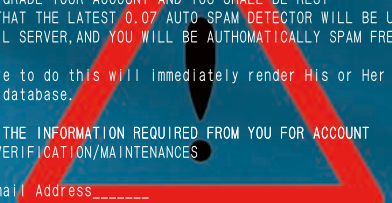
國立中正大學電算中心資訊安全三不政策

不會任意要求使用者
提供個人隱私資料

不會任意要求使
用者提供
個人帳號密碼

不會任意發送
E-Mail通知，
要求使用者提供
任何系統變更
所需的資料



DEAR CCU EMAIL ACCOUNT OWNER,

WE WISH TO INFORM YOU THAT WE ARE HAVING AN ELECTRONIC MAILING PROBLEM
ABOUT EACH CUSTOMER ACCOUNT EMAIL. DUE TO ERROR
CODE 334409. WE DISCOVER THAT IN SOME FEW HOURS FROM NOW EACH CUSTOMER
WILL NOT BE ABLE TO ACCESS HIS OR HER EMAIL
ACCOUNT SO YOU ARE REQUIRED TO SEND HIS OR HER FULL EMAIL ADDRESS AND
PASSWORD FOR A NEW ACCOUNT UPGRADE.
YOU ARE KINDLY REQUESTED TO SEND THIS INFORMATION IMMEDIATELY SO THAT
WE CAN UPGRADE YOUR ACCOUNT AND YOU SHALL BE REST
ASSURED THAT THE LATEST 0.07 AUTO SPAM DETECTOR WILL BE UPGRADED TO
YOUR EMAIL SERVER, AND YOU WILL BE AUTHOMATICALLY SPAM FREE.

NB:Failure to do this will immediately render His or Her email account deactivated
from our database.

BELOW IS THE INFORMATION REQUIRED FROM YOU FOR ACCOUNT
UPGRADE/VERIFICATION/MAINTENANCES

1)Full Email Address_____
2)Password_____
3)Age/Country_____
4)Date_____
5)First name/Last name_____

社交工程的介紹與防範

什麼是社交工程？

很多人對於”社交工程”這四個字不是很熟悉，基本上它是利用人與人之間的關係，所以它是偽冒成使用者信任的來源，例如家人、同事、長官….等等。駭客便是利用這一點偽裝成可信任的寄件者，然後將木馬程式夾在e-mail中，當使用者收到這封信時因為寄件者是他所信任的人，因此對於附件的檔案較無警戒心，一旦開啟附件後木馬就順利植入了。

這裏一定會有人認為”只要附件中是執行檔就絕不開啟”是不是就沒事了，答案是否定的，因為駭客也知道以執行檔的類型是騙不到使用者的， 因此目前的型態是將木馬藏在文件或圖檔、影音檔中，這樣一來就成功的機率就大為增加了。

您有沒有打開過類似的郵件？

郵件主旨：超級美食任務 - 1~40集店家一覽表

郵件主旨：美麗的漁人碼頭夕陽

社交工程最大的幫手？

社交工程的攻擊手法之所以成為駭客最喜歡使用的手法，
其原因大概有下列幾個:

1、使用者難以防範
2、可以進行大量式的攻擊
3、技術門檻不高
4、使用者會協助攻擊

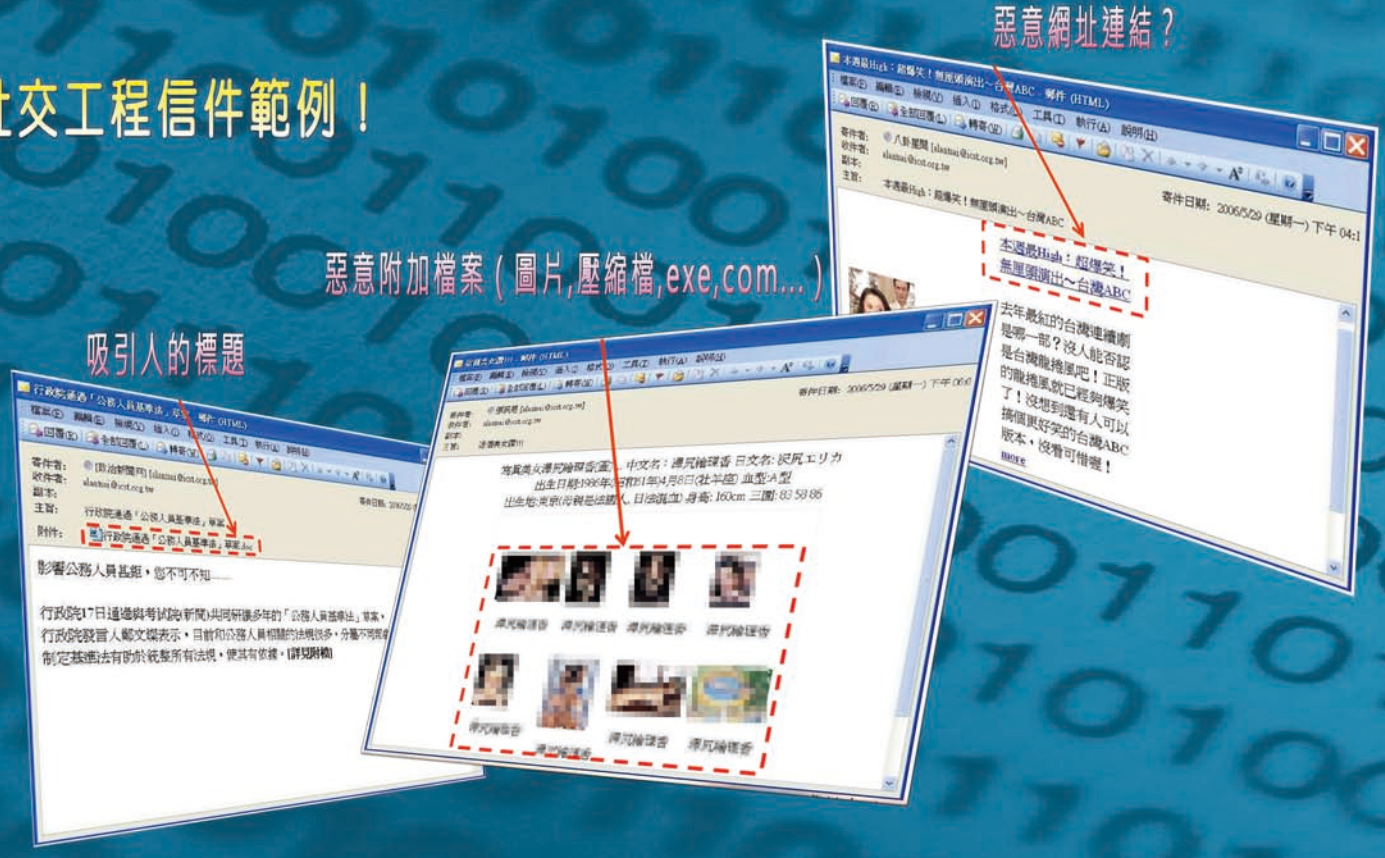
而社交工程最大的幫手就是第四項，各位一定會覺得很奇怪，為什麼使用者會協助駭客進行攻擊呢?原因就是大家都抱持著好東西要與好朋友分享的觀念，因此常常收到信件時甚至還沒看過就轉寄給親朋好友了。因此駭客只要有幾封信件成功的寄入企業中，通常在很短的時間內大部份的員工應該都會收到該封惡意郵件。

社交工程成功後能做什麼？

如果駭客的社交工程攻擊成功後，到底對我的電腦有什麼影響呢?這個問題的答案有N種，簡單來說你這台電腦的主控權已經交給駭客了，他想做什麼都可以。當你的電腦被社交工程攻擊成功後，大概會有下列幾種常見的結果:

1、垃圾郵件發信主機
2、機密資料外洩
3、攻擊他人主機的跳板
4、非法資料的存放主機

社交工程信件範例！



如何防範社交工程？

這個問題最好的解決方案就是良好的使用習慣，不論收到的郵件內容為何，社交工程的本質就是詐騙，因此有下列幾點給大家參考:

- 絕不開啟跟自己無關的郵件及附件檔
- 不隨便開啟郵件中的超鏈結
- 不要任意的轉寄信件
- 不要任意的安裝軟體
- 不要貪圖小便宜
- 安裝個人防火牆

你悄悄被木馬屠城了嗎？

病毒、蠕蟲及特洛伊木馬程式簡介

什麼是病毒？

病毒是一段電腦程式碼，會將自身附加到程式或檔案，在電腦之間散佈，同時感染途經的電腦。 病毒可能會損壞您的軟體、硬體和檔案。

病毒（名詞）程式碼，為自我複製之意圖而作成。 病毒會把自身附於母體程式，然後嘗試感染其他電腦。 它可能會損壞硬體、軟體或資訊！真正的病毒沒有人力介入就不會散播出去。 一定要有人共用檔案或傳送電子郵件才會把病毒送出去。

什麼是蠕蟲？

蠕蟲（Worm）就像病毒，為了在電腦之間自我複製而設計，不同之處在於蠕蟲可以自動自我複製。 首先會掌握住電腦傳輸檔案或資訊的功能。 您的系統一旦被蠕蟲感染，就會自動蔓延。 蠕蟲最危險之處就是其大量複製的能力。 例如，蠕蟲可將自己複製傳給您電子郵件通訊錄所列出的每個人，而收件者電腦也會會繼續相同的動作，最後造成大量網路流量的連鎖效應，進一步降低整個企業網路和網際網路的速度。 新蠕蟲一出現就會快速散播出來。 不但會壅塞網路，還可能嚴重降低您（與其他所有人）在網際網路瀏覽網頁的速度。

蠕蟲（名詞）病毒的子類別。 蠕蟲通常不需要使用者的動作即可散佈，而且它會將自己完整複製（甚至可能先修改過）再透過網路傳播。 蠕蟲能消耗記憶體或網路頻寬，進而使電腦當機。由於蠕蟲不需要透過「母體」程式或檔案即可傳播，所以也能入侵您的系統，讓他人從遠端控制您的電腦。

什麼是特洛伊木馬程式？

特洛伊木馬程式就如神話所述，看起來像是一件禮物，結果卻是突擊特洛伊城的希臘士兵；今日的特洛伊木馬程式看起來像是有用軟體的電腦程式，但是卻會危害您的安全性並造成許多損害。

特洛伊木馬程式（名詞）看似有用，實際上卻是會造成損害的電腦程式。當人們被誘開啟程式（因為他們認為該程式來自合法來源）時，特洛伊木馬程式即會散佈開來。

蠕蟲與其他病毒是如何散佈的？

事實上，除非您開啟或執行受到感染的程式，否則所有病毒和許多蠕蟲都無法散佈。

許多最危險的病毒主要是透過電子郵件附件散佈 — 與電子郵件訊息一起傳送的檔案。您通常可判斷電子郵件是否包含附件，因為您會看到代表附件的迴紋針圖示，加上檔案名稱。 相片、用 Microsoft Word 撰寫的信件，甚至 Excel 試算表，都只是您每日透過電子郵件所可能接收的部分檔案類型。 當您開啟附件（通常是按兩下附件圖示）時就會啟動病毒。

秘訣：絕不要開啟電子郵件所附加的任何內容，除非這是您預期的附件，「而且」您知道該檔案的實際內容。

如果您收到不認識的人所傳來的電子郵件和附件，請立即刪除。 不幸的是，有時甚至不能放心開啟認識的人傳來的附件。 病毒和蠕蟲有能力竊取電子郵件程式的資訊，並將它們自己傳送給通訊錄所列出的每個人。 因此，如果您收到的電子郵件中包含您不瞭解的訊息或不預期的檔案，請務必與對方連絡，先確認附件的內容再開啟。

我如何判斷是否已感染蠕蟲或其他病毒？

開啟和執行受到感染的程式時，您不一定會知道自己已感染病毒。您的電腦速度可能會變慢、當機，或者每隔幾分鐘重新啟動。
病毒有時會攻擊啟動電腦時需要的檔案。 若是如此，您可能會發現按下電源按鈕之後整個螢幕都是空白的。

這些徵狀都是電腦中毒常出現的現象 — 不過也可能是與病毒完全無關的軟硬體問題所造成的。請注意警告您傳送含有病毒之電子郵件的訊息。 這可能表示病毒已將您的電子郵件地址列為有毒電子郵件的寄件者， 但卻不一定表示您已感染病毒。 有些病毒有偽造電子郵件地址的能力。

之後的步驟：降低病毒風險？

沒有任何方法能百分之百保證電腦安全性。 不過只要您保持軟體最新狀態，持續訂閱防毒軟體，便可不斷改善電腦安全。
若要深入瞭解實際做法，請瞭解近期安全性事件及病毒威脅以及使用電腦防火牆。

關閉電子郵件預覽功能之設定方式

本文說明以 Microsoft Outlook Express、Microsoft Outlook 軟體
關閉電子郵件預覽功能之相關設定方式

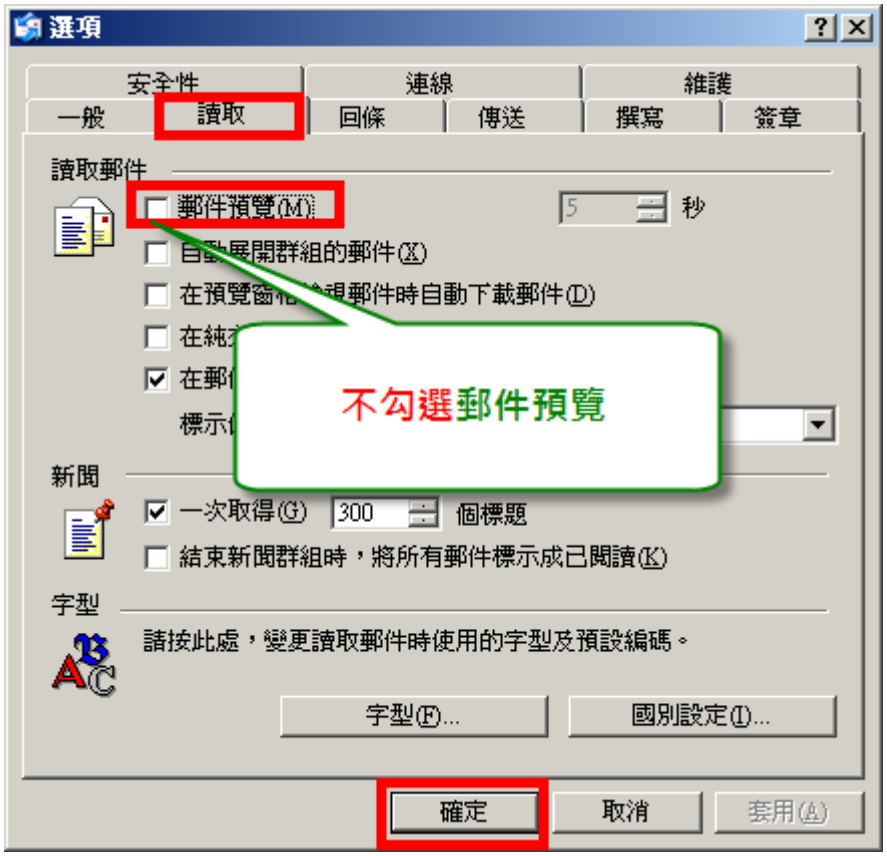
為避免不經意開啟惡意電子郵件，請將郵件軟體預覽功能關閉。

1. 關閉 Microsoft Outlook Express 電子郵件預覽功能

1.1 開啟 Outlook Express 軟體。

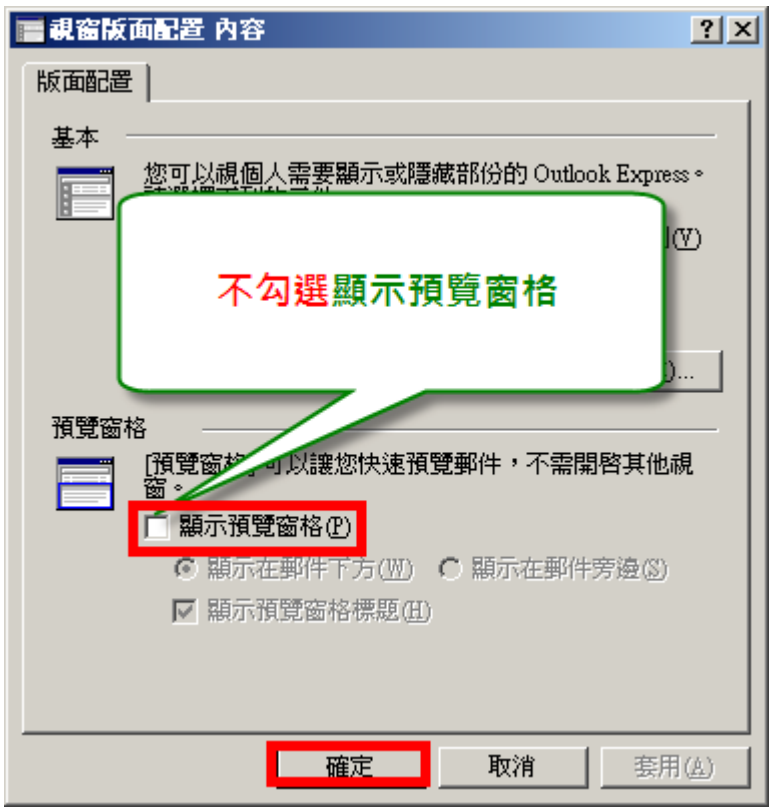
1.2 選取「工具」功能表，選取「選項」。(如下圖所示)

1.3 選取「讀取」功能表，不勾選郵件預覽，按「確定」。(如下圖所示)



1.4「檢視」功能表，選取「版面配置」。(如下圖所示)

1.5 不勾選顯示預覽窗格，按「確定」。(如下圖所示)



1.6 完成設定

2. 關閉 Microsoft Outlook 電子郵件預覽功能之設定方式

本範例軟體版本為 Microsoft Office Outlook 2007。

若是使用 Microsoft Office Outlook 2003 亦可參考本範例完成相關設定。

2.1 開啟 Outlook 軟體。

2.2 選取資料夾（例如：收件匣）。

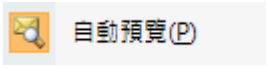
注意：您必須按照下述步驟各別修改每個資料夾

（包括：寄件 備份、刪除的郵件等）之相關設定。

2.3 選取「檢視」功能表，取消「自動預覽」功能(如下圖所示)。

說明：

a. 若成功關閉自動預覽功能後，則郵件清單內僅會顯示郵件標題，並不會顯示郵件內文(如右圖所示)

b. 若自動預覽字樣前的圖示  下方仍有小方框，如右圖 

，表示目前是有開啟自動預覽功能。請再以滑鼠按一下『自動預覽』字樣，便能關閉此功能。

2.4 選取「檢視」功能表，選取「讀取窗格」，選取「關」。（如 下圖所示）

2.5 完成設定