

社交工程與惡意郵件防制

楊峻榮

yang@mail.ncku.edu.tw

2011/08/31

大綱

- 什麼是社交工程
- 惡意郵件解析
- 惡意郵件防制
- 教育部-惡意郵件攻防演練

什麼是社交工程

什麼是社交工程

- 社交工程(Social Engineering)，是以影響力或說服力來欺騙他人以獲得有用的資訊或達到其目的，這是近年來攻擊者常用之攻擊手法之一。
- 利用人性的弱點進行詐騙，是一種非全面技術性的資訊安全攻擊方式，藉由人際關係的互動進行非法行為。
- 現有技術上之軟硬體安全防護系統難以防制。
- 等同於社會上之詐騙手法（如詐騙電話…）。

社交工程可應用之弱點

- 助人的天性
- 同情心
- 貪念
- 好奇心
- 怕麻煩
- 缺乏警覺
- 過於相信別人

社交工程常應用之題材

- 政治
- 色情
- 休閒養生
- 贈品、抽獎
- 愛心捐獻
- 影音媒體
- 業務職務相關
- 系統管理

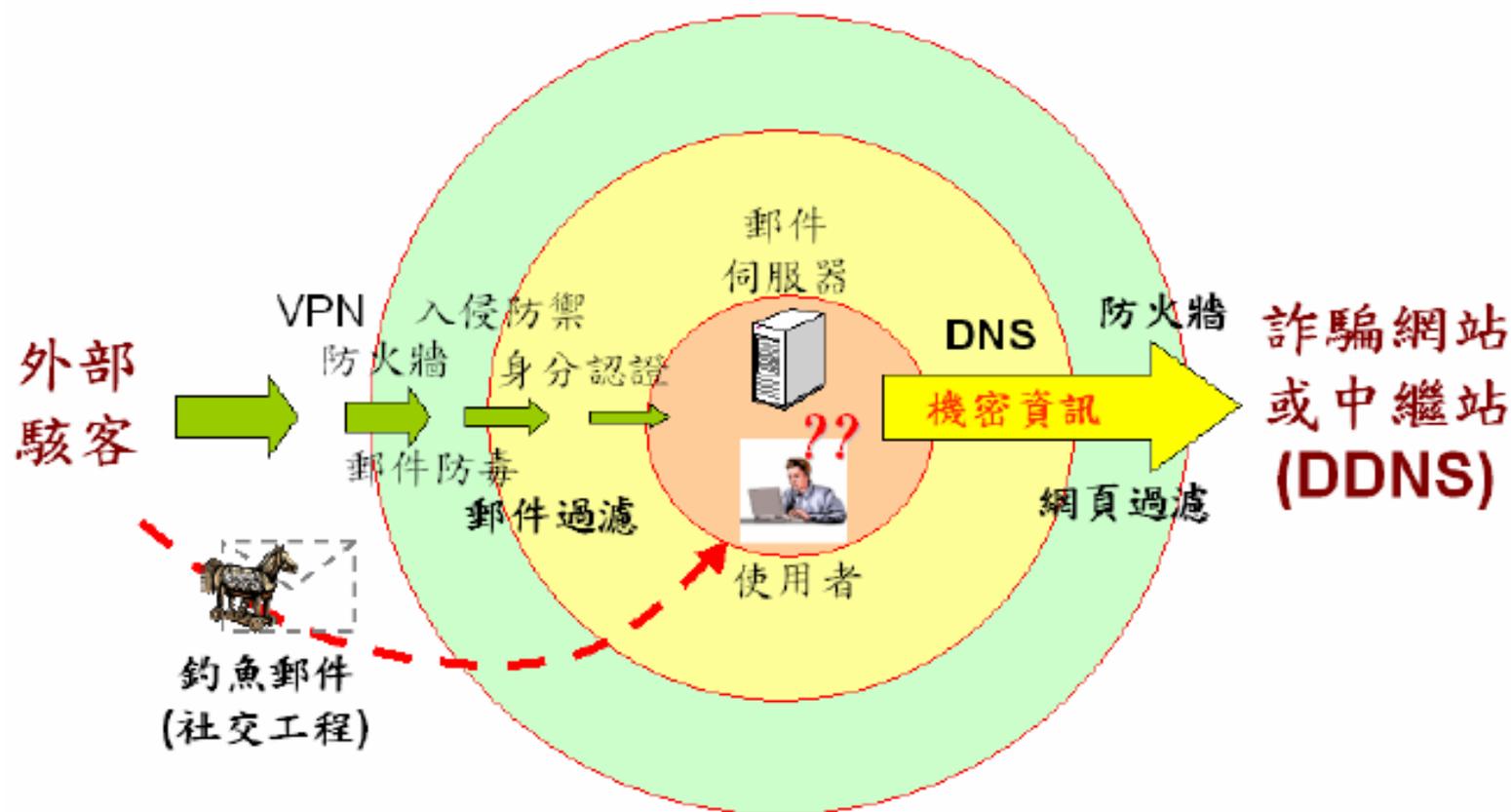
社交工程常用攻擊方法

- 在電子郵件內含惡意內容
 - 惡意連結
 - 惡意程式
- 網路釣魚網站
- 圖片中含惡意內容
- 電子郵件詐騙帳密及個資
- 即時通詐騙

網路釣魚(Phishing)

- 常見的社交工程，以惡意連結進行攻擊，運用各種人性弱點吸引使用者連結至phishing網頁
- 一般是利用email來引誘連結，利用下列方式讓受害者不易查覺：
 - 近似網址
 - <http://www.hinet.net>
 - <http://www.hl.net.net>
 - 偽造網頁：製作與原來完全一樣的頁面，以騙取重要的相關資訊。
- 其目的為：
 - 廣告目的(不斷開啟惡意廣告)
 - 攻擊目的(植入後門程式)
 - 金錢目的(詐騙行為)
 - 竊取帳號密碼與個人資料

釣魚郵件攻擊示意圖



網路釣魚手法與技術

行為階段	目的	手法	使用技術
灑網階段	誘騙使用者點擊連線上特定網站	針對不特定多數人寄發大量郵件夾帶URL	以郵址產生器亂數產生隨機式郵寄名單
			以軟體程式抓取公開的郵件地址
			以感染病毒方式散布郵件，同時複製病毒或植入木馬程式
收網階段	使用者自動輸入資料或竊取個資	設置虛假網頁，讓使用者陷於錯誤	註冊近似網址
			利用瀏覽器漏洞
		利用真實網站指令的漏洞	利用轉址技術
			網頁夾帶木馬程式

社交工程詐騙例—My Card

- 兩階段循環式社交工程。
- 第一階段詐騙：
 - 先製作釣魚網頁以收集MSN帳號、密碼。
 - 先由遭破解之MSN帳號登入，以“衝人氣”為由，誘導受害者A點連結假登入網頁，以騙取帳號密碼。
- 第二階段詐騙：
 - 用盜取到的受害者A之MSN帳號上線後，針對MSN帳號裡的朋友進行詐騙。
 - 詐騙方式是要受害者B幫他去超商買「**My Card**」的點數，買好之後幫他開卡。
 - 由於MSN上的好友名單通常都是好朋友或親人，既然是好友親人開口，大概都很少會拒絕或起疑。
- MSN非端點對端點連線，故不易追查詐騙者。

惡意郵件解析

惡意郵件種類

- 廣告信件
 - 廣告信件除了浪費使用者時間外，至少不會產生直接且立即的危害。
 - 防制機制：Anti-Spam。
- 病毒信件
 - 雖然病毒程式對於電腦系統會產生實質破壞，然而藉助於防毒軟體技術的進步，目前電腦病毒的威脅對於一般已安裝防毒軟體的使用者而言，屬於可控制的風險。
 - 防制機制：防毒軟體
- 釣魚（Phishing）信件
 - 目前最流行的釣魚目的，多是以竊取使用者資料並且實質獲利為主。
 - 防制機制：安全意識與概念。
- 木馬（Trojan）信件
 - 木馬程式，因為屬於主動式攻擊行為，一旦電腦遭受入侵，立即面臨資料外洩風險。
 - 防制機制：防毒軟體。
- 網頁綁架
 - 點選惡意連結後，開瀏覽器首頁遭置換或自動彈跳出廣告或不雅頁面。
 - 防制機制：防間諜軟體。

電子郵件社交工程的攻擊步驟

- 有心人在電子郵件內放置惡意程式或連結
- 將信件寄給特定或不特定對象
- 收件者開啟信件
- 啟動或下載惡意程式
- 輸出收件者資料

詐騙信件-1_1

Dear Account User,

This message is from webmail messaging center to all webmail account owners. We are currently upgrading our data base and e-mail account center. We are deleting all unused webmail account to create more space for new accounts. To prevent your Account from closing you will have to update it by providing the information requested below:

Confirm Your Account Details

Webmail ID:

Password:

DOB:

You will be sent a new confirmation alphanumerical password so that it will only be valid during this period and can be changed after the process.

Thanks for your understanding.

Webmail Administrator.

Warning!!! Account owner that refuses to update his or her account within seven days of receiving this warning will lose his or her account permanently.

詐騙信件-1_2

Welcome To National Cheng Kung University Department of Database/mail server Information Technology Service Center

This message is from our NCKU Mail server database/mail server Information Technology Service Center. Your mailbox has exceeded the storage limit which is 20GB as set by your administrator, you are currently running on 20.9GB, you may not be able to receive some new mail until you re-validate your mailbox.

We will deactivate some account from our database to enable us create more spaces for up coming subscribers

But to prevent this you have to confirm your account immediately after you receive this notification. To confirm and to keep your account active during and after this process, please reply to this message with the below account informations

Do confirm your account details below.

1. First Name & Last Name:
2. User Name & Password:
3. Retype Password:

Warning Code: ID67565

詐騙信件-2



-----Original Message-----

From: Spam security Customer Service [mailto:XXXXXX@mail.ncku.edu.tw]

Sent: Thursday, May 13, 2010 3:55 AM

To: xxxxx@mail.ncku.edu.tw

Subject: Your e-mail will be blocked

Your e-mail will be blocked within 48 hours for a spam if it was an error,
please open the attached file

Thank You.

Spam security Customer Service

詐騙信件-3_1

Welcome to National Cheng Kung University



Dear Client,

Do you have a new email address to your webmail account , or started verification of the existing e-mail address. To check whether the owner of this address e-mail, click on the The following link
Your email address ensures you can safely get to your account if your password is lost or stolen.
You must verify your email address before you can use ncku webmail
For your own safety, please e-mail updated information. If this information changes, please, Always update, log in to your account and change the "Settings" area.

Your Email address account verification.

<http://mail.ncku.edu.tw/cgi-bin/owmmdir/openwebmail.pl>

http://www.kollerit.ch/uploads/tx_ablinklist/ncku.htm

詐騙信件-3_2

----- Original Message -----

Subject:Upgrade Your Webmail Account

Date:Sat, 16 Apr 2011 01:10:58 -0000

From:NCKU Webmail Service<sheldon@yonsei.ac.kr>

To:undisclosed-recipients;



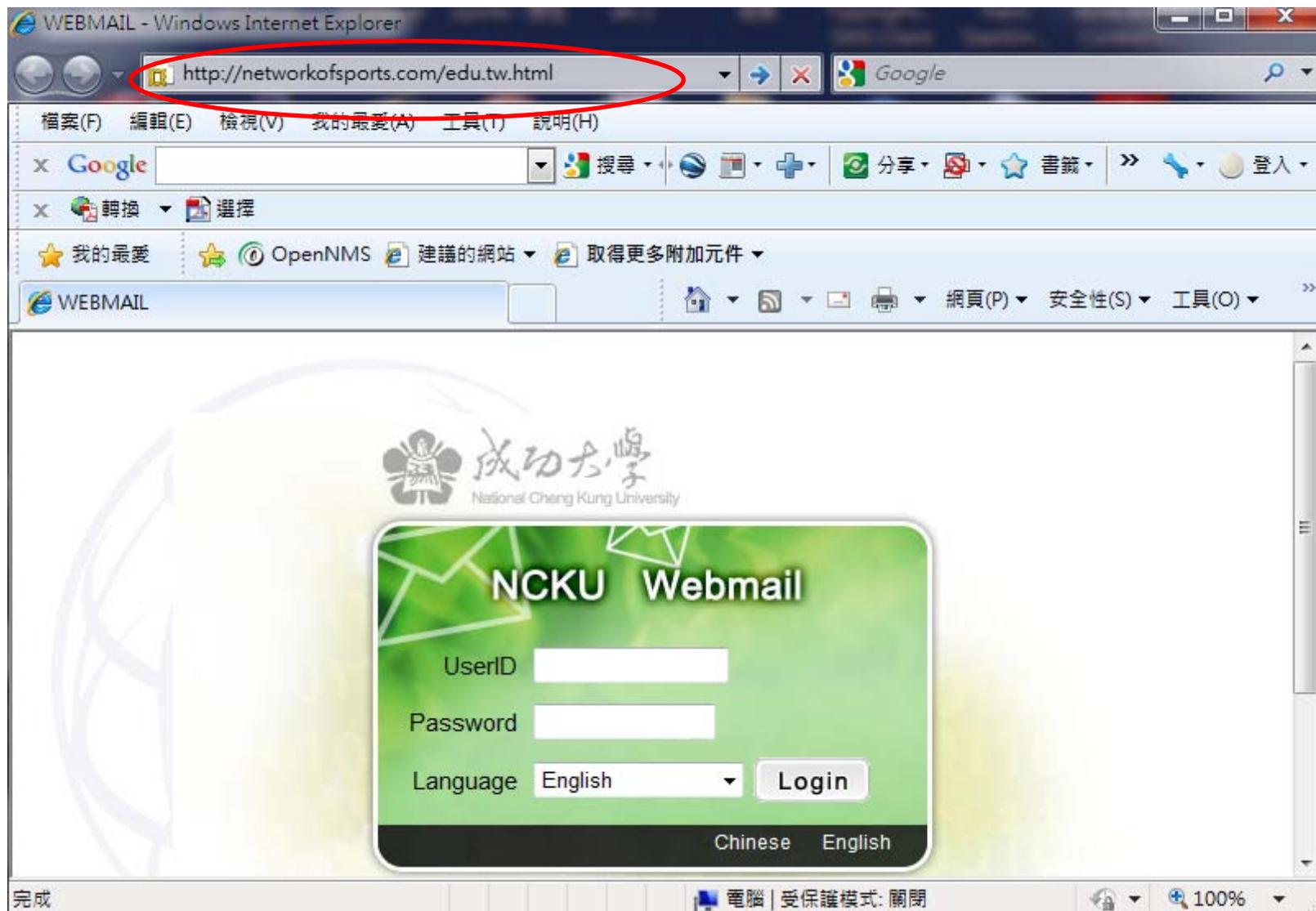
Dear Student/Staff,

Access to e-mail is about to expire,
We recommend that you upgrade your account to avoid the suspension.

Please click on the link below to update your account.
<http://ncku.edu.tw/>

Thank You.
National Cheng Kung University.

詐騙信件-3_3



惡意郵件防制

惡意郵件防制之道

■ 基本要求

- 電腦基本安全機制
- 讀取信件之基本概念與警覺性

■ 依需求

- 郵件安全設定

■ 進階

- 表頭及來源分析

電腦基本安全機制

- 提供安全環境，在不慎開啟惡意附件或點選惡意連結時，仍可能降低危害。
 - 安裝防毒軟體，確認定期更新定義碼，並且定時進行全機掃描。
 - 安裝防間諜程式軟體（ **Microsoft Windows Defender** 、 **Lavasoft Ad-Aware** ），確認定期更新定義碼，並且定期進行全機掃描。
 - 定期執行Windows update與office update，並且更新瀏覽器版本，避免因為軟體先天缺陷造成的安全漏洞。

讀取信件要領

- 先確認寄件者。
 - 是否為您認識的人或業務需要。
- 確認郵件主旨。
 - 是否為奇怪的主旨，或與寄件者不搭的主旨。
- 確定郵件內容是否與寄件者或主旨有關
- 確定郵件內容是否得宜。
 - 例如是否得提供個資料機敏資料。
- 是否非得開啟附件或點選連結。
- 是否須向寄件者確認。

讀取信件注意事項

- 寄件者是很容易假冒的，若發覺信件內容與寄件者之前所寄的內容差異大時，請向寄件者詢問（例如此寄件者原先都寄中文信，而收到其英文信……）。
- 來路不明之信件不予理會，直接刪除或避免按照信件內容指示行事，也不要開啟附加檔案，以免導致中毒或資料外洩。
- 遇到任何要求提供密碼或個人資訊的情況，請勿理會。本中心或mail系統之管理者決不可能要求使用者以mail方式回覆密碼。
- 若要求提供資料之信件，可先詢問承辦單位是否屬實，且不用該信件或網頁提供之查詢資訊。
- 天上不會掉下來禮物，愈好康的信件愈有問題，例如點選連結即可得到禮物。
- 要發揮愛心前，也需事先查證，例如某某組織需要善心捐款。
- 點選信件內附之網頁連結前，請再三確認該連結是否有異狀。例如網址之domain看起來很怪異或是網址使用 IP_address。
- 看似無害之信件也儘可能不要開啟，如廣告信件。
- 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。
- 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。
- 若來信有疑，無法確認是否為惡意信件，可來電詢問(校內分機61016)，或將該信件「另存新檔」後以附加檔方式寄至yang@mail.ncku.edu.tw。

讀信軟體安全設定

- 讀信軟體即是以POP/IMAP協定將信件由mail server下載至PC來讀取，如Windows Live Mail、Outlook express、Outlook等。
- 其讀信之基本安全設定如下，並可交互配合使用：
 - 關閉信件預覽功能
 - 只列出寄件者及主旨，需讀取信件時再點選，是否讀取由寄件者及主旨來判斷。
 - 以純文字開啟信件
 - 不受信件本文內之惡意內容影響，唯無法顯示其格式。
 - 關閉自動下載圖檔
 - 不受圖片之惡意連結或惡意內容影響，有需顯示時再按〔下載〕鍵。
- 建議設[關閉信件預覽功能]+[關閉自動下載圖檔]

關閉信件預覽功能

- Windows Live Mail
 - 選取【檢視】／【版面配置】
 - 不勾選【顯示預覽窗格】
- Outlook express
 - 選取【檢視】／【版面配置】
 - 不勾選【顯示預覽窗格】
- Outlook 2010
 - 選取【檢視】／【讀取窗格】
 - 選擇【關閉】
- Outlook 2007
 - 選取【檢視】／【讀取窗格】
 - 選擇【關閉】

以純文字開啟信件

■ Windows Live Mail

- 選取【工具】／【選項】／【讀取】
- 勾選【在純文字中讀取所有郵件】

■ Outlook express

- 選取【工具】／【選項】／【讀取】
- 勾選【在純文字中讀取所有郵件】

■ Outlook 2010

- 選取【檔案】／【選項】／【信任中心】／【信任中心設定】／【電子郵件安全性】
- 勾選【以純文字讀取所有標準郵件】

■ Outlook 2007

- 選取【工具】／【信任中心】／【電子郵件安全性】
- 勾選【以純文字讀取所有標準郵件】

關閉自動下載圖檔

- Windows Live Mail
 - 選取【工具】／【安全性選項】／【安全性】
 - 勾選【阻擋HTML電子郵件中的圖片和其他外部內容】
- Outlook express
 - 選取【工具】／【選項】／【安全性】
 - 勾選【阻擋HTML電子郵件中的圖片和其他外部內容】
- Outlook 2010
 - 選取【檔案】／【選項】／【信任中心】／【信任中心設定】／【自動下載】
 - 勾選【不自動下載HTML電子郵件訊息或RSS項目中的圖片】
- Outlook 2007
 - 選取【工具】／【信任中心】／【信任中心設定】／【自動下載】
 - 勾選【不自動下載HTML電子郵件訊息或RSS項目中的圖片】

Webmail讀信安全設定

- 如下之安全設定，於〔設定〕／讀取相關設定

讀信相關設定	
閱讀信件時控制列位置:	在上面 ▾
預設表頭:	簡單表頭 ▾
讀信時, 使用信件本身字集:	<input type="checkbox"/>
讀信時, 使用固定寬度字型:	<input type="checkbox"/>
讀信時, 使用笑臉圖示:	<input checked="" type="checkbox"/>
以文字方式顯示 HTML 郵件:	<input checked="" type="checkbox"/>
以超連結方式顯示圖片附件:	<input checked="" type="checkbox"/>
關閉郵件內的 Java Script:	<input checked="" type="checkbox"/>
關閉郵件內的 embed/object/applet 標籤:	<input checked="" type="checkbox"/>
關閉郵件內的內嵌連結:	只關閉 CGI ▾
傳送讀取回條:	要求確認 ▾

Webmail讀取html內容信件

- 信件內容無問題時再點選+html+以html格式顯示其內容:



字集 utf-8 > big5 -- 選擇回信底稿 -- 收件匣 搬移 複製

◀ 126/1108 +html+ 以 Html 模式顯示

日期: 29 Aug 2011 06:00:49 +0800 完全表頭

寄件者: "Email Administrator" <admin@email.ncku.edu.tw> <SpamAdmin@email.ncku.edu.tw>

收件者: z7512003@email.ncku.edu.tw

主旨: 國立成功大學隔離信件通知

國立成功大學隔離信件通知

國立成功大學隔離信件通知

z7512003@email.ncku.edu.tw,您好:

自從上次您接到此封通知信之後, 郵件過濾系統新發現了 1 封隔離信件, 郵件隔離區累積信件 1 封, 新增信件如下:

隔離的電子郵件

寄件者
主旨
日期
釋出 "Tenable Network Security" <Tenable... [MARKETING] Tenable Network Security News - August 2011 28 Aug 2011

Check可疑信件

- 檢查信件內容
 - 信件內容、連結、附加檔名
- 檢查表頭
 - Check原始出處
 - Check Reply-To
- 使用nslookup命令
 - Check Domain name -> IP address
 - 配合 whois

查看信件表頭

■ Outlook Express

- 由信件列表選取該信件按右鍵
- 選取 內容 / 詳細資料 / 郵件原始檔

■ WebMail (OpenWebMail)

- 由信件列表點選取該信件
- 列出信件內容時按「完全表頭」

mail 表頭的欄位

■ Return-Path:

- 此一欄位的e-mail address是由寄信的client在MAIL FROM：指令中傳送的sender's e-mail address。

■ Delivered-To

- 收件者email_address

■ Received:

- 郵件傳送過程中所經過的SMTP server(mail servers)，因此可能好幾欄，其傳送順序為由下往上。

■ From:, To:

- 這兩個欄位，是一般郵件閱讀軟體所顯示的“寄信者”及“收信者”，也就是如傳統信紙上的寄件者及收件者
- 這兩個欄位只是提供資訊給郵件閱讀郵件程式參考，和信件的傳遞是沒有關係的。

■ Reply-To

回信時之接收者Email address

■ Subject:

- 信件主旨。

■ Date:

- 發信者發出信件的時間點，此欄位僅供參考，並不能作為重要依據。

以郵件軟體(OE)寄出之表頸

Return-Path: <eagleuser@lina.es.ncku.edu.tw>

X-Original-To: yang@mail.ncku.edu.tw

Delivered-To: yang@mail.ncku.edu.tw

Received: from ms8.cc.ncku.edu.tw (ms8.cc.ncku.edu.tw [127.0.0.1])

by ms8.interscan (Postfix) with ESMTP id 8E43C17FF6

for <yang@mail.ncku.edu.tw>; Thu, 30 Apr 2009 01:00:29 +0800 (CST)

Received: from mailgate2.ncku.edu.tw (gateway2.ncku.edu.tw [192.168.1.202])

by ms8.cc.ncku.edu.tw (Postfix) with ESMTP id 5DB3818001

for <yang@mail.ncku.edu.tw>; Thu, 30 Apr 2009 00:31:52 +0800 (CST)

Received: from csie.ncku.edu.tw [(140.116.247.2)] by mailgate2.ncku.edu.tw

(envelope-from <eagleuser@lina.es.ncku.edu.tw>)

(Mailgate1 with TLS)

with ESMTP id 1224315827; Thu, 30 Apr 2009 00:31:57 +0800

Received: from [140.116.78.120] (alumni.es.ncku.edu.tw [140.116.78.120])

by csie.ncku.edu.tw (8.13.8+Sun/8.13.7) with ESMTP id n3TGRQJq003818

for <yang@mail.ncku.edu.tw>; Thu, 30 Apr 2009 00:27:42 +0800 (CST)

To: yang@mail.ncku.edu.tw

From: =?big5?B?pqikaqR1rOyk5bHQsPKq97d8IA==?= <leeps@mail.ncku.edu.tw>

Reply-To: =?big5?B?pqikaqR1rOyk5bHQsPKq97d8IA==?= <leepss@yahoo.com>

Subject: =?big5?B?pHWs7Kh0pM3Cvrd+wXC9y7d8Lbx4pH7Fb6FJJiM4MjA3Ow==?=
Date: Thu, 30 Apr 2009 01:07:33 +0800

X-LibVersion: 3.3.2

以webmail寄信之表頭-1

X-Symantec-TimeoutProtection: 0
Return-Path: <testmail@mail.ncku.edu.tw>
X-Original-To: yang@mail.ncku.edu.tw
Delivered-To: yang@mail.ncku.edu.tw
Received: from ms7.cc.ncku.edu.tw (ms7.cc.ncku.edu.tw [127.0.0.1])
by ms7.interscan (Postfix) with ESMTP id 13317B89102
for <yang@mail.ncku.edu.tw>; Wed, 6 May 2009 11:52:20 +0800 (CST)
Received: from ([127.0.0.1]) by ms7.cc.ncku.edu.tw
(InterScan E-Mail VirusWall Unix); Wed, 06 May 2009 11:52:20 +0800 (CST)
Received: from mailgate2.ncku.edu.tw (gateway2.ncku.edu.tw [192.168.1.202])
by ms7.cc.ncku.edu.tw (Postfix) with ESMTP id E6051B890F9
for <yang@mail.ncku.edu.tw>; Wed, 6 May 2009 11:52:19 +0800 (CST)
Received: from ms13.ncku.edu.tw [(192.168.1.13)] by mailgate2.ncku.edu.tw
(envelope-from <testmail@mail.ncku.edu.tw>)
(Mailgate1)
with ESMTP id 1757683983; Wed, 06 May 2009 11:52:19 +0800
Received: from mail.ncku.edu.tw (ms13.ncku.edu.tw [127.0.0.1])
by ms13.ncku.edu.tw (Postfix) with ESMTP id 40BA614F0CAA
for <yang@mail.ncku.edu.tw>; Wed, 6 May 2009 11:52:19 +0800 (CST)
From: "testmail" <testmail@mail.ncku.edu.tw>
To: yang@mail.ncku.edu.tw

以webmail寄信之表頭-2

Return-Path: <a129123403@yahoo.com.tw>

X-Original-To: yang@mail.ncku.edu.tw

Delivered-To: yang@mail.ncku.edu.tw

Received: from ms8.cc.ncku.edu.tw (ms8.cc.ncku.edu.tw [127.0.0.1])

by ms8.interscan (Postfix) with ESMTP id 999AC17FC4

for <yang@mail.ncku.edu.tw>; Wed, 29 Apr 2009 21:10:53 +0800 (CST)

Received: from mailgate1.ncku.edu.tw (gateway1.ncku.edu.tw [192.168.1.201])

by ms8.cc.ncku.edu.tw (Postfix) with ESMTP id 81C1C17FB8

for <yang@mail.ncku.edu.tw>; Wed, 29 Apr 2009 21:10:53 +0800 (CST)

Received: from web73202.mail.tp2.yahoo.com [(203.188.201.22)] by

mailgate1.ncku.edu.tw (envelope-from <a129123403@yahoo.com.tw>)(Mailgate1)

with ESMTP id 943006835; Wed, 29 Apr 2009 21:10:57 +0800

Received: (qmail 95264 invoked by uid 60001); 29 Apr 2009 13:10:57 -0000

Received: from [163.29.61.252] by web73202.mail.tp2.yahoo.com via HTTP; Wed, 29 Apr 2009 21:10:57 CST

X-Mailer: YahooMailClassic/5.2.20 YahooMailWebService/0.7.289.1

Date: Wed, 29 Apr 2009 21:10:57 +0800 (CST)

From: =?big5?B?tL+m0MJF?= <a129123403@yahoo.com.tw>

Subject: =?big5?B?RlehRyCyxKRAprinQLd+?=

To: yang@mail.ncku.edu.tw

得知郵件內連結之內容(OE)

郵件原始檔

Content-Type: text/html;
charset="big5"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; charset=3Dbig5">
<META content=3D"MSHTML 6.00.6000.16825" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV>
<P>=B4=FA=B8=D5=B4c=B7N=B3s=B5=B2</P>
<P>http://www.ncku.edu.tw</P></DIV>
</BODY></HTML>

寄件者: yang 收件者:
主旨: test

測試惡意連結

<http://www.ncku.edu.tw>

得知郵件內連結之內容(WebMail)

The screenshot shows a webmail interface with a blue header bar containing the email address `yang@mail.ncku.edu.tw`. Below the header, there are navigation icons for '返回' (Return), '列印' (Print), and '網路硬碟' (Network Drive). The main content area displays the email details:

- 字集: big5 *
- ◀ 1 ▶ **-html-**
- 日期: Fri, 1 May 2009 16:...
- 寄件者: "yang" <yang@ncku.edu.tw>
- 收件者: "yang" <yang@ncku.edu.tw>
- 主旨: test ||
- 測試惡意連結
- <http://www.ncku.edu.tw>

A '內容' (Content) dialog box is open over the email content, showing the following information:

- 一般 (General) tab
- Icon:
- 210.210.9.9
- 通訊協定: HyperText 傳輸通訊協定
- 類型: 9/ 檔案
- 網址 (URL): http://210.210.9.9/

The dialog box has buttons for '確定' (OK), '取消' (Cancel), and '套用(A)' (Apply).

Domain name與IP 查詢

- Check 連結連結之Domain name為何IP address(校內為140.116.XX.XX)
- 雖為校內IP address，但也有可能是該主機中毒或遭入侵而發惡意信件
- 開始/所有程式/附屬應用程式/命令提示字元
- 鍵入 nslookup命令後，輸入欲查詢的 Domain name 或IP address。



```
C:\> 命令提示字元 - nslookup

Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\security>nslookup
Default Server:  apple.ncku.edu.tw
Address:  163.28.113.1

> www.ncku.edu.tw
Server:  apple.ncku.edu.tw
Address:  163.28.113.1

Name:    www.ncku.edu.tw
Address:  140.116.241.51

>
```

教育部-惡意郵件攻防演練

攻防演練時程

- 提報演練名單：4月(各機關學校提報行政人員郵件名單)。
- 各機關學校辦理教育訓練：4月(全部行政人員)。
- 進行第1次演練：5月。
- 各機關學校辦理再教育訓練：6月至8月(開啟、點閱惡意郵件比率較高人員)。
- 進行第2次演練：9月。
- 各機關學校辦理再教育訓練：10月(開啟、點閱惡意郵件比率較高人員)。

提報名單

- 所有email.ncku.edu.tw之個人帳號，即ZXXXXXXX，共1840筆
- 提報資料並含單位姓名

攻防演練內容

- 郵件主題分為政治、公務、健康養生、旅遊等類型，郵件內容包含連結網址或word附檔。
- 由技術小組以偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象，當收件人開啟郵件或點閱郵件所附連結或檔案時，應留下紀錄，俾利後續統計惡意郵件開啟率及點閱率。
 - 惡意郵件開啟率：
 - 開啟惡意郵件之人數/參演人數。
 - 惡意郵件點閱率：
 - 點閱惡意郵件所附連結或檔案之人數/參演人數。
 - 惡意郵件開啟下降率：
 - $-(\text{本年度惡意郵件開啟率}-\text{比較基準})/\text{比較基準}$
 - 原則上，比較基準為前年演練之惡意郵件開啟率。
 - 惡意郵件點閱下降率：
 - $-(\text{本年度惡意郵件點閱率}-\text{比較基準})/\text{比較基準}$
 - 原則上，比較基準為前年演練之惡意郵件點閱率。

100年5月教育部演練信件內容

編號	信件類別	信件標題
Letter 1	旅遊圖片類	【HiNet 旅遊網】深度旅遊團 超低價好康!!
Letter 2	生活類	五月報稅天 網路報稅讓麻煩省一半！
Letter 3	知識類	超重要！不要再相信網路謠言「生命三角」
Letter 4	科技類	台灣之光！日內瓦展 我發明奪42金 世界第一！
Letter 5	美女類	大陸美女-范冰冰 為了拍 MV 露點也願意！
Letter 6	美容類	完美牙齒整型 五大注意事項
Letter 7	旅遊類	騎鐵馬逛八里 便道成車道 車友爭相樂活
Letter 8	時事類	從日本核災看輻射線對眼球的影響！
Letter 9	財經類	凍漲七年 軍公教終於要加薪了！
Letter 10	健康類	外食族 如何吃得更健康？超商減肥法！
Letter 11	新奇類	巨無霸高麗菜 重30台斤超吸睛！

演練結果

學校名稱	Total		Average
	開啓信件	點選連結	
成功大學	26.58%	19.17%	22.88%

	單位 測驗人數	開啓人數	點擊人數	開啓人數 百分比	點擊人數 百分比	開啓人數 基準值	點擊人數 基準值
200905				2.80%	0.72%	16.00%	9.00%
200909	1119	37	24	3.31%	2.14%	16.00%	9.00%
201005	1235	39	36	3.16%	2.91%	10.00%	6.00%
201009	1236	41	18	3.32%	1.46%	10.00%	6.00%
201105	918	244	176	26.58%	19.17%	10.00%	6.00%

攻防演練因應之道

- 如上章節[惡意郵件防制]所描述之方式。
- 關閉信件預覽或使用Webmail讀信
- 非得開啟信件預覽，設定為文字模式(OE等mail client及Webmail皆可設定。
- 不讀取非來自本校且非職務上之訊息。
- 本次提報名單含單位姓名，故演練信件內容可能含此資訊，請注意!
- 若有可疑信件，請洽61016 。

Q & A