

快速連結

- [本組最新消息](#)
- [資通安全](#)
- [聯絡我們](#)

收到此電子報是因為您是本組的服務對象，詳情請參閱發行說明

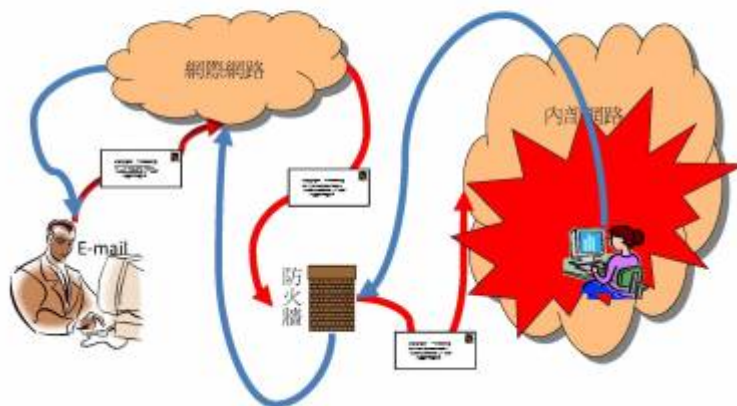
2010.05 第十四期：當心電子郵件社交工程攻擊

社交工程防護 123

政府機關的電子郵件社交工程演練又要來了！電子郵件社交工程攻擊常利用好奇心、興趣來吸引使用者開啟信件，一旦不小心或是誤開啟此類信件，就可能被植入惡意或後門程式，並讓電腦成為被入侵者所控制的殭屍電腦。為讓自己的電腦遠離危險，防護工作不能少：

現在網路攻擊模式

1. 在電子郵件內放置有害程式或連結 2. 反向輸出使用者資料



1. 基本的防護

- 作業系統更新
- 應用軟體更新
- 防毒軟體、個人防火牆

2. 再多一點的防護

- 調整收信軟體設定
 - 不自動下載圖片
 - 關閉信件預覽功能
 - 以純文字開啟信件
 - 常見收信軟體之設定建議如下：[Outlook 2007](#)、[Outlook Express](#)、[Live mail](#)
- 熟悉所使用軟體基本設定

3. 近乎完美的防護

- 改變使用習慣
 - 查明信件的來源：瞭解[如何查看 mail header](#)
 - 釐清寄件者身份：以電話向寄件者確認、郵件驗證機制、附件加密..等方式

詳細資訊請參閱 [電子郵件社交工程教育訓練投影片](#)

其他參考資料：[教育部98上半年度電子郵件社交工程演練結果說明](#)、[教育部98下半年度電子郵件社交工程演練結果說明](#)

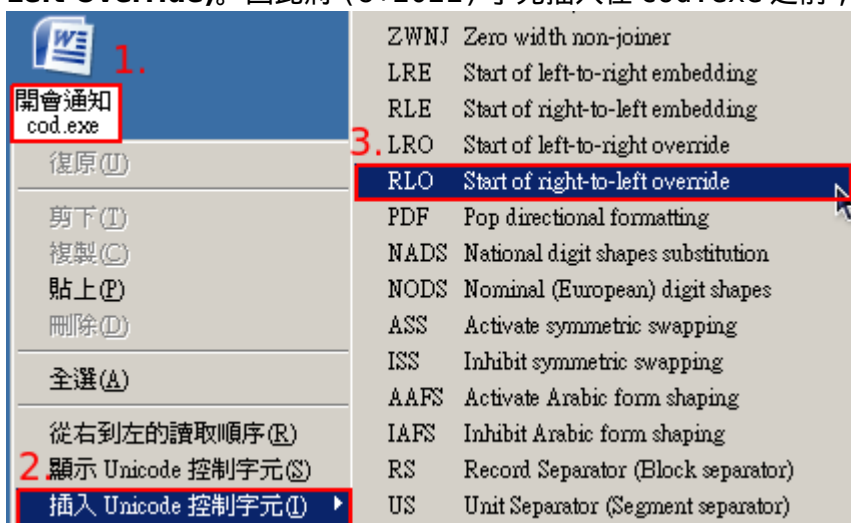
新型社交工程攻擊手法通知 **Unicode Spoofing**

國家資通安全會報 - 技術服務中心近日發現，駭客大量利用新式誘騙手法誘騙使用者執行惡意程式。使用者一旦誤點擊誘騙檔案，電腦隨即遭植入惡意程式，駭客將可進一步控制使用者的電腦。全文詳見 [國家資通安全通報應變網站](#)

該手法利用特殊 **Unicode** 控制字元 (**U+202E RIGHT-TO-LEFT OVERRIDE**)，配合字型造成顯示上的誤導，讓使用者以為是一般檔案，但實際上為有害的惡意程式。

例如，有心人士可能將惡意程式命名為「開會通知 (**U+202E**) cod.exe」，而使用者可能看到的檔名卻為「開會通知 **exe**.doc」，讓使用者誤開啟檔案或執程式。手法說明如下：

- (**U+202E**) 為 Unicode 控制字元，該字元為不可視字元，可控制後續字元由右至左顯示 (**Right To Left Override**)。因此將 (U+202E) 字元插入在 cod.exe 之前，就會讓使用者看到 exe.doc



- 使用者看到的檔案名稱為「開會通知 **exe**.doc



參考網址

- [Right-to-Left-Override Unicode Spoofing](#)
- [Phishing Defense against IDN Address Spoofing Attacks](#)
- [Phishing fun with Unicode](#)
- [Unicode Character 'RIGHT-TO-LEFT OVERRIDE' \(U+202E\)](#)
- [Unicode Character 'POP DIRECTIONAL FORMATTING' \(U+202C\)](#)

訊息快報

1. 學生宿舍分機年度關閉及重新申請相關事宜

為配合學年度結束及學生宿舍寢室更換，本組於六月八日(二)將關閉學生宿舍區寢室分機，即日起，開放受理下學年度學生寢室分機申請...[閱讀全文](#)

2. 99/6/1(二)起計通中心將進行校園無線網路 PEAP 認證之 SSID 由 nthu 更名為 nthupeap 作業

目前本校 PEAP 認證之基地台識別碼名稱(SSID)是 nthu 為考量用戶（來賓）以 PEAP 認證方式使用無線網路前未完成額外設定，易誤用 SSID nthu 而導致無法使用無線網路。故本中心自 99/6/1(二)起，將校園無線網路 PEAP 認證之 SSID 由 nthu 更名為 nthupeap...[閱讀全文](#)

3. 新功能上線：個人網頁被下載量偏高通知信

自 6 月起，對於使用本組信箱帳號所製作的個人網頁，若被下載的資料量或次數偏高者，將寄信通知使用者該日網頁被下載情況，以供使用者自行參考，及附帶提醒[相關的注意事項](#)...[閱讀全文](#)

資安資訊

1. 微軟安全性工具

透過微軟所提供適用於 windows 平台的工具與技術來評估漏洞和加強安全性。這些工具可以協助您進行下列工作：

- 安全性更新管理
- 安全性更新偵測
- 安全性評估
- 鎖定、稽核和入侵偵測與修復
- 病毒和惡意軟體防護與移除

詳情請參閱微軟安全性 [TechCenter](#) [安全性工具](#)

2. 資安漏洞通告

1. Microsoft PowerPoint “OEPlaceholderAtom” 無效索引紀錄遠端程式碼執行漏洞 (2010/05/21)
2. Microsoft Paint JPEG 影像處理整數溢位漏洞 (2010/05/18)
3. Microsoft Excel FNGROUPNAME 紀錄遠端程式碼執行漏洞 (2010/05/14)
4. WebKit 跨域樣式表請求資訊外洩漏洞 (2010/05/11)
5. Microsoft Excel Object Type Confusion 遠端程式碼執行漏洞 (2010/05/07)
6. XnView DICOM 影像處理整數緩衝區溢位漏洞 (2010/05/04)
 - 詳情請參閱國家資通安全通報應變網站：[弱點通告](#)

好康分享

國家高速網路與計算中心 服務介紹 - 教育訓練服務

國網中心有許多優質服務及教育訓練提供學術研究人員（教授、學生）申請，特將好消息轉知讀者，如有需要可自行接洽，本期摘要教育訓練服務並提供國網中心各項服務連結如下：

- [教育訓練服務](#)：國網中心提供各類軟硬體教育訓練課程，並建置遠距即時互動教學平台，藉由高效

能計算與網路技術在科學與工程應用計算的能量，擴散高速計算與網路技術及其在專業科學與工程應用領域的經驗。

◦ 服務項目

- 提供各類專業應用領域的教育訓練課程
- 課程內容包涵計算流體力學、計算固體力學、計算法學、計算物理、化學資料庫、科學視算、自由軟體
- K-12科學研習課程
- 中小學教師教育訓練
- 非正規教育認證課程

◦ 聯絡窗口

- 竹科 - 高速計算事業群 (03)5776085-351 賴小姐
- 中科 - 前瞻系統事業群 (04)24620202
- 南科 - 先進網路事業群 (06)5050940-758 陳小姐

◦ 服務對象：除部分特定課程有限制外，任何人皆可報名參加。

◦ [NCHC 教育訓練網](#)

- 其他服務連結：[高速計算服務](#)[學研網路服務](#)[資料儲存服務](#)[校園無線漫遊服務](#)[軟體與資料庫服務](#)[化學與生物資料庫服務](#)[溝通合作平台](#)

詳情請參閱[國網中心服務專區](#)

發行說明：

電子報內容包含校園網路、網際網路應用、資通安全、校園電話等服務說明與各項公告，以及相關領域的專題報導。本刊物以網路系統組服務用戶為發行對象，訂閱者可收到定期電子報及不定期公告，建議您長期訂閱以獲得最新資訊。

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/mailling:201005_14

Last update: **2010/06/01 08:20**

