商業電郵詐騙

商業電郵詐騙

偽冒電郵是騙徒常用的詐騙手法之一。

當付款到期時，騙徒可能發送一封看似由供應商發出的電郵，內容模仿真實訊息的格式與語氣。他們會聲稱您的付款銀行資料已更新，並提供新的賬戶資料，要求您按指示付款。

這類電郵往往難以辨識：

- 騙徒常會使用供應商的真實電郵地址，或偽裝成極為相似的地址。
- 他們會製作看似真確的發票。
- 供應商員工的電郵簽名亦可能毫無異樣。
- 訊息內容往往帶有急切語氣，例如聲稱與敏感交易有關，需即時匯款。
- 騙徒可能已掌握整段電郵往來紀錄，並能以相似語氣及措辭回覆。
- 最重要的是——所要求的付款往往確實到期。
- **唯一的分別可能只是銀行賬戶資料已被更改。**

電郵入侵如何發生？

電郵賬戶盜用

- 騙徒使用駭客技術或已竊取的賬戶資料，入侵企業的電郵賬戶。
- 電郵賬戶詳細資訊可能是因網路釣魚或資料外洩，而被騙徒獲取。
- 不法份子可能會蒐集有關使用者的聯絡人資料、郵件撰寫風格和個人資料，使他們的所杜撰的訊息看起來更可信。

偽冒電郵

- 不法份子開立一個與真實電郵地址非常相似的賬戶。
- 或者他們可能利用偽冒的電郵格式和標題，企圖令收件人不容易察覺，並將其當作為真實的郵件來回覆

冒充高層主管詐騙

不法份子假冒公司的高層人員

- 他們通常向財務部門發送電郵，要求緊急匯出一筆大額款項，原因可能是用於收購項目或其他重要交易。
- 被冒充的高層主管往往正值休假或不在辦公室，令相關細節難以即時核實。
- 騙徒可能透過網絡釣魚攻擊或資料外洩入侵電郵賬戶，並從公司網站或社交媒體收集資訊，以增加訊息的可信度。