永遠走在最前面
Always Ahead

社交工程防範認知

掌握先機 即時回應

課程大綱

① 社交工程介紹

② 網路釣魚

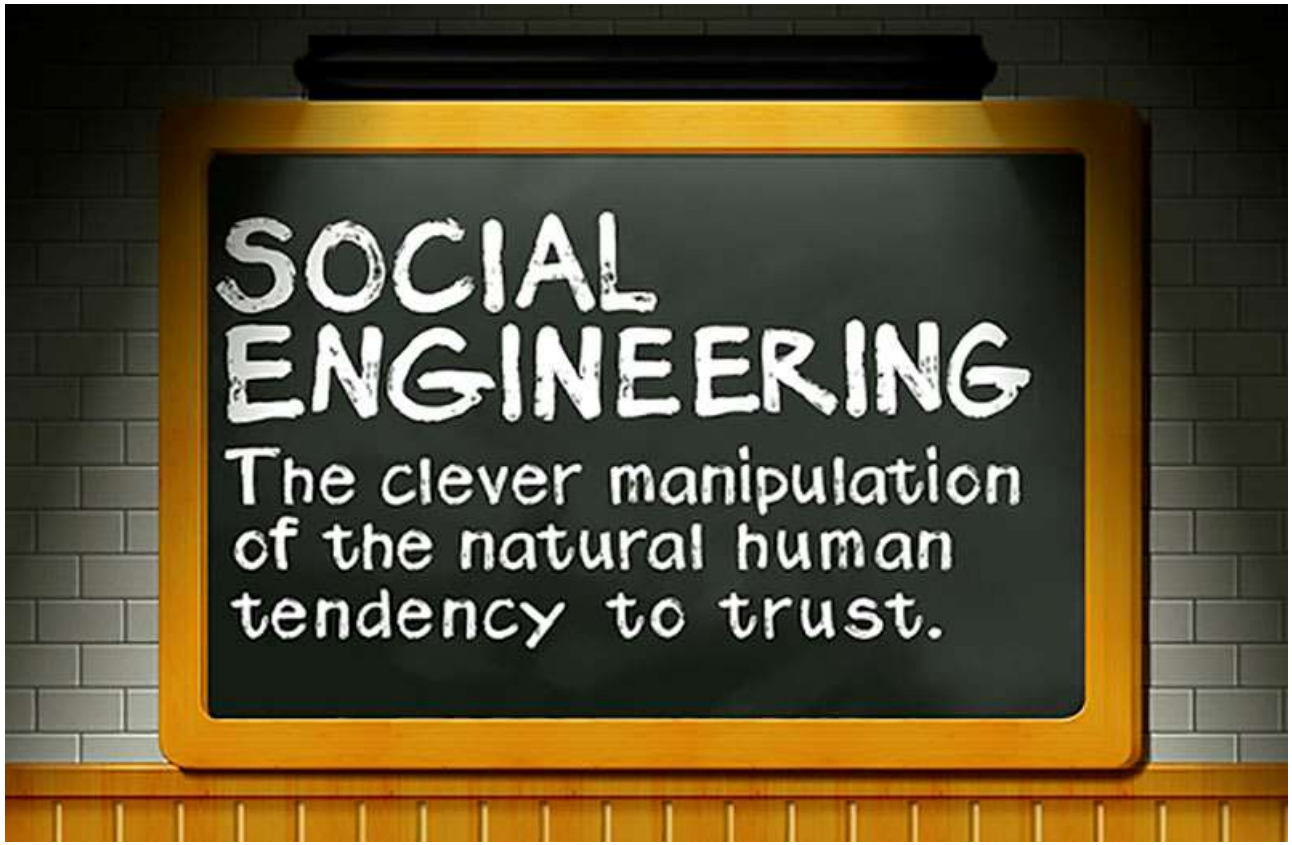
③ 社群詐騙

④ 變臉詐騙(BEC)

⑤ 假新聞

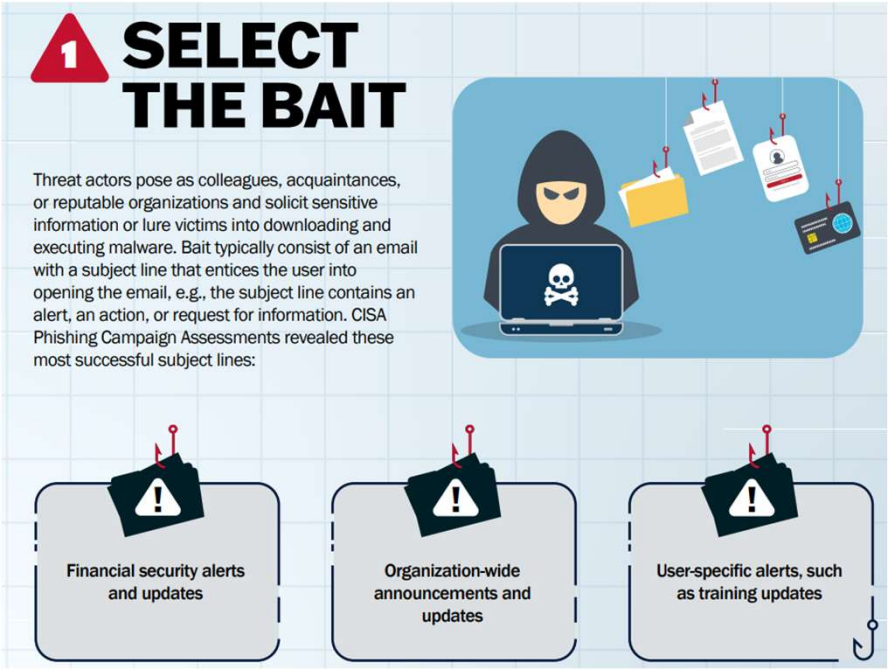
溫習一下...

- 社交工程是?


SOCIAL
ENGINEERING
The clever manipulation
of the natural human
tendency to trust.

社交工程與網路釣魚趨勢(1/2)

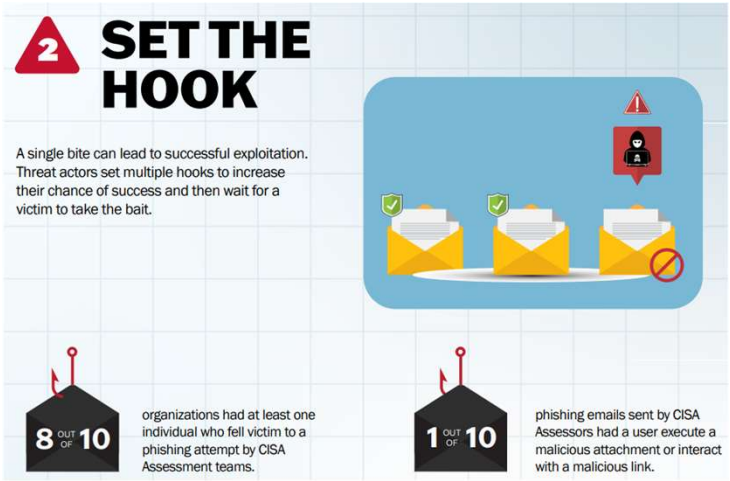
- 網路釣魚是一種社交工程的手法
- 冒充信賴的同事與組織，企圖引誘受害者上當
- 可利用的管道多元，包含電子郵件、通訊軟體或SMS簡訊，以及電話等
- 常見題材
  - 財務相關安全通知與最新消息
  - 全公司公告與最新消息
  - 針對受害人的通知，例如員工訓練消息
- 現在有許多衍伸手法
  - 社群詐騙
  - 變臉詐騙（BEC）
  - 假新聞

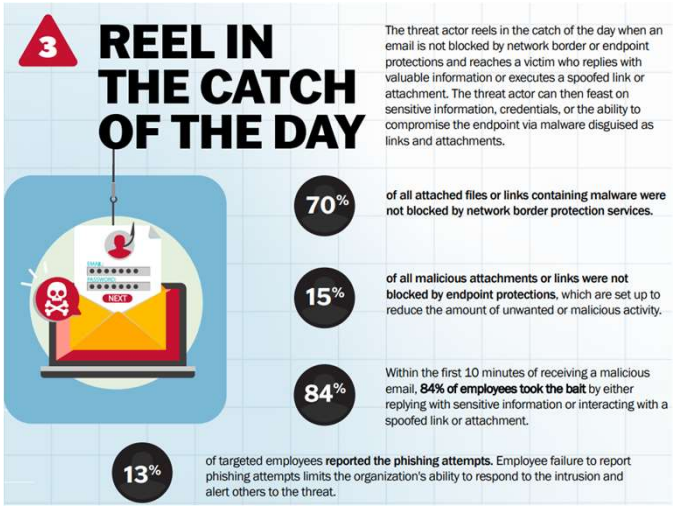


資料來源: Phishing Infographic (cisa.gov)

社交工程與網路釣魚趨勢(2/2)

- 美國CISA 2023/2 Phishing Infographic報告指出
  - 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
  - 70%的惡意程式或惡意連結未被網路邊界防護服務阻擋
  - 15%的惡意程式未被端點防護產品阻擋
  - 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





資料來源: Phishing Infographic (cisa.gov)

網路釣魚(Phishing) - 釣魚網站、社交工程郵件

網路釣魚

- 網路釣魚(Phishing)，是一種企圖從**電子通訊**中，透過偽裝成信譽卓著的法人媒體以獲得如**用戶名、密碼和信用卡明細**等個人敏感資訊的犯罪詐騙過程。
  - 這些通訊都聲稱（自己）來自於風行的**社群網站**（YouTube、Facebook、Line）、**拍賣網站**、**網路銀行**、**電子支付網站**、或**網路管理者**（網際網路服務提供者、公司機關），以此來誘騙受害人的輕信
  - 網釣通常是透過**e-mail或者即時通訊**進行
  - 它常常導引用戶到**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
  - 就算使用強式加密的**SSL伺服器認證**，要偵測網站是否仿冒實際上仍很困難
  - 網釣是一種利用社交工程技術來愚弄用戶的實例
  - 它憑恃的是現行網路安全技術的不足
  - 嘗試透過立法、用戶資安意識培訓、宣傳、與資安防護等措施對抗日漸增多網釣案例

Ref: https://zh.wikipedia.org/wiki/網路釣魚

反網路釣魚工作小組(APWG)

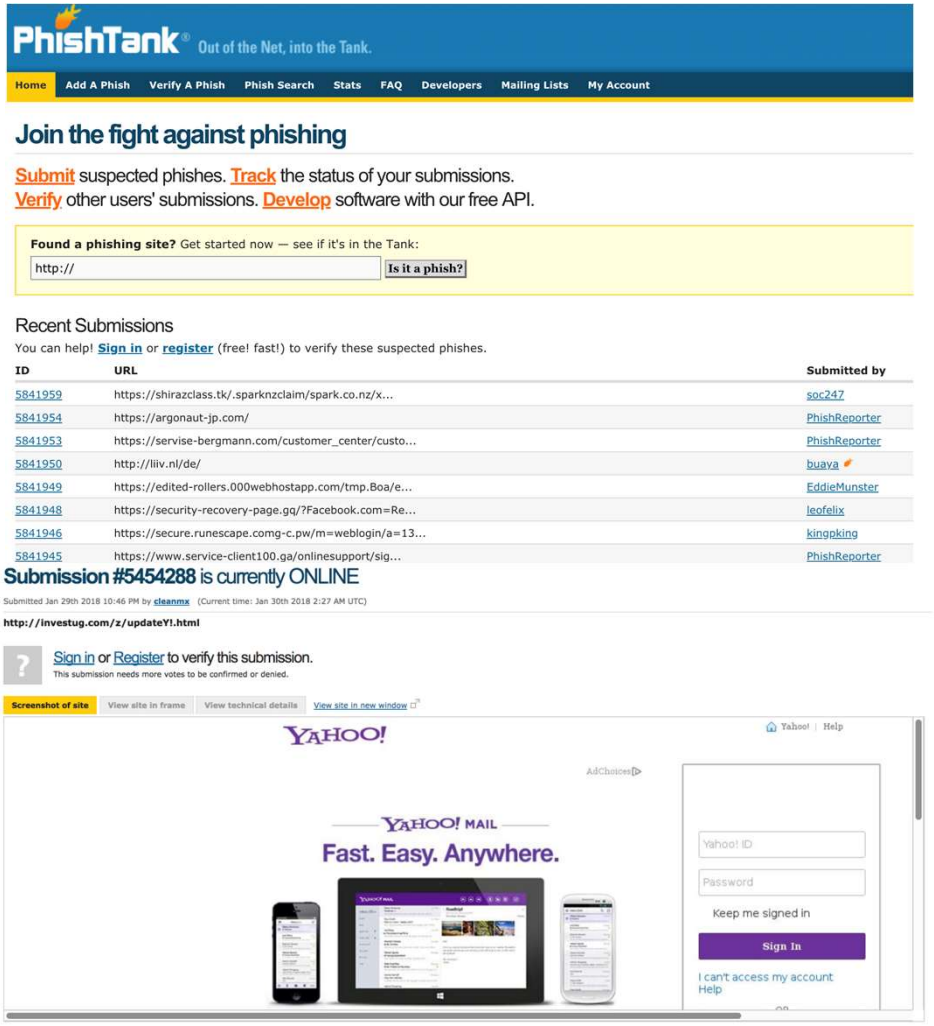
- https://apwg.org/
- 反網路釣魚工作小組（APWG）是一個國際聯盟，匯集了受網路釣魚攻擊影響的企業，安全產品和服務公司，執法機構，政府機構，行業協會，區域性國際條約組織和通信公司
- 專注於**詐騙電子郵件**、**釣魚網站**、**網址嫁接**和**電子犯罪**的研究與情資，近年也開始研究**加密貨幣**
- APWG由David Jevans於2003年創立，擁有來自全球1700多家公司和代理商的超過3200多名會員
  - 成員公司包括BitDefender，Symantec，McAfee，VeriSign，IronKey和Internet Identity等領先的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

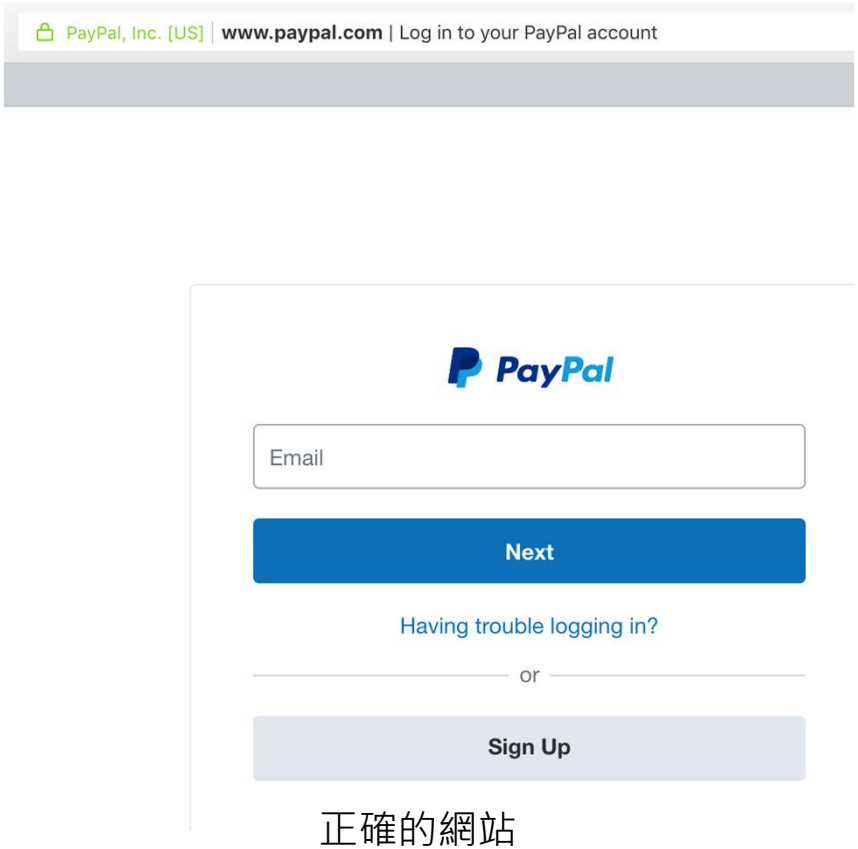
- PhishTank是基於社群的反釣魚攻擊服務
- PhishTank於2006年10月2日作為**OpenDNS**的子公司建立，用戶可以從世界各地向其匯報釣魚網站，經其他用戶以投票的形式認證後，即通過公開的API共享給所有使用PhishTank服務的機構和個人



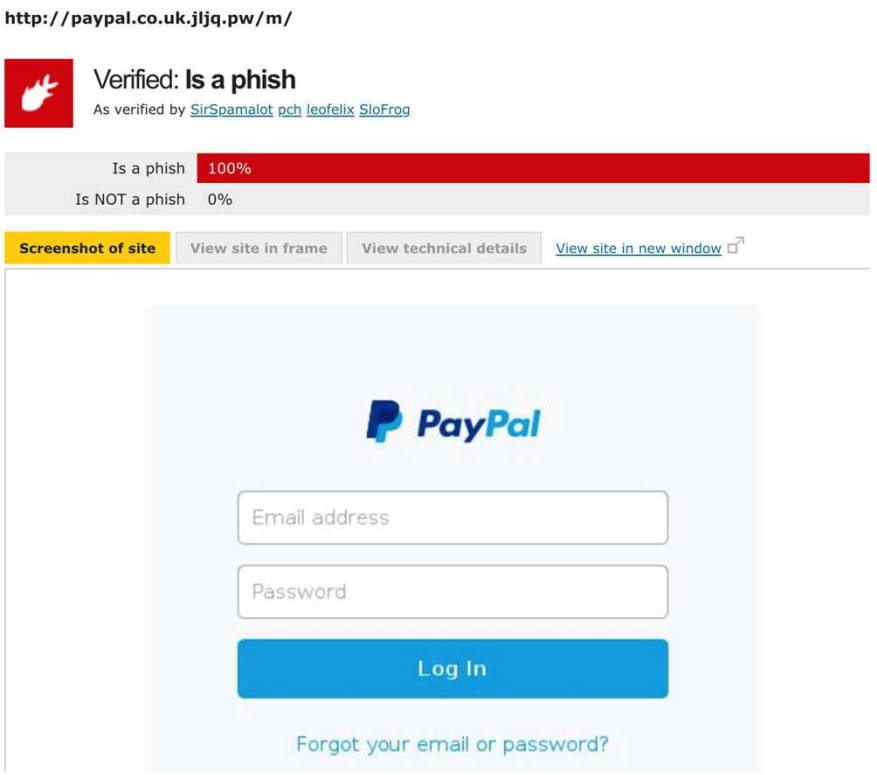
Ref: https://zh.wikipedia.org/wiki/PhishTank

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

臉書成溫床 一頁商店詐騙竄升

2017-10-23

〔記者陳宜加、姚岳宏／台北報導〕網路科技普及，更多消費者習慣於網路購物，但新興「一頁商店」詐騙型式竄起，每年新增近千件，臉書成為最大溫床。受害者受「限時優惠」、「七天無條件退貨」條件吸引，最後收到舊報紙、垃圾，卻無法退換貨，求償無門。

台北陳先生上月透過臉書廣告，購買時下流行「仿真肌肉內衣」受騙。（記者陳宜加攝）

所謂「一頁商店」，即透過平台或臉書廣告，仿冒知名品牌或平台業者名稱，搭配超低折扣優惠，但商品僅單一頁面，沒有賣家或商品來源等資訊。

買千元仿真肌肉內衣 卻拿到廉價上衣

像是台北陳先生上月透過臉書廣告，購買時下流行的「仿真肌肉內衣」，每件要價上千元，賣家宣稱貨到付款、享有七天鑑賞期。但收到實品卻是一件普通白色上衣，坊間賣不到兩百元，他聯繫賣家退貨事宜，才發現對方所留聯絡資訊為假，物流公司則表示代收貨款，無法協助追回款項。

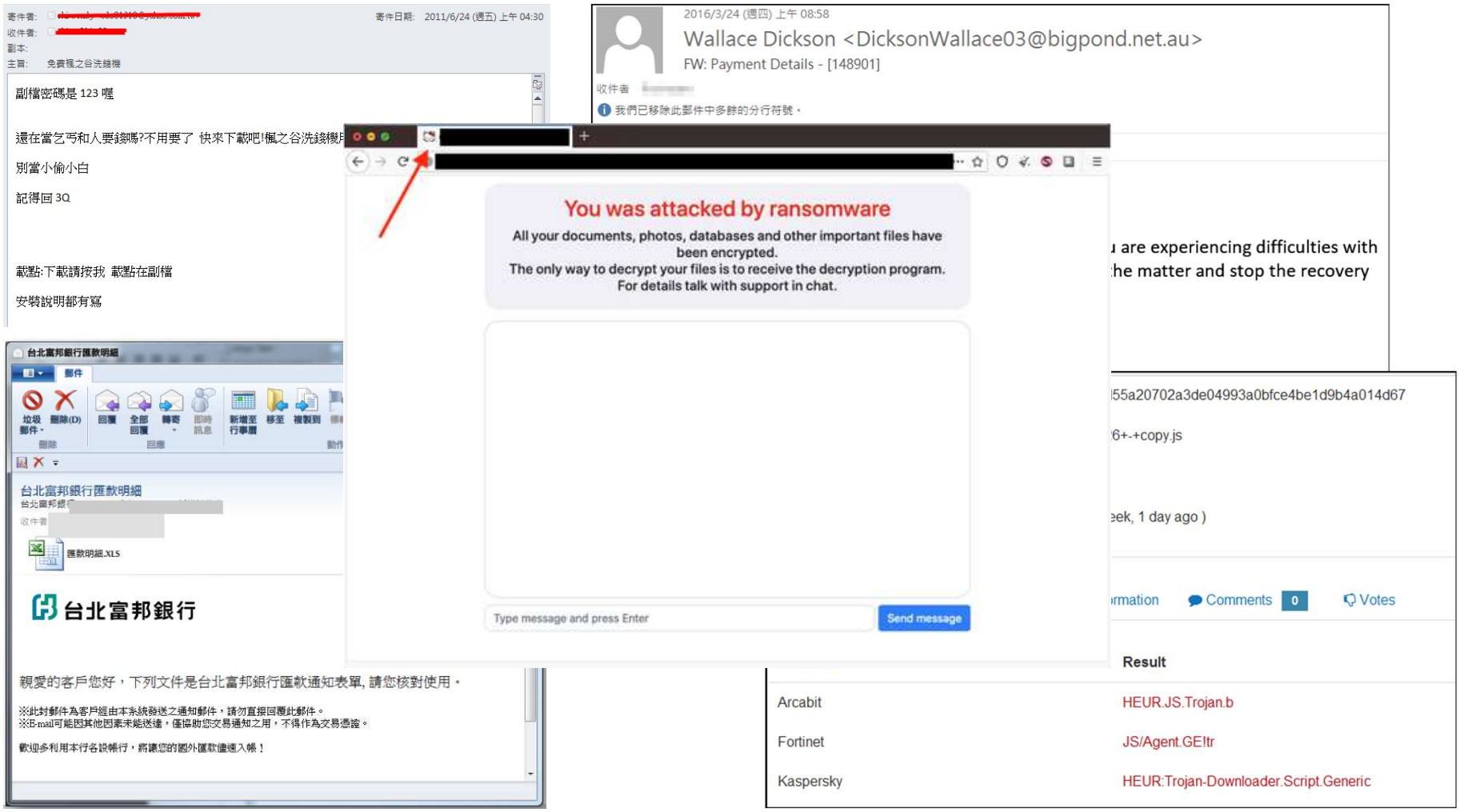
Ref: http://news.ltn.com.tw/news/life/paper/1145620

單頁式網站詐騙特徵


只賣單項商品
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
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
品質保證
貨到付款
7天鑒賞期
免費到府收送
在線服務支持
全年無休
在線咨詢
訂單查詢
立即購買

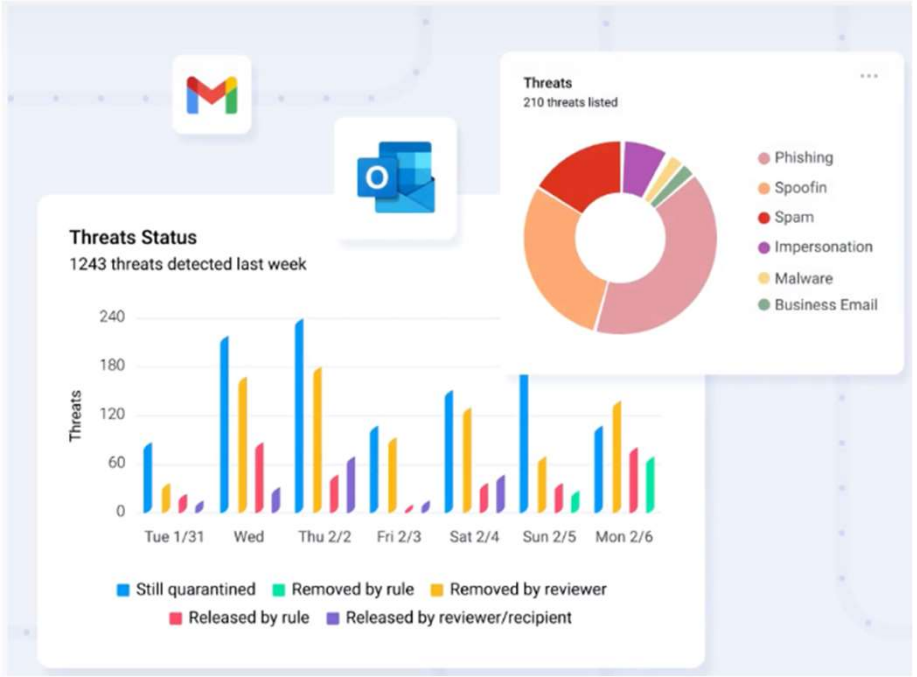
避免點擊可疑社交工程郵件比以往重要



釣魚攻擊統計

根據Must-Know Phishing Statistics 2023調查

- **75%**企業曾經遭遇過釣魚攻擊
- **96%**的釣魚攻擊來自電子郵件(其餘3%為惡意網站、1%為電話)
- 每次資料外洩事件平均造成392萬美元損失(每筆掉失資訊約帶來150美元成本)
- 常見的釣魚信件主旨**關鍵字**
  - Urgent, Request, Important, Payment, Atten
- 最常見被冒用的品牌



Ref: Must Know Email Phishing Statistics in 2023 | Trustifi

慎防假冒銀行釣魚簡訊詐騙

假冒銀行釣魚簡訊詐騙規模擴大，繼國泰世華、台新銀行後，中國信託今日也出現遭冒名的狀況，金融業者與民眾可千萬注意

近半個月來，假冒國內金融機關釣魚簡訊詐騙的狀況相當不尋常，不只出現假國泰世華、假台新銀行的釣魚簡訊，已造成30多位民眾上當受害，損失金額超過500萬元，今日（2月9日）再度出現假中國信託的釣魚簡訊。

文/ 羅正漢 | 2021-02-09 發表

讚 6.7 萬 按讚加入iThome粉絲團 讚 4,513 分享

最近半個多月來，國內多家金融機關與刑事警察局都發出慎防釣魚網站的警告，因為有網路犯罪集團接連假冒國泰世華、台新銀行名義發送大量釣魚簡訊，誤導民眾至偽裝金融網銀的釣魚網站，騙取用戶帳號與密碼，同時還騙取用戶所收到從銀行發出、綁定信任裝置所需的OTP碼，藉此將民眾的網銀帳戶，非法綁定至歹徒持有的手機裝置，以進行非約定轉帳進而盜轉成功，短短一週多的時間，已有30多位民眾上當受騙，受害金額超過500萬元。由於這樣的釣魚詐騙簡訊接連發生，現在，其他國內銀行雖尚未出現被假借其名義的狀況，但多數也都已經發出公告，提醒民眾注意。

關於釣魚詐騙網站的問題，其實一直都在，企業如何降低自家公司業務與品牌遭濫用的風險，是持續面臨的難題。但這次詐騙集團鎖定金融業假冒並發送釣魚簡訊，已連續2週密集出現，相當不尋常，詐騙者都是利用接近週五連假前夕發送釣魚簡訊，而且是假借國內不同金融機構名義，並製作了數十個不同的釣魚網站，嚴重為影響國內金融安全。刑事警察局研判，未來網路犯罪集團仍有可能持續以各家金融名義及不實內容來詐騙，因此提醒民眾，收到假冒銀行、郵局等金融機構名義或來路不明的簡訊，千萬不要相信或點選連結，並注意核對所附網址列是否正確。

事實上，在這一個月內，網路犯罪集團所偽冒金融業的釣魚網站，確實不只上述兩家銀行，還有1月中旬的中華郵政，以及今日（2月9日）的富邦人壽與中國信託，顯然詐騙規模有擴大的跡象，加上年關將至，民眾可能不易求證，因此，所有民眾都必須要提高警覺，並且務必謹慎檢視隨附網址連結的正確性，避免遭遇釣魚簡訊或釣魚郵件而上當受騙。

2021農曆年前偽冒臺灣金融機關釣魚網站情形

日期	管道	內容	追查釣魚網站數目	國人受害情況
2021年1月6日	釣魚郵件 釣魚網站	疑似偽冒中華郵政寄送釣魚郵件，竊取個人敏感性資料	1個	不確定
2021年1月27日	釣魚簡訊 釣魚網站	簡訊內容：【國泰世華】您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用	6個	根據警方2月6日統計，已接獲89件通報，25件被害人帳戶已遭盜用，損失金額達518萬元
2021年2月5日	釣魚簡訊 釣魚網站	簡訊內容：【台新銀行】您好,由於網路銀行版本更新,請於2月6日前登入進行驗證否則將停用您的使用權限,超時請至臨櫃辦理	17個	根據警方2月6日統計，已接獲10件通報，7件被害人帳戶已遭盜用，損失金額達55萬元
2021年2月9日	釣魚網站	疑似偽冒富邦人壽公開網站	1個	不確定
2021年2月9日	釣魚簡訊 釣魚網站	簡訊內容：【中國信託】你的網路銀行更新失敗，請立即輸入你的驗證碼以更新資料，超時請重新輸入。	11個	根據警方2月9日統計，已接獲一件通報，尚未有受害者報案

資料來源：刑事警察局、FISAC、iThome整理，2021年2月9日

Ref: https://www.ithome.com.tw/news/142711

Apple用戶是網路釣魚一大目標

Unsurprisingly, Apple customers are the most common phishing target

Ben Lovejoy - Apr. 14th 2020 5:17 am PT @benlovejoy

Given the demographic of Apple customers, it's no surprise to learn that they are the most common phishing target.

A new security report found that a full 10% of all phishing attempts were trying to get hold of Apple ID credentials, ahead of Netflix at 9% and a surprising third choice …

Check Point Research's Q1 2020 Brand Phishing Report found that Yahoo took third place.

> *The top brands are ranked by their overall appearance in brand phishing attempts:*
>
> *1. Apple (related to 10% of all brand phishing attempts globally) 2. Netflix (9%) 3. Yahoo (6%) 4. WhatsApp (6%) 5. PayPal (5%) 6. Chase (5%) 7. Facebook (3%) 8. Microsoft (3%) 9. eBay (3%) 10. Amazon (1%)*

The firm said that although most phishing attacks were emails directing to a fake website, the use of fraudulent apps is growing.

> *In a brand phishing attack, criminals try to imitate the official website of a well-known brand by using a similar domain name or URL and web-page design to the genuine site. The link to the fake website can be sent to targeted individuals by email or text message, a user can be redirected during web browsing, or it may be triggered from a fraudulent mobile application. The fake website often contains a form intended to steal users' credentials, payment details or other personal information […]*
>
> *Web phishing was the most prominent at 59%, followed by mobile phishing as the second most attacked platform compared to Q4 of 2019, where it ranked third […]*
>
> *The most likely industry to be targeted by brand phishing was technology, followed by banking and then media. This illustrates a broad spread of some of the best-known and most used consumer sectors, particularly during the coronavirus pandemic and associated quarantine, whereby individuals are grappling with remote working technology, potential changes to finances, and an uplift in home entertainment services such as streaming.*

Apple is the most common phishing target due to the high value of Apple IDs on the dark web. A report back in 2018 found that they sold for a higher price than any other non-financial credentials.

Ref: https://9to5mac.com/2020/04/14/most-common-phishing-target/

疫情發燒，駭客利用偽造影音登入頁面竊取資料

大量駭客利用偽造 Netflix 與 Disney+ 登入頁面竊取用戶個資

單單在上週於網路上就被發現超過 700 個偽造頁面。

2020-04-22

Entertainment 娛樂　　8 小時前　343

編輯 : Michael Chu

早先 Netflix 才公開在 2020 年第一季，全球用戶成長超過 1,577 萬人， 全球付費用戶在第一季截止前來到 1.8 億人，遠遠超過公司目標兩倍之多。

然而正因為使用人數激增，不肖駭客便看中了這一點，包括 Netflix 和 Disney+ 等，單單在上週於網路上已經被發現超過 700 個偽造登入頁面，將網站架設的與該影音串流平台十分類似，混淆使用者，在網站內架設購買流程甚至免費帳戶的優惠服務，以獲取個人信息與信用卡資料等。

Mimecast 網路犯罪專家 Carl Wearn 表示：「可疑網域名稱急速增加，它們冒充個大串流媒體巨頭。這些詐欺網站通常通過提供免費訂閱吸引毫無戒心的公眾，竊取有價值的數據，包括姓名、地址和其他個人信息，甚至信用卡的詳細資料。」

> Mimecast's Brand Exploit Protect finds 700 fake Netflix pages in single week via @guardiannews https://t.co/Xo4YsTp0Mw pic.twitter.com/v8L30y6chG
>
> — Mimecast (@Mimecast) April 20, 2020

各位近日在使用網頁登入 Netflix 與 Disney+ 等串流平台時還需多加留意，避免落入圈套。除此之外，另可關注其他影劇類消息：

1. 《Star Wars》外傳劇集《The Mandalorian 2》第二季首部宣傳預告正式發佈
2. 曼巴歸來 – 消息稱 Kobe Bryant 個人全新傳記紀錄片正在製作中

DISNEY　NETFLIX

Jonathan Nackstrand/Afp/Getty Images

Ref: https://hypebeast.com/zh/2020/4/hackers-creating-fake-netflix-disney-plus-pages

40萬Office 365、OWA 郵件帳密被釣魚竊取

釣魚郵件以合法網域掩護發動攻擊，40萬Office 365、OWA郵件帳密被竊

釣魚信件內容包含冒充的Zoom視訊連線邀請連結，以及騙取用戶輸入OWA或Office 365帳密

文/ 林妍溱 | 2021-03-25 發表

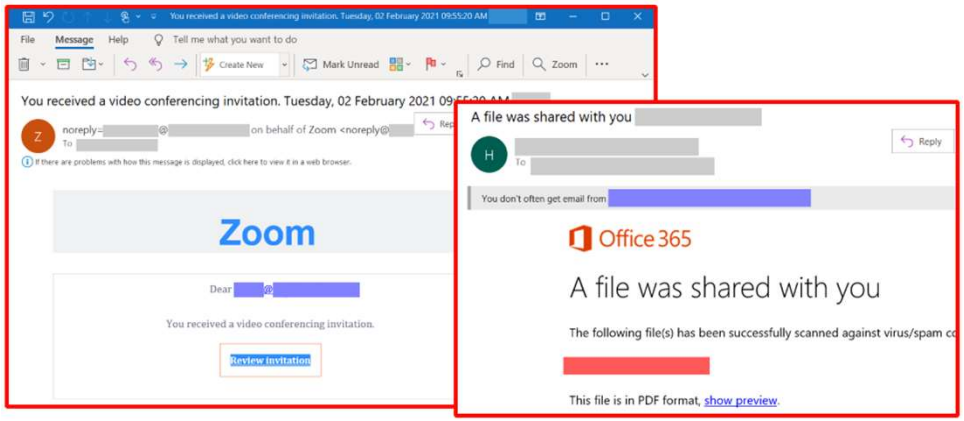
按讚加入iThome粉絲團

微軟本周稍早發出公告，駭客正利用包括Google App Engine在內的合法網域發送釣魚信件，繞過郵件安全過濾機制入侵企業，已有超過40萬的Office 365及Outlook Web Access (OWA)登入帳密遭竊走。

這波攻擊是WMC Global發現的Compact Campaign釣魚攻擊的一部份，從去年12月開始持續活動至今。釣魚信件內容包含冒充的Zoom視訊連線邀請連結，騙取用戶輸入OWA或Office 365帳密。迄今已經有40多萬筆帳密遭竊。

Compact Campaign得逞原因是它利用被駭入的合法郵件服務業者的網域發送信件，而成功避免郵件過濾封鎖。遭利用的郵件服務業者一開始以SendGrid為主， 去年多了Amazon SES (Simple Email Service)，今年一月又新增Mailgun等服務。但微軟安全情報小組最近偵測到，攻擊者還使用Appspot.com網域為不同釣魚郵件收信者建立不同的URL。Appspot.com是Google App Engine的網域名。透過濫用合法網域，將可提高釣魚郵件躲過網域信譽為基礎的過濾機制。

微軟的Defender for Office 365已經可偵測這波攻擊。但微軟指出，這波釣魚郵件攻擊是利用被駭的郵件行銷帳號為之，因此微軟強烈建議企業重新檢討郵件傳送規則，允許大量例外的規則可能讓釣魚信件乘虛而入。



Ref: https://www.ithome.com.tw/news/143441

結合電話客服誘騙安裝惡意程式

釣魚信件有新手法，以電話客服誘騙用戶安裝惡意程式

傳統釣魚信挾帶的惡意程式，容易被安全軟體偵測攔截，新攻擊手法將用戶引導離開郵件管道，再由假客服電話指導被害者下載惡意程式

文/ 林妍溱 | 2021-05-28 發表

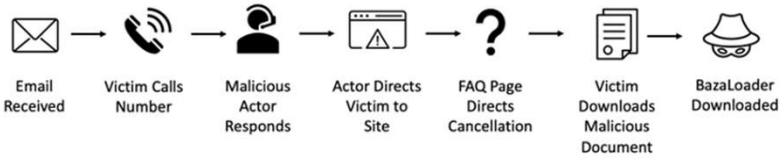
按讚加入iThome粉絲團

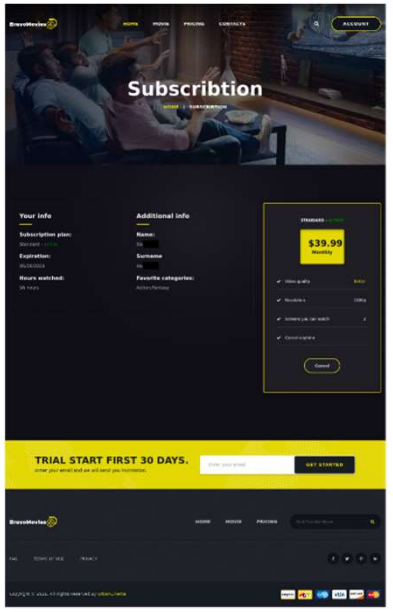
因應安全軟體愈來愈能過濾釣魚信件，歹徒也發展出新招數，以成功散佈惡意連結或惡意軟體。安全廠商Proofpoint發現新的釣魚郵件攻擊，會結合電話客服中心誘使用戶下載惡意軟體。

研究人員本月發現一批釣魚信件散佈名為BazaLoader的後門程式。該公司是於2020年4月首次觀察到BazaLoader，和Trickbot木馬程式有很強關聯性，目前也經常被歹徒用於下載Ryuk、Conti勒索軟體。

今年2月，BazaLoader是經由釣魚信件傳佈，冒充藥商或內衣、鮮花服務，而最新的一波釣魚郵件則偽裝成串流影音娛樂服務BravoMovies，告知用戶免費試用的服務已經到期，將開始經由信用卡收費。信中告知，用戶如果不願訂閱，應以郵件所附電話號碼，聯絡客服中心取消。信以為真的用戶就會因此踏入陷阱。

為取信於用戶，它和一般釣魚郵件一樣，利用網路上的資源製作精美的影片，但特別的是，它加入名為BazaCall的手法，引導用戶經由網站上FAQ頁的電話和歹徒互動。當用戶打電話給客服中心時，「客服人員」會引導用戶前往網站「取消訂閱頁」下載一個Excel檔（如下圖）。這個檔案含有巨集，一經開啟，就會下載BasaLoader。





Ref:
1. https://www.ithome.com.tw/news/144691
2. https://www.proofpoint.com/us/blog/threat-insight/bazaflix-bazaloader-fakes-movie-streaming-service

釣魚郵件夾帶WIM映像檔散佈木馬程式

研究人員發現WIM映像檔格式被用於釣魚郵件攻擊

攻擊者為了避免釣魚郵件遭到防護系統攔截，很可能會在附件上採用一些較為少見的檔案格式。近期Trustwave揭露一起濫用Windows映像檔格式（WIM）的攻擊行動，意圖散布木馬程式Agent Tesla

為了規避郵件防護系統的偵測，攻擊者也在釣魚郵件夾帶的附件上，嘗試使用較為少見的檔案格式，企圖躲過檢查。新加坡電信（Singtel）旗下的資安公司Trustwave，他們近期發現有攻擊者寄出的釣魚郵件中，開始使用Windows映像檔格式WIM（Windows Image Format），來做為附件檔案的格式，散布2020年下半全球第3大的惡意軟體Agent Tesla。

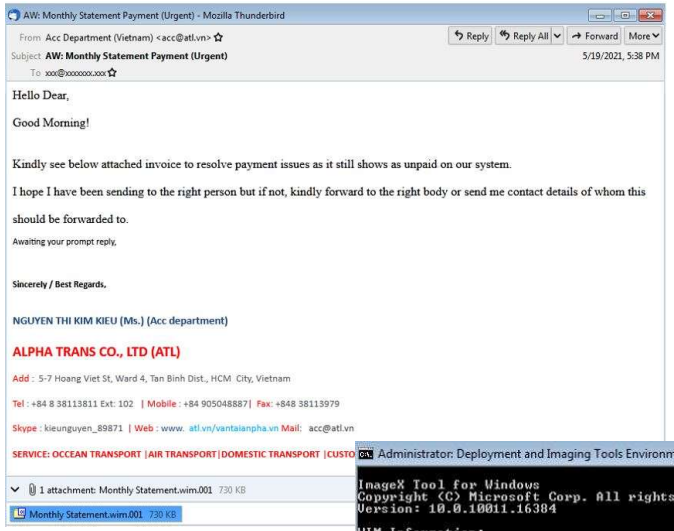
使用這種不常見的附件檔案格式並非首例。過往攻擊者曾經濫用於釣魚郵件的檔案格式，是光碟映像檔案，包含了ISO、IMG，以及DAA（Direct Access Archive）等格式。

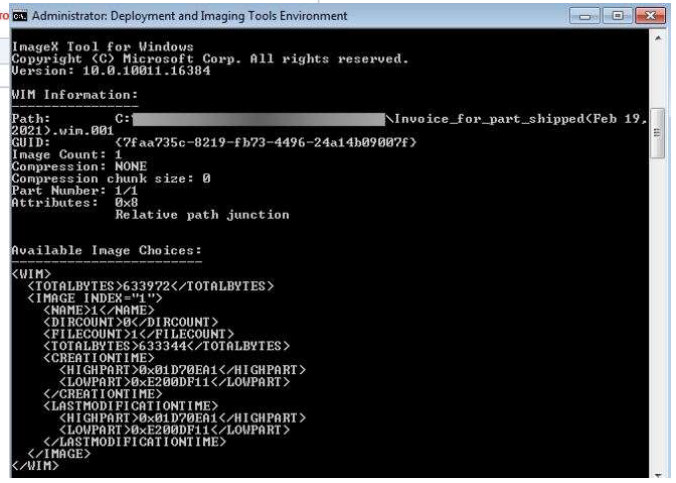
但有別於上述的光碟映像檔格式，WIM是微軟自Windows Vista開始，設計用來封裝Windows作業系統的安裝檔案，以便網管人員部署使用，並能被多款壓縮軟體和光碟映像軟體存取，例如7Zip、PowerISO，以及PeaZip等。

然而，Trustwave的研究人員指出，他們近期看到釣魚郵件夾帶這種格式的附件檔案，攻擊者假冒DHL、Alphatrans等貨運公司，寄送發票或是托運單的名義，來散布這種釣魚郵件。

.....

接著，研究人員又透過十六進位編輯器開啟附件檔案，他們發現WIM檔案裡藏匿了相同檔名的EXE可執行檔，Trustwave指出，他們所有看到的WIM附件檔案裡，都存在惡名昭彰的RAT木馬程式Agent Tesla，這個惡意程式是由.NET編寫而成，一旦觸發將會完全控制受害電腦，並且會藉由多種管道外洩資料，這些管道包含了HTTP、SMTP，以及FTP等通訊協定，還有即時通訊軟體Telegram等。而能使用上述的通訊協定與Telegram外洩資料，也與Sophos在今年2月揭露的Agent Tesla第2版、第3版所具備的能力相同。





Ref: https://www.ithome.com.tw/news/145336

駭客使用多種編碼混淆企圖騙過防護偵測

釣魚郵件攻擊出現新手法，駭客採用摩斯電碼、ASCII等多種編碼來混淆附件內容

微軟揭露自2020年7月開始出現、為期一年的釣魚郵件攻擊，攻擊者在郵件裡挾帶了宣稱是發票的HTML檔案，來竊取Office 365帳密。為了規避郵件防護系統的偵測，攻擊者不只採用數種編碼法混淆，並且平均每37天就更換新的手法

文/ 周峻佑 | 2021-08-13 發表　　按讚加入iThome粉絲團

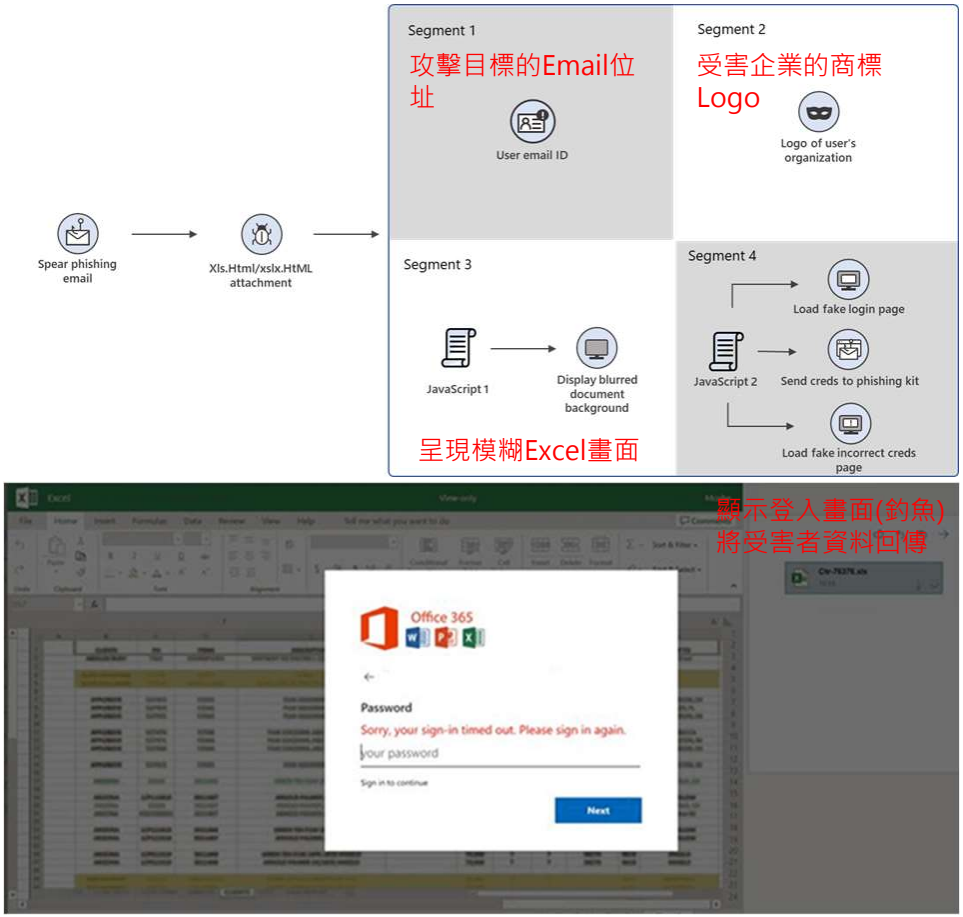
攻擊者為了避免釣魚郵件遭到攔截，附件檔案很可能會利用較為少見的檔案格式，來挾帶作案工具，例如，光碟映像檔（ISO、IMG），甚至是Windows映像檔格式（WIM）等，這些檔案格式對於部分郵件防護系統而言，無法解讀其中的內容，沒辦法得知是否有害。

但最近也有攻擊者改變策略，使用一般郵件可能會出現的附件檔案類型，來挾帶含有攻擊意圖的工具，避免因採用了較少見的附件檔案格式，而被網管人員列為黑名單封鎖的情況。

最近微軟揭露一起挾帶HTML檔案的釣魚郵件攻擊，攻擊者以寄送發票為幌子，目的是要偷取使用者Office 365的帳密。這起攻擊行動自2020年7月出現，為期至少一年，而當中較為特別的地方就是，攻擊者藉由Base64、ASCII、Unicode、摩斯電碼，將HTML程式碼混淆，來規避郵件防護系統檢查內容的範圍，而且，攻擊者每隔1到2個月（平均間隔37天），便會調整、改進編碼搭配的方式，使得這類釣魚郵件的附件更難被察覺異狀。

攻擊者將HTML程式碼的內容，拆成4個模組處理

值得留意的是，並非整個HTML檔案的程式碼，攻擊者都會採用相同的編碼進行混淆，而是有可能在不同的程式碼片段，利用2至3種編碼。微軟指出，從HTML程式碼的功能來看，大致可區分為4個模組。



Ref: https://www.ithome.com.tw/news/146181

釣魚網站利用CAPTCHA機制躲避偵測

釣魚郵件攻擊濫用網址重新導向、雲端服務與自動化真人檢測服務CAPTCHA

微軟揭露一起透過合法網域寄件、並搭配重新導向的網址按鈕，誘騙使用者網路服務的帳密，為了規避資安防護的偵測且取信受害人，攻擊者還運用了CAPTCHA與郵件檢測畫面

文/ 周峻佑 | 2021-08-31 發表

讚 6.7 萬 按讚加入iThome粉絲團 讚 59 分享

網路釣魚攻擊手法推陳出新，日前有攻擊者利用驗證真人與機器人的CAPTCHA機制，誘騙受害者下載金融木馬，而根據資安業者Greathon的統計，濫用Google Meet和Google DoubleClick等工具，重新導向到其他網站的釣魚攻擊手法，也日益升溫，如今攻擊者也將這些方法運用於釣魚郵件上。

在微軟最近揭露釣魚郵件攻擊行動當中，我們同樣看到類似的手法。在這事件裡面，駭客為了迴避偵測，廣泛使用合法的寄件者網域名稱，這些網域包含國家級網域（ccTLD）、遭駭的合法網域名稱，以及攻擊者所持有、由網域生成演算法（DGA）所產生的網域名稱。微軟發現，至少有350個網域名稱被用於此次攻擊行動，研究人員認為，這突顯了一個現象，那就是：有許多駭客投入相關攻擊行動。

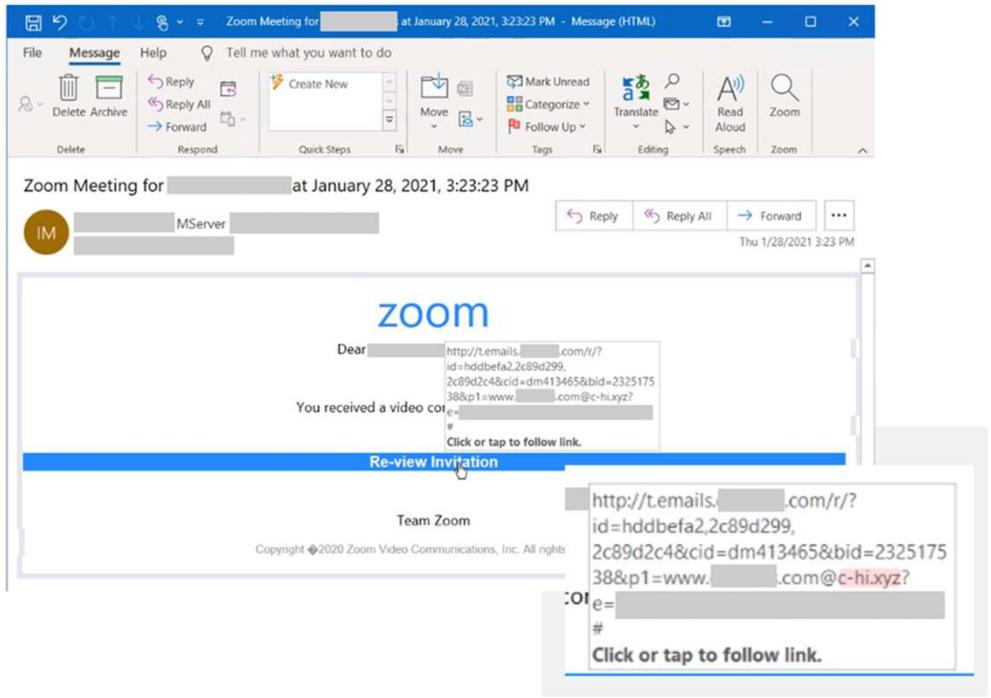
釣魚郵件以通知信為幌子，主旨含有收信人資料與時間

關於這波攻擊行動裡的釣魚郵件有哪些共通特徵？微軟指出，信件內容都存在相當顯著的點選按鈕，誘使收信人按下去，以便將他們帶往惡意網站。

再者，信件的主旨內容，往往包含收件人的使用者名稱，以及所屬的網域名稱，甚至是日期、時間，以便取信收件人，讓他們相信是針對自己而來的通知。由於網域名稱很可能與組織的名稱相同，使得這類通知看似從組織或是企業所發出。

這些信件的主旨，包含了收件人組織將於指定時日舉辦Zoom Meeting的線上會議，或者是使用者密碼異動通知等，而讓受害者信以為真。

一旦收信人信以為真，點選信件裡的按鈕，就會重新被引導到攻擊者的網站。但為何釣魚信件裡的連結能通過郵件防護系統的檢查？微軟指出，原因是在於攻擊者使用了特別製作的URL，這些網址看起來是對應合法組織的網域名稱，實際上是透過重新導向的方式，將使用者引導到攻擊者的網站。由於重新導向的做法在企業也相當常見，因此IT人員也很難直接封鎖具有這類URL的電子郵件。



Ref: https://www.ithome.com.tw/news/146468

國內中小電商遭網釣攻擊鎖定

國內中小電商遭新型網釣攻擊鎖定，佯稱商品瑕疵，內容本土化且量身客製，客服員工開啟附件就被竊取帳密

近半年以來，國內出現鎖定電商客服人員盜取帳密的釣魚郵件，假冒消費者客訴來信，並清楚提及收件者公司的品牌與產品名稱，國內已有電商營運長公布遇害經歷，所幸當下能及時反應，不只相關電商同業要注意，隨著這類釣魚範本的發展，針對企業且高度量身打造的偽裝內容可能更普遍。

文/ 羅正漢 | 2021-09-24 發表

今年以來，國內出現多起鎖定客服人員的釣魚郵件，並具有在地化且自製程度很高的內容，以引誘不知情的企業員工開啟附件，目的就是要讓木馬程式側錄受害電腦的帳號密碼，或是入侵電腦。而近期這樣的事件之所以受到注目，是有人在社群網站分享接獲這類客訴釣魚郵件的經驗。

值得關注的是，從網友們公布的釣魚信內容可以看出，網路攻擊者假冒消費者以Gmail個人信箱來信，郵件內容都是正體中文，沒有簡體與亂碼，相當符合本地用戶信件撰寫方式；同時，信中內容提及收件者所屬公司的名稱與產品，謊稱之前已買過該組產品，因發現產品有瑕疵，要業者盡快回覆處理。顯然這樣的詐騙內容，已經過量身打造而讓人很難起疑心。

而出現這樣的釣魚郵件案例，不僅讓外界更清楚網路攻擊者的社交工程手法變化，也突顯了本土化，以及高度量身打造的釣魚郵件，其實都已更為普遍，此次鎖定客服人員的攻擊，就是一例。

國內中小電商頻接獲假客訴信，有營運長分享員工遇害經驗

以近期案例而言，在9月6日，有網友表示，公司的同事收到一封假借消費者名義的客訴信，信中指責該公司保養品出貨後就不顧售後服務，並提及電商的品牌與產品名稱，對方還附上了壓縮檔與密碼，說明附件內容是包裹與瑕疵照片。所幸她之前就看過相關提醒，有其他電商老闆在臉書分享遇害經過，因此，很早就將這樣的情資轉發到公司群組提醒，因此同事並未上當。

而這個透過臉書轉貼而曝光的事件，其實是發生在今年5月。有一家電商營運長分享了遭遇網路攻擊的經驗，他們就是因為開啟了假冒客訴信的釣魚郵件附檔而受害，幸好這家公司即時因應，而未受到重大影響，但也希望其他公司注意到這樣的威脅。

我們後來找到這家業者了解經過，該電商營運長表示確有其事，而且，直到9月9日他們依然收到假冒客訴釣魚郵件。

1.利用加密碼的壓縮檔規避郵件掃毒
2.開啟後內容是可執行檔而非圖檔

Ref: https://www.ithome.com.tw/news/146877

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

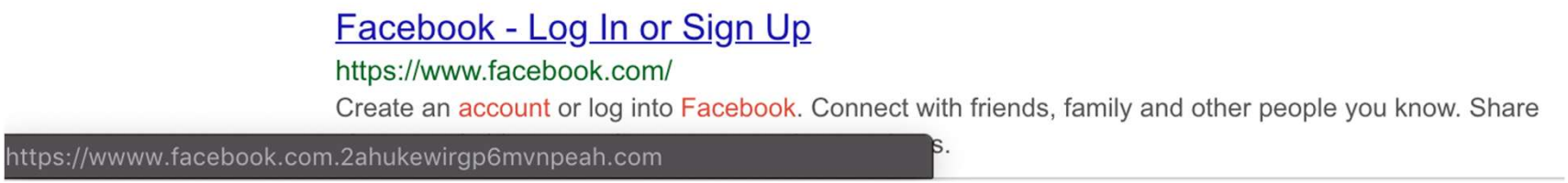
網址/超連結混淆偽裝 (1/2)

- 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)

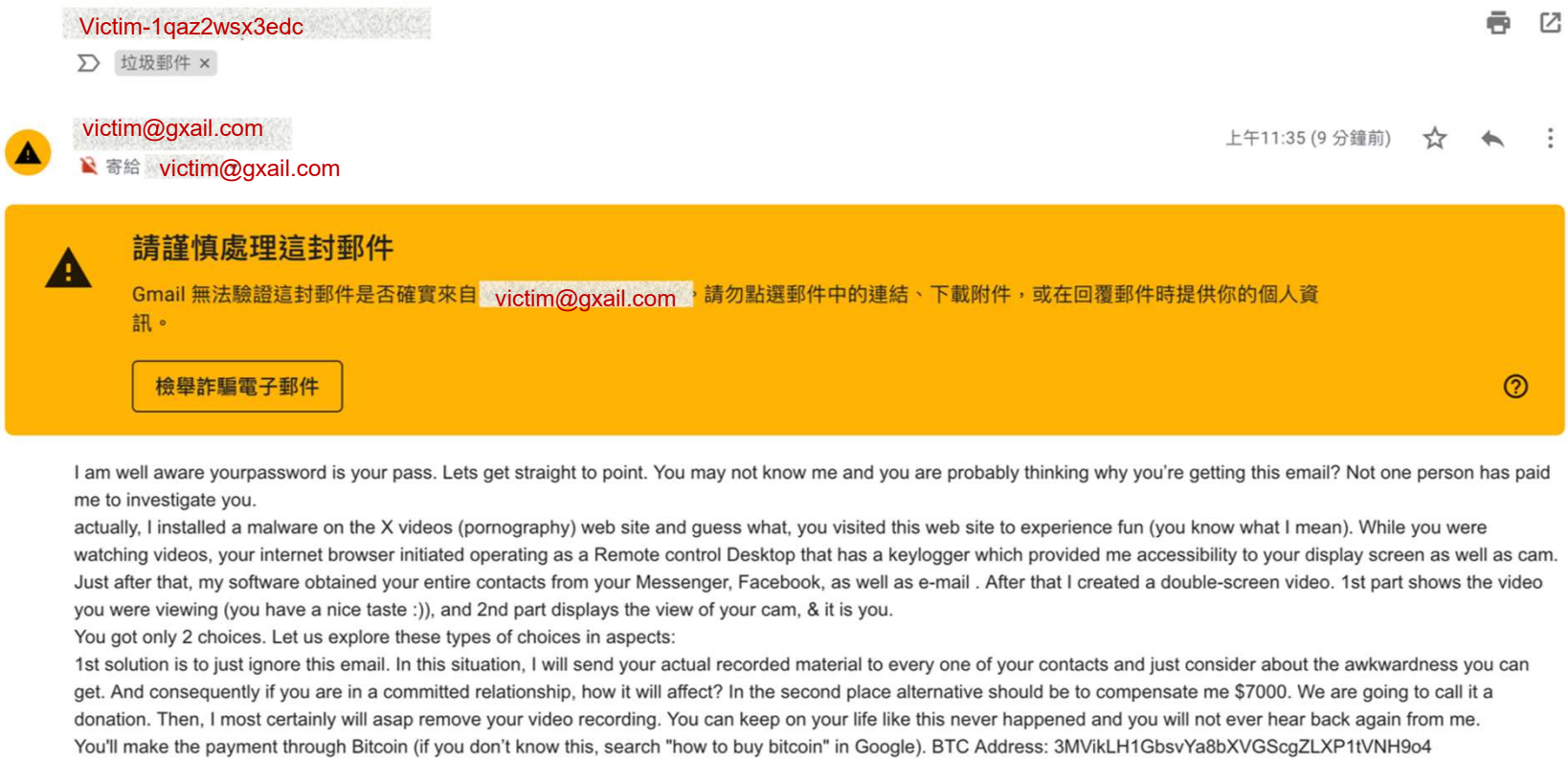
- 超連結顯示與實際連結網址不同
  - www.facebook.com

實際連結網址　　顯示的網址

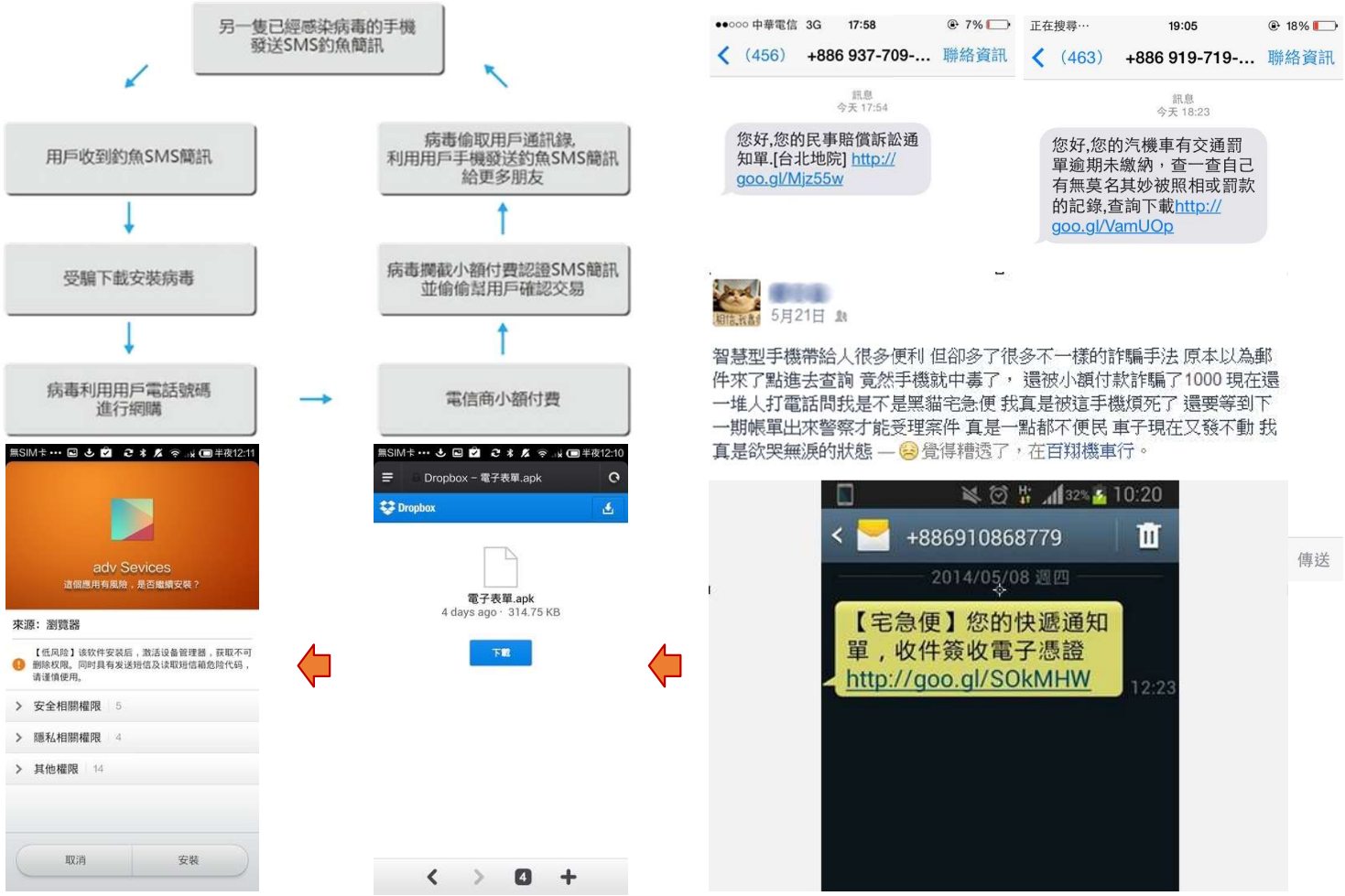


- 網址重新導向或短網址
  - https://www.example.com/login.html?redir=https://www.fake.site
  - https://goo.gl/wbJJxL
  - https://ppt.cc/flhXKx

信箱容易偽造，不可輕信

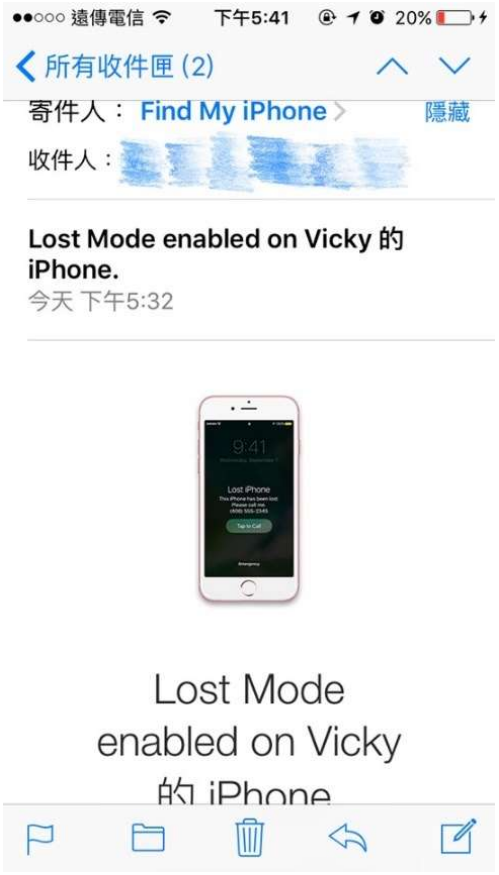

Victim-1qaz2wsx3edc
垃圾郵件 ×
victim@gxail.com
寄給 victim@gxail.com
上午11:35 (9 分鐘前)
請謹慎處理這封郵件
Gmail 無法驗證這封郵件是否確實來自 victim@gxail.com，請勿點選郵件中的連結、下載附件，或在回覆郵件時提供你的個人資訊。
檢舉詐騙電子郵件
I am well aware yourpassword is your pass. Lets get straight to point. You may not know me and you are probably thinking why you're 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郵件 (1/2)

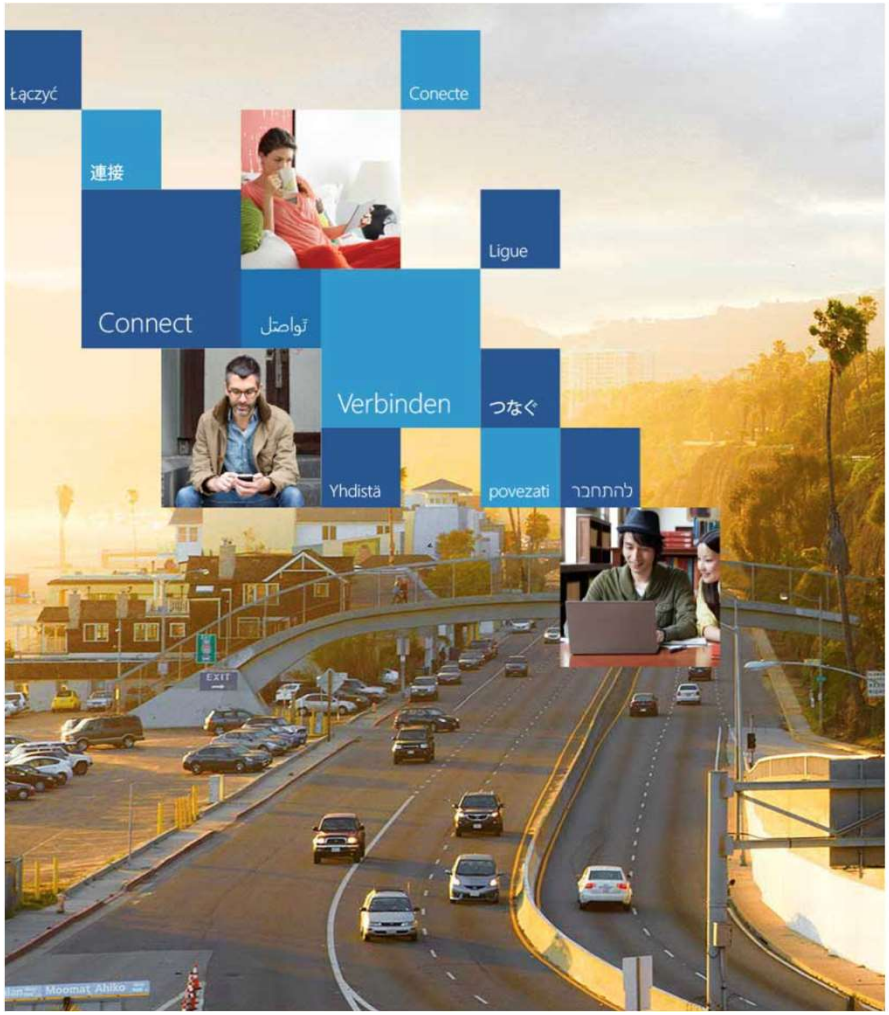


行動裝置上的惡意釣魚郵件(2/2)

Case: Find My iPhone釣魚郵件



Demo: Fake365 釣魚網站



Office 365

Sign in with your organizational account

someone@example.com

Password

Sign In

Keep me signed in

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MS、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/

日本網路釣魚對策指引

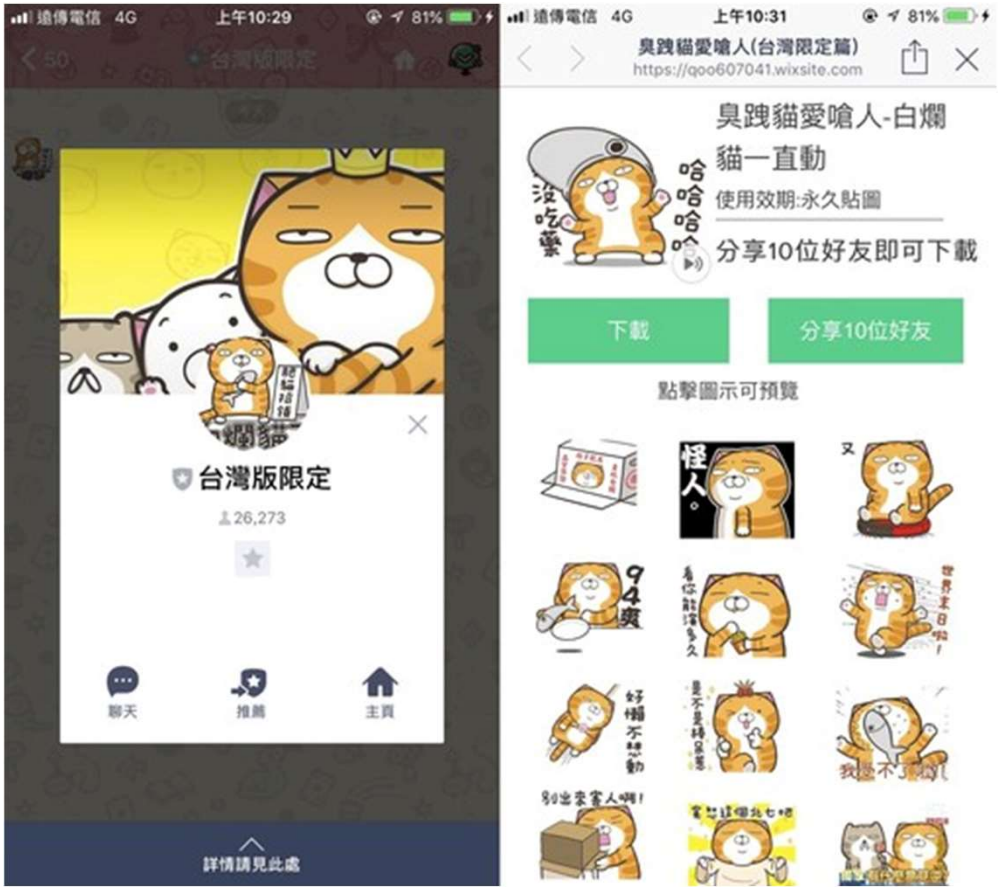
- 日本「網路釣魚對策委員會」出版「網路釣魚對策指引」提供各界參考，協助網站經營者與使用者防患未然
- 5大重點對策
  - 對發送給使用者的電子郵件實施「**釣魚郵件對策**」，如導入S/MIME (Secure Multipurpose Internet Mail Extensions)、DMARC(Domain-based Message Authentication, Reporting & Conformance)等
  - 啟用多因子身分驗證 (Multi-Factor Authentication, MFA)，如登入時輸入一次性密碼、使用生物辨識技術等**驗證登入是本人所為**
  - 網站經營者應具備「域名即品牌」認知，反覆**向網站使用者宣傳正確域名**
  - 所有網頁均須透過**HTTPS加密傳輸**的方式存取資料
  - 網站經營者應成立網路釣魚詐騙**專責小組**，必要時應設置24小時服務窗口

Ref:
https://blog.twnic.tw/2021/07/15/19117/

網路釣魚(Phishing) - Line、Facebook社群詐騙

Line、Facebook社群詐騙 (1/5)

Line、Facebook社群詐騙 (2/5)



Ref:

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

Line、Facebook社群詐騙 (3/5)

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

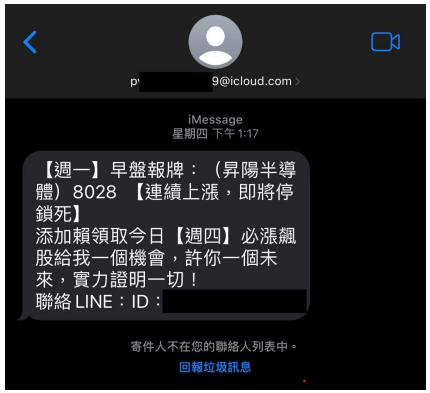
- 透過簡訊、社群網站要受害人加Line進入投資群組

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 (4/5)

【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

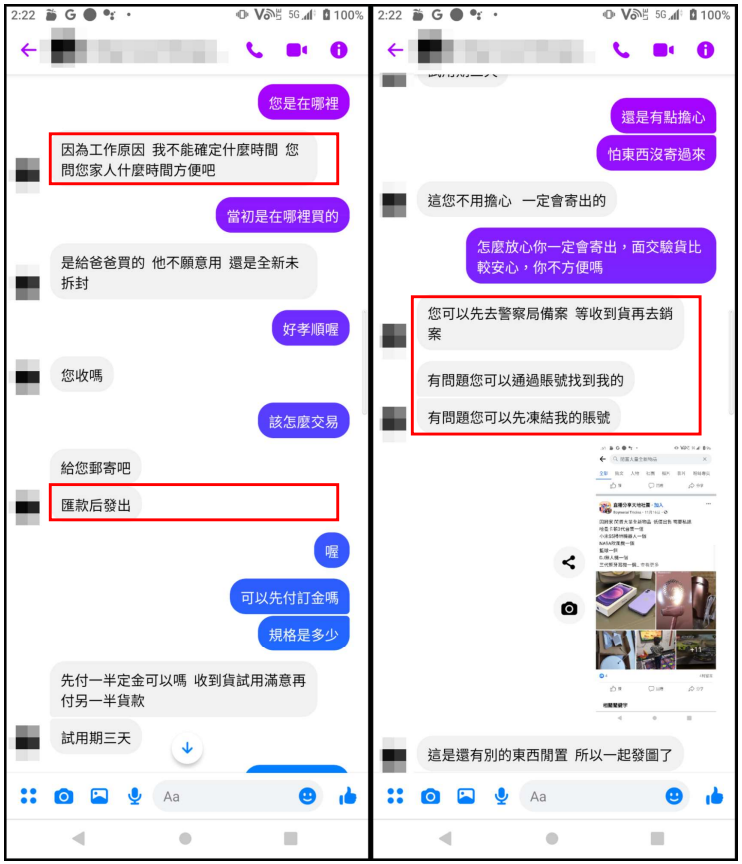
- 例如Line Pay
- 收款之後封鎖被害人，人間蒸發

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 (5/5)



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

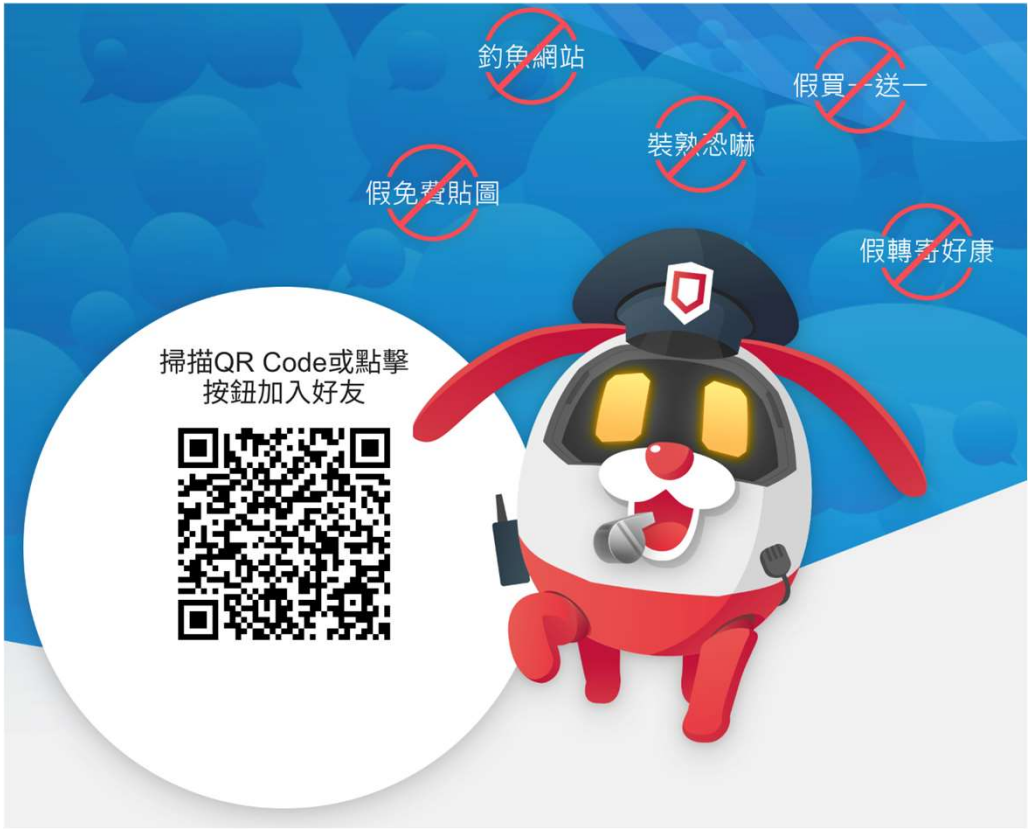
Line 官方資安宣導


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。
假網站
storeline4.weebly.com
LINE MOBILE
正版
tw.linemobile.com
LINE MOBILE
4G終身吃到飽
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
知名品牌週年慶活動開跑！
500禮券立刻領
★ 點此選取分享 25 位好友後領取
分享後若無通知，聯絡客服領取
500
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！
加入好友
優惠領取中心 阿甜
加入
聊天

165 反詐騙宣導


辨識詐騙招數
1 賣家要求加LINE 獲取寄送資訊(姓名、電話、取貨超商)
2 賣家商品多卻無評價，短暫成立賣場，騙完收工。
3 平臺顯示【尚未出貨】卻收到取貨簡訊由物流公司送出，非平臺
4 賣家聯絡電子郵件來自中國 ▸例如 @163.com
5 賣家帳號遭拍賣平臺停權▸ 已有民眾遭騙通報
6 超商取貨後立即檢視商品 錄影 拆封確認商品內容、留存包裹上方寄送資訊及顧客聯小白單
送好康，贈貼圖 買一送一真的假的？
LINE 趨勢科技防詐達人
退款自救行動 $
1
★把握申請退款時間退款找寄件人（物流公司）
★包裹上有物流公司電話，直接聯繫公司辦理退款。
★包裹上無物流公司電話，聯絡取貨商業者提供該公司電話跟E-mail，再致電或寄 E E-mail，詢問退貨流程。
2 物流公司關係企業很多(名稱很多)，電話也非常難打，必須有相當的耐心!
內政部警政署 刑事警察局
TREND MICRO 趨勢科技
FB搜尋：165反詐騙宣導

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...
【日本原裝進口】
高性能4K高清數...
NO!
下午2:31
汪！危險！訊息或
網頁內有不安全連
結。
下午2:31
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...
臉書各大社團都有
的 #詐騙廣告 #臉...
上午11:36
使用說明 | 分享給好友

趨勢科技防詐達人(2/2)

趨勢科技 防詐達人

防詐騙瀏覽器 最新詐騙情報 關於我們 常見問題 我要回報

最新詐騙情報

最新文章

2022-03-09

沒有購物卻收到「您訂購的商品已送達7-11」簡訊還加上查件抽獎連結？幽靈包裹不要領，可疑連結不要點

你的711到貨簡訊也突然多了「查件抽獎」連結嗎？還有民眾是根本沒有訂貨，卻一樣收到這樣的到貨通知，到底是發生什麼事？防詐達人帶你看看這樣的簡訊暗藏什麼陷阱，遇到這樣的幽靈包裹你該怎麼做

YOUTUBE 頻道

訂閱網站

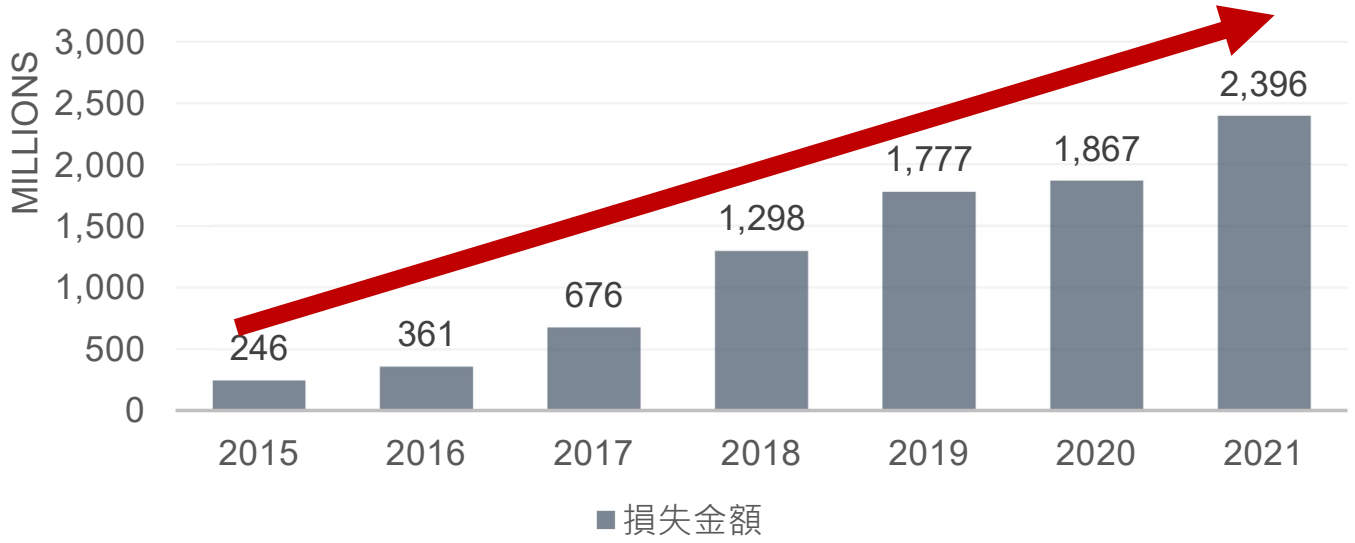
Ref: https://getdr.com/category/recent-new/

網路釣魚(Phishing) - BEC變臉詐騙

(商業電子郵件詐騙)

BEC變臉詐騙簡介

- 變臉詐騙(Business Email Compromise，亦稱「商務電子郵件入侵」)，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2021年損失金額來到$2,395,953,296 (23.9億)



Ref: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

BEC 商務電子郵件入侵

美國2020年網路犯罪報告：投訴案件數比前一年大增69%，損失42億美元

全美今年有高達79萬多筆涉嫌網路犯罪的投訴，其中以郵件、簡訊等管道發送的網釣詐騙，以及付錢卻沒收到貨的電商詐欺為大宗

文/ 陳曉莉 | 2021-03-18 發表

讚 6.8萬 按讚加入iThome粉絲團 讚 0 分享

2020 CRIME TYPES

By Victim Count

Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342
Non-Payment/Non-Delivery	108,869
Extortion	76,741
Personal Data Breach	45,330
Identity Theft	43,330
Spoofing	28,218
Misrepresentation	24,276
Confidence Fraud/Romance	23,751
Harassment/Threats of Violence	20,604
BEC/EAC	19,369

2020 Crime Types *Continued*

By Victim Loss

Crime Type	Loss
BEC/EAC	$1,866,642,107
Confidence Fraud/Romance	$600,249,821
Investment	$336,469,000
Non-Payment/Non-Delivery	$265,011,249
Identity Theft	$219,484,699
Spoofing	$216,513,728
Real Estate/Rental	$213,196,082
Personal Data Breach	$194,473,055
Tech Support	$146,477,709

據FBI旗下網路犯罪投訴中心（IC3）統計，全美去年79萬多筆的投訴案中，受害人數最多的是郵件/語音/簡訊/網址嫁接等各種手法的網路釣魚（左圖），損失金額最高的則是商業電子郵件詐騙（BEC）（右圖）。

資料來源: iThome

鎖定目標 → 社交工程 → 潛伏與監控 → 執行詐騙

BEC詐騙持續攀升

【2021資安大預測】趨勢3：BEC詐騙｜商業電郵詐騙持續攀升，防不勝防

攻擊者暗中掌握企業資金往來情況，詐騙手法更加趨於隱密且精細，就連自動轉寄規則也成濫用對象，受害者難以察覺有異

文/ 周峻佑 | 2021-01-11 發表

隨著疫情的蔓延，居家辦公變成常態，電子郵件是極為重要的溝通管道之一，駭客也盯上這樣的情勢，從中進行詐騙。在2020年被揭露的商業電子郵件詐騙（BEC）攻擊事件中，不少駭客刻意採取幾可亂真的手法，讓收信者難以察覺異狀而上當。

這種精心策畫攻擊策略，也導致一旦攻擊成功，得手的利益相當可觀，受害者察覺被騙往往為時已晚，金錢損失難以追回。回顧2020年，5月有數件此類詐騙事件被公布，包含了駭客冒名向臺灣銀行洛杉磯分行轉帳得逞，以及私募基金被騙的情況，然而直到受害者察覺不對勁並展開調查，錢已經被轉走數星期甚至數個月。

針對BEC攻擊的態勢，郵件安全業者Abnormal Security，在2020年第3季的研究報告中指出，他們看到相關的攻擊數量持續增加，比起同年第2季，第3季攻擊事件增加15%。而且，該公司也提出警告，幾乎是所有主要的產業，遭遇BEC詐騙的現象都有明顯成長。

值得留意的是，縱觀許多資安廠商的年度預測報告，鮮少特別呼籲大家要重視BEC詐騙攻擊升溫的趨勢，但這種現象已有數家郵件安全業者提出警告，表示這種攻擊極為難以發現，卻接連在各行各業發生，對於這種可能被輕忽的現象，我們也認為大家需要關注。

自2019年底到2020年下旬，BEC電郵詐騙事件不斷攀升。根據郵件安全廠商Abnormal Security發布的2020年第3季調查報告，第3季比起上一季的攻擊事件多出15%。圖片來源 / Abnormal Security

攻擊者對於受害組織交易模式掌握程度極高，操控郵件內容行騙

究竟這種詐騙手法造成的危害有多嚴重？根據FBI揭露的數據，他們在2019年獲報近2.4萬件BEC詐騙案件中，總共造成約17億美元的損失。而在2020年4月下旬，臺灣銀行洛杉磯分行向金管會通報的詐騙案件，因該分行未確認匯款資料正確性就進行轉帳，結果被騙走45萬美元，相當於新臺幣1,350萬元。

不光是金融單位被當作下手目標，駭客也可能鎖定有大量資金往來的組織。例如，2020年5月，Check Point揭露英國私募基金2019年遇害，被騙110萬英鎊；而這樣的事件，甚至出現在政府機關旗下的組織。隸屬於挪威外交部的國家投資基金Norfund，他們於同月坦承遭到BEC詐騙，損失1千萬美元。

但為何會上當？以上述的3起事件而言，臺灣銀行歸咎是人為疏失，經手人員在確認客戶的資料不夠確實所致；不過，其餘2起私募基金的部分，Check Point與Norfund則是透露較多發現，並且不約而同指出駭客的手法精細，對於受害組織的資金往來瞭若指掌，捏造收信人難以辨識的詐騙郵件，操弄郵件對話而得手。

這種攻擊者已經摸清攻擊目標底細，掌握郵件往來內容並進行操控的現象，將是企業在防範BEC電子郵件詐騙所需面臨的挑戰。

Ref: https://www.ithome.com.tw/news/142114

BEC佔比不大，但金錢損失最為慘重

2021 CRIME TYPES

By Victim Count

Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing/Vishing/Smishing/Pharming	323,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729
Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,522	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	395
*Descriptors**			
Social Media	36,034	Virtual Currency	34,202

2021 Crime Types continued

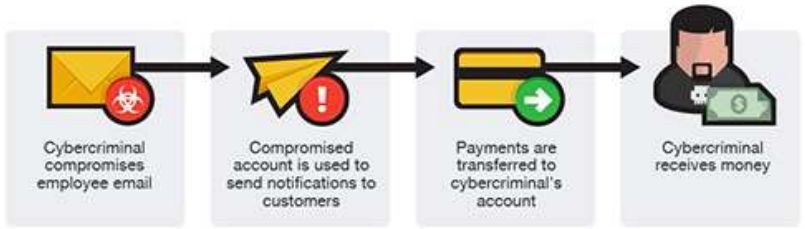
By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950
*Descriptors***			
Social Media	$235,279,057	Virtual Currency	$1,602,647,341

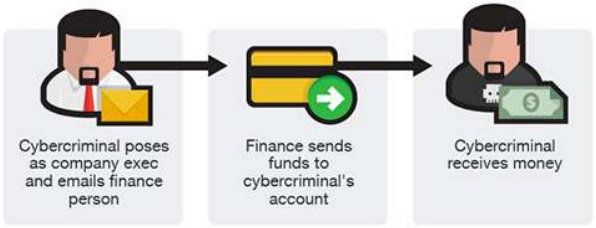
資料來源: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

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**

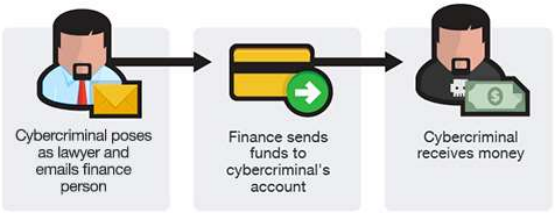


  - **Case 2: 偽造身份(CEO、CFO、CTO)**

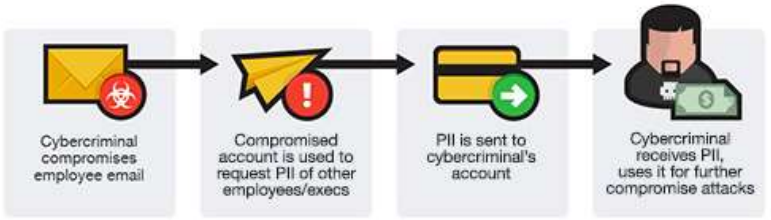


  - **Case 3:入侵員工的電子郵件信箱**

  - **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/

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)

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**標題黨**，主要都是靠所產生的**廣告收入，不管內容的正確與否**
  - 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

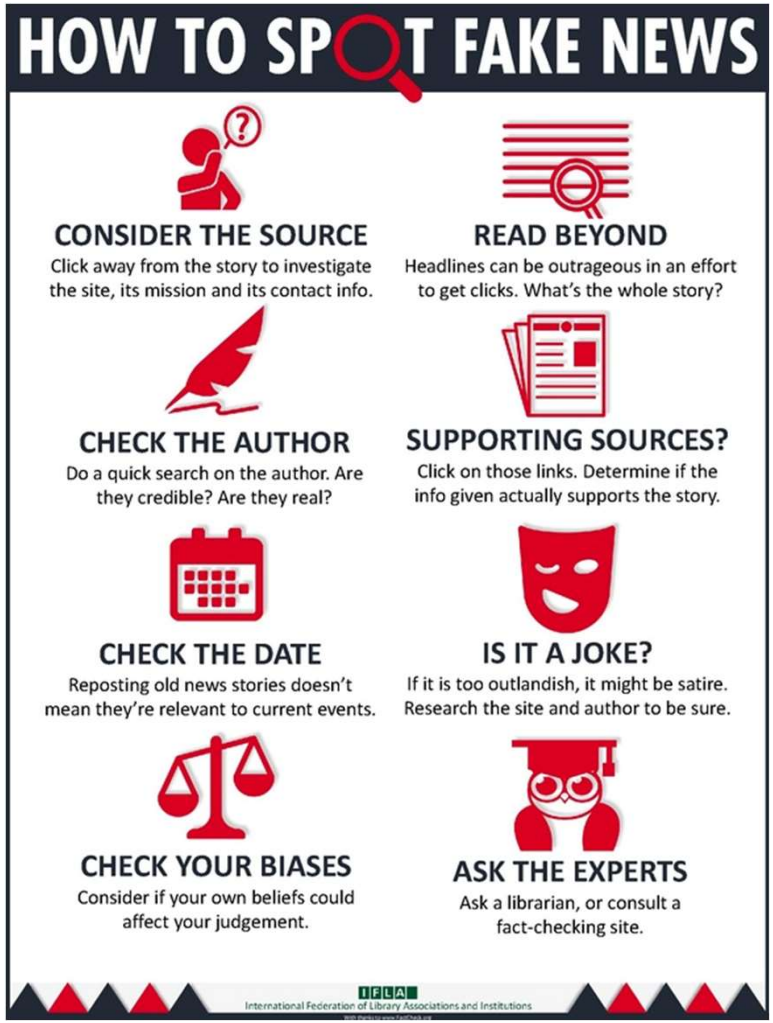
第 一 章 妨害安寧秩序

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。

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 冠綸 | 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。

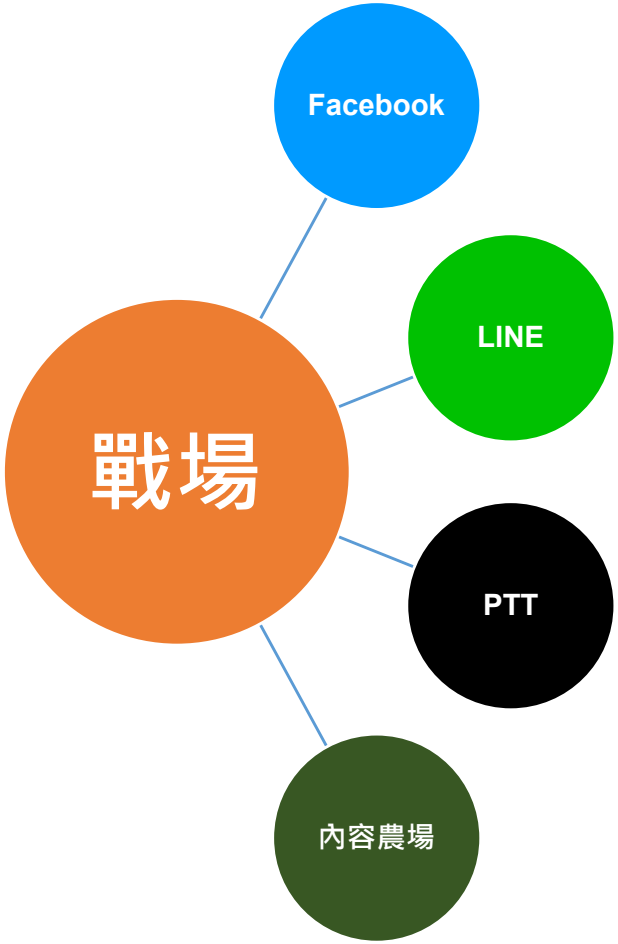
所幸人們對於深偽影片的使用有所警覺，該影片很快就被揭穿。在第一時間，澤倫斯基本人也在Telegram頻道上傳影片反駁自己曾經要求烏克蘭軍隊投降。他說，如果他呼籲投降，那會是要求俄羅斯軍隊放下武器，回去自己的國家。

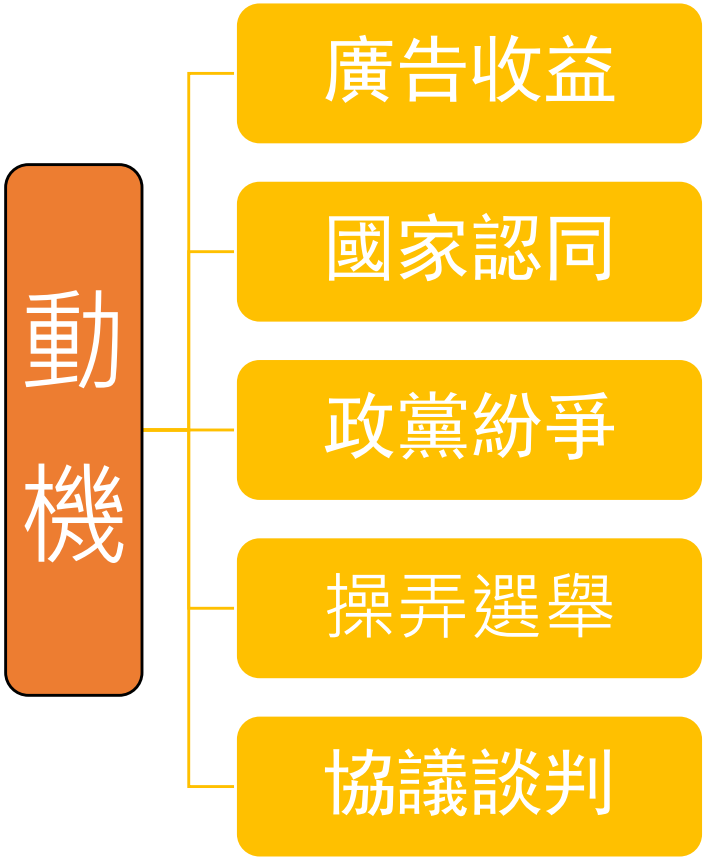
在台灣，也可能因為Meta的即時處置，在中文臉書平台上並沒有相關影片流傳。

> 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

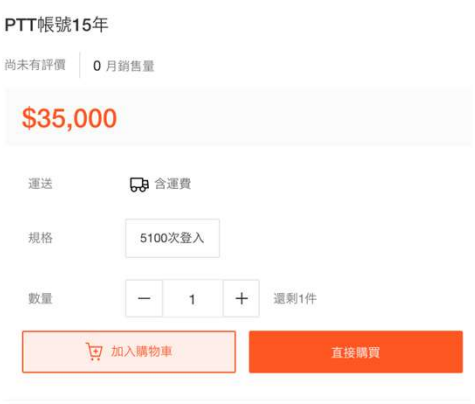
Ref: https://tfc-taiwan.org.tw/articles/7099

假新聞的在台灣的戰場與動機





秤斤論兩行情：買榜、刷評、按讚、賣帳號



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/tQQ1a2V.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**

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

FB 失智症權威醫師失智了！？

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

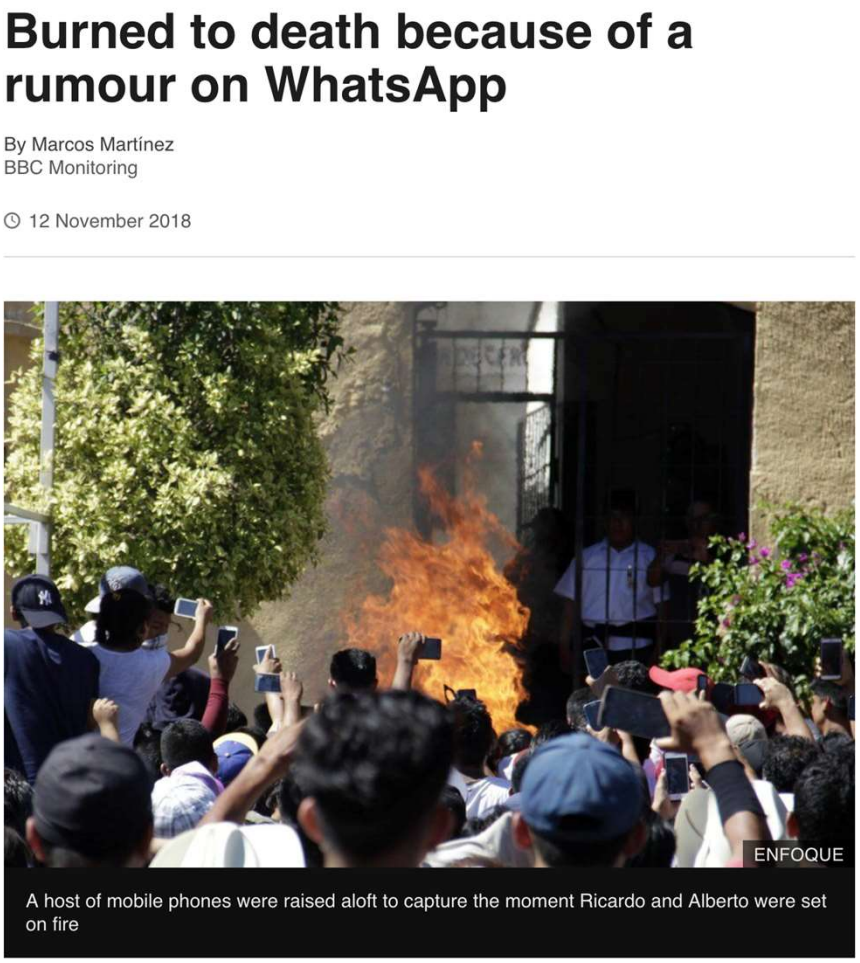
「失智症權威醫師劉秀枝失智了！」這樣的消息最近在臉書瘋狂轉貼，許多人按讚，並留言表示惋惜、不捨。不過，當事人劉秀枝並沒有失智，她謝謝大家關心，並調侃自己，「這個消息是正確的，只是提早了廿年。」

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

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 • 專用軟件 •

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

藍脊

藍色的天空，藍色的海，藍色的曲調，深入骨髓。

Previous post:

日本研發全球首部經電潛艇　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 • 社交媒體 •

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 禁員工款 Starbucks 反制

Next Post:

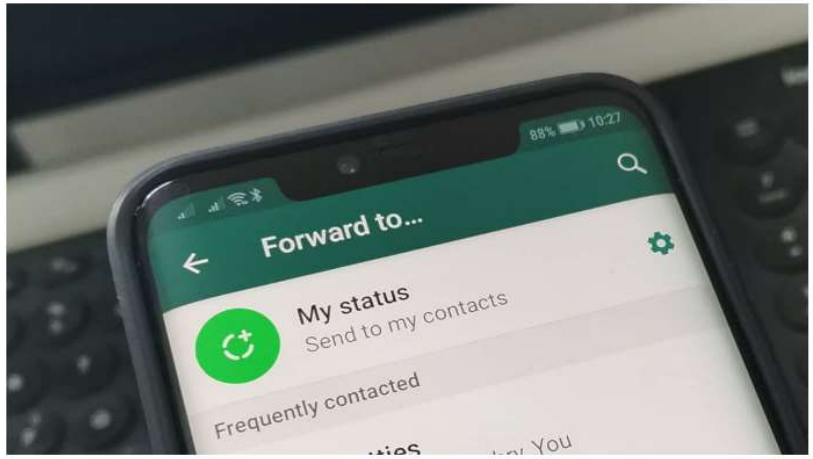
iOS 詐騙 App 出現　按手指查健康即付100美元

- 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。

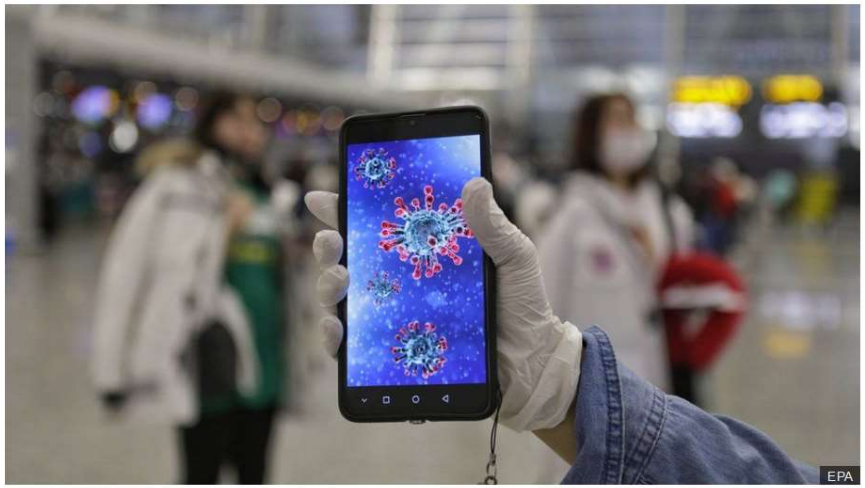
2020 年 4 月 7 日　　Tweet

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

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。中央社記者張茗嗯攝 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 | 林芷蓤 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

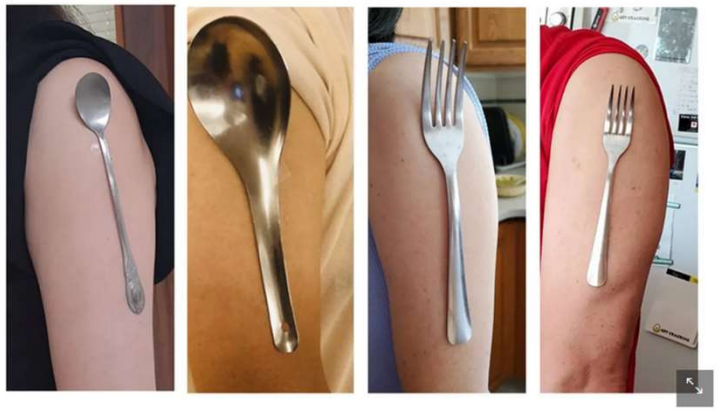
「聽說打疫苗會變身萬磁王？」到底誰說的？是不是真的？

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

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/

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)

- 網傳解放軍擊落台灣戰機 【錯誤】

查核報告: https://tfc-taiwan.org.tw/articles/7096

事實查核報告 (2/3)

- 網傳各國酒駕刑罰文章「世界上酒駕最嚴的懲罰：發現一次直接槍斃」

【部分錯誤】


事實查核報告#1466

網傳各國酒駕刑罰文章「世界上酒駕最嚴的懲罰：發現一次直接槍斃」？

部分錯誤

發布日期／2022年1月25日

經查：

【報告將隨時更新 2022/1/25版】

一、新加坡對酒駕的刑罰，單純酒駕為罰款、吊銷執照或監禁，若造成嚴重傷亡，可判鞭刑不超過6下。

二、日本對酒駕的刑罰，酒駕司機、車輛提供者、酒精提供者和乘客皆會被處以不同程度的有期徒刑和罰款。

三、法國對酒駕的刑罰包括監禁、罰款、吊銷駕照、參加道路安全講習課程、扣押或沒收車輛。傳言僅稱「沒收汽車」，說法不精準。

四、傳言對立陶宛、愛沙尼亞、拉脫維亞、馬來西亞、俄羅斯、澳洲、美國、土耳其、英國的酒駕刑罰，均為錯誤描述。

五、傳言宣稱「保加利亞、薩爾瓦多」的酒駕刑罰為「槍斃」，經查兩國的酒駕刑罰並無「槍斃」。

因此，傳言為「部分錯誤」訊息。

查核報告: https://tfc-taiwan.org.tw/articles/6876

事實查核報告 (3/3)

- 網傳圖卡「核蛋來了」，並稱「不是白色蛋殼都不要吃」、「近日盡量不要去大賣場買雞蛋」？【錯誤】


事實查核報告#1564

錯誤

網傳圖卡「核蛋來了」，並稱「不是白色蛋殼都不要吃」、「近日盡量不要去大賣場買雞蛋」？

發布日期／2022年3月9日

經查：

【報告將隨時更新 2022/3/9 版】

一、農委會與蛋商、賣場均指出，台灣從3月8日起到3月底，從日本進口雞蛋的專案，供應給食品加工業者，而不是零售通路。

二、網傳圖卡挪用圖庫照片，卻誤稱為日本雞蛋來台；專家也指出，無法用蛋殼顏色辨別產地。

傳言挪用圖庫照片，誤導讀者以通路、蛋殼來辨別蛋品產地，因此，為「錯誤」訊息。

查核報告: https://tfc-taiwan.org.tw/articles/7058

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

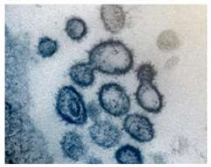

【錯誤】網傳「山東蘭陵县146萬人，目前無一感染...分析原因：他们是大蒜种植区...蘭陵農田...


【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...

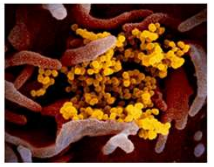

【錯誤】網傳「鐘院士的防病毒高招：建議各位去醫院或其他公共場合之前用淡鹽水漱一下嘴...


【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，...

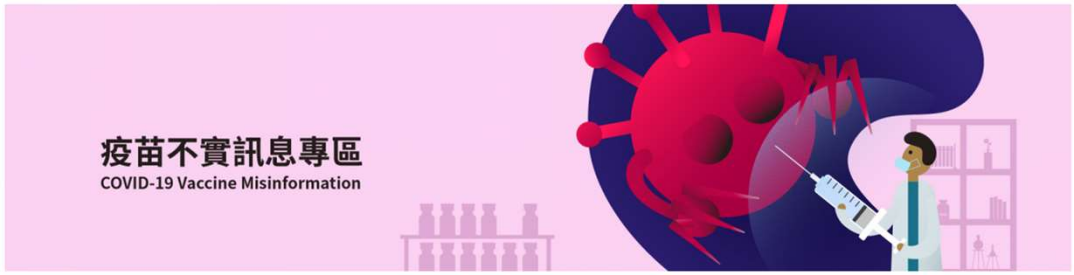
【錯誤】網傳「由於NCP新型冠狀病毒，有0～24天的潛伏期...專家提供一方法讓你盡早知道自...


【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

事實查核報告 (疫苗不實訊息專區)



【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...

【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...

【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...

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

MyGoPen｜這是假消息

- https://www.mygopen.com

Ref: https://www.mygopen.com/2022/03/strawberry.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

蘭姆酒吐司

謠言這樣說：最近有蠻多朋友傳來一張圖片，要蘭姆酒吐司解答是正確還是不正確。圖片分成上下半部，上半部寫著：「政府新式照相機。8顆鏡頭＋中間的紅外線發射燈，只要你在紅燈下使用手機包你中彈。」接著下半部就寫著：「請記得別在停紅燈時看手機，機車1000，汽車3000。」附上一張紅色罰單。到底，這張圖片可信還是不可信呢？可傳還是不可傳呢？

破解關鍵點：政府新式照相機，專門拍紅燈下使用手機？

這張圖片有錯也有對，一開頭「政府新式照相機」這一段就是錯的！蘭姆酒吐司之前的破解文其實有提過喔，謠言所說的新式照相機，其實要拍的對象不是民眾，別太過緊張；至於紅燈下使用手機行不行，當然是不行的！停等紅燈時拜託忍一忍，要是手指忍不住滑手機，小心錢包準備失血囉！

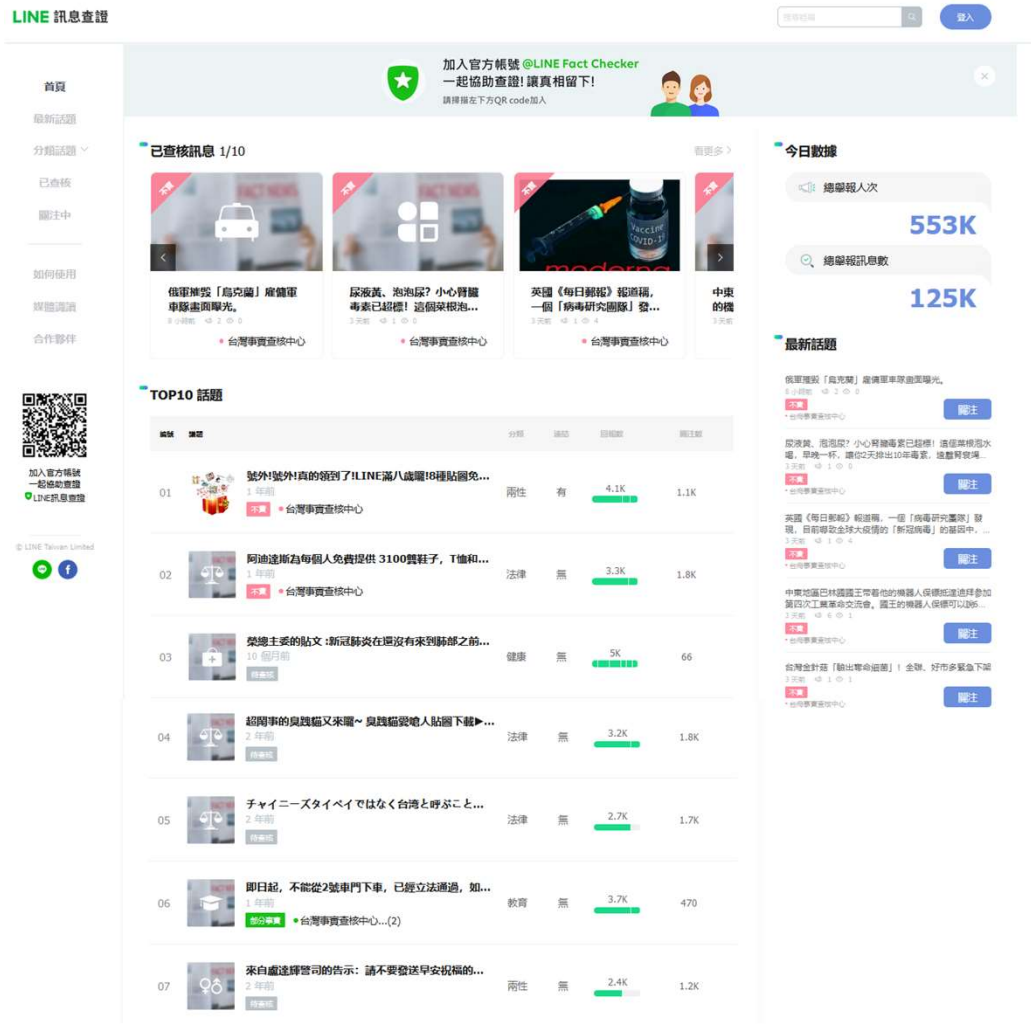
謠言圖片，請勿再轉發

謠言圖片，請勿再轉發

Ref:
https://www.rumtoast.com/
https://rumtoast.com/8578/

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、蘭姆酒吐司等查核機構合作
- 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
- 行政院農業委員會-爭議訊息澄清專區(含食安)
  - https://www.coa.gov.tw/faq/faq_list.php
- 內政部刑事警察局-闢謠專區
  - https://165.npa.gov.tw/#/articles/rumor
- 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
- 衛生福利部食品藥物管理署-謠言終結機
  - https://article-consumer.fda.gov.tw/rumor_list.aspx?subjectid=1
- 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

課程結束

Thank You!