竄改商務電子郵件詐騙案例

臺中市某鞋品貿易公司日前遭詐騙集團鎖定，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」字之差使公司損失數十萬元，令他後悔不已。

由於電子郵件便利及低成本之特點，廣受企業界的喜愛，但若作為企業內外的溝通渠道，有關資料安全、詐騙及駭客防範措施，就成為企業管理的重大挑戰。詐騙集團看準一般商務公司慣用電子郵件進行聯繫，透過攔截信件往來內容，模仿原本往來郵件的語氣發信給被駭企業之客戶，謊稱因特殊狀況需要更改匯款銀行帳號，甚至附上高層主管親筆簽名的授權書取信於人，並以極為類似的假電子郵件帳號進行混淆。甚至，部分歹徒是資安高手，透過破解密碼直接駭入公司的電子郵件系統，透過真正的郵件帳號發信要求變更受款帳號，若匯款者疏於再次確認，十分容易落入歹徒陷阱，等到真正的請款者催繳

貨款，才驚覺遭詐，但已為時已晚。

刑事警察局提醒，電子郵件使用上雖然便利但安全堪慮，易遭攔截冒用，若交易方突然要求更改匯款帳戶及帳號資料，務必循原有連絡方式與其再次確認。使用合法授權之防毒軟體，有效降低歹徒侵入盜取個資詐騙的機會。定期更新密碼，最好每個應用程式都設定不同的密碼，以免歹徒駭到一組密碼後，就能無限暢遊各私人網域。傳送重要文件，凡事加密，避免資料外洩。最後，公司內部應落實資安管理，研擬防杜駭客入侵措施，以免成為詐騙集團眼中的肥羊。