國立虎尾科技大學人事服務電子（e）報

111 年 5 月　　國立虎尾科技大學人事室編製

「人事服務電子報」(簡稱人事ｅ報)，內容涵蓋、教職員喜訊、每月新知、法令宣導、人事動態、環保節能、生活知識、各類活動訊息等。各單位如有須同仁瞭解事項，都可透過本報轉知，本報為溝通之橋樑，每月透過電子郵件傳送全體同仁參考，如有任何訊息，歡迎來信提供及指教。(來信信箱：personel@nfu.edu.tw)

壹、 每月新知

一、檢送「公職人員利衝迴避法案例」彙編手冊（如附件），請查照。(111 年 5 月 3 日虎科大人字第 1110004473 號書函)。

二、檢送「教育部及所屬機關（構）學校 111 年度強化公務人員終身學習及專書閱讀推動計畫」1 份，請查照。(111 年 4 月 27 日虎科大人字第 1110004301 號書函)。

三、行政院人事行政總處公務人力發展學院與大學院校簽訂英語學習合作備忘錄，提供公務人員進修語言課程優惠方案，請查照。(111 年 5 月 2 日虎科大人字第 1110004449 號書函)。

四、檢送行政院人事行政總處(以下簡稱人事總處)辦理本(111)年度「新進人員英語力提升研習班」課程表及報名表各 1 份，請查照。(111 年 5 月 18 日虎科大人字第 1110005115 號書函)。

五、本校為配合教育部推動公務人員專書閱讀活動，辦理「逆轉恨意」專書導讀會，請本校同仁踴躍報名參加，請查照。(111 年 5 月 9 日虎科大人字第 1112300253 號書函)。

貳、 人事動態

動情形	服務單位	職稱	姓名	生效日期	備註
新進	電子計算機中心	助理員	雷惠淳	111.05.11	職務代理人.
留職停薪	進修推廣部 推廣教育中心	助理員	許立臻	111.05.02	留職停薪期間 111.05.02-113.05.01.
留職停薪	電子計算機中心 資訊服務組	技術員	許栢誠	111.05.03	留職停薪期間 111.05.03-111

					.08.31.
調任	教學發展中心 (大學社會責任實踐 中心籌備處)	專案助理	張曼萱	111.04.06	1.原教學發展中心策略企劃組專案助理。 2.技專校院高等教育深耕計畫人員."
調任	教學發展中心 (大學社會責任實踐 中心籌備處)	專案助理	林姿伶	111.04.06	1.原藝術中心專案助理。 2.技專校院高等教育深耕計畫人員.
職務變更	電子計算機中心 系統設計組	技術員	蘇煥傑	111.04.29	原電子計算機中心系統設計組專案助理.
辭職	學生事務處 學生輔導諮商中心	專案助理	武逸凡	111.05.01	技專校院高等教育深耕計畫附錄 2 人員.
辭職	學生事務處 學生輔導諮商中心	專業 輔導人員	許英鴻	111.05.13	教育部補助大專校院聘用專兼任專業輔導人員計畫 人員.
資遣	機械與電腦輔助工程系	產學攜手專班約用人員	陳俊亦	111.05.21	
離職	休閒遊憩系	研究組員	黃晨昕	111.05.01	

參、宣導事項：

一、資安相關新聞：

(一)臺灣百貨業者的網站、帳密保護、郵件安全尚待加強

(資料來源:https://cymetrics.io/zh-tw/latest/all/YnCOHBIAACUAMxgO)

最近 3 年受到疫情的衝擊，百貨業者紛紛進行數位轉型，推出電子支付工具與電商網站，但在此同時資訊安全也相形變得更加重要，有資安業者針對臺灣百貨業者進行調查。資安業者 Cymetrics 近日針對臺灣前十大百貨業者檢測資安曝險的情況，結果發現，這些百貨公司的網站普遍出現配置不當，或

是元件沒有即時更新的情況，攻擊者很可能藉由跨網站攻擊繞過相關安全驗證機制，或是利用舊版軟體的已知漏洞入侵。再者，電子郵件安全與帳號保護的部分，也出現仍需加強的情況。研究人員指出，有半數業者疏於電子郵件安全防護，亦有高達 4 家業者曾出現帳號資料外洩的事故，而可能成為攻擊者下手的目標。

(二)駭客藉由 USB 隨身碟散播蠕蟲程式，並濫用威聯通網路設備回傳受害電腦資料(資料來源：https://redcanary.com/blog/raspberry-robin/)

近年來駭客多半透過網路釣魚來投放惡意程式，但濫用 USB 儲存裝置的攻擊手法仍有事故發生。資安業者 Red Canary 揭露自 2021 年 9 月出現的 Raspberry Robin 攻擊行動，駭客利用 USB 儲存裝置散布蠕蟲程式，然後濫用受害電腦的 Windows Installer 處理程序（msiexec.exe）來存取駭客的基礎設施，這些設施多半由威聯通（QNAP）的設備組成，並在發出的 HTTP 請求裡包含了受害者的使用者名稱與電腦名稱。除此之外，駭客也運用洋蔥網路（TOR）的節點來增加 C2 中繼站的數量。

研究人員指出，他們已經在高科技與製造相關產業看到相關攻擊行動，但尚未確認受害組織之間是否存在關連，也無法判斷攻擊者的目的，不過，很可能是為了在受害電腦持續監控，駭客成功入侵後會部署惡意 DLL 程式庫，並透過 Windows 內建的應用程式來側載執行。

(三)駭客濫用 Google 的 SMTP 中繼服務發送釣魚郵件

(資料來源：https://www.avanan.com/blog/the-gmail-smtp-relay-service-exploit)

駭客發動釣魚郵件攻擊的手法，也出現濫用電子郵件服務的現象。資安業者 Avanan 提出警告，他們在 4 月看到攻擊者濫用 Google 的 SMTP 中繼（SMTP Relay）服務情況大幅增加，研究人員在 2 個星期的時間收到 2.7 萬封釣魚郵件，這種郵件透過上述服務寄送，從而隱藏信件的真實來源。

研究人員指出，只要這些採用 Gmail 的組織沒有適當的 DMARC 郵件驗證協定配置，攻擊者就能藉由這種方式，把釣魚郵件送到受害者的信箱。研究人員於 4 月 23 日向 Google 通報駭客的攻擊行動，但 Google 對於此事尚未做出回應。

二、校內資安暨個資保護相關訊息：

(一)因應 Google 所發佈之「Workspace for Education 儲存空間政策異動」，本校教職員工生 Google 帳號空間減縮至3 GB。

(二)111年5月31日前未將用量降至限額(3 GB)下，先將該帳號停權；若申請復權，必須切結在111年6月24日前將用量降至3 GB 內；111年6月27日起，將未申請復權及超額者的帳號刪除。