這是公司內部社交工程測試郵件，如果您已經看到本檔案內容，代表您可能缺乏足夠的資安意識，請您參考下列資訊

採取的關鍵步驟可以分為三個階段：立即行動、理解攻擊手法、以及未來預防。

## 一、 立即行動與應變

如果員工懷疑自己已經落入了社交工程的陷阱（例如，點擊了惡意連結、輸入了密碼、或下載了附件），應立即執行以下步驟：

### 1. 立即向 IT 部門報告：

1. 這是最重要的一步。放下手邊所有工作，立即透過電話或公司指定的安全管道通知 IT 或資安團隊。資安事件需要快速反應。

2. 誠實告知所有細節：點擊了什麼、輸入了什麼資訊、以及是否有下載任何檔案。資訊越完整，IT 團隊就能越快進行損害評估與處理。

### 2. 更改密碼：

1. 如果曾在釣魚網站輸入密碼，請立即變更該帳號（及任何使用相同密碼的帳號）的密碼。

2. 確保新密碼是強度高且獨一無二的。

### 3. 隔離或關閉受影響的設備：

1. 如果懷疑電腦中毒（例如電腦運行緩慢、出現不尋常的彈出視窗），請中斷網路連線（拔掉網路線或關閉 Wi-Fi），以防止惡意軟體在公司內部網路擴散。

## 二、 理解攻擊手法與安全意識提升

發生事件後，應協助員工理解他們是如何被利用的，這是建立長期安全意識的基礎。

### 1. 學習識別「誘餌」和「緊迫性」：

1. 社交工程攻擊者擅長利用人類的情緒。提醒員工注意那些要求「立即行動」、「獎金發放」、「帳號即將停用」等具有強烈情感驅動的詞語。

2. 學會質疑：為什麼這封重要的郵件會用這種不尋常的方式發送？

2. **訓練「暫停、思考、查證」的習慣：**

1. 鼓勵員工收到可疑郵件時，先「暫停」手邊動作，仔 it「思考」這封郵件的合理性，最後透過官方管道「查證」。

2. **查證方式：** 不要回覆可疑郵件本身。應該另外開啟一個新的訊息或致電 HR/IT 部門，透過已知的、受信任的聯絡方式來確認資訊真偽。

3. **學會檢查寄件者與連結：**

1. 指導員工如何詳細檢查寄件人的電子郵件地址（而不僅是顯示名稱）。

2. 教導他們在點擊連結前，將滑鼠游標停留在連結上方，查看實際的目標網址是否指向預期的公司官方網站。