



數位發展部資通安全署
Administration for Cyber Security, moda

防範社交工程，守護全民資安

洞察騙局，從識破謊言開始

數位發展部資通安全署



社交工程為主要資安威脅來源之一



近期資安署資安月報統計：

> 30%

威脅屬社交工程等資訊收集類

什麼是社交工程？

壞人利用你的
信任、恐懼和好奇心，
讓你**主動交出**你的
金錢、資料或帳號權限。





社交工程手法

手法



釣魚郵件



惡意簡訊

工具



偽冒網站



偽冒檔案



偽冒連結

目的



竊取資料



騙取金錢



控制電腦





偽冒政府簡訊



竊取資料



別上當！ 這個簡訊是假的

[數位發展部]
恭喜你！！政府發放\$6000
還稅於民，如何快速領取請點
擊下面連結 ([https://
shuweibu6000.com/](https://shuweibu6000.com/))

假！

先查證，勿轉傳

請認明：申領網址首段一定是 **gov.tw** 結尾

※網址首段是像這裡 <https://moda.gov.tw/press/clarification/378#qaH3521>

※不在首段就不是政府網址 <http://shufabu6000.com/moda.gov.tw/>

高雄區監理所：本所發現
現有未處理之交通違規，
請於收到簡訊後24小時內
辦理，以免產生高額罰款，
敬請配合。網路繳費請至
以下連結：

<https://tw.thbgov.com>

【衛福部】疫情補貼根
据条件你可领五萬，即
將過期請網路領取點註
冊提 [https://
www.margov.tw](https://www.margov.tw) 領申請
(複製網址到瀏覽器打
開)

簡訊連結至惡意網
站，誘使使用者輸
入個資或服務帳密。



偽冒連結或網站：假政府或假服務

騙取金錢

BE8.RM-Mvdis監理信箱 收件匣 ☆

SEO欠賬催繳 11:47
寄給我 ▾

「完項不延遲，守法最放心」

本所依據監理系統資料顯示，您所登記之車輛於下列時間及地點，涉及違反道路交通管理處罰條例相關規定，經依法舉發在案，特此通知，敬請查明並於期限內完成處理程序。

請於 114年7月2日（含）前 完成繳納，逾期未繳將依法加徵滯納金，並移送強制執行。

繳納方式
為提供便利服務，您可選擇下列任一方式繳納罰單：

1. 【網路繳費】監理服務網繳費登入官網 → 交通違規繳費。
2. 【ATM轉帳／網銀繳費】依據繳款單上虛擬帳號

交通違規(含強制險)查詢及繳納



- 一、交通違規紀錄不會即時更新，需待舉發機關入案後，才可於線上查詢到。
- 二、請注意，若使用本功能繳費完成，每筆違規皆會收取一筆手續費

步驟一：

步驟二：

1. 騙取輸入身分證字號及車牌號碼

身分證字號：Q000000000

車牌號：QQQ-000

查詢

可線上繳納

下列罰單可做線上繳納：

違規日	事由	罰鍰	應罰末日
114年08月01日	在禁止臨時停車處所停車	900	114年09月15日

線上繳費

回上一步

2. 透過假罰單資訊騙取信任

Q000000000 本次繳費清單：

違規日	事由	應罰末日	罰鍰
114年08月01日	在禁止臨時停車處所停車	114年09月15日	900元

共 1 筆，總金額：900元

信用卡繳費

持卡人名字：

信用卡卡號：0000 0000 0000 0000

有效日期：MMYY

安全碼CVV：000

3. 騙取銀行信用卡資料



偽冒網站：常用通訊軟體下載

控制電腦

假Line下載網站：

linekr.com
https://www.linekr.com

Line中文版下載
支持免費語音、視頻通話和多樣化聊天功能，豐富的表情包和貼紙讓交流更生動。最新版line下載支持windows、電腦桌面版、安卓手機版... Line中文版進行個性化設置，包括...

linec-tw.com
https://www.linec-tw.com

LINE下載官方網站
造訪LINE下載官網，免費下載LINE電腦版和手機版。支援Windows、Mac、Android和iOS設備，輕鬆安裝並使用LINE與好友保持聯絡。在官網上，您可以找到適合不同設備的...

line-china.com
https://www.line-china.com

LINE中文版- 永遠在你身邊
LINE中文汉化版是由LY Corporation所开发的即时通信平台，Line中文用户之间可以通过互联网在不额外增加费用情况下，与其他用户发送消息及观看直播欢迎下载体验。

linekr.com

假Skype：

Google skype 網頁版

skypezh.com
https://www.skypezh.com · 轉為繁體網頁

Skype网页版- Skype

Skype是一款即时通信应用软件，可通过一个(版)等。下载Skype可以随时随地与任何人保

skypezh.com

假Teams：

teansms.multiscreensite.com
https://teansms.multiscreensite.com

Microsoft Teams

Teams 2025最新版本 — 高效沟通协作平台，Microsoft 办公更灵活高效。

teansms...

駭客使用與通訊軟體名稱相近網址欺騙使用者點擊後執行惡意程式，你的電腦就變成駭客拿來攻擊別人的跳板！



偽冒網站：惡意的假副檔



控制電腦



Tue 8/26/2025 9:20 AM

吳先召 <cassiisulikgov1e@outlook.com>

██████████ 案件

收件者 ██████████.gov.tw

gPNRzL 密碼.png
17 KB

投訴書.zip
1 MB

經密碼加密之
惡意附檔

您好，我又做出瞭如下補充，我去問了當天和我一起去的朋友，他有拍了一些照片，我讓他發了過來，當時和朋友還聽到了██████、██████這兩個名字，希望能夠查清楚是否為內部人員，如果不是剛好也能夠澄清之前的內容

駭客將密碼以圖片顯示以規避偵測

壓縮檔含**惡意程式**，藉由圖片密碼解壓縮後，點擊將執行惡意程式，並連線至駭客控制之**中繼站**，進而劫持個人設備，成為駭客利用的工具



停、看、聽 — 資安防護三步驟



停：冷靜！不要點擊



看：檢查！判斷寄件者與內容

聽：通報！尋求協助





「停」— 不輕信、不點擊



不開啟

- 可疑郵件勿開啟
- 公務信箱不可用於私人用途



要關閉

- 關閉郵件預覽
- 關閉自動下載

避免有害內容在沒有注意到的情形下進入個人電腦



要設定

- 純文字模式開啟信件
- 垃圾郵件過濾機制

現在大多數電子郵件軟體都會提醒垃圾郵件，使用時要多注意



「看」— 火眼金睛，洞察偽裝！



要辨識

- 確認對象
- 主旨和自身的關聯性



要檢查

- 語氣過於緊急或情緒化
- 文法或用字錯誤



要識破

- 附帶的網址不符或非必要/可疑附件
- 要求提供敏感資料或付錢



識破主旨陷阱

濫用信任

年度健檢通知

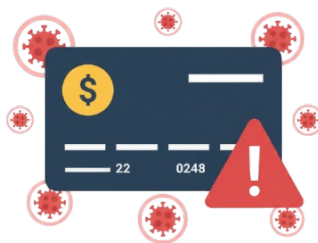


普發現金
已開放登記



訴諸恐懼

您的信用卡已暫停使用



帳號異常登入



引發好奇心

會員限時降價！



OOO已接受
您的交友邀請





識破寄件者陷阱

看寄件者名字、地址及信件內容的關聯性



這封信是你預期會收到的嗎？

如果沒有，而且要求你儘快處理，或是要求你立刻點擊、匯款或提供個人資料/帳號密碼，那通常就是個警訊。



內容與寄件者相符嗎？

如果是銀行寄來的信，內容卻是關於交通罰單，或是同事寄來的信卻要你更新信用卡資料，這就是個大問題。



識破檔名和附檔名破綻



副檔名是檔案的真實身分，駭客常用偽裝來欺騙你！

<p>高風險 (絕對不要打開!)</p>	<p>.exe .vbs .js .iso .pif(執行檔)</p>
<p>中風險 (內容可能有問題!)</p>	<p>.zip .rar .7z (壓縮檔)</p>
<p>開啟前要注意 (我認識寄件者嗎?)</p>	<p>.pdf .docx .xlsx .pptx .jpg</p>



最右邊一點後面文字(zip)才是真正的副檔名！

不確定嗎? **Virus Check** 可以幫忙!



線上檢測可疑檔案

惡意檔案檢測服務

Virus Check

Integrate static and dynamic cybersecurity analyzing skills;

Detect hidden malware in a comprehensive manner



檔案上傳 File Upload

選擇檔案 沒有選擇檔案

提醒您，檔案上傳功能僅限電腦版，手機版僅提供查詢功能。

壓縮檔密碼 Unzip password

限長度為 10 碼以內的英文字母與數字

E-mail

Virus Check

台灣惡意檔案檢測服務
無檔案外洩疑慮!

<https://viruscheck.tw>



識破假政府機關網站破綻

認明政府機關網址為 **.gov.tw** 或政府專用短網址



網址主機名稱以.gov.tw結尾之政府網址 (例如：xxx.gov.tw)



政府專用短網址 <https://gov.tw/xxx>



gov.tw不在網址首段結尾，就不是政府網址 <https://xxx/-gov.tw>

網址小知識-主機名稱怎麼找?

◆ 一般網址長這樣：

➤ <https://moda.gov.tw/press/370>

網址由**第一個單斜線"/"**隔開，最左邊有點"."的首段就是**主機名稱**。

本例主機名稱就是 moda.gov.tw

➤ <https://moda.gov.tw>

沒有單斜線，整段就是主機名稱，確認是**以.gov.tw結尾**

◆ 有時網址**不會**有前面的https://

例如 t.ly/mvdis.gov.tw

主機名稱是t.ly (同樣用第一個單斜線判斷)

◆ 假裝有gov.tw以混淆視聽

<https://gov.tw.official-site.com>

主機名稱是.com

真

假



識破假政府機關簡訊破綻

認明政府專屬短碼簡訊發送方為 **111**



111只有政府機關和公營事業可以申請發送



簡訊號碼顯示為111，即為政府或公營事業發出



簡訊號碼如果不是111，就要小心注意！



「聽」——冷靜查證，即時通報！



要查證

- 必要時以電話或電子郵件向寄件者確認郵件真偽



要通知

- 可疑郵件勿開啟，並通知相關資安人員處理或通報
- 請利用<**165反詐騙諮詢專線**>
<**數發部網路詐騙通報查詢網**>



要刪除

- 可疑郵件一律刪除

別讓你的信任被不法人士冒用了



停



看



聽

每一次**停看聽**，都是成功防禦
多一份謹慎，就是對自己的安全多一份保障



信賴資安 守護臺灣



數位發展部資通安全署

Administration for Cyber Security, moda