

資安事件宣導

釣魚郵件 (Phishing email)

釣魚郵件實際案例

- 近期本校許多師生收到要求續訂電子郵件的通知信，這是典型的釣魚郵件的詐騙手法，切勿相信！

親愛的國正成大學帳戶使用者，

我們注意到您的國立中正大學電子郵件帳戶已幾乎超過其限制。從現在起，您可能無法發送或 接收消息。

按一下下面的連結續訂您的帳戶； 表面上看起來是本校網域

<https://webmail.ccu.edu.tw/cgi-bin/owmmdir2/openwebmail.pl>

無法續訂電子郵件帳戶。它將被永久禁用。

<http://www.123formbuilder.com/form-5354037/ccu-edu>

=====

不要將您的密碼或個人資訊發送給任何人

=====

感謝您的理解。

國家中成大學系統技術支援小組

版權所有 (C) 2020國中成大學保留擁有權利。

滑鼠指向連結網址，出現真正的連結點不一致

- 經追查發現，點擊信中的連結並填寫了帳密之後，使用者收到的信件以及所回的信件，均會被傳送到駭客設定的信箱。

什麼是釣魚郵件

- 駭客以假冒的身分（例如：中正大學、資訊管理者、銀行、電商平台、...）發送信件給使用者，製造急迫或利多的情境，致使使用者在威脅或利誘下疏於求證而提供個人的帳號密碼等資料，例如：
 - ✓ 您的郵件帳戶已超過限制，您可能無法接收消息，請點選下面連結以續訂帳戶 <http://.....>
 - ✓ 感謝您對XX的支持，為了提供更好的服務品質，請點選這裡，將可加大信箱空間。
 - ✓ 交易已完成，請點開附檔以確認發票是否正確。

釣魚郵件常見手法

- 誘騙使用者回信提供帳密或個人資料。
- 誘騙使用者點選連結，收集使用者的帳密及個資。
- 誘騙使用者點選連結，藉以植入惡意程式。
- 以系統更新為由，誘使使用者執行附加檔案，藉以植入惡意程式。

釣魚郵件的危害

- 竊取個資、帳密及信用卡卡號等資料。
- 綁定此 email 帳號的社群網站、拍賣網站... 等，也可能被用來進行詐騙。
- 通訊內容被窺探，其中可能包含個人及學校的機密或敏感資料。
- 點擊惡意連結或附加檔案，可能致使電腦被入侵或植入後門程式。

如何防範釣魚郵件

- 千萬別在信中回復個人敏感資料(身份證字號、出生年月日、密碼...)。
- 信中威脅將帳號停用，請勿驚慌先判斷真偽。
- 若非認識或正在等待的郵件，切勿點開附檔或圖片。
- 如無法確認郵件中的連結是否正常，請不要點擊。
- 定期清理郵件，避免保留過多信件而超過個人允許的容量。

資料參考來源

- [回顧 2018 您不可不知的 Top 5 電子郵件詐騙手法！](#)
- [釣魚/詐騙信件手法解析](#)
- [網路釣魚（維基百科）](#)
- [如何辨別釣魚郵件](#)