重新認識釣魚郵件威脅！

壹、概述：電子郵件威脅存在多年，僅管防護功能與資安意識也不斷演進，但釣魚郵件也在進化，而現在愈來愈多網路攻擊以此做為開端，令人防不勝防。

我們時常看到網路釣魚、網路詐騙相關的資安新聞，多數企業與個人可能已經知道，普遍這些攻擊的一開始，多半是透過電子郵件、即時通訊軟體與社群網站作為管道，可能引導用戶至假冒的釣魚網站，騙取用戶個人資訊及密碼，但現在更常見到的是，成為網路詐騙、勒索、滲透等一連串網路攻擊的開端。

近年網路攻擊手法中，讓企業損失慘重的商業電子郵件詐騙（Business E-mail Compromise，BEC），就是一例，這種攻擊方式可說是將社交工程手法運用到極致，先是透過釣魚郵件，取得公司郵件帳密並掌握交易資訊，再伺機假冒公司 CIO 或合作廠商，寄送詐騙電子郵件，要求匯款至指定帳戶或變更匯款帳號，讓使用者誤以為是對方而上鉤不自覺。根據內政部警政署刑事警察局提供的統計資料顯示，2017 年受理的商業電子郵件詐騙案件有 54 件，損失金額是 1 億 8736 萬。

貳、許多網路攻擊的第一步都是從釣魚郵件出發，並以目標式攻擊為主

一、近年持續造成災情的勒索病毒，也有許多透過電子郵件引人上鉤的手法，並且是偽裝成職務、生活相關的正常郵件。像是欺騙人力資源部門，偽裝成求職者履歷信，或是利用快遞或郵寄通知，帳單或訂單，或是退稅或發票等假冒內容，引誘各職務員工上鉤，以及利用應用程式漏洞、巨集，或是放入惡意網站的網址方式，讓使用者觸發攻擊，然後要脅

使用者給付比特幣贖金，才可能解密電腦檔案。

二、例如去年臺灣發生的遠東銀行 SWIFT 系統盜轉事件，根據防毒軟體大廠 McAfee 的調查報告指出，駭客入侵最早的起使點，就是兩封附件藏有後門的釣魚郵件。

三、而其中一封釣魚郵件，是偽裝成一個加密 PDF 線上文件的開啟連結，另一封則是偽裝成「Docusign 文件」連結，當使用者點擊連結來開啟文件，都會導向至一個惡意程式網站，並下載惡意軟體到使用者電腦。

四、顯然，現在網路犯罪者在使用釣魚郵件的方式上，變得更具針對性，再加上這些網路攻擊與詐騙，也會透過釣魚郵件的方式，利用社交工程手法，來誘使用戶上鉤，都讓電子郵件帶來的風險變高，要面對的威脅範圍比過往更大。(本文摘錄 2018 年 01 月 21 日網路 IThome 新聞報導)

參、預防來路不明電子郵件之方法

一、不隨意開啟郵件(注意陌生之寄件者)。

二、不定期修改電子郵件密碼。

三、取消郵件預覽。

四、不隨意下載附件。

五、確認寄件人與主旨的關係。

六、謹慎點選郵件中的超連結。

七、善用密件收件人。

八、不隨意留下郵件地址予他人。

九、定期自我執行病毒與後門程式掃瞄。

十、盡量使用純文字模式開啟信件。

高雄市內門區公所政風室 關心您