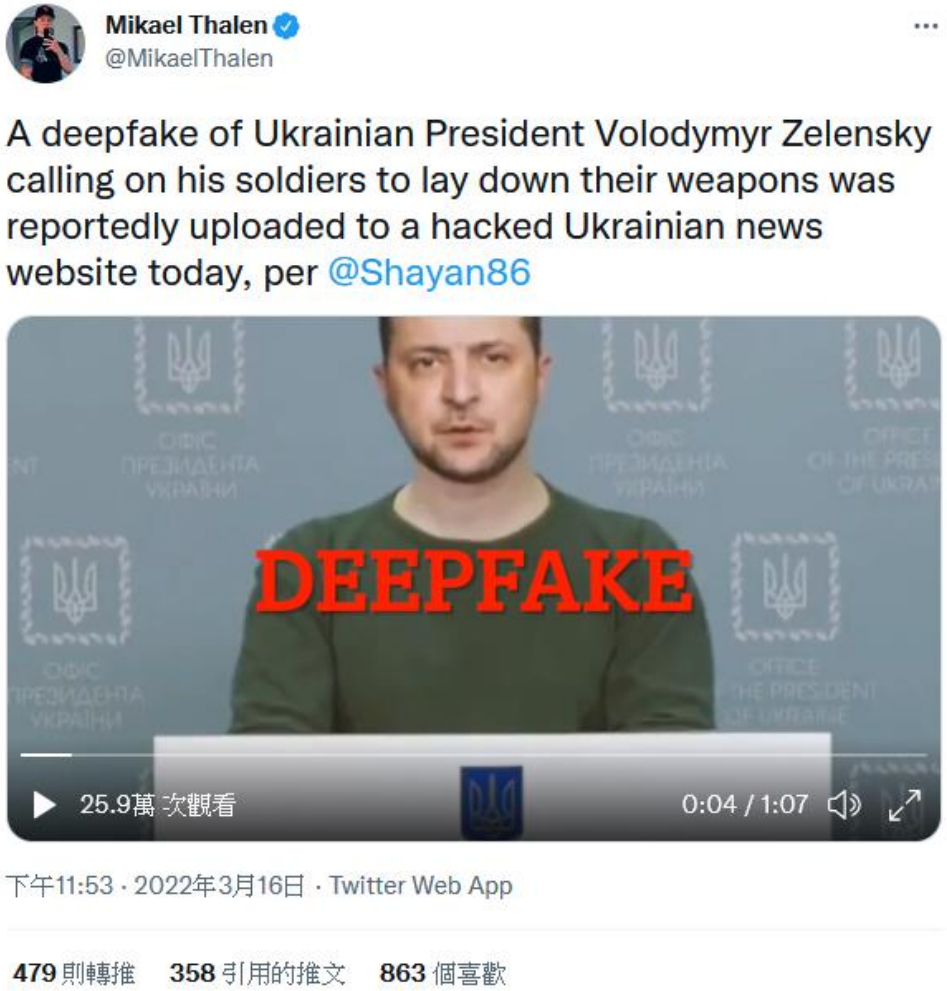
一支宣稱是烏克蘭總統澤倫斯基呼籲烏克蘭士兵放下武器投降的深偽影片（Deep Fake）昨天（16日）出現在網路上，所幸科技公司快速採取行動，移除影片相關內容，該深偽影片並未在社群平台廣泛流傳，僅在俄羅斯網路世界有較長的生命週期。

專家說，這可能是烏俄戰爭以來製作最為精細的深偽影片。令人注意的是，儘管一些粗製濫造的變造影片在戰事以來在社群平台上流傳，但此次有駭客將深偽影片發布在數個烏克蘭新聞網站，包括在電視頻道《Ukrayina24》的新聞直播節目上放上字幕跑馬燈，增加了該影片的可信度。

所幸人們對於深偽影片的使用有所警覺，該影片很快就被揭穿。在第一時間，澤倫斯基本人也在Telegram頻道上傳影片反駁自己曾經要求烏克蘭軍隊投降。他說，如果他呼籲投降，那會是要求俄羅斯軍隊放下武器，回去自己的國家。

在台灣，也可能因為Meta的即時處置，在中文臉書平台上並沒有相關影片流傳。

> As a matter of principle, I never post or link to fake or false content. But @MikaelThalen has helpfully whacked a label on this Zelensky one, so here goes.
>
> I've seen some well-made deepfakes. This, however, has to rank among the worst of all time.pic.twitter.com/6OTjGxT28a
>
> — Shayan Sardarizadeh (@Shayan86) March 16, 2022



Ref: https://tfc-taiwan.org.tw/articles/7099

Deepfake換臉影片

網紅小玉用Deepfake「換臉」製作不雅片，判賠100萬！AI怎麼會變犯罪工具？

數位時代
2022年12月12日

2022.12.12更新

網紅「小玉」朱玉宸與助理莊炘睿利用Deepfake（人工智慧深偽技術），把高雄市議員黃捷、空服員的臉，「換臉」至色情片牟利，自109年7月起至110年10月共牟利新台幣1,300餘萬元，新北地院近期判賠受害者黃捷、空服員等各新台幣100萬元。

不只是黃捷，就連立法委員高嘉瑜、「雞排妹」鄭家純也是受害者。黃捷指出，感謝法官還給受害者公道，寒冬中給受害者一些安慰。不過更迫切的仍是數位性暴力的修法，包括懲處、防範及補救下架機制，但願不會再有人因為性影像的威脅和流傳而擔心受怕。

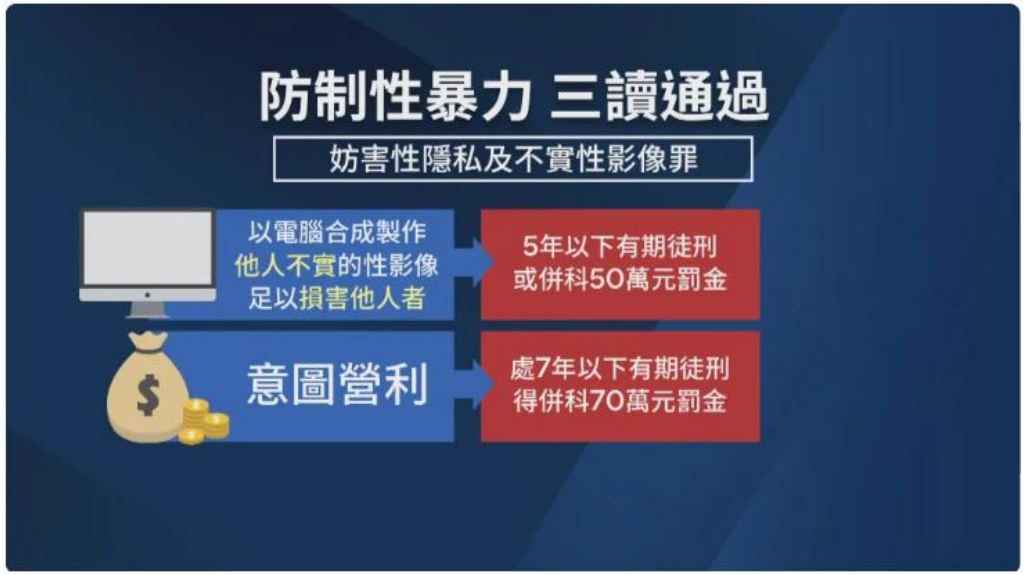
究竟「Deepfake」技術是如何做到以假亂真的換臉，下文帶您一探究竟。

愚人節當天，知名YouTuber小玉上傳了一則影片，畫面中顯示高雄市長韓國瑜身穿藍色襯衫，用誇大的言詞說著無俚頭的話。原來，這是小玉為了向民眾呼籲假新聞的風險，而利用Deepfake技術所製造出來的假影片。該影片很快就上了熱門影片排行，掀起網友熱議。

Deepfake，中文譯作「深假」或「深偽」，是一種透過人工智慧（AI）中的deep learning（深度學習）技術所創造出的fake（偽造）訊息。Deepfake技術可以用於影像及聲音，只需要仿造對象的人物影音素材，就能製造出唯妙唯肖的假影片。

修法過關！賣Deepfake換臉不雅片 最重判7年

趙翊絜
2023年1月8日

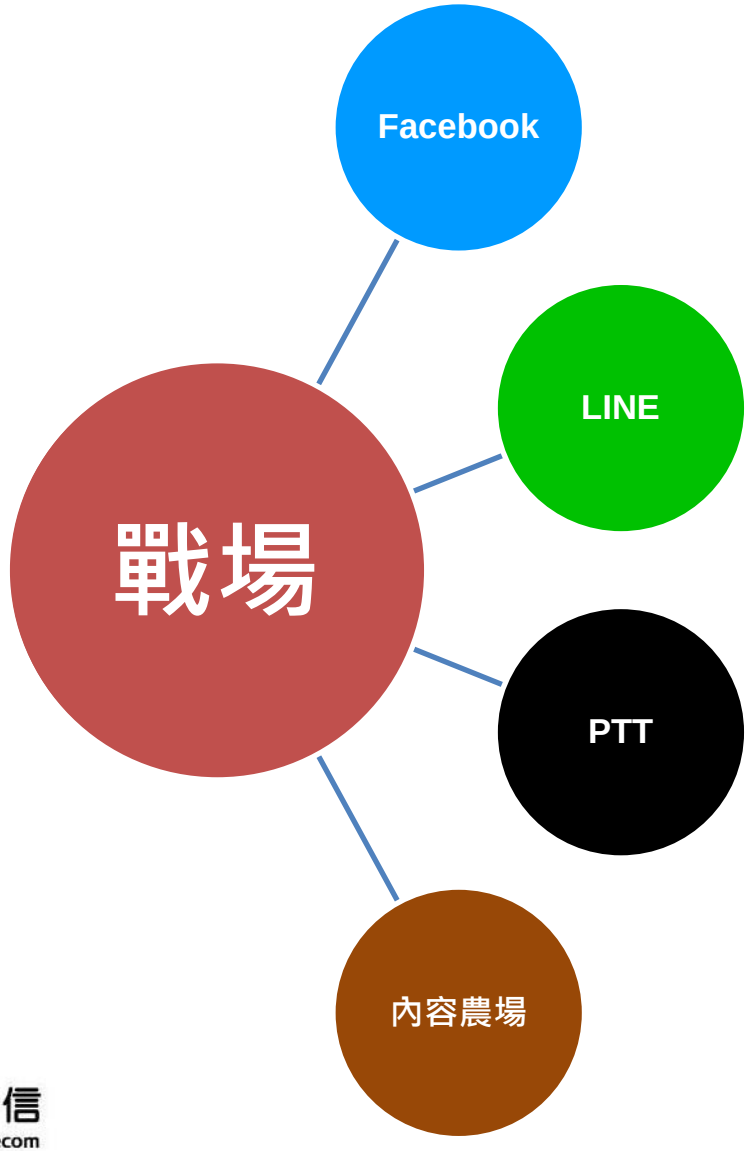


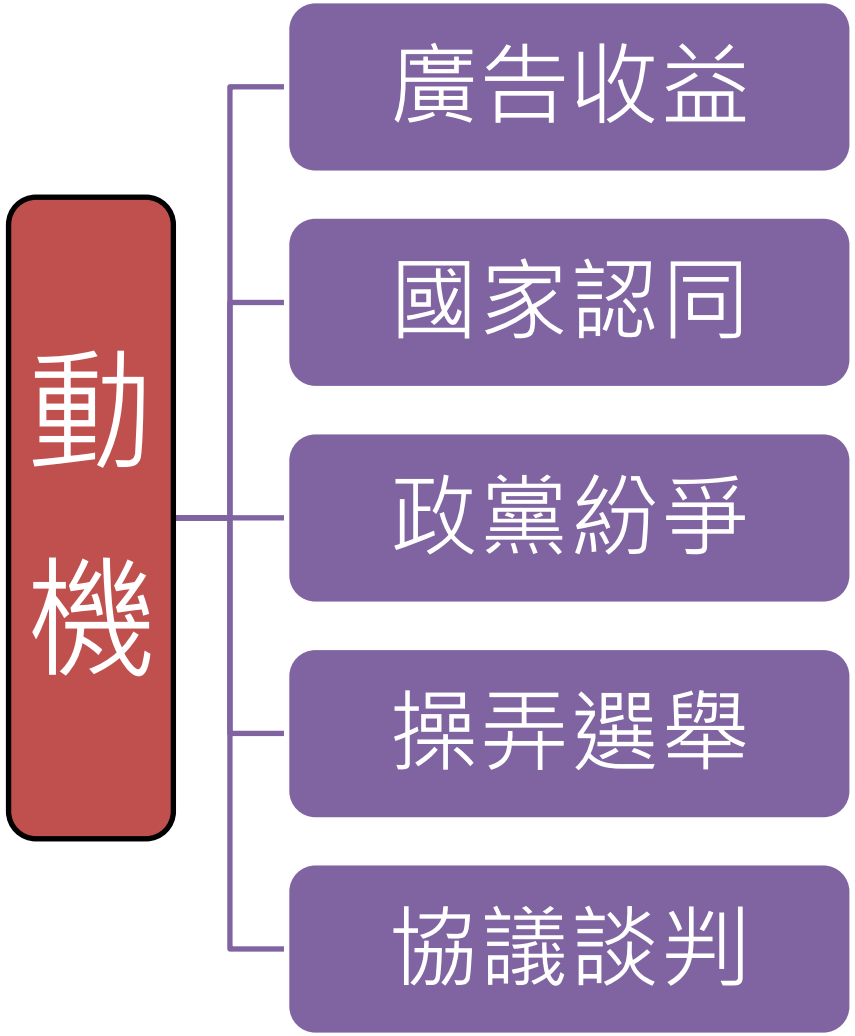
網紅小玉利用深偽技術，販售名人不雅片，卻因法規不足，一審被依違反個資法，輕判5年6個月，這讓眾多受害者無法接受。為了防堵這種情況，立法院院會昨天三讀通過刑法修正案，如果製作不實性影像，最重可處7年以上有期徒刑。

網紅小玉：「小玉這個人啊！」利用Deepfake軟體，把自己變臉換成韓國瑜，網紅小玉就是用這個深偽技術，合成不雅影片販售牟利。網紅小玉：「向所有被害人，在這邊致上非常誠摯的歉意，對不起。」開庭時刻意低姿態鞠躬道歉，小玉販售不雅片，一審被依違反個資法，判5年6個月，可以易科罰金，就怕類似案件再重演。

Ref: https://ynews.page.link/RQa4u
https://ynews.page.link/p7pWU

★假新聞的在台灣的戰場與動機





中華電信 Chunghwa Telecom

秤斤論兩行情：買榜、刷評、按讚、賣帳號

PTT帳號15年

尚未有評價 | 0 月銷售量

$35,000

運送 含運費

規格 5100次登入

數量 − 1 + 還剩1件

加入購物車 直接購買

蝦皮優選 PTT 看板 代發文 推文 寄信 打廣告 推廣文 100次 300次 1000次 帳號 DCARD 可參考

5.0 ★★★★★ | 15 評價 | 51 月銷售量

~~$198~~ $98 - $398 5折

運送 免運優惠

運費 $0

規格

已登入100次帳號 代 推文、發文

已登入200次帳號 代 推文、發文

已登入300次帳號 代 推文、發文

已登入1000次帳號 代 推文、發文

發文後，協助轉寄站內信，1次(10封內)

Facebook 真人讚 /直播 /讚 /留言讚 /粉絲專業讚 /觀看人數 /追蹤人數 /台灣真人讚 /五星評價/FB

5.0 ★★★★★ | 1282 評價 | 9814 月銷售量

~~$900 - $3,800~~ $9 - $340 0.1折

賣場折價券 現折$70 現折$105 現折$260

運送 免運優惠

運費 $0

規格

100個全球真人貼文讚 50個台灣真人貼文讚

100個台灣真人貼文讚 永久貼文自動台灣讚(無時間限制)

100個粉絲專頁全球真人追蹤+讚 100個粉絲專頁台灣真人追蹤+讚

10個留言全球真人讚 10個留言台灣真人讚

YOUTUBE訂閱/分享/留言/客製化留言/喜歡/不喜歡/直播人數/IG/FB/臉書/FACEBOOK

4.7 ★★★★★ | 12 評價 | 2 月銷售量

$30 - $100

運送 免運優惠

運費 $0

規格

影片觀看次數 1000次 影片喜歡 100個 影片不喜歡 100個

真人訂閱 100位 客製化留言 10則 分享影片到FB 500次

直播人數 5000人2小時(需拍7個數量 終身保證訂閱100個=50元

中華電信 Chunghwa Telecom

假新聞造謠 逼死外交官

15 Dec 2018

「台客困關西靠陸援助」造謠者抓到了！法官裁定不罰

編輯 談雍雍 報導 2018/12/15 07:47

小 中 大

作者GuRuGuRu (GuRuGuRu)
看板Japan_Travel
標題Re: [新聞] 中使館派車接關西機場陸客，要台灣人自稱
時間Thu Sep 6 10:41:22 2018

我推文有提到
我是針對這篇文章 而非任何機關
在事情發生當下真的很慌並且身心俱疲
我其實是希望辦事處能給一點方向
我當然清楚找住宿交通是自己的事情
但我第一次來日本自助就遇到這種事
理所當然是想徵詢駐日辦事處的建議
後續我也是靠自己找到住宿及交通
單純只是希望在這種時候 與其發垃圾文
不如真正做些有實質幫助的事情
這篇文也提供給日後要出國旅遊的國人
一個...方向和經驗分享

雖然是垃圾新聞，但我還是想回覆。
手機回文版面會很亂請別介意
我是昨天搭乘中使館的巴士回到大阪市區的台灣人
從一開始在機場時
完全沒有任何人告知我們有分所謂中國人的車
或是外國人的車什麼
我們也就傻傻的看到公告說第一航廈一樓有車會接駁我們搭高速船到神戶
我們也就收拾行李到一樓去排隊
當時的人龍用兩張照片描述
https://i.imgur.com/tCQ1a2V.jpg

- 事件起因是一名PTT鄉民「GuRuGuRu」，於9月6日在旅日版發文稱，他受困關西機場時，靠著中國駐日使館巴士回到大阪市區，之後打給台灣駐日辦事處尋求其他相關協助，但卻被對方冷回
- 文章一出，瞬間發酵！而後「**中國外交使館積極派車接送中國遊客、但台灣駐日單位卻無作為**」的訊息充斥媒體版面，使得駐大阪辦事處承受龐大輿論批評！甚至一周後，駐大阪辦事處處長蘇啓誠竟傳疑因**壓力過大而輕生**
- 事後警方查出造謠的網友「GuRuGuRu」，是台北一名游姓男大生，將他移送法辦，但**法官認為，謠言內容未造成民眾生命威脅，不符《社會秩序維護法》要件，裁定免罰**

中華電信 Chunghwa Telecom

Ref: https://news.tvbs.com.tw/politics/1047928

墨西哥2名男子因為假消息被活活燒死

Burned to death because of a rumour on WhatsApp

By Marcos Martínez
BBC Monitoring

12 November 2018

A host of mobile phones were raised aloft to capture the moment Ricardo and Alberto were set on fire

- 墨西哥2名男人子因為輕罪被警察拘捕抓進小房間(看守所)
- 村民聽信WhatsApp上的謠言相信兩人是涉嫌兒童綁架的犯人
- 雖然警方有解釋闢謠，但村民不相信，還繼續透過WhatsApp傳播號召
- 人潮隨著時間增加，最後暴民衝進警局把兩名男子拖出，淋上汽油點火焚燒

Ref: https://www.bbc.com/news/world-latin-america-46145986

印度WhatsApp假訊息害命

How WhatsApp helped turn an Indian village into a lynch mob

19 July 2018 Share

Mohammad Salman was beaten on false rumours he was a child kidnapper

A 32-year-old Indian software engineer has become the latest victim in a spate of mob lynchings, allegedly spurred by child abduction rumours spreading over WhatsApp. BBC Telugu's Deepthi Bathini reports on how the attack unfolded.

"They kept hitting us, demanding to know how many children we had kidnapped," says Mohammad Salman, who is still in shock, his body bruised and his face scarred with stitches.

On 13 July, Mr Salman, 22, and his two friends were brutally beaten by a mob that suspected them of kidnapping children. The last thing he remembers seeing was his friend, Mohammad Azam, being dragged away with a noose around his neck. Mr Azam died from his injuries.

假新聞致印度逾20死 WhatsApp祭防堵新招

分享 分享 留言 列印 存新聞 A- A+

2018-07-20 17:21 中央社 新德里20日綜合外電報導 讚 0 分享

印度WhatsApp用戶盛傳若干有關孩童綁匪及其他罪嫌的不實訊息，導致過去兩個月來，全印有20多人被暴民施以私刑致死。在當局施壓下，WhatsApp今天宣布將推出防堵謠言的新功能。

這家臉書（Facebook）旗下的公司表示，將在印度測試限制用戶轉發消息，及限制一次只能轉發5段對話的功能。

WhatsApp也於聲明中表示，將「刪除媒體訊息旁的快速轉發鍵」。

WhatsApp說：「我們認為這些變革有助維持設計WhatsApp為私訊應用軟體的初衷，但我們將持續評估相關狀況。」

在印度總理莫迪（Narendra Modi）政府的壓力下，WhatsApp已經宣布推出新功能，協助用戶辨識訊息是否曾被轉發。

WhatsApp還買下印度報紙的全頁廣告，教導讀者辨識不實訊息的方式。但印度電子及資訊科技部昨天稍晚仍發布措辭強烈的聲明，指WhatsApp採取的措施仍不足以遏止不實訊息。

這個部門表示：「WhatsApp未充分解決平台上充斥大量假訊息的問題。」

聲明也指出：「當有人惡意轉傳謠言及假新聞時，用於此類傳播的媒介也責無旁貸。若（WhatsApp）仍保持沈默，將被視為教唆方而面臨相應的法律訴訟。」（譯者：鍾佑貞/核稿：陳政一）

Ref: https://www.bbc.com/news/world-asia-india-44856910
https://money.udn.com/money/story/5641/3263814

WhatsApp假新聞防制措施 (1/2)

Whatsapp 於印度使用流動宣傳車 講解如何分辨假新聞

讚好此文 讚好 70 分享

十月 14, 2018 • 應用軟件 •

在社交平台和即使訊息服務上出現的假新聞散佈問題，在世界各地都有出現。印度方面同樣相當注重這個問題，有見及此 WhatsApp 就在當地透過宣傳車，向居民講解如何避免散播假新聞，改善網絡公民意識。

WhatsApp 與當地電訊商 Reliance Jio 合作，在印度 10 個城市用流動宣傳車向市民講解如何安裝 WhatsApp，以及如何在 WhatsApp 上分辨出假新聞和流言。同時 Reliance Jio 表示，目前 WhatsApp 已經可以在其使用 KaiOS 的 JioPhone 上使用，覆蓋 2,500 萬名用家。這些手機價格只是 20 美元左右，因此相當受印度用家歡迎。

印度當局之前曾經針對假新聞問題點名批評 WhatsApp，也曾經因為加密問題與印度政府意見不合。不過印度目前是 WhatsApp 相當重視的市場，因此類似今次的宣傳計劃，也是要改善其形象，希望得到當地人民和政府的接納。

來源：TNW

About the Author

藍骨

藍色的天空，藍色的海，藍色的曲調，深入骨髓。

Previous post:
日本研發全球首部鋰電潛艇　料 2020 年正式服役

Next Post:
Apple 將在加拿大推出 iPhone XR 專用透明殼

WhatsApp 推出電視廣告 教育印度用戶防範假新聞

讚好此文 讚好 49 分享

十二月 4, 2018 • 社交網絡 •

不少假新聞透過 WhatsApp 在印度傳播，甚至導致人命傷亡，令這即時通訊軟件近期飽受壓力，就連政府部門都指責 WhatsApp。為了教育用戶不要散播假新聞，WhatsApp 曾經在印度報章刊登全版廣告，現在更進一步，於當地電視台賣廣告嘗試引起用戶的關注。

WhatsApp 於印度兩個州舉行選舉前推出 3 款廣告，廣告以「分享快樂，不是傳聞」為題，這是 WhatsApp 有史以來首條電視廣告。每條廣告長 1 分鐘，會以當地 10 種語言於電視、Facebook 和 YouTube 三大平台播出。其中一條廣告以喜歡分享食譜的女主角作為出發點，她的食譜吸引很多朋友讚賞，有一日朋友要求她散佈謠言，女主角的媽媽說轉發沒所謂，但女主角則曉以大義表示不可以散佈謠言，最後將訊息刪除並將散佈謠言者封鎖。

About the Author

唐美鳳

世界要變得更好，不單靠科技就可以辦到。待人好一點，每天做一件好事，你都可以做得到！

Previous post:
Starbucks 禁客人以免費 Wi-Fi 上載網 YouPorn 禁員工飲 Starbucks 反制

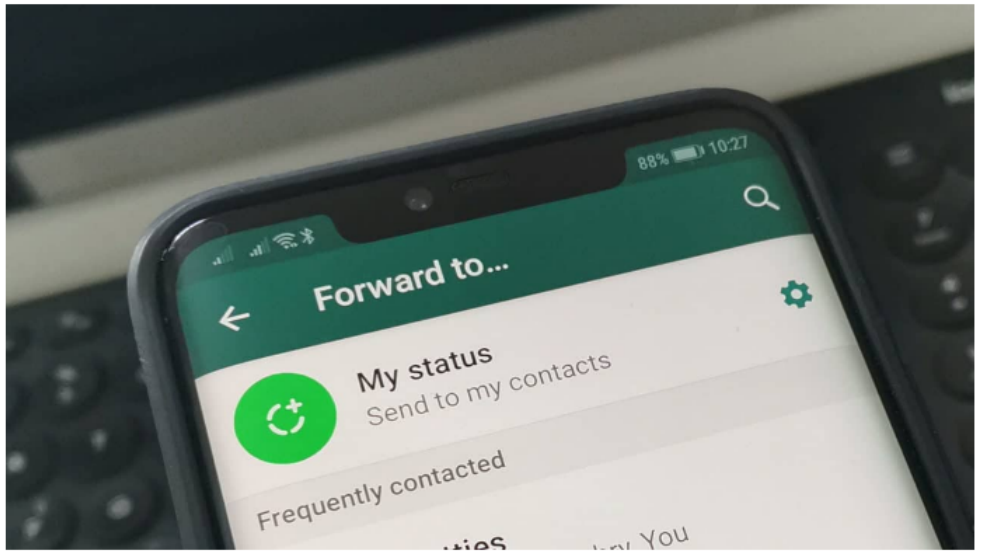
Next Post:
iOS 詐騙 App 出現　按手指查健康即付100美元

- 平台或許要為假新聞的散佈附上責任
- 但問題的源頭應該是散發假新聞的人、以及輕信假新聞的施暴者

Ref: https://unwire.hk/2018/10/14/whatapps-using-street-theater-to-fight-fake-news/software/
https://unwire.hk/2018/12/04/whatsapps-first-ever-tv-commercial-warns-against-fake-news-in-india/life-tech/social-network/

WhatsApp假新聞防制措施 (2/2)

WhatsApp 限制訊息轉寄 「雙勾號」訊息只能向一位用戶轉發



不少人都會收過由其他 WhatsApp 用戶傳來的疫情消息，但大部份未經審查，其真確性存疑。WhatsApp 為免其用家使用其 APP 亂轉未經核實的訊息，在今日（7 日）出聲明，指以後通過五個或更多人發送的訊息將被定為「高度轉發」訊息，每位用家只能轉發給一個人。

WhatsApp 指，由於武漢肺炎疫情持續，人們比以往更加仰賴使用 WhatsApp 聯絡，而他們發現，轉寄訊息的數量暴增，憂慮助長虛假資訊的散播，故實施此限制，旨在降低不實信息在 WhatsApp 中的傳遞速度，從而減少假新聞的傳播。

保持 WhatsApp 的的個人化與私密特性

數十億人目前因 COVID-19 新冠肺炎疫情無法與親友見面，他們比以往更加仰賴使用 WhatsApp 聯絡。大家在這場危機中使用 WhatsApp 和醫生、老師、或是受到隔離的親友交流。 因此，您所有經 WhatsApp 收發的訊息與通話都預設為端對端加密，讓您可以安心進行最私密的對話。

去年我們推出了可多次轉寄訊息的功能。這些訊息附加 雙勾號 標籤，表示此訊息並非來自您熟悉的聯絡人。和您日常經 WhatsApp 傳寄的訊息相較，這些訊息其實沒有那麼私密。因此，我們現在推出限制轉寄功能，讓這類訊息同時只能轉寄至一個對話。

身為個人訊息服務提供者，我們這些年來採取多種措施來維護使用者間對話的私密性。例如我們設定了 訊息轉寄限制 以減少訊息瘋傳，隨後我們立即發現全球訊息轉寄的總數減少了 25%。

難道所有經轉寄的訊息都不好嗎？當然不是。我們知道很多使用者轉寄的是實用的資訊、有趣的影片、玩笑式的惡搞內容，或是他們覺得富有深意的感言或祈禱文。最近幾週，大家也使用 WhatsApp 來組織 群體行動，表達對第一線醫療人員的支持。但同時我們也發現訊息轉寄的數量暴增，導致使用者反映這種情況讓人無所適從，也助長虛假資訊的散播。我們認為有必要減緩這類訊息傳播，以維持 WhatsApp 個人間私密對話的特色。

此外，我們也正直接與包括世界衛生組織和 20 餘國衛生機構等政府與非政府組織合作，讓大家可以獲得正確資訊。這些具公信力的機構總共已直接傳送了數億則訊息給需要資訊和建議的人。您可以在我們的 新冠病毒資訊中心，了解更多我們對此議題所做的努力，並將可能的虛假資訊、騙局、和謠言送交 事實查核機構 進行查證。

我們認為現在是大家最需要私密聯絡的時刻。在這場前所未見的全球危機中，我們的團隊正在努力維持 WhatsApp 正常運作。我們會持續聆聽您的意見回饋，並改善在 WhatsApp 上分享資訊的方式。

2020 年 4 月 7 日 Tweet

Ref: https://unwire.hk/2020/04/07/whatsapp-forward/life-tech/social-network/
https://blog.whatsapp.com/Keeping-WhatsApp-Personal-and-Private

FB 失智症權威醫師失智了！？

黃清江
2018年9月18日

失智症權威醫師劉秀枝 失智了
國立陽明大學兼任教授、臺北榮總特約醫生。台灣失智症研究與治療的權威，更是她那個年代裡，少數可以當上主任的女醫生。
劉秀枝醫生這次刊登一封非常感人的信，平靜地道出輕度失智者的心聲，此信係獲得這位可敬的女士同意後刊載。
親愛的朋友：
我寫這封信只是想告訴大家我失智了。不過，不必震驚，目前還是輕度，否則我也無法寫這封信。當然，有些字眼想不起來，許多事情無法串在一起，思緒也常會中斷，因此這封信是在妹妹幫忙之下完成的。今年70歲的我，比各位年長許多，常和大家一齊聚餐、打高爾夫球、出國旅遊，相識相知，受大家的照顧已20年。妹妹常怪我不用心，丟三落四，一問再問，還把約定日期搞錯。
在一次出門忘了關水龍頭，把水塔裡的水流光後，妹妹帶我去看神經科醫師，經過仔細檢查，醫師告訴我得了失智症，是大腦退化所造成的阿茲海默症，並且開藥讓我服用，希望能退化得慢一點。從此，當我又忘了，妹妹不再有「不是告訴過你了」的責備語氣，或我反覆說時，也不會有「你說過好幾次了」的奇怪眼神，反而是輕聲細語的說「沒關係」或「我替你記住就好」，我就知道我是真的病了！我的高爾夫球技一向差，但最近半年來，連每一洞打了幾桿都記不清楚，到底揮的是第二桿還第三桿？球友都會幫我算桿數或請桿弟幫我算。那天打了幾洞後，我忽然問：「我們現在是打第一洞嗎？」看到球友們驚愕的眼光，我覺得是對大家承認我失智的時候了。
醫師說生病並不可恥，身體每一個器官都可能生病，失智症是大腦的疾病，就好像膽結石是膽囊的疾病；乳癌是乳房的疾病一樣。然而，我變得很沒有信心，容易恐慌，因為我不知道我將要踏出去的每一步對不對，要說出的話是不是已經說了多次，而且心裡想的無法表達，愈急愈講不出來。我常覺得氣喘不過來，在餐廳吃一頓飯，會上好幾次洗手間，兒子帶我去看心臟科和泌尿外科醫師，都說沒事，是因為緊張的關係。我瞭解我的記性和其他認知功能就像雙手握滿東西般，一面走，會一件一件的掉，甚至像沙灘上腳下的流沙，會很快的流失。也許有一

失智症權威醫師 劉秀枝：我沒失智

【聯合報／記者魏忻忻 / 台北報導】

劉秀枝對退休生活早有規畫，近年除了教學 ，還到處遊山玩水。圖 / 劉秀枝提供

「失智症權威醫師劉秀枝失智了！」這樣的消息最近在臉書瘋狂轉貼，許多人按讚，並留言表示惋惜、不捨。不過，當事人劉秀枝並沒有失智，她謝謝大家關心，並調侃自己，「這個消息是正確的，只是提早了廿年。」

劉秀枝是台北榮總一般神經內科前主任，已經退休的她，雖然不再看診，仍經常回醫院教學。為什麼會傳出她失智了？源於她兩年多前在聯合報元氣周報專欄的一篇文章。當時她以寫信的方式，以第一人稱記錄一位非常親近的親戚得知自己失智的心情。不料，這篇文章引來誤會，許多人以為是她失智了。

文中強調：「這封信獲得這位可敬的女士同意後刊登」，這位可敬的女士是指劉秀枝的親戚。但臉友轉貼文章時，可敬的女士卻被改成劉秀枝本人。於是從轉寄文章看起來，劉秀枝的確失智了，且消息獲得她本人同意而轉寄。劉秀枝說，這傳聞一開始是用電子郵件轉寄，最近又在臉書上傳布。

Ref: https://health.udn.com/health/story/6631/364704

新冠肺炎假新聞不斷 (1/2)

武漢肺炎：隨疫情擴散全球的五大假新聞

2020年 1月 29日 分享

新型冠狀病毒在全球蔓延，各國媒體都爭相報道，相關的假消息也隨著病毒蔓延。

從「蝙蝠湯」，到「病毒是政府製造出來的生物武器」，這些假消息在網絡不斷傳播。BBC國際媒體觀察部（BBC Monitoring） 選出了其中一些假消息，探究它們的來源，也分析它們有多可信。

「蝙蝠湯」

疫情初期，外界曾遍都在探討病毒的來源，其中最廣泛傳播的訊息不乏指控武漢人吃蝙蝠等野味，令這種病毒感染人類。

其中一段錄影顯示，一名中國女子拿著一隻已經煮過的蝙蝠，形容蝙蝠吃起來「很像雞肉」，引起網絡上反彈，批評中國一些人吃野味的習慣，就是引起新型冠狀病毒的原因。

但這個片段其實不是在武漢拍攝，而是中國著名旅遊節目主持汪夢雲2016年在西太平洋島國帕勞拍攝的旅遊節目。新型冠狀病毒疫情爆發後， 一些人把舊片段翻出來，重新上傳到網絡。

2020/04/14 19:38

抗疫淪人權災難？中國「大外宣」造謠

房業涵 黃建熒 台北報導

新型冠狀病毒造成全球超過190萬人感染，尤其歐美的疫情嚴重，開始有訊息不斷的轉傳「只要從義大利回鄉的塞內加爾人全部就地槍斃」，身體被包得像垃圾，卡車像倒垃圾一樣的倒下去，另外，網路上也有人列舉包括義大利、英國與美國等國家，放棄治療年長病患的規定，強調中國細心治療年長病患，從未放棄老人的救治，事實恐怕不是如此，真相是中國網軍藉由他國疫情進行大外宣，今天的華視打假特攻隊！

只要從義大利回鄉的塞內加爾人，全部就地槍斃，卡車像倒垃圾一樣地倒下去，影片長達30秒，強調國家的醫療匱乏，只能這樣面對病毒和生命！流傳影片追真相，我們實際檢索關鍵字在YOUTUBE反搜，發現到這是塞內加爾新聞媒體Dakaractu TV的部份片段有完全相同之處，但標題卻是機場應急計劃實兵演習，跟疫情完全無關。

Ref: https://www.bbc.com/zhongwen/trad/chinese-news-51293515
https://news.cts.com.tw/cts/international/202004/202004141997138.html

新冠肺炎假新聞不斷 (2/2)

武漢肺炎／網傳自評表可測風險 指揮中心闢謠

最新更新：2020/02/28 22:04

網路流傳一則「武漢肺炎高危險群自評表」，可輕鬆測出染病風險。中央流行疫情指揮中心監測應變官莊人祥28日晚間闢謠表示，該表格目的是在疫情出現社區傳播時，用來辨別是流感還是武漢肺炎，並非民眾自我篩檢依據。中央社記者張茗喧攝 109

武漢肺炎》網傳染疫自救影片 食藥署闢謠：切勿輕信莫轉傳

新頭殼newtalk | 林芷湲 綜合報導
發布 2020.03.17 | 12:58

食藥署提醒民眾切勿因聽信偏方而延誤就醫。 圖：取自youtube

武漢肺炎（COVID-19）疫情持續於全球肆虐，為不少民眾都開始尋求自保的方式，近日網路上就流傳著一段「美華裔專家揭秘新冠機理及自救措施！必看救人方法！」的影片，食藥署今（17）日即發文提醒，目前醫學研究針對新型冠病毒之特性仍未完全瞭解，在沒有確切證據的論述基礎下民眾切勿輕信，也避免再轉傳親朋好友。

Ref: https://www.cna.com.tw/news/firstnews/202002280310.aspx
https://newtalk.tw/news/view/2020-03-17/376270

網路流傳疫苗不實訊息

健康關係 > 健康醫療

「打疫苗變萬磁王」謠言來自她！骨科醫師帶頭「反疫苗」，吸金6000萬

「聽說打疫苗會變身萬磁王？」到底誰說的？是不是真的？

文–王茜穎・未來城市
發布時間：2022-02-25

1498
瀏覽數

曾有一段時間網路卻瘋傳打完疫苗後，人體忽然獲得磁力，能吸附金屬餐具、餐盤、手機、鑰匙和硬幣的影像。

該謠言最知名的源頭坦佩尼（Sherri Tenpenny），是來自美國俄亥俄州的骨科醫生。

不少台灣人也跟風「萬磁王」，把金屬物品吸到手臂上。圖片來源：台大醫院粉專

疫苗假訊息都來自這12人

根據「對抗數位仇恨中心」（Center for Countering Digital Hate）今年的報告，臉書和推特上65%的疫苗假消息主要來自12人，名為「假消息12人」（The Disinformation Dozen），坦佩尼名列其一。該中心估計，這些反疫苗網紅在臉書、YouTube、Instagram 和推特上擁有超過5,900萬名粉絲。

她在俄亥俄州州議會的聽證會上一鳴驚人。她以專家身份作證，新冠疫苗的棘蛋白上有「金屬片」，打了疫苗不只會讓人「磁化」，還會跟所有的5G基地台連線，上傳不明資料，呼應疫苗是比爾蓋茲要在人類身上植入追蹤晶片的掩護，讓她從反疫苗的小圈子紅上主流媒體。

她的證據？她說就是你網路上看到的那些照片。

現場還有人證，自稱是護士的奧弗霍爾特（Joanna Overholt）試圖用脖子吸住鑰匙以證明坦佩尼的論點。「那你向我解釋為何鑰匙會吸在我身上？」她對在場的議員說，奈何鑰匙不配合，一直掉下來。

坦佩尼的聽證會影片立刻在網上瘋傳，為此美國疾管局已經出來闢謠。

「接種新冠疫苗不會讓你產生磁性，包括你手臂在內的接種處。」美國疾管局在官網上澄清，並公開在美獲得緊急使用授權的三款新冠疫苗（輝瑞、莫德納、嬌生）的成份。

Ref: https://www.cw.com.tw/article/5120216 圖片來源為講師Line

烏俄戰爭假新聞 (1/2)

謠言風向球

分享：

【謠言風向球】烏俄戰爭假訊息進化 三種手法攻擊媒體可信度

更新日期：2022-03-12

記者馬麗昕、陳慧敏／報導

烏俄之戰開打超過兩週，全球事實查核組織協力破解上千則假訊息，台灣事實查核中心也破解超過31則假訊息。查核中心觀察，在中文世界的烏俄戰爭假訊息有一類是攻擊主流媒體的可信度，攻擊的手法有三種，一種是用假訊息直接抹黑媒體，另一種是以「假」的事實查核抹黑媒體，第三種是用真實的查核結果，製造媒體亂報的現象。其意圖很簡單，就是要把讀者帶離開可信的消息來源。

造謠者攻擊「媒體可信度」，烏俄戰爭並不是特例，過去在不同的社會事件，造謠者在發動各種假訊息，意圖影響民眾，同時也會發動假訊息或抹黑言論，來攻擊主流媒體和查核組織，意圖切斷民眾的可信消息來源。

在烏俄戰爭的假訊息，查核中心觀測到，這一類攻擊媒體可信度的手法有三種：

攻擊媒體手法一：用假訊息指稱主流媒體造假

查核中心近期破解一則熱傳在中文世界的假訊息，其中一則挪用奧地利環保倡議團體的行動藝術，指控「西方媒體報導俄烏衝突陣亡者，直播鏡頭裡的屍體卻突然掀開蓋在臉上的黑布」；另一則傳言是挪用科幻電影的片段，卻指稱是「西方媒體擺拍俄羅斯轟炸烏克蘭平民」。這類假訊息挪用電影、行動藝術等內容，指稱主流媒體造假。

攻擊媒體手法二：用「假的」事實查核 貶低媒體

假訊息的另一個招式是使用「假的」事實查核，創造出主流媒體使用假照片、製作假新聞的印象。比如，有一則傳言是仿效查核報告的格式，宣稱「非常神奇，CNN的記者上次死於阿富汗 ，今天又再次神奇滴死於烏克蘭！現在連相片都懶得換了。」實際上，照片主角其實是活躍的電玩直播主，不是CNN記者。傳言偽裝成「查核報告」格式，借用查核組織的可信度，企圖騙取讀者信任。

另一則傳言把各國際主流媒體使用的一張烏克蘭受傷婦女的新聞照片，卻偽造為「假的查核報告」，宣稱「衛報：幾年前的瓦斯爆炸圖片也拿來冒充普京入侵……這些年你還在吃主媒的飼料？是不是口味有點重？」。

這種把真實照片用「假查核報告來偽破解」的手法，直接攻擊媒體可信度，但其回馬槍也剛好打中「查核組織」，讓讀者閱讀和接收「查核報告」時，也會搞不清楚真假，產生混淆。

攻擊媒體手法三：用闢謠結果來製造媒體亂報的現象

查核中心近期觀測到，有一系列傳言羅列許多「闢謠內容」，宣稱「台灣的媒體一直在跟著美國播報假新聞」、「網民開始會質疑綠徵新聞的真實度了，因為從這場戰爭開始台灣的媒體一直在跟播假新聞」。

檢視其闢謠內容，有些是查核報告曾發布的闢謠資訊，也夾雜著假的事實查核。這類傳言蒐集真假闢謠資訊，把砲口轉向，指控台灣媒體是造謠者，用來攻擊「台灣媒體」，貶低台灣媒體的可信度。

另一篇中國網站簡體字文章〈俄烏戰爭：世界媒體統一口徑，全球主義大團結，造假加統一口徑援烏責俄，到底誰被洗腦了？〉，就有相同的套路，它羅列18則「闢謠內容」，然後指控「世界媒體」的可信度。

關注中國資訊戰的《台灣民主實驗室》近期也發布文章〈烏俄戰爭：中文資訊操作觀察〉就提到，從3月3日開始，中國影音平台上流傳一則影片指控 BBC造假烏克蘭民宅遭俄軍轟炸影片，宣稱「西方媒體與社群媒體聯合造謠抹黑煽風點火」。此類以假借查核報告形式，來攻擊西方媒體誠信度的手法，已成為趨勢。

面對混亂的資訊生態，民眾被闢謠、反闢謠、查核報告、真新聞和假訊息弄得一頭霧水，要謹記的是，造謠者的意圖是讓我們覺得疲勞，放棄追求真實，甚至放棄閱讀相關資訊。只有持續關注此議題的資訊，尋找和建立可信消息來源的清單，不斷閱讀和交叉比對各種資訊，才能獲得珍貴的真實訊息。

Ref: https://tfc-taiwan.org.tw/articles/7077

烏俄戰爭假新聞 (2/2)

確實為烏俄戰爭被炸傷婦女

CNN的记者 上次死于阿富汗，今天又再次 死于乌克兰!

1. CNN集團官方推特帳號並未有網傳@CNNAfghan、@CNNUKR帳號
2. 照片中人物為電玩直播主，並非記者

挪用奧地利環保倡議團體的行動藝術

Ref:
https://tfc-taiwan.org.tw/articles/6996
https://tfc-taiwan.org.tw/articles/7022
https://tfc-taiwan.org.tw/articles/7029

境外資訊戰手法不斷翻新，假新聞威脅不容忽視

境外資訊戰手法不斷翻新，假新聞威脅不容忽視

作者 侯 冠州 | 發布日期 2021 年 09 月 30 日 10:44 | 分類 社群，科技生活，網路 分享 分享 Follow 讚 30 分享

來自境外的假新聞攻擊手法（或稱資訊戰）不斷翻新，不僅對政府單位造成威脅，現在就連資安業者也深受其害。資安情資研究公司杜浦數位安全（TeamT5）日前遭不實消息指控，聲稱 TeamT5 獲台灣政府授意，對日本政府與各大日本企業進行釣魚攻擊並大量收集個人資訊等；對此，TeamT5 除了發表聲明駁斥之外，TeamT5 執行長蔡松廷也呼籲，對於來路不明的新聞要保持存疑，並進一步求證，不要輕易相信和轉發，否則會變成假新聞傳播的幫兇。

緊跟時事議題，假新聞傳播防不勝防

此一事件發生在中秋連假前夕，有日本、台灣的內容農場，引述中國內容農場的不實消息，指控 TeamT5 利用網路釣魚方式誘使使用者點擊「驗證所有權」或「更新付款訊息」的網路釣魚連結，該連結則會連到偽造的日本亞馬遜登入頁面，就可以藉此蒐集使用者帳號密碼、憑證以及其他個人資訊等。此外，TeamT5 不僅竊取日本民眾個資，更入侵日本重要企業，像是軟銀、三和化學，以及其他研究、醫學機構；而這些作為都是經台灣政府授意。

蔡松廷表示，這種假新聞攻擊手法其實滿常見，算是一條龍的製造方式。後端有人負責製造假新聞，而前端則是有人負責經營社群平台，如 Facebook 粉專、Twitter 等的假帳號。通常會先做好一些假新聞上架內容農場，接著由前線的人在各種社群上轉發、散播；甚至這些假帳號還會留言、帶風向等。

TeamT5 也觀察到，像這種來自境外的假新聞攻擊常緊跟時事議題，並隨著關注的議題增加傳播手法，像是除了文字內容，還會有迷因圖、梗圖、影片或主題標籤（Hashtag）等。更甚者，就連語文種類也逐漸增加，譬如從一開始的中文，到日文、英文或是歐洲語系等。

根據 TeamT5 觀察，這種來自境外的假新聞，通常都會有兩種散播途經，一種是大家所熟悉的社群平台，創建假帳號開粉專，開始在粉專上丟許多迷因、梗圖散播。另一種則是透過「官方媒體」，因為官媒的觸及率更廣，更適合散布。

新聞 RSS

TeamT5 杜浦數位安全針對假新聞攻擊之澄清

2021. 09. 21 | TeamT5 Media Center Share:

圖片來源：Freepik

正值中秋連假之際，某特定內容農場開始散播關於 TeamT5 的謠言。該謠言以日文撰寫，其內容指稱 TeamT5 對日本政府與各大日本企業進行釣魚攻擊並大量收集個人資訊云云。

TeamT5 在此嚴正聲明，前開網路謠言絕非事實，TeamT5 從未從事任何網路攻擊的行動，更不會接受任何客戶委託進行網路攻擊之行為。

TeamT5 追查後發現，該造謠者係利用內容農場商業模式讓該不實內容於中文和日文的內容農場偕同轉發。但該內容不僅偽造釣魚信件的截圖，其內更有大量日文文法錯誤與錯字，還有許多中文詞彙假冒在其中，種種跡象均顯示該謠言撰稿者係偽冒成日文母語人士撰寫日文新聞稿。

初步分析後，TeamT5 情資團隊認為這起謠言的手法符合我們過往研究的國家級駭客散播不實新聞的戰術、技術和流程（Tactics, Techniques, and Procedures, TTPs）。目前 TeamT5 已將相關分析與證據備份，並已通報請台日雙邊的調查單位協助偵查。

謹再次重申，TeamT5 自創立以來，協助所有的客戶與夥伴阻擋各類網路威脅。我們過去、現在以及未來都不會主動發起或接受委託從事任何網路攻擊活動。

Contact: PR@teamt5.org

Ref:

1. https://technews.tw/2021/09/30/fake-news/
2. https://teamt5.org/tw/posts/clarification-on-malicious-disinformation-targeting-teamt5/

假造投開票做票不實影片被法辦

網傳「中選會選務人員作票」 檢調鑑定影片經剪接 涉誹謗偵辦中

2024-05-02 10:37 聯合報／記者房荷庭／台北即時報導

分享 31 分享

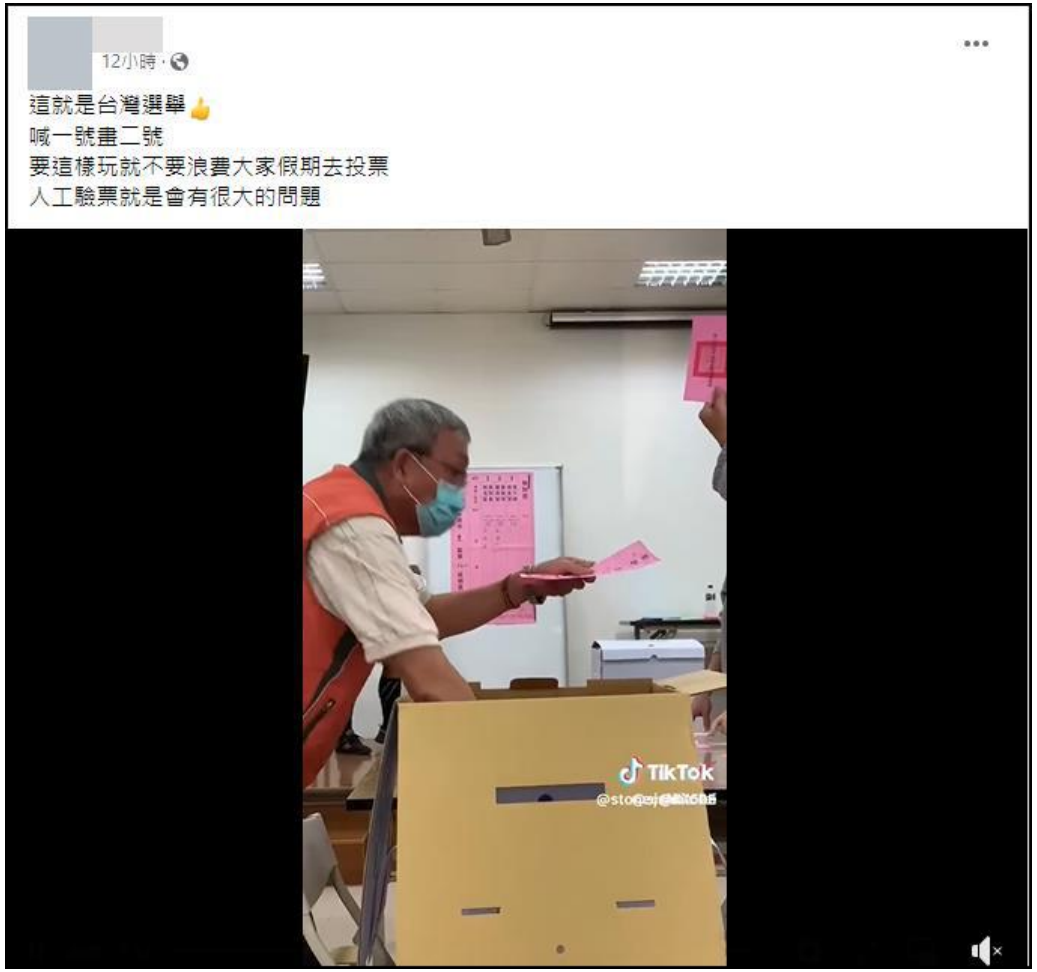
今年總統立委二合一選舉開票期間，網路社群平台大量流傳多則指稱中央選舉委員會選務人員作票以及選務不公等不實影片，檢調查出，一名李姓男子在TikTok帳號上傳影射開票所選務人員作票影片，經鑑定為遭剪接的不實影片，涉犯誹謗，全案偵辦中。

檢調查出，先前網路流傳一則指稱台南市東區第1340號投開票所選務人員作票影片，影片呈現「唱票員喊1號、記票員畫記2號」等畫面，經鑑識後發現是剪接不同時序的影像，意圖誤導民眾有選務人員偏袒特定候選人。

台北地檢署及調查局溯源調查，確認該影片出自台南市李姓男子的TikTok帳號，今年4月22日約談李男到案，李坦承確剪輯合成「唱票員喊1號、記票員畫記2號」影音、公開發布至個人TikTok帳號、YouTube頻道帳號及大陸抖音帳號。

檢調指出，大量網民觀看後該影片後心生不滿，轉傳影片至社群平台Dcard、Facebook及YouTube，李所為足以致生損害中選會與選務人員之名譽，嚴重傷害國人對選舉公正性的信賴。

調查局指出，總統副總統選舉罷免法、公職人員選舉罷免法及刑法，均已規範製作或散播選舉相關不實訊息須負刑事責任，呼籲民眾謹慎識別網路假訊息確實查證，切勿任意製作或轉傳不實訊息，以免誤蹈法網。



Ref: https://udn.com/news/story/7321/7937130

打擊錯誤訊息！台灣事實查核中心成立

- https://tfc-taiwan.org.tw/

事實查核報告 (1/3)

- 網傳台灣地震導致花蓮空軍基地F-16戰機鼻翼折斷【錯誤】

✕錯誤 政治與政策

分享：

【移花接木】網傳「台灣地震導致花蓮空軍基地F-16戰機鼻翼折斷」？

更新日期：2024-04-12

事實查核報告#2961

錯誤

【移花接木】網傳「台灣地震導致花蓮空軍基地F-16戰機鼻翼折斷」？

發布日期／2024年4月12日

經查：

【報告將隨時更新 2024/4/12版】

台灣東部海域4月3日上午7時58分發生規模7.2地震，花蓮受災嚴重。中國社群平台流傳一張「戰機鼻翼折斷」圖片，稱是台灣Ｆ-16因地震而損壞。這是真的嗎？

一、經查，傳言圖片為1992年8月24日安德魯颶風摧毀美軍F-16C戰機畫面，與2024年4月3日台灣地震無關。

二、台灣媒體報導與空軍司令部回應指出，在地震發生後，花蓮空軍基地修護棚廠內6架F-16型機及2架F-5型機，因地震滑動觸及工作架等，造成表面輕微擦傷，經檢測並無影響機身，均可立即修復，不影響戰備任務。

花蓮空軍基地F-16確實受到這次地震影響，有輕微受損，但傳言影用1992年美軍戰機受損畫面，刻意誤導為台灣空軍戰機受損畫面，為「移花接木」的錯誤訊息。

查核報告: https://tfc-taiwan.org.tw/articles/10479

事實查核報告 (2/3)

- 網傳邊開車邊吃東西是危險駕駛行為，直接扣牌6個月【部分錯誤】

部分錯誤 政治與政策

分享：

【部分錯誤】網傳影片「邊開車邊吃東西是危險駕駛行為，直接扣牌6個月」？

更新日期：2024-03-01

事實查核報告#2885

部分錯誤

網傳影片「邊開車邊吃東西是危險駕駛行為，直接扣牌6個月」？

發布日期／2024年3月1日

經查：

【報告將隨時更新 2024/3/1版】

一、《道路交通管理處罰條例》第43條規定，禁止在道路上蛇行或以其他危險方式駕車，否則將處罰鍰、禁止駕駛並吊扣該汽車牌照6個月。不過，法規並未具體列出「其他危險方式」有哪些，也沒有明文規定開車時不能飲食。

二、警方表示，「危險駕駛」的認定依據是「駕駛人開車時的行為是否影響行車安全」，而不是有無飲食。例如，開車時為了整理頭髮而雙手離開方向盤，就可能涉及危險駕駛。

三、駕駛人因開車吃東西、危險駕駛受罰時有所聞。警方提醒，雖然法規並未明文規定開車時不能飲食，或是不能單手握方向盤，但為了行車安全，駕駛人最好能專心開車，不要一邊駕車一邊做其他事情。

邊開車邊吃東西若造成危險駕駛，確實可能處罰鍰、扣牌6個月，但並非開車吃東西就會被認定為危險駕駛而扣牌。因此，傳言為「部分錯誤」訊息。

結論

【報告將隨時更新 2024/3/1版】

一、《道路交通管理處罰條例》第43條規定，禁止在道路上蛇行或以其他危險方式駕車，否則將處罰鍰、禁止駕駛並吊扣該汽車牌照6個月。不過，法規並未具體列出「其他危險方式」有哪些，也沒有明文規定開車時不能飲食。

二、警方表示，「危險駕駛」的認定依據是「駕駛人開車時的行為是否影響行車安全」，而不是有無飲食。例如，開車時為了整理頭髮而雙手離開方向盤，就可能涉及危險駕駛。

三、駕駛人因開車吃東西、危險駕駛受罰時有所聞。警方提醒，雖然法規並未明文規定開車時不能飲食，或是不能單手握方向盤，但為了行車安全，駕駛人最好能專心開車，不要一邊駕車一邊做其他事情。

邊開車邊吃東西若造成危險駕駛，確實可能處罰鍰、扣牌6個月，但並非開車吃東西就會被認定為危險駕駛而扣牌。因此，傳言為「部分錯誤」訊息。

查核報告: https://tfc-taiwan.org.tw/articles/10348

事實查核報告 (3/3)

- 網傳加油站傳單不要拿，傳單上有迷魂藥【錯誤】

✕錯誤 生活

分享：

【錯誤】網傳音檔「某里長提醒人蛇集團手法，加油站傳單不要拿，傳單上有迷魂藥」？

更新日期：2024-05-06

事實查核報告#2997

錯誤

網傳音檔「某里長提醒人蛇集團手法，加油站傳單不要拿，傳單上有迷魂藥」？

發布日期／2024年5月6日

經查：

【報告將隨時更新 2024/5/6版】

一、刑事局表示，台灣截至目前並無發生民眾拿傳單後頭暈昏迷、警局驗出傳單有毒等事件。

二、傳言音檔聲稱是來自高雄鳥松里里長的提醒。鳥松里長表示，網傳音檔不是他的聲音，也非其所錄製或發布的內容。鳥松里也沒有發生網傳有人拿了加油站傳單後暈眩、報警化驗傳單上有迷魂藥的事情。

高雄市政府警察局、刑事警大隊、仁武分局鳥松分駐所均指出，傳言音檔所述內容是假訊息，從未接獲網傳聲稱的迷魂藥傳單報案案件。

三、毒物專家說，依傳言情境，要透過接觸傳單毒物在短時間內頭暈昏迷相當困難，實務不太可能發生。

四、傳言最早來自國外舊謠言變形，並在2019年、2022年、目前在中文網路世界流傳不同版本內容。

因此，傳言為「錯誤」訊息。

查核

查核點一：網傳音檔「不要拿加油站傳單」是真的嗎？

近期是否有相關事件？

（一）刑事局表示，台灣截至目前並無發生民眾拿傳單後頭暈昏迷、警局驗出傳單有毒等事件。

（二）傳言音檔聲稱是來自高雄鳥松里里長的提醒。查核中心致電詢問鳥松里里長謝唐欽，他表示，網傳音檔不是他的聲音，也不是其所錄製或發布的內容。鳥松里也沒有發生網傳有人拿了加油站傳單後暈眩、報警化驗傳單上有迷魂藥的事情。

高雄市政府警察局仁武分局鳥松分駐所表示，傳言音檔所述內容是假訊息，分駐所沒有受理過有民眾報案發生類似情況。

此外，高雄市政府警察局、刑事警大隊均表示，從未接獲網傳聲稱的迷魂藥傳單報案案件。

網傳手法是否合理？

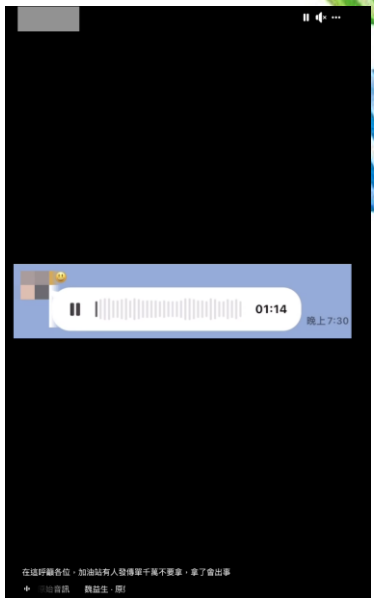
查核中心在第1883號查核報告曾訪問毒物專家楊振昌，他表示，依傳言情境，要透過接觸傳單毒物在短時間內頭暈昏迷，相當困難，不太可能發生。如果毒物是塗抹在傳單上，除非發傳單的人有經過縝密的保護，否則也有中毒的可能性，這與傳言提及的隨機發傳單給人的情境也不太相符。

查核點二：傳言流變為何？

查核中心在2019年8月發布第139號查核報告，曾就網傳「在加油站加油，拿了一張廣告名片後頭暈目眩」進行查核，顯示傳言是美國2008年流傳的謠言轉化而來。

在2022年8月傳言出現變形版本，第1883號查核報告顯示，當時傳言出現不同地點包含「最近恆春有人發傳單，不要拿」、「南部的群友，說台南發現有於加油站發廣告傳單」、「我朋友在嘉義市加油拿人發傳單被放藥頭暈暈」、「近期我家人朋友在下新庄有遇到陌生人發傳單」。

因此，傳言最早來自國外舊謠言變形，並在2019年、2022年、目前在中文網路世界流傳不同版本內容。



查核報告: https://tfc-taiwan.org.tw/articles/10548

事實查核報告 (新冠肺炎專區)

COVID-19 新冠肺炎專區

有看有保庇，一起來防疫！

遏止不實訊息傳播，也是一道重要防線。

防疫需要整個社會團結，對疫情謹慎以對，分享正確資訊，採取合宜的措施。然而對於新型流行傳染病的恐懼和焦慮，可能讓不實訊息趁勢蔓延，進而導致整個社會的恐慌，甚至引起人與人之間的不信任、猜忌或質疑，不實訊息儼然已經成為防疫必須面對挑戰之一。

台灣事實查核中心為了防堵新型冠狀病毒相關的不實訊息，參與國際事實查核聯盟體系（IFCN）組織的工作平台，與來自全球各地的事實查核組織協同工作。查核中心將在防疫期間，持續整理與武漢肺炎相關的查核報告，盼能減緩社會大眾對疫情的恐慌。

本中心特別感謝 新興科技媒體中心 協助解讀科學原始研究、引介學者和專家，以及各領域學者、專家、醫師在此關鍵時刻，撥冗接受查核中心諮詢及採訪。

本中心近期也發現，不少讀者對於疑似不實訊息的識讀能力及查證能力增加了！除了主動提出申訴，也會附上自行查證的初步結果，或是在報告刊登以後，提出疑問、糾正或補充，在此感謝各位讀者。

我們樂見大家持續共同參與事實查核工作，也歡迎讀者與持續關注疑似不實訊息流傳情形，在不實訊息的防疫陣線，與我們一起努力。

而防疫專區讓你眼花撩亂嗎？很簡單，加入台灣事實查核中心的LINE聊天機器人@tfctaiwan，你把傳言整段轉分享給我們，就能得到答案，或啟動我們的查核機制喔。

偏方篇

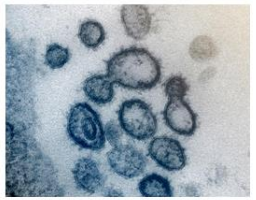
【錯誤】網傳「山東蘭陵县146萬人，目前無一感染...分析原因:他们是大蒜种植区...蘭陵農田...

【錯誤】網傳「武漢的病毒一碗煮沸的濃大蒜水就能喝好」、「將大蒜搗成泥，用力吸到肺...

【錯誤】網傳中國疾病防預中心通告：「經武漢新型冠狀肺炎病員檢測結果都未曾有飲茶習慣...

【錯誤】傳言引述文獻指稱「紅茶與普洱茶，抗冠狀病毒...紅茶跟普洱茶所含的茶黃素（TF3）...

個人防疫作為篇



【部分錯誤】網傳「武漢肺炎已經定名為SARI了，確定是SARS的強進化病毒...目前市面上所有...

【部分錯誤】網傳「好消息！新病毒不耐高溫。冠狀病毒在56攝氏度、30分鐘就死亡了...新病...

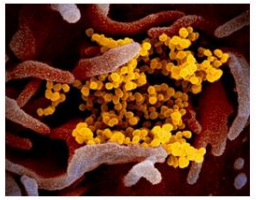
【錯誤】網傳「鐘院士的防病毒高招：建議各位去醫院或其他公共場合之前用淡鹽水漱一下嘿...

【錯誤】網傳「帶毛領或是絨線的衣服外套，較容易吸附病毒」？

症狀與檢測篇

【錯誤】網傳「我同學的嫡親外甥...在深圳醫院工作...剛剛來電讓我轉告訴朋友們：感冒時，...

【錯誤】網傳「由於NCP新型冠狀病毒，有0～24天的潛伏期...專家提供一方法讓你盡早知道自...



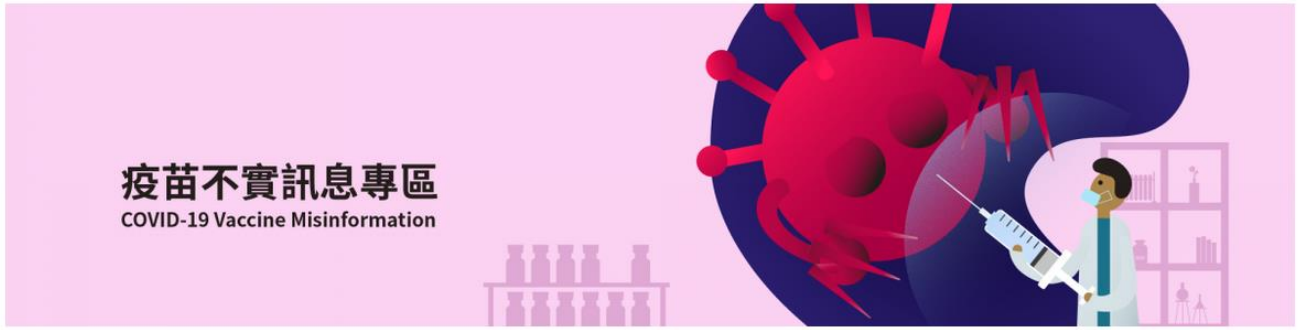
【部分錯誤】網傳「這是每天 #COVID-19感染的情況，請大家注意...」？

【錯誤】網傳「作者陳敏芳女士是台大醫學院院長董大成教授的長媳，定居美國西雅圖，分享...

Ref: https://tfc-taiwan.org.tw/topic/3826

中華電信 Chunghwa Telecom

事實查核報告 (疫苗不實訊息專區)



【部分錯誤】網傳「休士頓名醫毛志江、何樹平，雙雙得新冠重症去世...兩位醫生早已接種過...

【錯誤】網傳「輝瑞、莫德納的mRNA疫苗是帶有遺傳因子的疫苗，會影響人體基因，有高度...

【錯誤】網傳「急徵疫苗預搶專員，無經驗可，每月實賺3萬元」？

【錯誤】網傳徵才貼文「嬌生疫苗徵醫療助理與防疫人員」？

不良反應事件

【部分錯誤】網傳照片為「輝瑞疫苗受試者4名出現顏面神經麻痺症狀」？

【錯誤】網傳圖片宣稱「美國疾控中心的統計數據顯示，美國人注射輝瑞等疫苗已造成死亡病...

【錯誤】網傳「去打新冠肺炎疫苗前，要吃飽再去，並建議先喝250CC溫水，可避免不良反...

【錯誤】網傳「打新冠疫苗前兩三天，禁止攝取所有的澱粉，讓身體發炎指數下降，每3個小時...

疫苗不實訊息專區

疫苗不實訊息 | 不良反應事件 | AZ疫苗開打 | 美國疫苗出事 v.S 中國疫苗好棒 | 其他疾病疫苗 | 研究與動態 | 國產疫苗不實訊息

疫苗不實訊息

【錯誤】網傳影片宣稱「特朗普黑幫全都接種了新冠疫苗！2020年4月20日，特朗普的新冠新聞...

【事實釐清】網傳「疫苗不要打！流感及新冠會變異是沒有可免疫的疫苗，只是用處理過的...

【錯誤】網傳「羅伯特・甘迺迪：mRNA疫苗直接干預患者的遺傳物質，會改變基因的遺傳...

【事實釐清】網傳「打完新冠疫苗，並非不會得Covid-19。打完疫苗後會有更多無症狀感染...

【錯誤】網傳訊息「未來開始施打AZ疫苗，可能會有血栓疑慮，可以現在開始多喝醋，舒活血...

【錯誤】網傳「免疫力差的人，打疫苗副作用也會比較多，甚至會死亡，想減輕疫苗的副作用...

【錯誤】網傳「打疫苗千萬不能揉，揉了極為容易產生血栓」？

【部分錯誤】網傳圖卡「長者高溫打疫苗要注意，應等身體狀況平穩再打疫苗，以防打完疫苗...

中華電信 Chunghwa Telecom

Ref: https://tfc-taiwan.org.tw/topic/5156

MyGoPen｜這是假消息

- https://www.mygopen.com

Home › 食安 › 紅茶

【易誤解】喝紅茶不能配花生？增強黃麴毒素？勿過度解讀！專家詳解

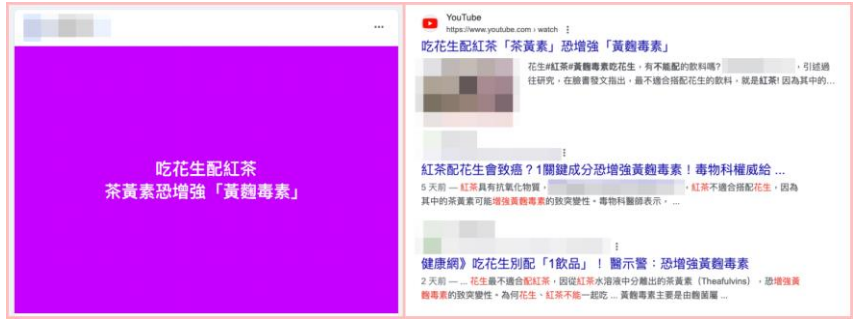
2024/5/5

你可以先知道：

（1）傳言出處為國際知名期刊、專家引用立意良善，但研究的實驗方法為「安姆氏測試」，不能推論為人體也是同樣效果，傳言說法並未提及連作者都說「人體尚待驗證」、易生誤導。

（2）研究是「黃麴毒素」的致突變性，所以只要花生或其他堅果、穀物、中藥，沒有發黴、沒有黃麴毒素，就不用擔心傳言所說的問題。

網傳「最不適合配花生的飲料是什麼」貼文，是由國內專科醫師在臉書分享，指出紅茶因為含有「茶黃素」（Theafulvins）會增強「黃麴毒素」的致突變性。但專家表示，該研究仍是非常初步的實驗，是利用鼠肝臟萃取物測試物質毒性的「安姆氏測試」（Ame's Test），是一種快速檢測、篩選物質的有效方法，但有偽陽性偏高的問題，且不能擴大解釋為在人體也是同樣效果，建議民眾只要不要食用發黴的花生，或是只要保存不當就容易受黃麴毒素真菌感染的食物，就能避免傳言所說的問題。

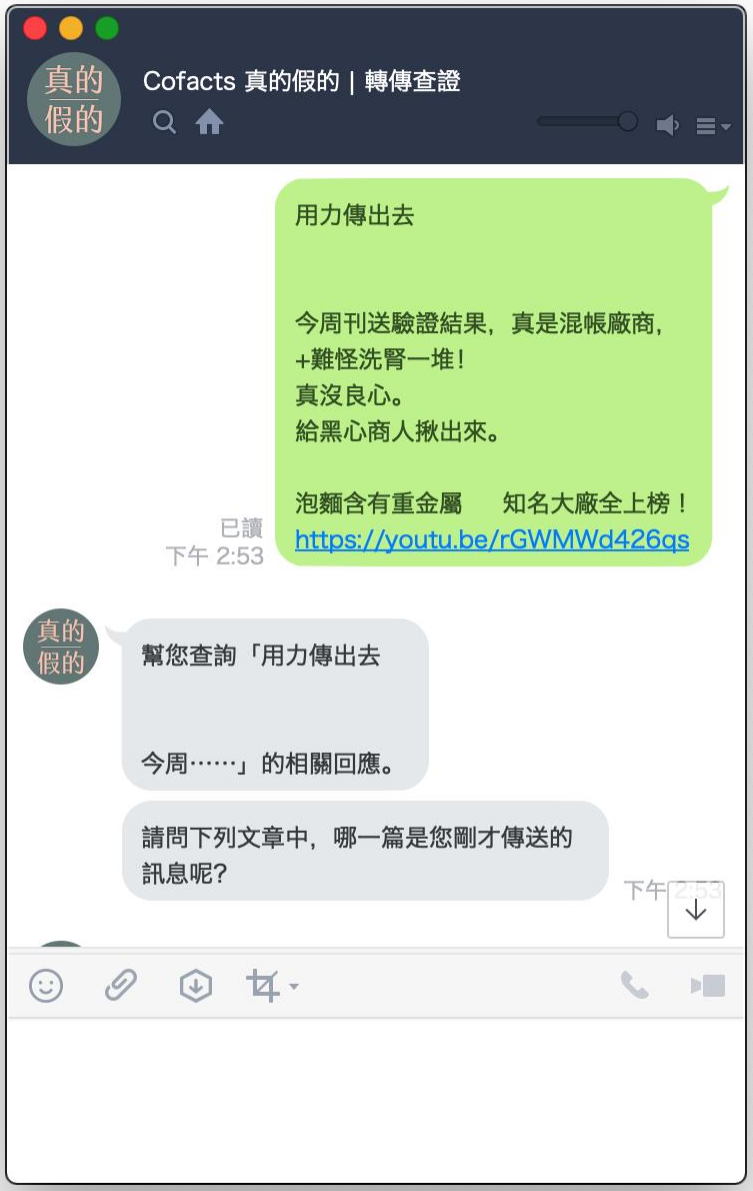


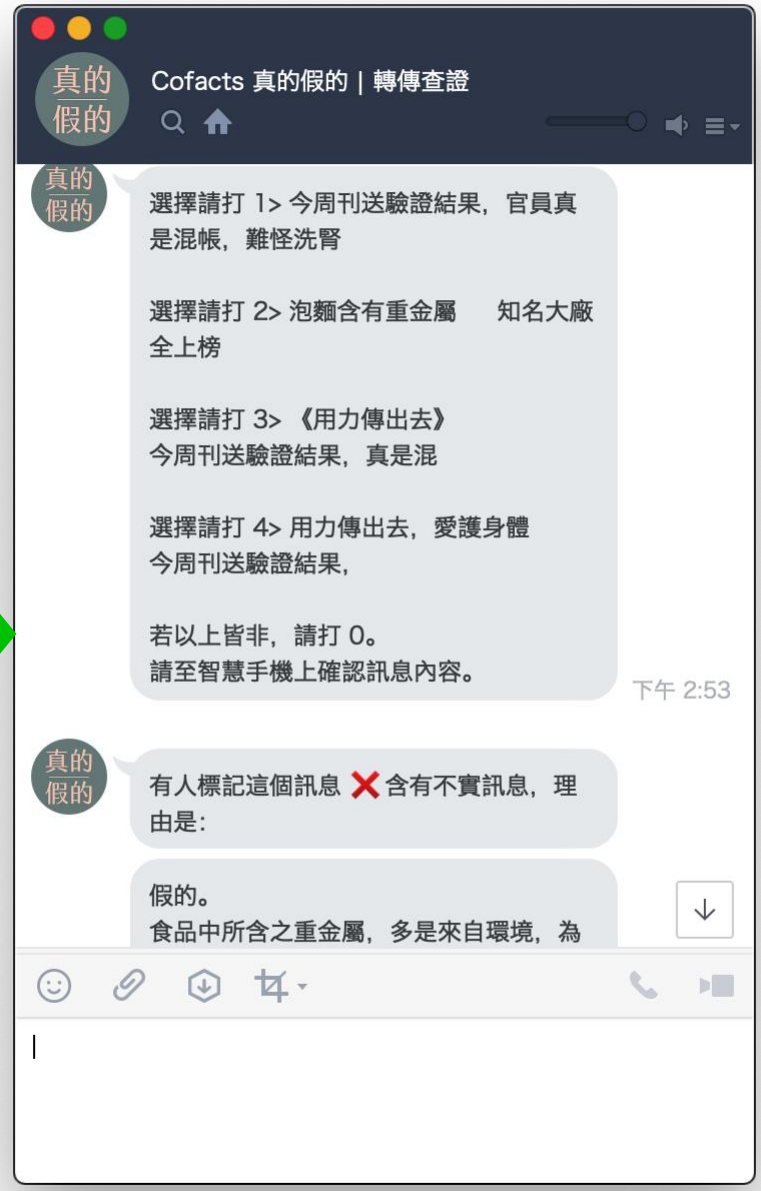
Ref: https://www.mygopen.com/2024/05/tea-peanut.html

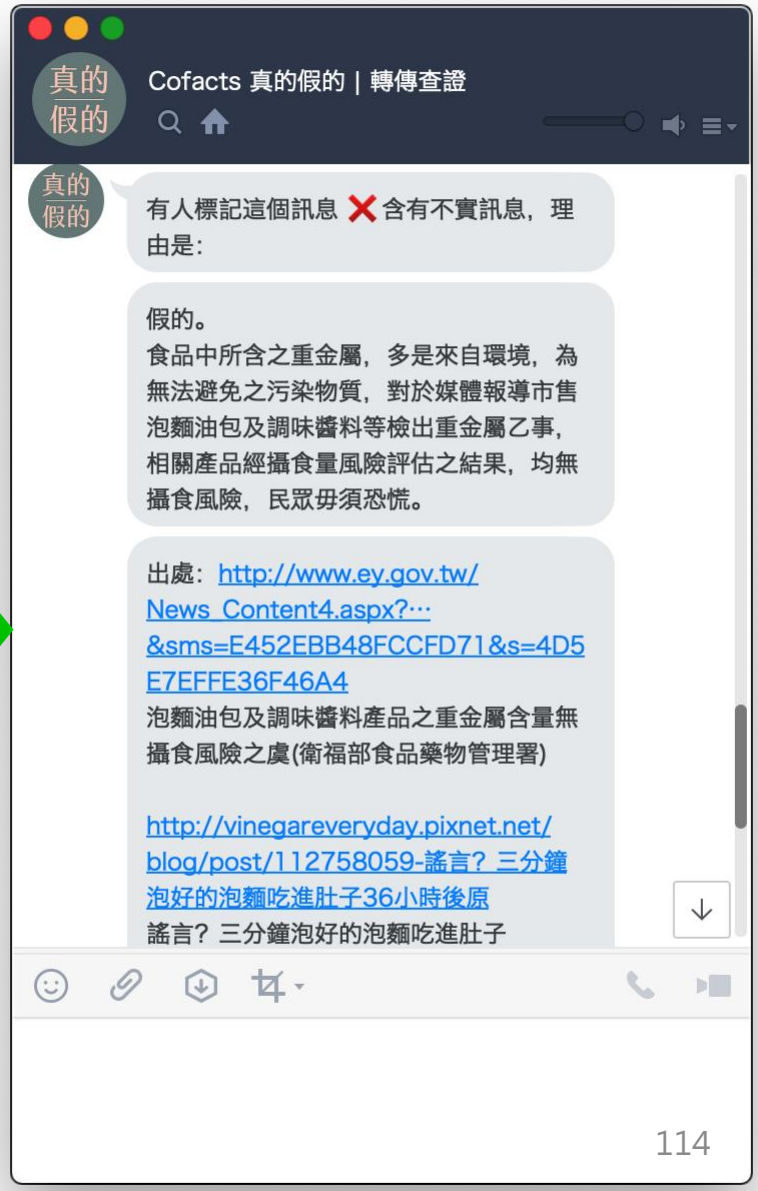
g0v Cofacts 真的假的 [LINE chatbot]

- https://cofacts.g0v.tw
- 「Cofacts 真的假的」是一套連結網路訊息與事實查核的協作型系統，其中：
  - **網路訊息**：透過 LINE chatbot 搜集使用者所回報的 LINE 上的轉傳訊息
  - **事實查核**：編輯們在網路上找到的現有查證文章或是撰寫的回應
  - **協作型系統**：任何人都可以轉傳訊息進來。並且，任何人都可以當編輯，一起在網站上面一同協作。產出的內容以 CC0 貢獻至公眾領域

Cofacts 真的假的

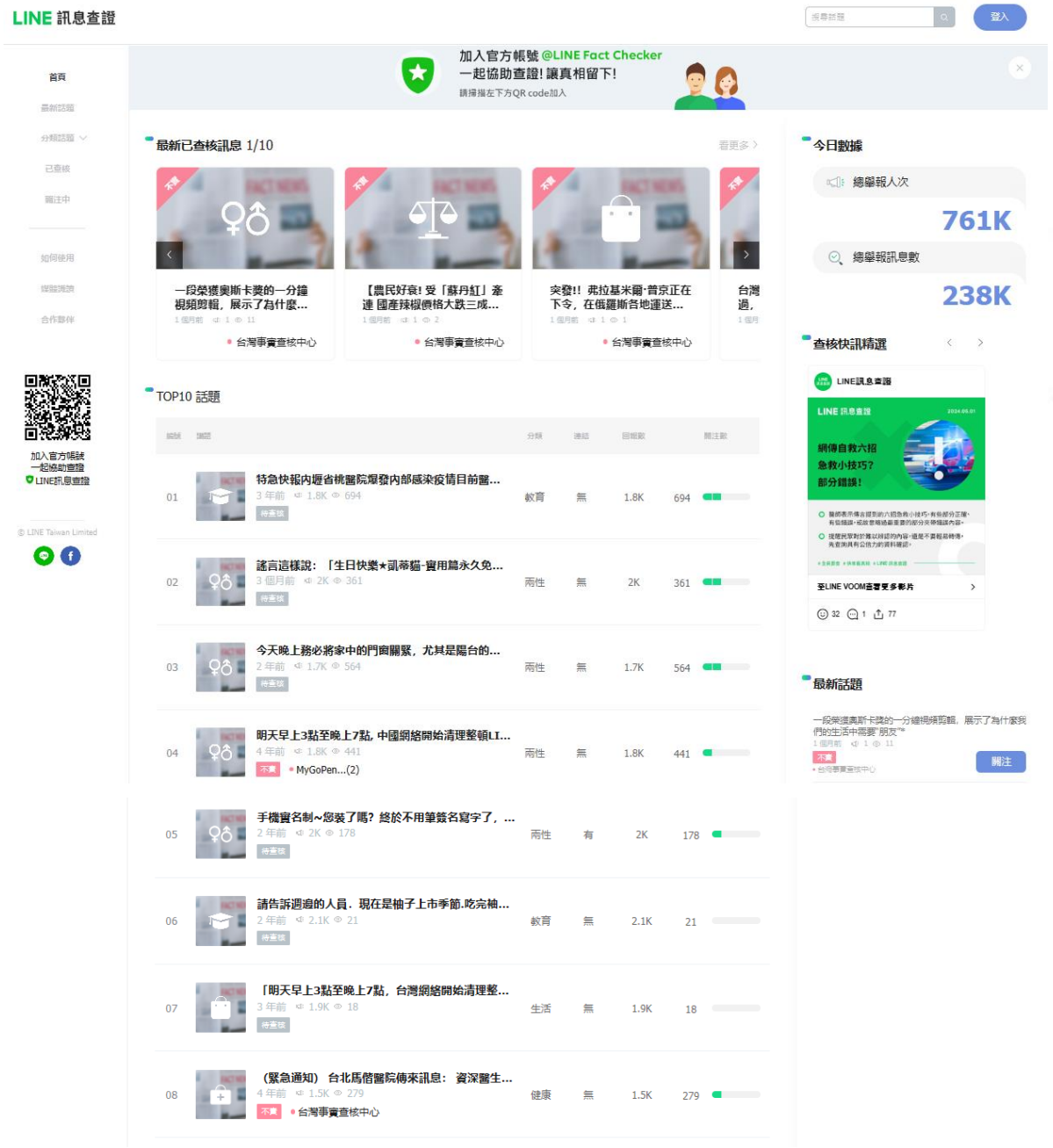






Line推出數位當責計畫

- Line是全台最多人使用的通訊軟體，受假消息的影響也是首當其衝
- Line於2019推出謠言查證官方帳號，只要將不確定真偽的訊息轉貼給此帳號，就能幫您做事實查核
  - 與Confacts、MyGoPen、台灣事實查核中心等查核機構合作
- 心存懷疑、查證、進而將查證結果回饋他人，達成更大的影響力



Ref: https://fact-checker.line.me

政府機關闢謠專區

- 行政院-即時新聞澄清
  - https://www.ey.gov.tw/Page/5519E969E8931E4E
- 農業部-即時新聞澄清
  - https://www.moa.gov.tw/theme_list.php?theme=rss_news&sub_theme=explain
- 內政部警政署刑事警察局-即時新聞澄清、165全民防騙網
  - https://www.cib.npa.gov.tw/ch/app/news/list?module=news&id=1886
  - https://165.npa.gov.tw/
- 國家通訊傳播委員會-即時新聞澄清
  - https://www.ncc.gov.tw/chinese/news.aspx?site_content_sn=3562&is_history=0
- 衛生福利部食品藥物管理署-食藥闢謠專區
  - https://www.fda.gov.tw/TC/news.aspx?cid=5049&cchk=55abc933-3e57-48db-afff-a8a4cc1e4ae0
- 衛生福利部國民健康署 - 真相與闢謠
  - https://www.hpa.gov.tw/Pages/List.aspx?nodeid=70

結論

- 釣魚網站、郵件，不斷的推陳出新，**強化自身的安全警覺**才是上策
  - 不要隨意點擊郵件中的**網址連結和附加檔案**
  - 收到不確定的可疑郵件，要**打電話或親自和本人確認**
  - 為所有的帳戶設定**不同的帳號和複雜的密碼**，並打開**二步驟驗證**
  - **別在沒有https的網站上輸入任何個資、密碼，就算有https也要再三小心**
- 對於假新聞的防治，不管是事實查核網站、政府法律規範，都只能治標，無法杜絕假新聞的產生，**謠言止於智者**，最終判斷還是得回歸到讀者的身上
  - **勿中標題殺人陷阱：不要只看標題就下結論，尤其是聳動標題**
  - **轉發分享訊息時，先停一停，想一想**
  - **發現假新聞、假消息，要勤於檢舉**


Value Creator for
Investors, Customers, Employees, and Society
感謝聆聽 敬請指教!