

高雄市政府警察局林園分局
104年預防犯罪宣導專題演講

網路駭客詐欺案件解析

電子郵件詐騙

模式與預防

報告人：林園分局偵查隊
偵查佐 羅莉吟



104年10月7日
於大發工業區服務中心



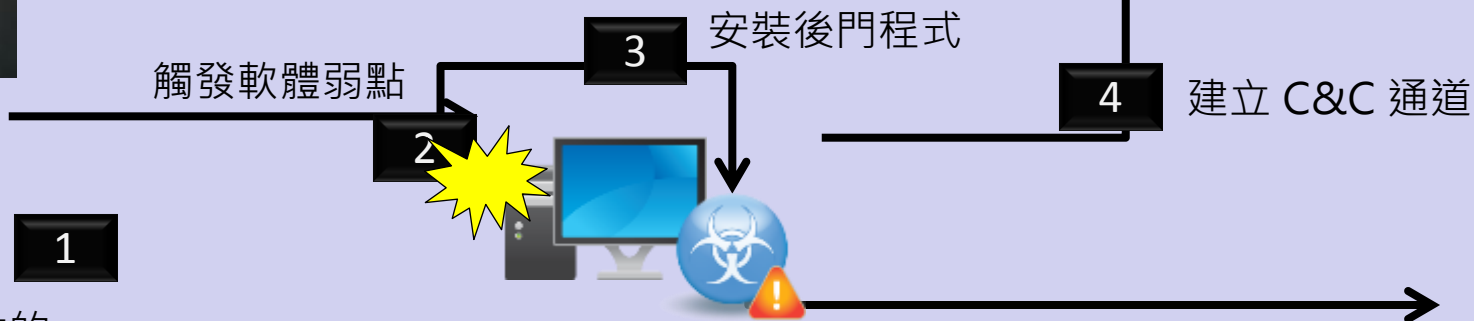
電子郵件安全問題成為近期詐騙新問題

- 統計2014年迄2015年3月底止受理竊改電子商務郵件詐騙匯款案件，被害**118**件，財損金額計新臺幣**2億8320**萬餘元。
- 統計偽冒電子郵件來源以**義大利、英國、印尼、馬來西亞、美國、波蘭、菲律賓、香港及泰國**等9國為主，受害年齡層分布於**25-65歲**，並以**30-59歲**居多(占**84.78%**)，且受害對象均係企業主或傳統經營鞋、服飾外貿公司。

太過相信電子郵件沒有先行查證

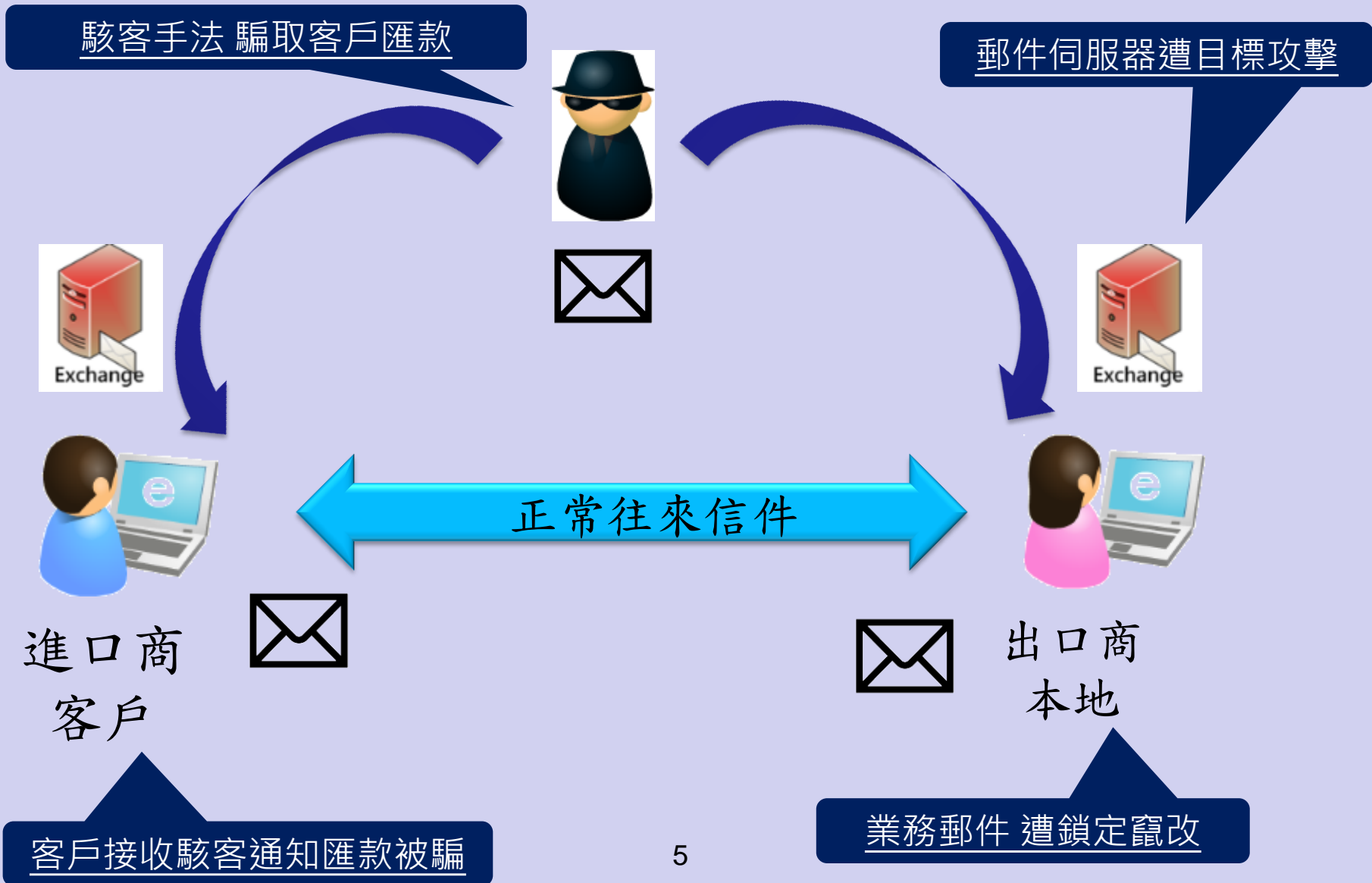
詐騙日期	詐騙內容摘要	縣市
104/01/09	B實業股份有限公司以e-mail方式向A企業訂購塑膠廢料一批，駭客冒充A企業要B實業股份有限公司將一半的貨款匯至國外WELL FARGO BANK銀行，之後又再來信告知匯款帳號有錯，被害人再匯款一次， 經向A企業取得聯繫後證實 ，才發現遭到詐騙。	高雄市
104/01/19	XX科技有限公司向外國廠商購買儀器，並於與該廠商用email聯絡期間遭犯嫌以與廠商相似之email詐欺， 被害人不疑有他 便以公司帳戶電匯歐元36879.05元(折合新台幣1,349,773元)給該犯嫌帳戶。	新北市
104/01/27	遭不明人士冒用其合作廠商B之假電子郵件(reXXXX@hotmail.com)向被害公司告知匯款之帳號需要變更，要求匯至美國舊金山(GARY WILLS之帳號)及波瀾之帳戶， 由於被害人無法確認駭客電子郵件真假不疑有他 ，於27日15時30分許將款項6926.24歐元，折合新台幣244,150元，匯給該不明人士。	新北市
104/02/09	被害人稱接收到假冒國外廠商e-mail，造成錯誤，前去玉山銀行林口分行臨櫃匯款至國外帳戶帳號PL391XXXX，共匯了美金290317.5元，折合約台幣9百多萬，不到1千萬元， 事後公司向國外廠商查證後 ，才發現遭人詐騙。	新北市
104/03/02	被害公司向阿曼ModernXXX採購版材，一開始匯了頭期款項美金15142.45元，後來有人假冒阿曼ModernXXX 電子郵件 ，表示因某些原因希望由被害有限公司先匯錢給對方，因此共匯了美金14085.72元， 最後聯繫上才發覺對方是假冒阿曼ModernXXXX ，因而受騙。	臺中市
104/03/16	報案人表示由於本身從事跨國貿易， 電子信箱疑似遭駭客入侵造成匯款帳戶有誤 ，信以為真，照指示辦理匯款至錯誤帳戶。	彰化縣

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



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！

直接入侵電子郵件，假冒發信騙取匯款



釣魚郵件與奈及利亞詐騙集團有關

The image shows a computer screen with two windows. The left window is an email client displaying an email with a subject line "Re: FW: FW: RE: RE: RE: Payment advice...PLEASE STOP PAYMENT FOR NOW UNTIL I GET BACK TO YOU". The email body contains text in Chinese and English, including "Thank you for the email but this is not for your Company high amounts for now due to yearly limit." and "Meanwhile, I have been in contact with your company col...". A red circle highlights the subject line and the sender information "Britta (ST-CO/RBU4-PUE)".

The right window is a web browser displaying the IP address lookup page for "41.71.173.170" on the website "MYIP.MS". The page shows details for the IP address, including the country "Nigeria", state "Lagos", and city "Lagos". A blue arrow points from the IP address "89.187.142.208" in the email header to the IP address "41.71.173.170" in the browser window.

Below the browser window, the text "奈及利亞" (Nigeria) is written in Chinese characters. At the bottom of the browser window, there is a red bar with the text "Summary on this IP Address - 41.71.173.170".

從郵件伺服器主機LOG可以發現很多 異常登入者IP，疑似遭到入侵

檔名	IP	國別	公司
[PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE YOU JI.eml	157.55.	United States	Microsoft
[PSPAM] Re Re SEHO-PROFORMA INVOICE.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] YOUJI YV-1600 +C.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] YOUJI YV-1600 +C[1]	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] YOUJI YV-1600 +C.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE YOU JI.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] YOUJI YV-1600 +C.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE [PSPAM] RE RE RE SEHO- YOU JI YV-1600ATC+C.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE [PSPAM] RE YOU JI.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE RE RE SEHO- YOU JI YV-1600ATC+C.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] RE RE SEHO- YOU JI YV-1600ATC+C.eml	157.55.	United States	Microsoft
[PSPAM] RE [PSPAM] YOUJI YV-1600 +C.eml	157.55.	United States	Microsoft
[PSPAM] RE RE RE RE SEHO- YOU JI YV-1600ATC+C.eml	157.55.	United States	Microsoft
[PSPAM] Re Re Re SEHO- YOU JI YV-1600ATC+C.eml	157.55.	United States	Microsoft
[PSPAM] RE SEHO- YOU JI YV-1600ATC+C.eml	157.55.	United States	Microsoft
[PSPAM] RE SEHO- YOU JI YV-1600ATC+C_Video 1.eml	157.55.	United States	Microsoft
[PSPAM] RE YOU JI.eml	157.55.	United States	Microsoft
COPY OF THE CABLE.eml	157.55.	United States	Microsoft
RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE YOU JI.eml	157.55.	United States	Microsoft
RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE YOU JI[1].eml	157.55.	United States	Microsoft
RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE YOU JI[2].eml	157.55.2.72	United States	Microsoft
RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE [PSPAM] RE YOU JI.eml	157.55.2.71	United States	Microsoft

發生駭客入侵後4W1H作法

When何時發生

Where哪裡出現問題

How如何發生的

What哪些可以佐證

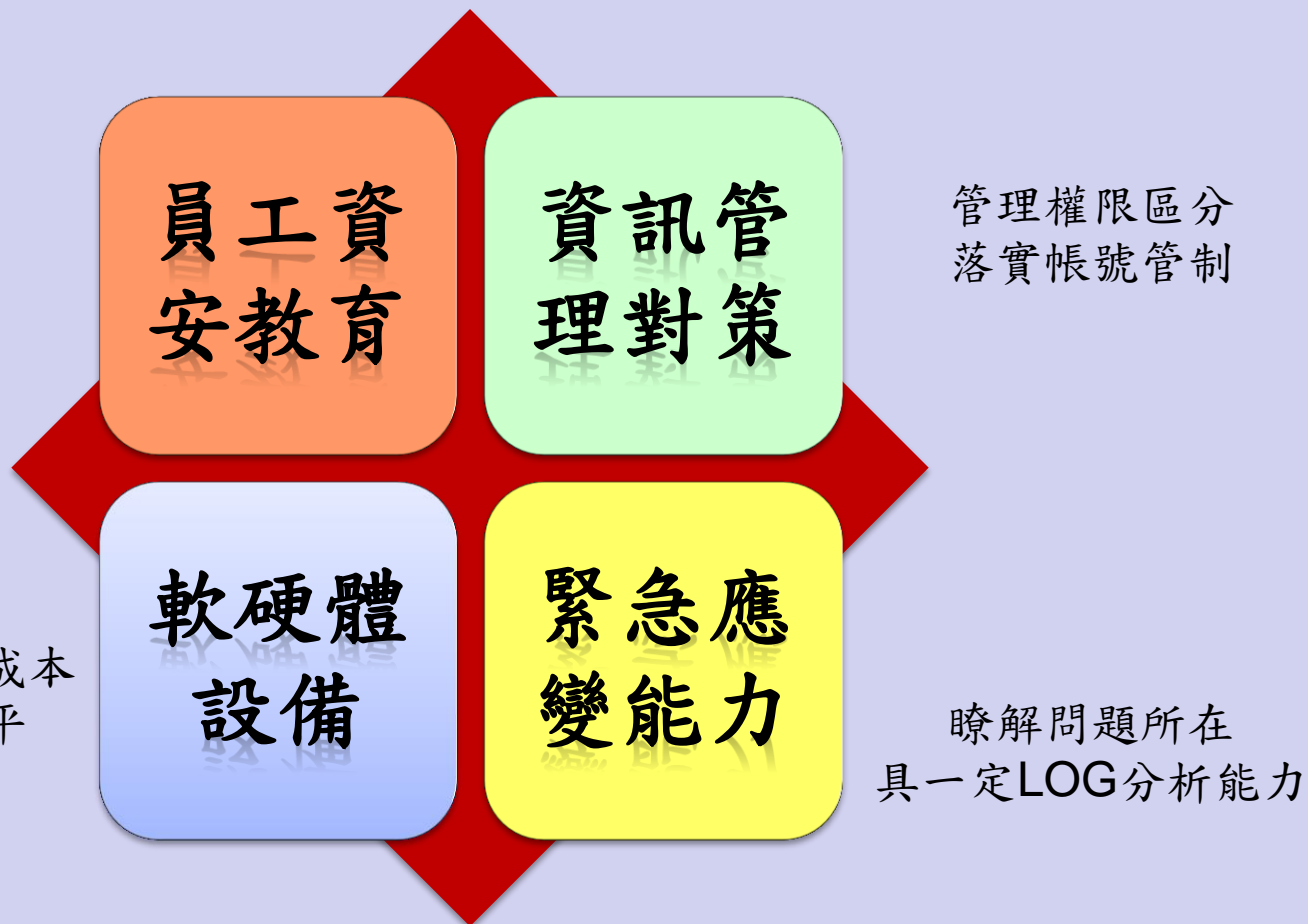
Who找誰可以追查來源

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。

ICT來臨的時代，不應全部仰賴設備



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。

感謝聆聽

如有任何問題，

歡迎撥打本隊專線07-6412704
或所轄大發駐在所07-7884000

林園分局關心你

