

彰化縣政府教育處 行政公告

承辦人：縣網中心 / 林金玉

受文者：彰化縣立青山國小

公告時間：中華民國113年08月21日 16:27

公告編號：11308184

速別：最速件

主旨：轉知本府政風處通告：請加強防範以「公職人員財產申報」為由之社交工程郵件攻擊

說明：

一、監察院近期發現駭客偽冒監察院名義，以公職人員財產申報為由，寄送含惡意附檔之社交工程釣魚郵件，誘導收件者開啓執行後即會連線至惡意中繼站。

已知攻擊郵件特徵如下，相關受駭偵測指標請參考。

(一)駭客寄送之主旨：「公職人員財產申報表」

(二)惡意附檔名稱：「公職人員財產申報表.rar」

(三)惡意中繼站: 38[.]60[.]198[.]164、tw[.]new-openai[.]com、ngo[.]91newai[.]com、38[.]54[.]50[.]46、154[.]90[.]58[.]189

(四)惡意附檔SHA1雜湊值：10f727be998e8c9c6449de97d1db3ff7d21ddab6

二、請各校提高警覺，如感覺有異請先查證，並避免點擊信件附檔，以免受駭。

註：相關網域名稱為避免誤點觸發連線，故以「[.]」區隔。

三、建議措施：

(一)確實更新防火牆並阻擋惡意中繼站。

(二)請留意相關電子郵件，注意郵件來源正確性，不要點擊不明來源郵件之附檔與連結。

(三)切勿於網頁隨意提供機密資訊，如：公務用電子郵件帳號、密碼、信用卡號碼等，以防個人資料與公務機敏資訊外洩。

(四)安裝防毒軟體並更新至最新病毒碼，開啓檔案前使用防毒軟體掃描郵件附檔，並確認附檔檔案類型，若發現檔案名稱中存在異常字元(如rcs, exe, moc等可執行檔案附檔名的逆排序)，請提高警覺。

(五)加強內部宣導與防範駭客利用電子郵件進行社交工程攻擊。

