

啥！帳號將被停用，真的嗎？…… 如何辨別釣魚郵件？

何謂「釣魚郵件」？


最近又有不少假冒資訊中心名義散發的系統通知郵件，主旨類似：「Attention: E-mail User」、「Confirm email」或「更新您的帳戶」等，意圖誘騙收件者提供帳號密碼、點選郵件所附的連結或執行附加檔案等。

此即所謂之「釣魚郵件」，利用假冒的身分，製造虛假急迫的情境，使人疏於求證而提供個人的帳號、密碼或卡號等機敏資料。常見的手法有：

- (1) 誘騙收件者回信提供機敏資料。
- (2) 誘騙收件者點選偽造的連結，藉以植入惡意程式或導向惡意的網站騙取資料。
- (3) 以系統更新名義誘騙收件者執行附加檔案，藉以植入惡意程式。

如何辨別釣魚郵件？

那麼，該如何辨別釣魚郵件呢？以下是釣魚郵件的範例：

日期: Wed, 16 Mar 2016 12:25:44 +0800  完全表頭

寄件者: "Ntnu.edu.tw" <a.esmaeili@alumni.ut.ac.ir> 非本校電郵地址

收件者: undisclosed-recipients::; 收件者不是我

主旨: Ntnu.edu.tw 使用者 詳列附件

Ntnu.edu.tw 使用者，

郵件內容語句不通順，看似翻譯而得

您已超出郵箱由 WEB 服務/管理員，設置 10 GB 存儲空間的限制，你將在發送和接收郵件直到你重新驗證您的郵箱有問題。您必須更新通過點擊下面的連結或複製粘貼連結到您的瀏覽器並填寫資料，以驗證您的郵箱。

要升級您的郵箱複製粘貼到您的瀏覽器的連結：[HTTP://formcrafts.com/a/18417](http://formcrafts.com/a/18417)

連結非本校網址

真誠，

[System Administrator Ntnu.edu.tw User®](#) 沒有本中心之署名

(C) 版權所有 2016

釣魚郵件範例（一）

From: 國立臺灣師範大學 [mailto:terpaul747@mail.ypu.edu.tw] 寄件人非本校之電子郵件地址
Sent: Thursday, October 29, 2015 10:13 AM
To: helpdesk@ntnu.edu.tw
Subject: 驗證您的信息 [helpdesk@ntnu.edu.tw]
Importance: High

你好 helpdesk@ntnu.edu.tw

我們最近重新的消息傳遞服務，並訪問你的帳戶僅限於重新確認你的詳細信息，請通過下面的鏈接登錄：

按住 CTRL 鍵再按一下滑鼠以追蹤連結 <http://thesunsetavern.com/wp-conte...>

ntnu.edu.tw ← 看似本校網址，將滑鼠移到上面，卻出現非本校網址。

此致，
國立臺灣師範大學

釣魚郵件範例 (二)

From: **National Taiwan Normal University** <webmail@ntnu.edu.tw> 假冒寄件者
Date: Wed, Mar 16, 2016 at 2:48 AM
Subject: Confirm email
To: 沒有收件者

-- 內容全部是英文，沒有中文
This message was sent automatically by a program on Webmail which periodically checks the size of inboxes, where new messages are received. The program is run weekly to ensure no one's inbox grows too large. If your inbox becomes too large, you will be unable to receive new email. Just before this message was sent, you had 18 Megabytes (MB) or more of messages stored in your inbox on your Webmail To help us re-set your SPACE on our database prior to maintain your INBOX, you must reply to this e-mail and enter your:

userID: {.....}
and Password {.....}

要求提供帳號及密碼

You will continue to receive this warning message periodically, If your inbox size grows to 20 MB, then a program on Bates Webmail will move your oldest email to a folder in your home directory to ensure that you will continue to be able to receive in coming email. You will be notified by email that this has taken place. If your inbox grows to 25 MB, you will be unable to receive new email as it will be returned to the sender. After you read a message, it is best to REPLY and SAVE a copy.

Thank you for your cooperation
National Taiwan Normal University 沒有資訊中心署名

釣魚郵件範例 (三)

釣魚郵件有什麼特徵？

從以上範例，我們可以歸納出一些釣魚郵件之特徵：

1. 寄件者非本校<user>@ntnu.edu.tw 電郵地址：

本中心所寄發之通知郵件，寄件者一定會用本校之電郵地址。若寄件者非本校<user>@ntnu.edu.tw 電郵地址，即可確定該郵件非本中心所寄發。

2. 沒有收件者或收件者不是您：

本中心寄發給您之通知郵件，您的電郵地址一定會在收件者列表中。不會有收件者不是您或沒有收件者之情況。

3. 要求您邀提供帳號及密碼，並要您限時處理，否則帳號將會被停用：

本中心不會以電子郵件方式要求用戶提供帳號及密碼等資料。收到要求提供帳號及密碼之郵件，鐵定是惡意

釣魚郵件。

4. 要求您點擊非本校 ntnu.edu.tw 網址之連結：

本中心寄發之通知郵件，若有連結，通常是含有 ntnu.edu.tw 之服務網址。若收到本中心之通知郵件，卻要求您點擊非本校 ntnu.edu.tw 網址之連結，應是釣魚郵件。但請留意：有些釣魚郵件的連結雖顯示為 ntnu.edu.tw 的網址，但實際上卻不是，需將滑鼠移到連結上面（僅須移動滑鼠，切勿點擊）方可確認。

5. 語句不通順，看似由其他語言翻譯而得：

本中心所寄發之通知郵件，語句應尚屬通順。那些語句明顯不通順之中文郵件，通常是國外駭客以網路翻譯工具翻譯而來的。

6. 全部英文，沒有中文

本中心所寄發之通知郵件，一定是中文或是中英對照的。若收到全部英文的通知郵件，肯定非本中心所寄發。

7. 沒有本中心之署名

本中心所寄發之通知郵件，一定會有本中心之中文或英文署名。

收到釣魚郵件應如何處置？

資訊中心不會以電子郵件方式要求郵件用戶提供帳號及密碼等資料，收到類似郵件，請直接刪除，不要回應或點選郵件上的連結。如有疑問，可將郵件轉寄至 sysadm@ntnu.edu.tw，亦可直接電洽本中心諮詢服務櫃台確認，電話為 (02)7734-3737。

電子郵件帳號密碼攸關個人權益及隱私，請妥善保護，勿隨意洩漏給他人。若不慎將帳號密碼外流，請速至本中心網路信箱變更密碼，網址為 <https://webmail.ntnu.edu.tw/wmail/chpw.php>。