資安月報八月號

釣魚攻擊 - 別讓騙子得逞！

康聯生醫
Healthconn

什麼是釣魚攻擊？

利用電子郵件、訊息或假網站來**誘騙使用者提供敏感信息**（如帳號密碼、信用卡資料）的攻擊方式。

通常**偽裝成看似可信的來源**，
如銀行、電商平台、或是公司內部的郵件，
以達到欺騙的目的。

常見的釣魚攻擊類型

- **電子郵件：**
  - 看似來自可信來源的郵件，誘導你點擊惡意連結或下載附加檔案
  - 例如：來自老闆的關懷信
- **仿冒網站：**
  - 這些網站通常看起來與真實網站一模一樣
  - 為了竊取你的登入憑證或支付信息而設計的
- **社交工程：**
  - 利用社交網絡或即時通訊工具，冒充你的朋友或同事
  - 索取個人資料或公司機密

如何辨識電子郵件釣魚攻擊？（一）

➢ 檢查寄件者的電子郵件地址：

- 許多釣魚郵件的寄件者地址看似來自可信賴的來源，但細看會發現差異，例如**錯別字或多一個字母**。
- 公司內部信件**請認明信箱**後面一定是 healthconn.com / coning-biotech.com

➢ 語法錯誤或不自然的語言：

- 釣魚郵件經常包含語法錯誤或不自然的語句
- 攻擊者使用了翻譯工具或不是母語使用者

康聯生醫 Healthconn

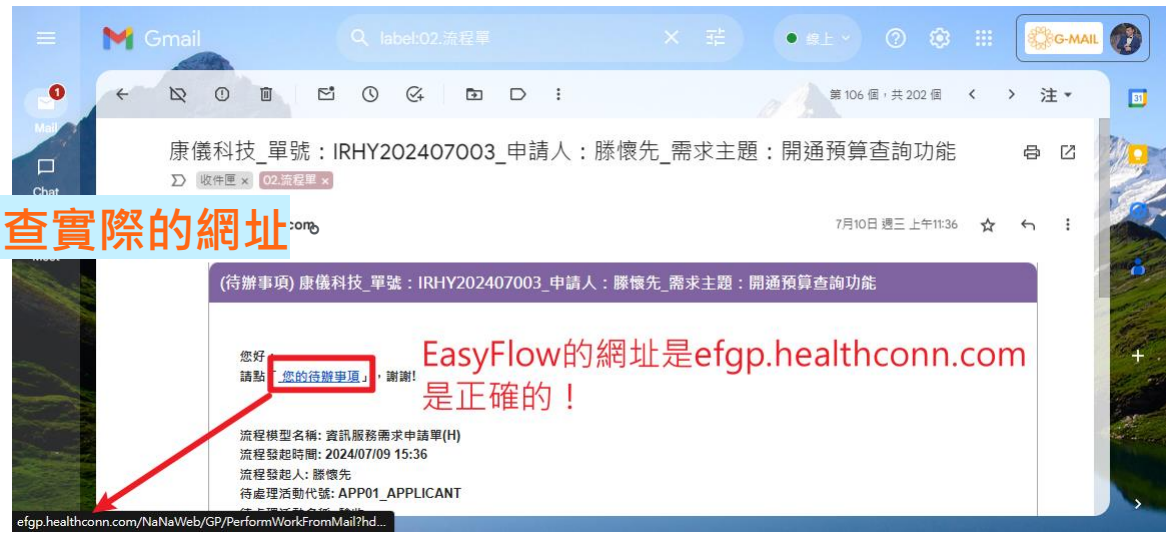
如何辨識電子郵件釣魚攻擊？（二）

➢ 不尋常的要求：

- 郵件要求你**提供密碼、個人資料或點擊連結以解決帳號問題**，往往是釣魚攻擊的徵兆。
- 可信的機構通常不會在未經確認的情況下要求這些信息。

➢ 檢查連結的真實性：

- 點擊信件連結之前，**將滑鼠懸停在連結上，檢查實際的網址**
- 如果網址與聲稱的網站不一致，請勿點擊。



康聯生醫 Healthconn

釣魚手法 - 仿冒網站

假裝是「大型企業」、「銀行」名義，發送簡訊給民眾，並附上網址。

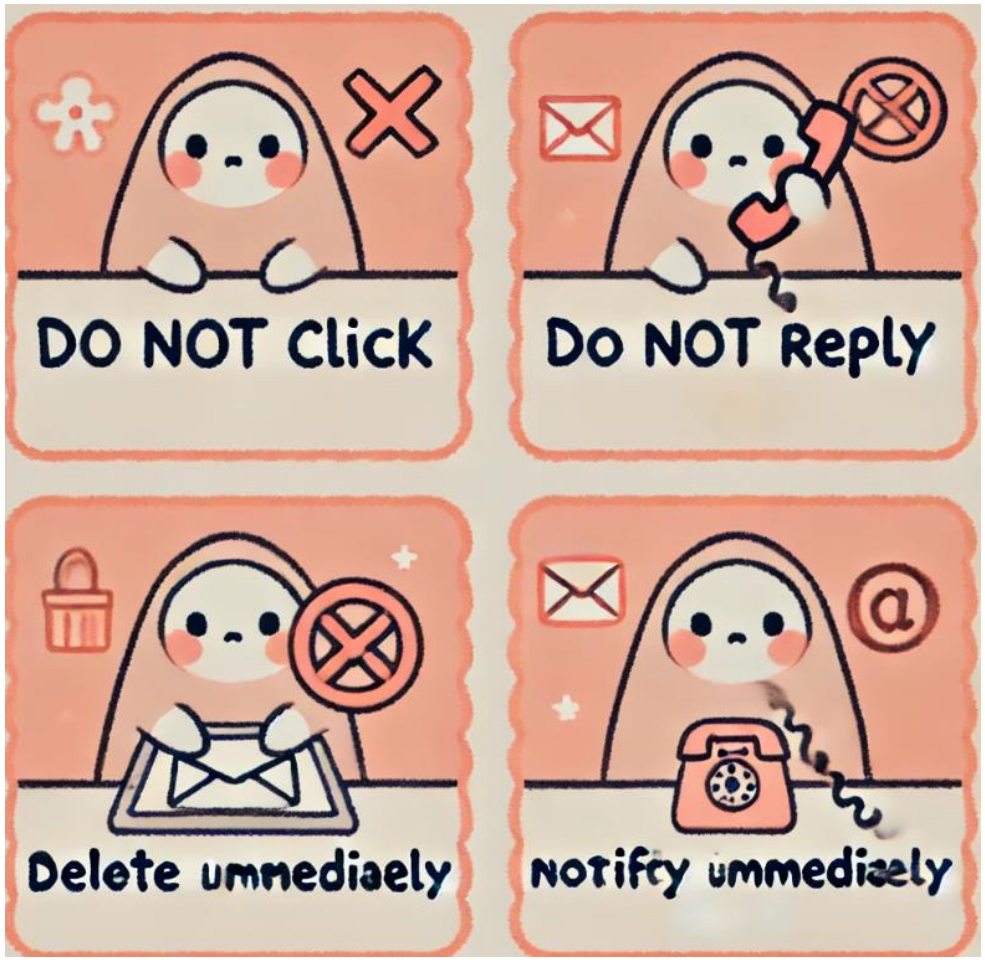
- 受害者一旦點進網址填寫信用卡資料
  1. 嫌犯趁機綁定其他支付工具（如：Apple Pay 、 Google Pay ）
  2. 騙客戶取得OTP驗證碼，進而盜刷

2023.09 金管會要求銀行若要取得客戶資訊，不能以簡訊方式傳送。

- 資料來源：https://money.udn.com/money/story/5613/7450766

收到釣魚信件怎麼辦？

收到疑似釣魚信件怎麼辦？



一. 不點擊

- **不要點擊**郵件中的任何連結、圖片或附件。

二. 不回覆

- **不要回覆**郵件，尤其是不要提供任何敏感資料。

三. 立即通知

- **通知ＩＴ**，並將可疑郵件標記為垃圾郵件。
- 不確定是否為釣魚信，可以通知ＩＴ一起確認。

康聯生醫 Healthconn

保護自己免受釣魚攻擊的最佳實踐

一. 保持警惕：

✓ 對於任何要求提供個人或公司資料的郵件或訊息都保持懷疑態度。

二. 定期更新密碼（參考資安月報2027.6月號）：

✓ 使用強密碼並定期更換，避免使用同一組密碼登入多個帳號。

三. 啟用兩步驟驗證（2FA、參考資安月報2024.7月號）：

✓ 即使攻擊者獲得了你的密碼，雙因素驗證仍能提供額外的保護。

四. 參加資安培訓：

✓ 不斷提升自身對釣魚攻擊的辨識能力，並了解最新的攻擊手法。

康聯生醫 Healthconn

謝謝

資料來源：ChatGPT、經濟日報

圖片：ChatGPT

本期撰稿人：Paul

康聯生醫
Healthconn