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

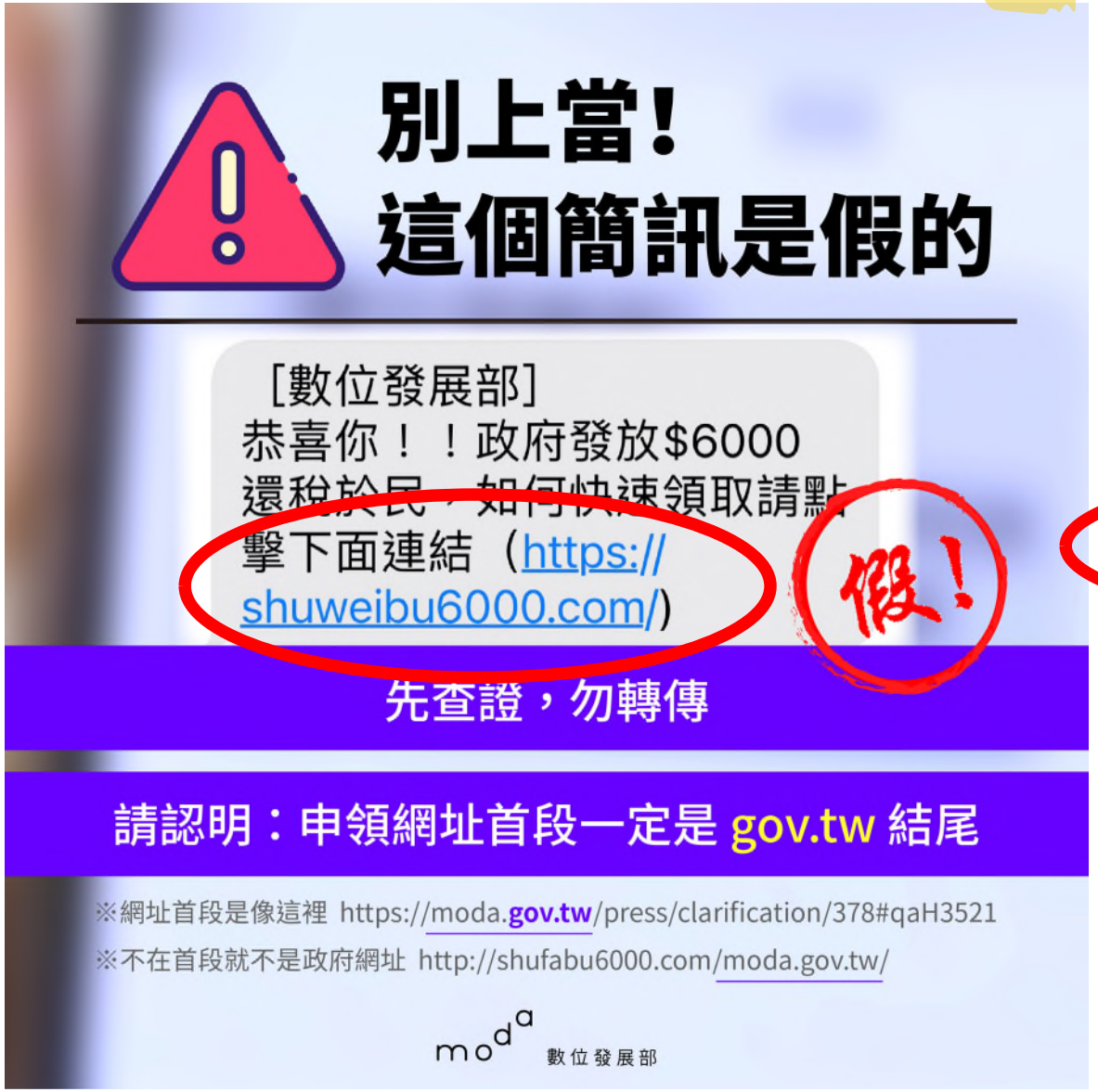
目的

竊取資料

騙取金錢

控制電腦

偽冒政府簡訊 竊取資料



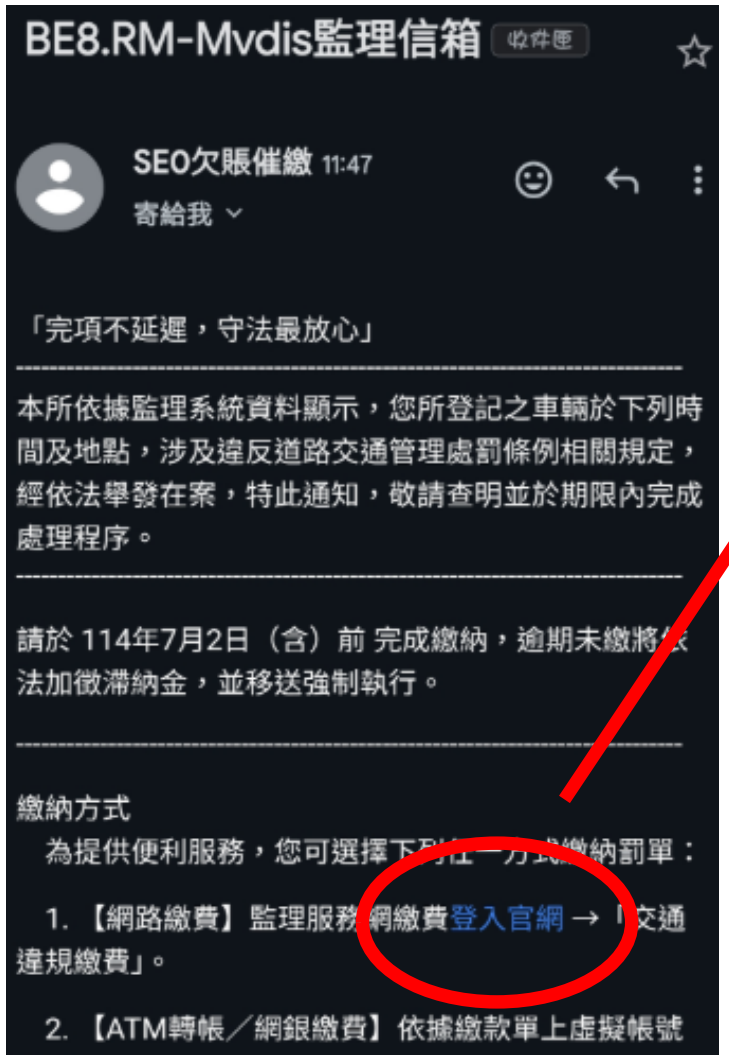
高雄區監理所：本所發現您有未處理之交通違規，請於收到簡訊後24小時內辦理，以免產生高額罰款，敬請配合。網路繳費請至以下連結：
https://tw.thbgov.com

【衛福部】疫情補貼根據条件你可领五萬，即將過期請網路領取點註冊提 https://www.margov.tv 領申请(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



1.騙取輸入身分證字號及車牌號碼

2.透過假罰單資訊騙取信任

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

假Skype：

skypezh.com

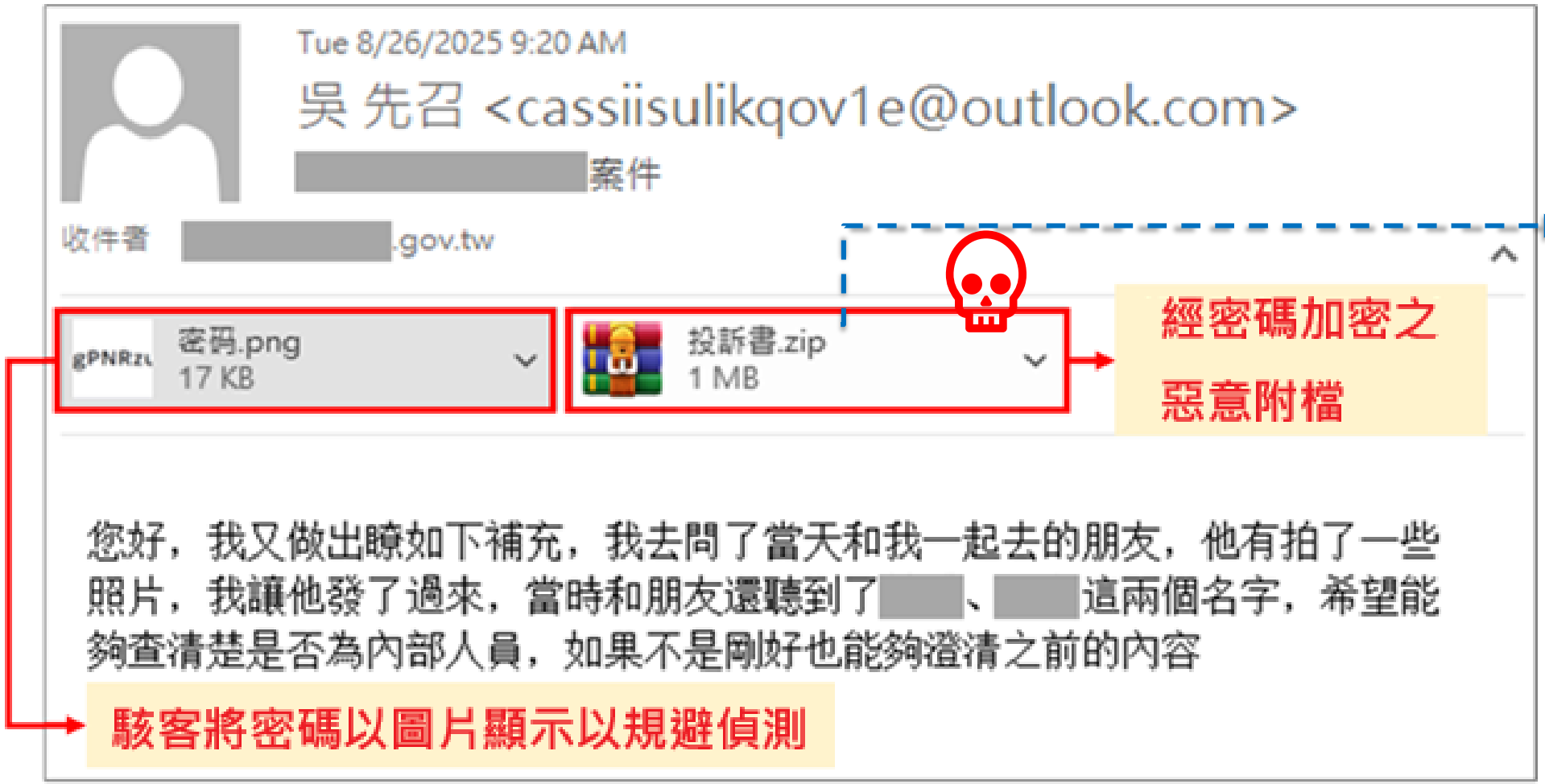
假Teams：

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



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！

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

(2-27-002591-2)202403_[C].pdf.zip 70KB

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

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** 真

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:// 假

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

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