苗栗縣政府政風處
10月份公務機密維護宣導

公務機密維護

「快篩」釣魚郵件不上鉤(上)

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

社交工程攻擊「以人為本」

人性弱點成最大資安漏洞

所謂的「社交工程」（Social Engineering），主要是利用人性的弱點：好奇心、本能反應、無知、信任、貪婪、恐懼、惰性、掉以輕心等，透過電話、電子郵件、簡訊、LINE或WhatsApp等IM即時通訊軟體等，用各種狡詐話術影響或說服攻擊目標，做出某些動作提供機密資料，或入侵其電腦、手機系統。

社交工程常見手法：釣魚郵件

社交工程的攻擊者往往偽冒知名官方組織、社群媒體平台、通訊錄中的同事、朋友發送釣魚郵件，透過各種話術，誘導收件者點擊郵件中所夾帶的惡意檔案、勒索病毒、虛假連結等，他們想釣的無非是你手中的個資、帳密、財務資料、電腦系統存取權限等重要機密，進而造成企業組織的損害與威脅。

搞懂釣魚郵件4模式，讓自己牢不可破

釣魚郵件4模式

利用你的恐懼心理

「您的電子信箱密碼即將到期，請立即透過附檔連結更新，以免帳號停用！」
「登入異常警告！請儘速進行帳號驗證，避免身分遭盜用！」
「信用卡付款失敗！請立即輸入驗證碼，以免影響自身權益！」

利用恐懼心理的釣魚郵件，就像是「做賊的喊捉賊」，偽冒帳號安全的重要通知信，**營造緊急氣氛，要求收件者「立即」完成郵件中的指令、點擊連結或打開附檔，否則後果將不堪設想**，迫使收件者乖乖照辦。明明是帳號「安全」通知信，卻是最「危險」。這類恐懼訴求的模式，同時也讓攻擊目標因為恐慌、急迫性而有失警覺，忘了先冷靜比對、判斷寄件者mail、外部連結之網域是否拼字有誤，是否為山寨、偽冒。

利用你的信任

這類的釣魚郵件，為了博取收件者的信任、降低警覺，往往**偽冒知名機構或是公司業務相關單位或人員**。內容看似不緊急，卻讓收件者認為有其「點擊」、「完成步驟」的必要性。

像是偽冒成寄送發票的郵件，在附檔中以ZIP壓縮檔夾帶有惡意的js（javascript)檔案，誘使收件者開啟發票附檔，觸發勒索軟體執行；偽冒購物平台的訂單確認通知，透過郵件裡附件內的連結，將收件人導向釣魚網站，以獲取帳密；偽冒快遞公司發送包裹狀態異常的通知信，提供你追蹤包裹狀態的惡意連結。

釣魚郵件4模式

利用你的好奇心

這類的釣魚郵件**以時事、新奇、健康、情色、團購優惠等為餌**。像是冒充社群網站的動態更新通知：「點擊看看誰對你的照片說讚」、「誰將你加為朋友狀態說讚」，或是「志玲姐姐行事曆下載」、「情色影片分享」等，目的就是要誘使你點擊郵件中的惡意檔案或連結。

近期還有駭客假冒疾管署之名，發送主旨為「您所在地區有3例確診病例，其中一名患者在過去14天中將您列為她的身體接觸者之一」的釣魚郵件，並附上惡意檔案，為增加可信度，**還刻意把寄件人名稱設為cdc.gov.tw**（cdc是疾管署，gov.tw為政府機關網址），魚目混珠。

利用你的貪小便宜

過去曾發生，駭客以「Apple 用戶可領取Apple Store好康禮物卡」折扣優惠為餌，誘騙收件者填寫個人甚至財務資料。又或是以「恭喜你中獎了」、「免費抽iPhone」為題設下圈套，郵件附檔**以「中獎名單」為名，行勒索病毒之實，讓你「中獎不成反中毒」**。

8大破綻
輕鬆揪出釣魚郵件

8大破綻

1、寄件者電子郵件名稱及地址有蹊蹺

釣魚郵件慣用手法之一：假冒知名機構。**仔細比對括號<>內的電子郵件名稱和地址**，就會發現和原版官方機構的名稱或郵件地址其實有所不同，魔鬼往往就藏在容易被忽略的細節中。.

2、幾可亂真的網址和網頁設計

釣魚郵件中所提供的虛假網頁超連結，乍看網址域名、網址、網頁版面設計都和正版官方網站極為相似，有時只有一個字母之差，若未加以察覺，很容易就誤入圈套。若是不確定，**可直接聯繫官方單位確認。**

3、內容字句語帶威脅

釣魚郵件內容可能會**語帶威脅**，例如「若是不立即進行驗證，帳號即將停用，後果自負」要求收件者務必立即按下按鈕或連結進行驗證。.

4、符號、亂碼、怪字、錯字連篇、全外文信

釣魚郵件容易出現不尋常的文法和用字，或是難以理解的**符號、亂碼、怪字**，又或是根本不逛國外網站，也沒有外國朋友的收件者，卻突然收到附有不明連結甚至附檔的**全外文**郵件。

5、這些檔案格式都很可疑

附檔名為**.exe.、.js、.jar、.bat、.cpl、.scr、.com、.pif、.vbs的執行檔、Office巨集檔案都要留意**。這類的惡意程式執行檔，有時會藏在RAR與ZIP的郵件附檔中。

8大破綻

6、這種檔名是披著羊皮的狼

你可能以為jpg檔應該安全無虞，但附件的壓縮檔解開後，顯示**01.exe、02.jpg、03.jpg的檔案**，Windows的檔案總管預設隱藏副檔名，使用者如果沒有開啟副檔名顯示，很容易因為誤判全為圖片檔而落入陷阱。甚至還有駭客狡詐的直接將附件檔名取為「01.jpg」，**完整副檔名其實是01.jpg.exe的惡意檔案**。

7、文件檔≠安全無虞

看中了很多人誤以為附檔為.doc的Word檔案或是.xls的Excel檔案，就安全無虞，有攻擊者以文件檔降低收件者的警覺。**像是.xls 格式之一的.xlsm**，其實就屬於可疑郵件。另外，只要Office軟體出現**安全性警告的巨集功能開啟提示**，也千萬不要直接點掉，務必停止動作，通知IT人員確認，以策安全。

8、要求提供重要資料

一般大型企業不會透過電子郵件詢問或要求使用者，提供重要甚至機敏資料。收到任何欲索取、驗證企業或個人資料，包括**郵件密碼、網路銀行的登入資料、或信用卡號碼等要求的電子郵件**，都務必提高警覺，守「密」如玉。

廉政專線：037-356639

苗栗縣政府政風處

關心您~