國立中興大學計算機及資訊網路中心電子報

2014 年 5 月

最新消息

1. 微軟宣布 Internet Explorer 出現安全性漏洞，請大家立即更新 KB2964358 修正程式

微軟宣布 Internet Explorer 出現重大安全性漏洞的，請大家立即更新 KB2964358 修正程式，不論你是使用 Windows 7, 8 甚至微軟宣佈不再支援的 XP (可能因這漏洞實在是太大了，不得不釋出對 XP 的修正程式)

也不論你是使用那一版的 Internet Explorer 都有「存取已刪除或錯置記憶體內容」的弱點風險 (CVE-2014-1776)。特別許多人慣用 IE 瀏覽器，以及用到電子公文或網路 ATM 的使用者，更要特別進行此部份的更新。

- 更新方法

  (1) 請各位教職人員以及同學到 Windows 控制台的「Windows Update」查看「檢查更新」。

  (2)若有代號為 KB2964358 的 IE 安全性更新，請立即下載更新。

  請一律由 Windows Update 更新，不要自行上網下載更新程式，以免遇到有心程式。

- 技術支援

  若需相關協助，歡迎上班時間與計資中心 資源管理組 詹先生聯絡，校內電話 04-22840309 轉 756。

2. Windows Server 2003 終止支援。

2015 年 7 月 14 日起，Microsoft 將不再提供 Windows Server 2003 的資訊安全更新、支援或技術內容更新。不管實體機器或是虛擬機器上的 Windows Server 2003 都將面對終止支援的問題。

- 由於不再提供資訊安全修補程式和 Hotfix，Server 和應用程式很容易遭受資訊安全威脅並造成停機時間。
- 過時軟體會產生法規與政策的風險。
- 如果用戶只是將原先使用的 Windows Server 2003 透過 P2V 的方式虛擬化，仍然是 Windows Server 2003。

  若需相關協助，歡迎上班時間與計資中心 資源管理組 林先生聯絡，校內電話 04-22840309 轉 732。

3. 電子郵件社交工程攻擊與防禦

教育部資訊及科技教育司對資安意識的落實與對社交工程等攻擊行為的資安警覺意識，於 2014 年 5 月中下旬起進行電子郵件社交工程演練，藉由模擬駭客寄送各種誘騙信件的手法給演練對象(即本校同仁)。當各單位收件人開啟郵件或點閱郵件所附連結或檔案時，即留下紀錄。針對開啟惡意郵件、點閱惡意郵件連結或檔案之人員需再次進行教育訓練加強宣導，以強化其警覺性。資訊安全已是所有同仁業務不可或缺的一環，請全校同仁一同協助，以確保行政工作之順暢。

- 注意事項

  (1)不要開啟不明信件：開啟信件前，務必先檢視寄件者資料，如有疑問，千萬不要開啟。

  (2)Outlook 使用者請設定郵件軟體安全性為「不要自動下載圖片」。

  (3)Webmail 使用者請進入「個人設定」→「使用環境」→「郵件」→「信件自動預覽」點選關閉，以免不小心按到開啟信件時，會自動下載到有問題的檔案，讓電腦產生安全漏洞。

(4)不點擊不明信件內之連結。

(5)不開啟不明信件的夾檔。

- 測試定義

(1)信件預覽：偵測受測者於收到警覺性測試信件後，預覽信件圖片或內容，因而被記錄者。

(2)連結點選：受測人員點選測試信件中之連結網址或附檔，因而被記錄者。

- 測試信件範例，如下表：

信件類別	信件標題
旅遊圖片類	【HiNet 旅遊網】深度旅遊團 超低價好康！！
生活類	五月報稅天 網路報稅讓麻煩省一半！
健康類	外食族 如何吃得更健康？超商減肥法！
科技類	台灣之光！日內瓦展 我發明奪 42 金 世界第一！
美女類	大陸美女-范冰冰 為了拍 MV 露點也願意！
美容類	完美牙齒整型 五大注意事項

中心服務介紹

1. 103 年度個人資料侵害事故緊急應變作業

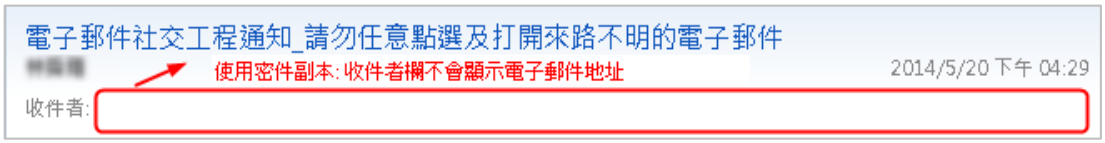
為避免國立中興大學(以下簡稱本校)因遭受個資侵害意外等事件，影響正常作業之運作與本校師生之個人權益，本中心於 103 年 4 月 15 日(星期二)上午進行個資侵害緊急應變模擬演練(圖一)，以提高本校同仁對個人資料安全管理警覺性；並強化熟悉本校之緊急應變程序(如通報應變程序等作業)，使本校之聲譽傷害降至最低、其日常作業能於最短時間內回復正常運作，以維護其作業之順暢與安全。

圖一、個資侵害事故緊急應變作業演練活動

2. 電子郵件密件副本簡介與使用

相信大家曾有過這樣的經驗，在一些朋友轉來轉去的信件中，在「收件者」這欄位一定會看到一些與你不相關的人(圖二)。對於這樣沒有經過自己同意而被公佈電子郵件的行為，在某些情境下，是會造成收信人的困擾，然而很多人卻忽略了這小小的「禮節」。就個資法推行的角度而言，電子郵件帳號足以識別特定自然人之資料，也是所有同仁業務中不可或缺的一環，而上述的情況，其實是可以利用密件副本(BCC)的功能來避免或保護的(圖三)。由於校內群組郵件寄送頻繁，建議寄送群組郵件時，請儘量使用密件副本。

圖二、群組信件寄送時未使用密件副本，收件人資料一覽無遺



圖三、使用密件副本的郵件，收件者欄位將不會看到其它收件者電子郵件地址

一、甚麼是密件副本

密件副本 (Bcc) 是看不見的複寫副本 (blind carbon copy) 之縮寫。如果您將收件者的姓名加入到某份郵件的這個方塊中，則會將一份郵件傳送給該收件者，且郵件的其他收件者看不到此收件者的姓名。

二、密件副本使用原因

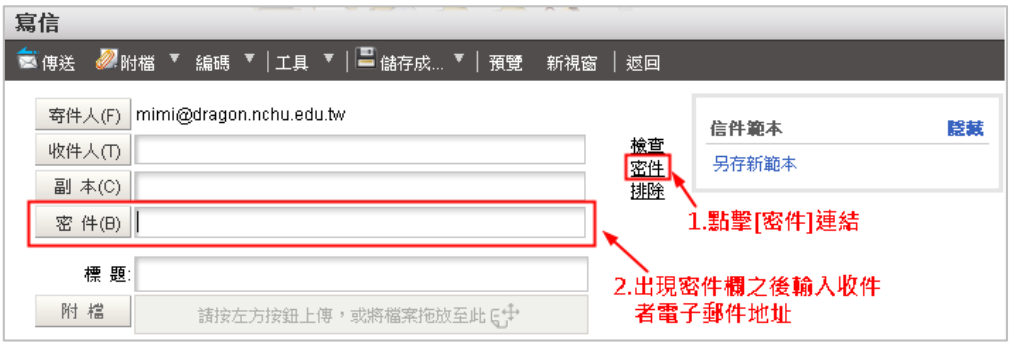
- 保障隱私：對收件者清單保密，但不洩漏他們的身分，[密件副本] 有助於尊重他人隱私。若您對多人傳送郵件或傳送較敏感的郵件時(例：職缺通知或獎懲會議通知)，可以使用 [密件副本]，對潛在收件者做到身分保密。
- 減少垃圾郵件：如果您將收件者名稱列在 [密件副本] 方塊中，隱藏其名稱，沒有人能夠從您的郵件複製收件者的電子郵件地址，進而可減少讓有心者收集、濫用。

三、如何使用密件副本

- 使用本校 Webmail

(1)進入本校電子郵件系統的信件畫面後，點擊[密件]連結

(2)在密件欄中輸入收件者的電子郵件即可

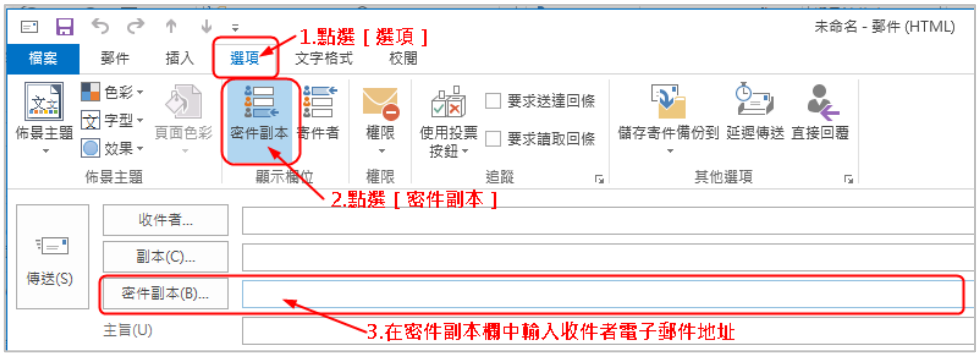


- 使用 Outlook

(1)點選 Outlook 工具列中的[選項]

(2)點擊[密件副本]按鈕

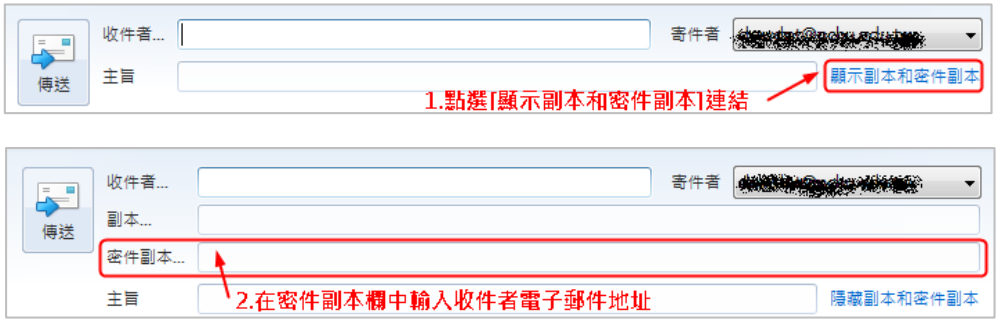
(3)在密件副本欄中輸入收件者電子郵件地址



- 使用 Windows Live Mail

(1)點選主旨欄旁的[顯示副本和密件副本]連結

(2)在密件副本欄中輸入收件者電子郵件地址



資訊新知

1. Adobe Flash 出現漏洞 駭客可遠程操控

IE 才剛爆出漏洞，而今天又有軟體出現了漏洞，這將可能會讓 XP 用戶受到更大的威脅。根據比特網報導，Adobe 公司在星期一表示發現 Flash 的新漏洞，這個漏洞會讓駭客從遠端控 Mac、Windows 及 Linux 系統的電腦，不過 Adobe 公司已經發布了更新版本，建議用戶要立刻更新來修復漏洞問題。

據了解，這次出現漏洞的 Flash 版本有，Windows 的 Adobe Flash Player 13.0.0.182 以及更早的版本、MAC 的 Flash Player 13.0.0.201 和更早版本、Linux Adobe Flash Player 11.2.202.350 和更早版本。而卡巴斯基檢測到因為這個漏洞受感染的案例有 30 多個，受到感染的大多在敘利亞，而這些受到感染的都是使用 Firefox 瀏覽器。

使用 IE 10、IE 11 以及 Chrome 瀏覽器的用戶會獲得自動更新，舊的 IE 或是 Mac OS X、Firefox 的

用戶要透過 Adobe Flash Player 下載中心來更新。提醒大家要去更新，尤其是還在使用 XP 系統的用戶。[聯合新聞網]

影像分享

白鷺鷥初長成@中興湖