張貼日期：2022/05/05

教育部惡意電子郵件社交工程演練提醒

主旨：教育部惡意電子郵件社交工程演練提醒

說明：
教育部為增進轄下各機關人員對資通安全的重視，每年定期進行兩次電子郵件社交 工程演練，由於您有可能因為不小心或無意間點擊了測試信件，導致本校演練成績不理 想，故特發此信通知您有關電子郵件社交工程應注意的事項，藉以瞭解社交工程的定義、 攻擊手法、及如何防範，以期能順利通過演練，並確實提升您的資安意識，進而保護你 個人電腦的資訊安全。

1. 社交工程攻擊的定義：
    1. 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法。
    2. 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件、社交軟體或網頁來進行攻擊。
2. 透過電子郵件進行攻擊之常見手法：
    1. 假冒寄件者
    2. 使用與業務相關或令人感興趣的郵件內容
    3. 含有惡意程式的附件或連結
    4. 利用應用程式之弱點(包括零時差攻擊)
3. 防範電子郵件進行攻擊之辦法：
    1. 設定更新各種作業系統、以及應用軟體。
    2. 必須安裝防毒軟體及防火牆，並確實更新病毒碼。
    3. 改變收信軟體安全性設定，如：以純文字模式開啟郵件、取消預覽郵件功能。
    4. 防止垃圾郵件，如：設定過濾垃圾郵件機制。

以上僅大略介紹電子郵件社交工程應注意的地方，以及避免攻擊的方式，請您如再收到類似信件時，不要大意開啟信件或預覽，以避免個人電腦資料外洩或中毒，造成各位工作上困擾，更多資訊請參閱下列網址：

https://net.nthu.edu.tw/netsys/security:social_engineering

計算機與通訊中心
網路系統組 敬啟