網路駭客詐欺案件解析

電子郵件詐騙

警政署刑事警察局

105年3月24日

大綱

一、前言

二、電子郵件進階持續性滲透威脅與攻擊

三、預防勝於治療

四、結語

刑事警察局

一、前言

隨著網路的發展，網路服務已深入生活的各個層面，民眾對於網路的依賴性也逐漸增加，衍生的網路犯罪問題亦逐漸上升，特別是網路拍賣、網路購物、虛擬點數交易及網路銀行盜用等涉及金流之詐騙行為，影響民眾生活甚鉅。

由於網路交易具備無遠弗屆，因此網路詐欺犯罪近年來趨向集團性分工結合科技工具運用，因此如何建構國內網站交易安全，不僅在警察機關必須強化偵查能力外，在預防犯罪則提升預防概念與提升網路安全機制，才能發揮功效。

二、電子郵件進階持續性滲透威脅與攻擊(Advanced Persistent Threat, APT)

攻擊階段 > 控制階段 > 活動與擴散階段

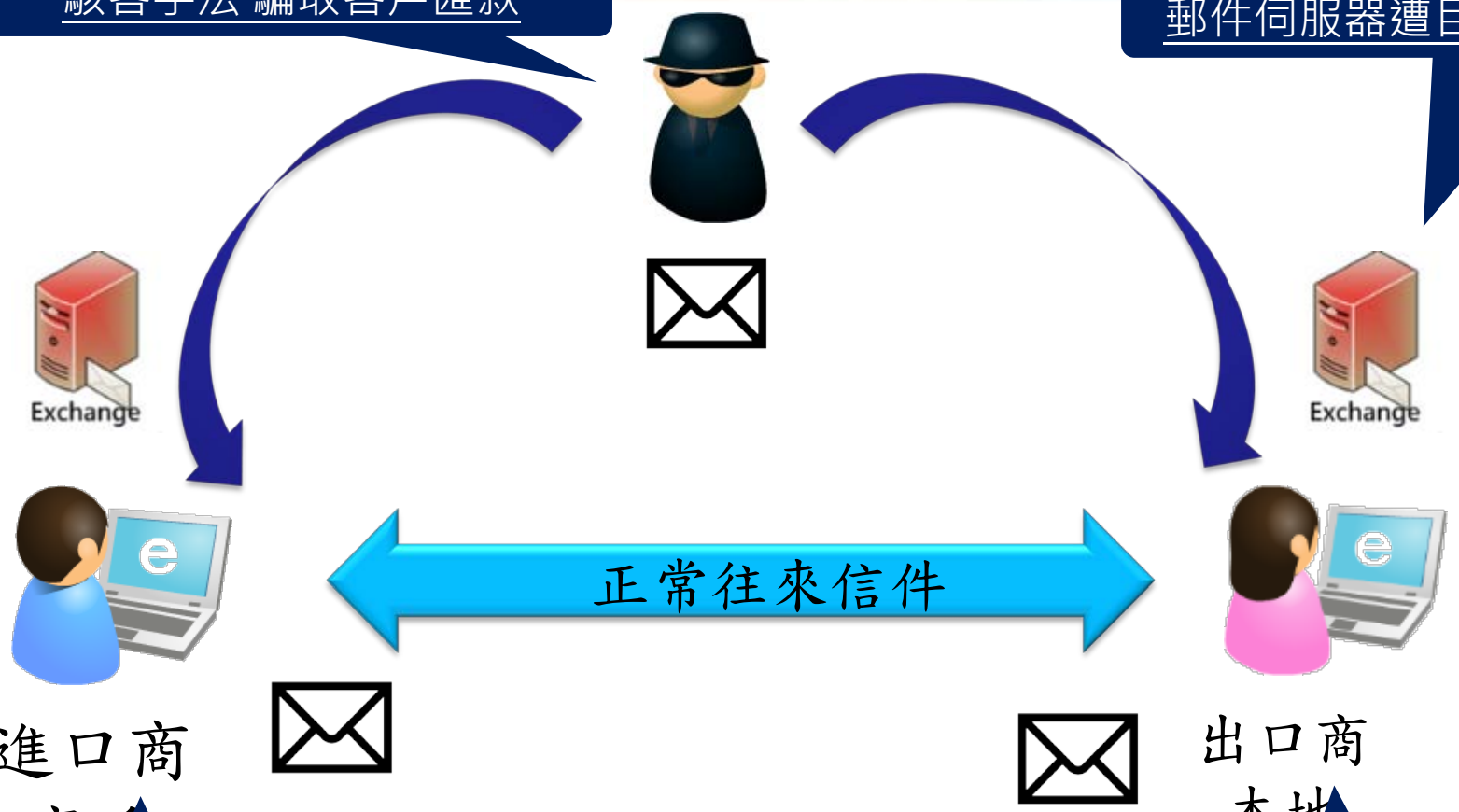
簡單的例子來說，詐騙集團為了要詐騙你的錢，花了很多心思去找有關你的資料，諸如電話、家人、上班地點、活動消費方式還有可能你的前科或小三的資料等，而**駭客現在的APT就使用各種方式蒐集你的資料，擺脫以往隨機找對象攻擊，現在是特定性，而最明顯特徵就是先從你的電子郵件下手！**

刑事警察局

直接入侵電子郵件，假冒發信騙取匯款

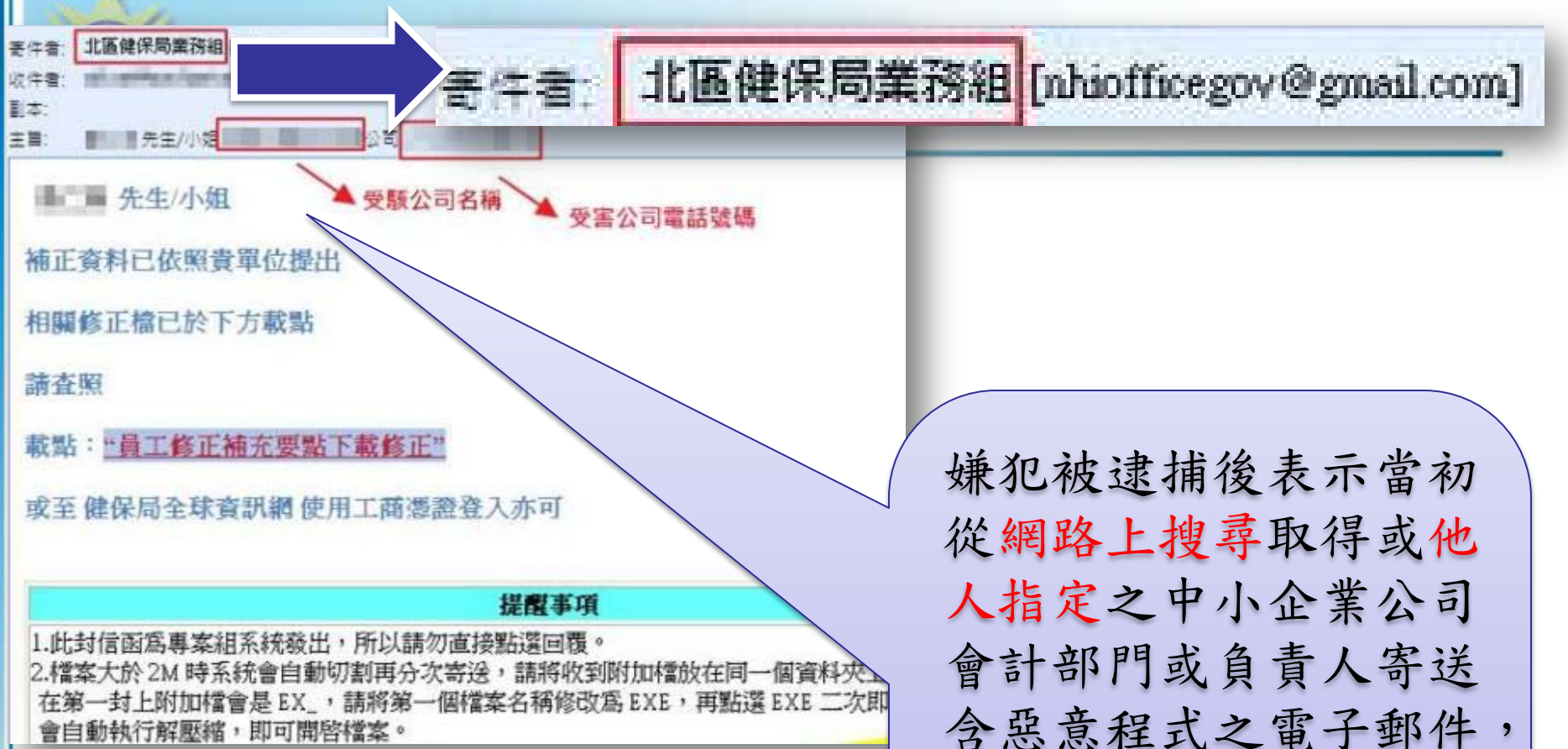
駭客手法 騙取客戶匯款

郵件伺服器遭目標攻擊



客戶接收駭客通知匯款被騙

業務郵件 遭鎖定竄改



嫌犯被逮捕後表示當初從網路上搜尋取得或他人指定之中小企業公司會計部門或負責人寄送含惡意程式之電子郵件，由於電子郵件主動出現對方姓名，多半不疑有他點選惡意程式並注入後門程式成功!

Gmail有駭客？刑事局籲提防

2015-04-11 19:10:02 聯合報 記者陳金松／即時報導

刑事局接獲檢舉，發現有民眾Google電子郵件（Gmail）疑似接獲假冒官方的駭客發送釣魚信件，試稱網獲駭客入侵，再提供假的連結誘騙民眾「重設密碼」；警方說，目前還沒有民眾被騙受害案例，但呼籲民眾提防。

假的?

真的?

單純從電子郵件內容真的無法辨識真假!!!!!!!

電子郵件最下方可以看得到每次登入的IP及目前有多少人登入，記得每天都看一下，比較保險!

三、預防勝於治療

企業安全建議作法

(一)加強公司所有個人電腦掃毒，使用合法授權之防毒軟體，以減少木馬或後門程式植入機會。

(二)使用免費之電子郵件信箱請注意帳號密碼安全，定期更新密碼。

(三)電子郵件屬低安全性之資訊交換格式，易遭篡改冒用，對於交易廠商突然變更收款帳戶，受款地或變更出貨地時，務必以電話、傳真或其他方式確認交易無誤。

(四)以電子郵件進行交易，應使用電子憑證以加強驗證。

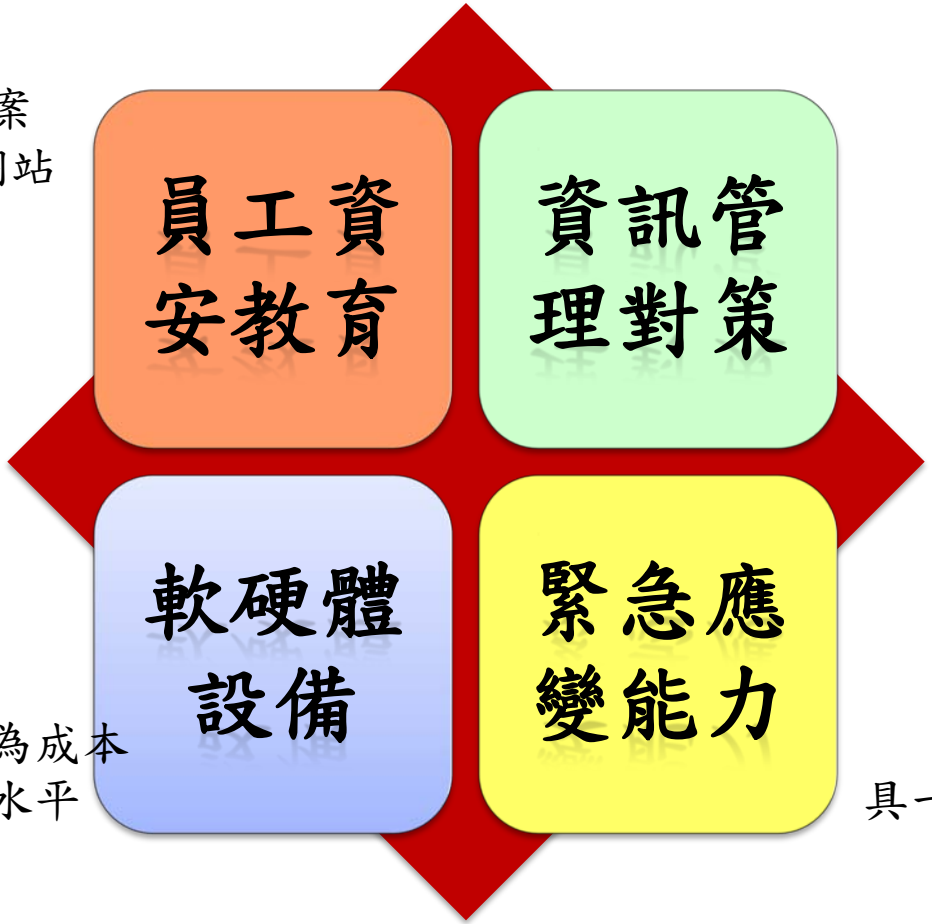
(五)電子郵件傳送訂單或出貨單等附件，請加密處理，防止資料遭到篡改、偽冒。

(六)強化公司內部資安管理，以減少駭客入侵機會。

(七)公司應將管理權限區分，落實帳號密碼管制。

ICT來臨的時代，不應全部仰賴設備

不亂下載檔案
不連結怪異網站



管理權限區分
落實帳號管制

應將資訊安全列為成本
具一定的資安水平

瞭解問題所在
具一定LOG分析能力

四、結語

網路新時代來臨與資訊大爆炸，企業應落實各項資安佈建與人才培育，不然所產生的詐騙犯罪造成的商譽損害將難以估計，未來誰能優先完成安全管理，就能獨佔鰲頭。