公務機密維護
「快篩」釣魚郵件不上鉤(下)

苗栗縣政府政風處
11月份公務機密維護宣導

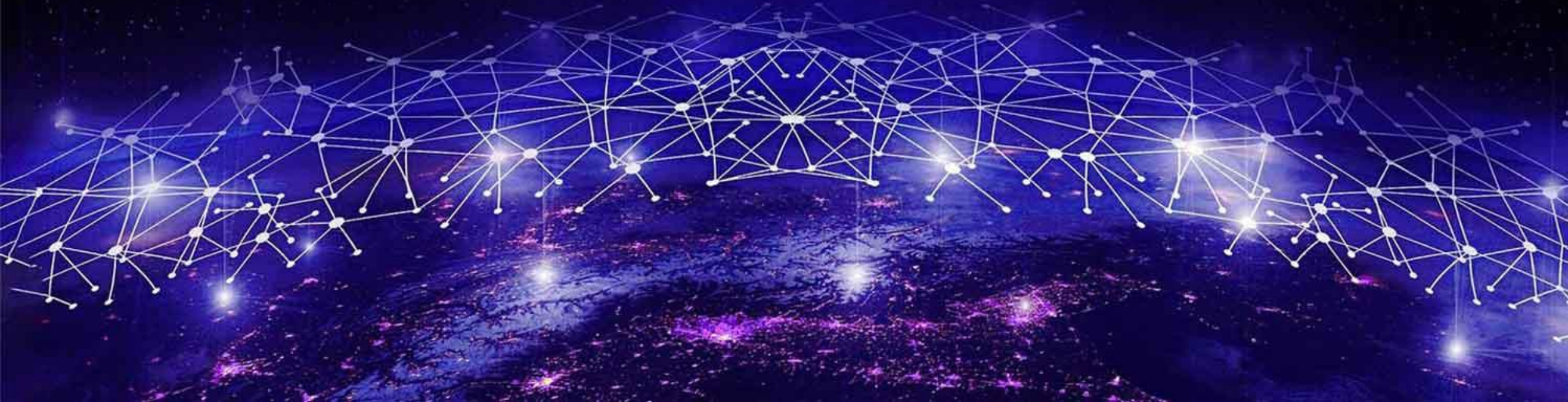
資料來源：SecBuzzer-資安威脅情蒐平台

01 搞懂釣魚郵件4模式，讓自己牢不可破

02 8大破綻輕鬆揪出釣魚郵件

03 3個不要的鐵則

04 6個必要的對策



預防勝於治療，除了透過上述的8大破綻「快篩」釣魚郵件外，請掌握「3不要、6必要」的原則，徹底防釣。

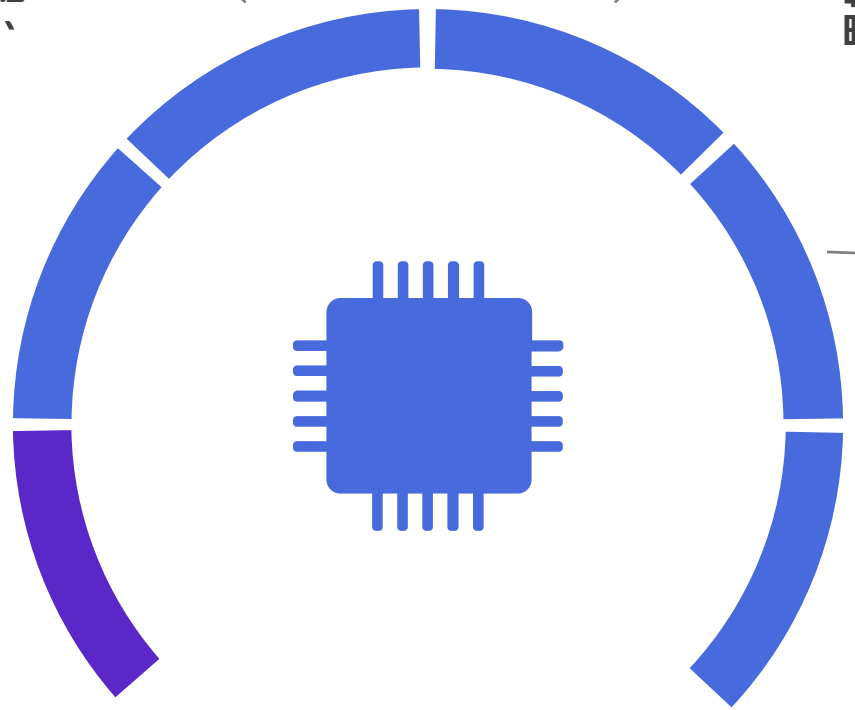
3個不要的鐵則

不要開啟信件：
發現可疑信件就不要開啟。.

不要下載附檔：
不輕易打開、下載郵件中的附件檔。

不要點擊連結：
不隨意點擊郵件中夾帶的網址連結。

6個必要的對策



1、安裝防毒軟體

透過防毒軟體於所有上網裝置包括電腦、手機、平板電腦，有效偵測釣魚郵件、病毒、間諜軟體、惡意軟體、木馬程式。.

2、開啟垃圾電郵過濾功能

透過增強垃圾郵件過濾功能，有效過濾及將已知的濫發、垃圾及釣魚郵件自動送往垃圾郵件匣，降低開啟可疑郵件的機率。

3、定期更改信箱密碼

定期更改信箱密碼，且不同平台設定不同的密碼組合，減低因長期使用同一組密碼而增加被盜用的風險。

4、停：停止所有點擊動作

收到可疑郵件，應立即提高警覺，第一時間停止所有動作。

5、看:看清楚郵件內容

仔細閱讀信件的大小細節，從郵件來源mail及連結眞僞、主旨、內文文法、用字、語言、附件檔案格式等大小細節，冷靜分析判斷是否爲釣魚郵件。

6、查：向來源機構查證眞僞

直接向發信來源的官方機構，甚至電子郵件服務供應商，查證郵件的安全性。

釣魚郵件7步驟緊急應變SOP

還是上鉤了怎麼辦？！

1、更改電子郵件密碼

立即登入帳號並更改密碼，以長且獨特、複雜、難以破解爲原則重設密碼，避免遭受進一步的攻擊。

2、啟用兩步驟驗證

啟用兩步驟認證，額外的步驟需要你手機上的認證碼，才能登入或變更帳號設定，如此一來，唯有手機持有者，才能取得認證碼。

3、重新檢查設定

掃描帳號設定，檢查是否出現任何可疑的異動，因爲駭客可能設定將你的電子郵件自動轉寄給他們，藉此接收登入資訊，並取得通訊錄。另外，若有用電子郵件簽名，也請檢查是否有可疑的變動。

4、掃毒揪出惡意軟體

帳號被駭時，可斷網執行或請資訊人員處理，立即掃瞄檢查所有裝置是否已經中毒，或是乍看安全無虞，其實已潛伏其他惡意軟體。若偵測到惡意軟體，務必再次變更密碼「並」重新檢查設定，因爲只變更密碼而沒有將系統清理乾淨，駭客很有可能透過惡意軟體，再次幫他們打開大門。

5、通知相關單位緊急應變

若已輸入重要個資，請立即通知相關單位，做緊急應變措施，把損失降到最低。例如，如果已輸入信用卡卡號，立即連絡信用卡銀行，告知已點擊不明連結，請求助查詢6、期刷卡紀錄，確認是否有遭盜刷，並建議辦理停卡，防止日後遭盜刷。

6、通知你的聯絡人

爲避免駭客透過你的通訊錄廣發釣魚郵件，請通知並提醒通訊錄好友，問題徹底解決前，請他們忽略來自你帳號的可疑郵件。

7、通報電子郵件服務供應商

檢舉回報此爲惡意郵件，請求其進行記錄及後續處理追蹤，以防止受害範圍擴大。

手機釣魚郵件自救SOP，再多做這3步驟

1、聯繫電信公司

通知電信公司，已點擊不明連結，要求關閉「小額付費」功能。

2、請交易平台取消交易

查詢確認手機的網路交易平臺（如：iTunes）是否有異常交易紀錄，如有立即尋求相關協助。

3、手機回復原廠設定

因點擊惡意連結，很有可能遭植入惡意程式，建議將手機內重要資料備份後，進行系統重置或回復原廠設定，以清除惡意程式。

結語

釣魚郵件的攻擊手法推陳出新，防不勝防，想要徹底防釣，技術性的郵件安全防護系統必須持續更新升級，其中包括郵件稽核、進階郵件威脅防護、應用威脅情報分析、機器學習、郵件簽章、郵件加密與網域驗證等機制，此外還有網頁郵件帳號安全的雙因素認證及異常登入警示，都是郵件資安的重要課題。同時不斷強化員工的資安意識，以守住最後一道防線，雙管齊下才能有效抵禦各種釣魚郵件的威脅。

根據 2019 年 美國電信業者Verizon的《數據失竊調查報告》指出，在企業執行的社交工程演練中，僅有 3% 的使用者會點擊未知的連結，儘管比起 2012 年的 25% 已大幅下降，可見企業用戶資安意識逐漸抬頭，但仍存在一定風險，無論是個人還是企業組織的一員，都應時時刻刻提高警覺，別讓自己成爲那有失警覺促成大錯的那3%。


廉政專線：037-356639
苗栗縣政府政風處
關心您~