張貼日期：2019/10/02

【資安漏洞預警】學術單位近日內陸續收到含有釣魚內容之資安通知信件，煩請各單位提高警覺

主旨：學術單位近日內陸續收到含有釣魚內容之資安通知信件，煩請各單位提高警覺

說明：

- 內容說明
  - 學術單位近日內陸續收到含有釣魚內容之資安通知信件，煩請各單位提高警覺。
  - 信件內容以舊有資安相關訊息為主，信件內容開頭以英文撰寫訊息，且附有超連結以供下載檔案。
  - 煩請各單位依社交工程防範作為提高警覺且不輕易點選或開啟不明來源信件之附檔或超連結，以維資訊安全。
  - 如收到相關類似信件，切勿點選信件中超連結，並將信件提供給TACERT(service@cert.tanet.edu.tw)以利相關資訊收集及分析。
    1. 電子郵件內容範例1：
       Hello,

       We need this reviewed, categorized and filed as soon as possible. Take a look and let me know how soon can you finish it.

       ATTACHMENT DOCUMENT(超連結，內含惡意程式)

       Thank you

    2. 電子郵件內容範例2：
       Hello,

       I believe we completely missed our target on this one, I need you to double check by how much. I attached the file for review below.

       ATTACHMENT DOCUMENT(超連結，內含惡意程式)

       Thank you

- 影響平台: 電子郵件
- 建議措施:
  1. 確認寄件者資訊及信件內容是否正確
  2. 不輕易點選或開啟不明來源信件之附檔或超連結
  3. 依社交工程防範作為提高警覺

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20191002_01

Last update: **2019/10/02 16:41**