網路安全宣導

商業電子郵件詐騙

別成為下一個受害者

企業主正成為網路犯罪中最脆弱的受害者與攻擊目標。

30億美元

2025年商業電子郵件詐騙損失
資料來源：美國聯邦調查局（FBI）

什麼是商業電子郵件詐騙？ 商業電子郵件詐騙（BEC）是一種詐騙手法，網路犯罪者透過**冒用他人電子郵件身分**，誘使企業匯款或提供敏感資訊。

警訊：BEC 辨識指標

相似網域
網域經過細微修改，例如加上連字號或替換字元（例如以數字 1 取代小寫「l」）。

可疑的付款要求
留意未經正式通知就出現的新銀行資訊或陌生帳號，例如「我們換銀行了」或「請匯到這個新帳戶」。

偽造的電子郵件往來
對話串劫持會利用既有的信任與脈絡：攻擊者入侵帳號後，先觀察進行中的對話，再於符合正常業務活動的時機插入訊息。

語氣或用詞異常
寫作風格、文法或措辭與寄件者平時的溝通方式不符。

時間點可疑
交易在接近下班時間，或週末、假日前夕發起。

簽名檔錯誤
冒充的寄件者，其簽名檔不正確或被簡化。

保護您的公司

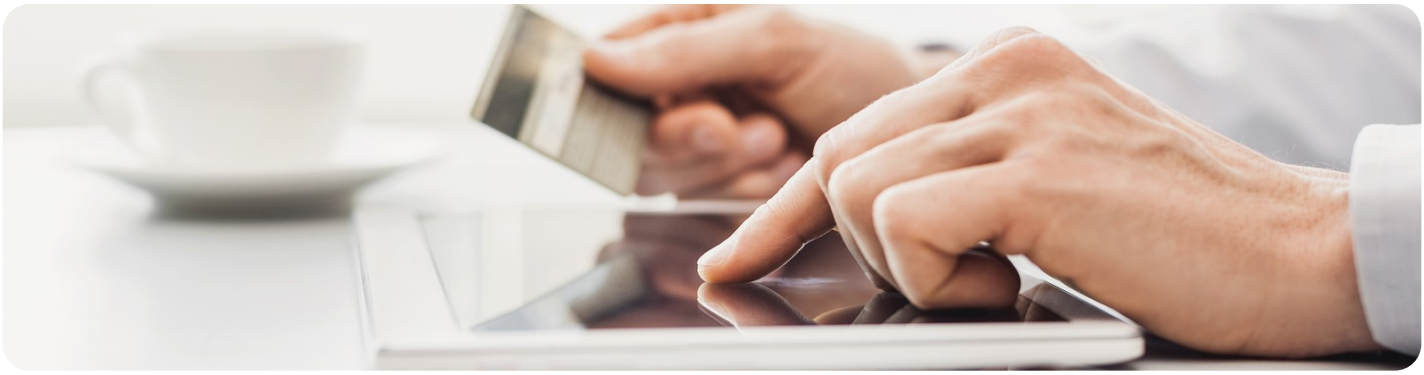
以其他管道驗證
務必透過可信的管道核實付款指示，例如撥打檔案中已知的電話號碼，而非電子郵件中提供的號碼。

要求雙重核准
電匯、ACH 發動及付款指示變更，至少須由兩人核准。完善的內部控制有助於防止詐欺交易。

仔細檢查電子郵件地址
留意寄件者地址是否有細微拼字錯誤、多餘字元或被竄改的網域。詐騙者經常使用偽造或相似的電子郵件帳號。

定期訓練員工
持續提供詐欺防範教育，讓員工能識別網路釣魚、偽造電子郵件與社交工程手法。

考慮投保網路保險
請洽詢您的保險業務員，了解網路保險是否能協助承擔詐欺及其他網路事件所造成的損失。



First General Bank
大 通 銀 行