

[首頁](#) / [資安宣導](#) / [資訊安全宣導](#)

注意E-Mail位址！台北市政府警察局提醒小心遭到商業電子郵件詐騙

發布日期：2019-11-14

字型大小：[小](#) [中](#) [大](#)

發布單位:TWCERT/CC

更新日期:2021-03-12

點閱次數:2447



由於國內的企業，經常習慣使用電子郵件與客戶聯繫，而歹徒可能在駭入公司系統後長期潛伏，並且觀察企業與合作單位之郵件的往來，或進行網路監聽，搜集並分析該公司的相關交易

資訊，並且藉由極為相似之電子郵件傳送給該公司進行詐騙。

案例：

臺中市某鞋品貿易公司遭詐騙集團鎖定，掌握林姓業務與國外合作公司(下稱A公司)有一筆應付款項，仿照A公司業務的電子郵件帳號「xxxxxdaixx@163.com」，設立名稱相似的

「xxxxxdeaixx@163.com」假帳號發信給該名林姓業務，謊稱原帳戶因稅務問題進行整併中，要求變更匯款帳戶至瑞典北歐斯安銀行之境外帳戶，林姓業務所屬公司因與A公司長期合作，遂不疑有他，直接以傳真銀行方式匯出臺幣數十萬元。孰料5天後，A公司通知並未收到匯款，林姓業務連忙找出當初聯繫之電子郵件內容，發現假帳號竟多了1個e字母，「e」字之差使公司損失達數十萬元。

類詐騙手法略述如下：

(一) 詐騙集團攔截被害人公司交易信件，並申請與企業客戶電子郵件地址相似度極高的假郵件使之混淆（如前揭案例僅多一個字母「e」，歹徒所設立「xxxxxdeaixx@163.com」電子郵件與原本使用「xxxxxdaixx@163.com」極為相似）。

(二) 模仿原本往來郵件的語氣發信給被駭企業之客戶，騙取企業或客戶變更匯款帳戶，藉機詐騙被害人將貨款匯至詐騙集團所預設帳戶。

(三) 取得企業客戶的信任而匯款，俟原受款客戶反映未收到貨款時，方知受騙。

因此，請使用者務必提高警覺，面對商業上的信件，務必細心觀察及多方檢視，以免遭到詐騙！