假郵件，真釣魚!出現「疫情應變計畫」社交工程郵件

根據政院最新一期資安月報，駭客藉台灣疫情嚴峻之際，利用機關郵件伺服器寄送主旨為「傳染性肺炎疫情應變計畫」之社交工程郵件，企圖針對特定機關人員發動魚叉式電子郵件攻擊，以提供疫情應變計畫為由，誘騙收件人開啟惡意郵件附檔。

事件調查後發現，受駭電腦為廠商設備，該廠商使用駐點人員閒置電腦建置視訊環境，因該電腦未執行系統更新與安全檢測等作業，導致存在安全性漏洞遭利用，引發內部主機發動攻擊，幸好相關活動紀錄被即時偵測，沒有發生實質損害。

提醒應避免使用非機關核發之設備，以加強資安管理。並要注意委外廠商建置環境的設備符合機關資安要求，避免個人或廠商的未經管制設備於機關環境中使用。設備也應將作業系統與防毒軟體更新至最新版本，並持續更新修補漏洞，以降低遭外部入侵風險。

文章摘自:資安人

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10017&mod=1