張貼日期：2008/09/17

請注意防範電子郵件詐騙

主旨：請注意防範電子郵件詐騙

說明：
一、網際網路上詐騙的事件層出不窮，詐騙集團常假冒單位名義發出難辨真偽的電子郵件來騙取您的帳號密碼，再利用詐騙所取得的資料，進行以下用途：

· 假冒該帳號使用者身份，藉以進行新的社交工程型網路詐騙。例如：取得您的電子郵件聯絡人資料，寄信或打電話給他們來詐騙金錢或郵寄非法程式使其電腦中毒或植入木馬。

· 常有使用者為求方便使用一組相同的帳號密碼，詐騙集團可用來猜測獲取使用者其他系統的帳號密碼。

二、因詐騙手法日新月異，為避免上當受騙，僅提供一些電子郵件詐騙的注意事項供您參考：

1.任何要求提供帳號密碼、身份證字號或個人資訊的信件，極有可能是詐騙，一定要提高警覺。系統管理者一定不會透過電子郵件索取使用者的密碼。
2.回信地址非發信單位所擁有，極有可能是詐騙，例如：本校的郵件網域一定為□□□□nthu.edu.tw□結尾。
3.不要點選不明信件中的連結網址，最好自己輸入，以免被偽造的網址所欺騙。
4.郵件中的附件，若不確定，請不要執行，極有可能導致中毒或資料外洩。
5.電子郵件來源判斷不易，即使看到署名是親朋好友或學校給您的郵件，若含有上述特徵也極可能是詐騙郵件。
6.許多詐騙信往往利用假日或非上班時段來寄發，造成收件者不易向相關人員或單位求證。
7.如果已不小心將密碼寄出或懷疑密碼已遭他人取得，請盡速更改密碼。
8.若您判斷為詐騙信，不予理會即可；如仍有疑問，請直接打電話向相關人員或單位求證，電話號碼一定要自行查證，不要用信件所提供的電話號碼。
〈註：本中心服務電話為 31000 分機。〉

三、此外，若密碼太簡單〈如：12345678〉容易被不法人士猜中，為保障您使用網路安全，建議加強密碼強度或不定期更改密碼，以減少密碼外洩所造成的損失。

四、案例說明

· 97年5月10日(六)部分mx.nthu.edu.tw用戶收到署名為□MX WebMail v1.0 Internet □□□Service ‹abuse@mx.nthu.edu.tw›□□表示系統要更新、要求用戶提供email密碼，不然可能停止帳號，但回信地址卻非本中心所擁有的‹Email.Upgrade@Gxxd.com›□

· 97年9月11日(四)部分校內老師表示收到主旨為 □Update Your NTHU Email Now.eml□ 署名為‹cyhuang@nxnx.edu.tw›□並在內文中以"NTHU messaging center"名義發送
詐騙信件，表示系統要更新，要求收件者需提供帳號、密碼等資料，否則會刪除該帳號。但該信件的回信地址並非中心所擁有的‹info.emailteams@gxxxl.com›□

--
計算機與通訊中心

網路系統組 敬啟