大學遭受網路攻擊、正在做反擊

駐芝加哥辦事處教育組

科羅拉多大學博爾德分校日前發生個資遭駭客入侵事件，由於學校拒絕配合駭客勒索條件，數千名學生和員工收到電子郵件通知他們的地址、電話號碼、社會安全碼，學業進展報告和財務文件遭洩，美國各地日前至少 9 所大學的學生和員工也收到了類似的警告。自 2020 年 3 月以來，新冠肺炎爆發後，網路犯罪分子利用疫情狀況加劇他們的威脅，校園網路勒索和勒索軟體攻擊案件持續增加，聯邦調查局自此開始關注追查。目前受此種網路攻擊影響的大學包括：邁阿密大學、馬里蘭大學巴爾地摩分校，耶希瓦大學，哈佛商學院，加州大學戴維斯分校和史丹佛大學醫學院等。

向高等教育機構提供有關網絡安全威脅的建議的全球保險經紀人保羅·B·戴維斯 (Paul B. Davis) 表示遠距教學與工作的迅速轉變讓他們的攻擊目標及攻擊面增大了，自疫情以來，他的客戶受網絡攻擊的數量和嚴重性大幅增加。他說越來越多的機構開始進行遠距工作，但並不是每個機構都擁有合適的管理。科羅拉多大學系統在傳輸包含受隱私法保護的個人身份訊息文件和數據資料時都會採取額外的預防保密措施，但是在一月下旬他們得知他們使用的第三方軟體全球雲端供應商 Accellion 遭到網路駭客入侵。科羅拉多州大學得知後立即關閉其文件傳輸服務作業，並切換到其他工具。

從 Comparitec 網站 2020 年的報告顯示，自 2005 年以來，某些學區和大學遭受了高達 1300 多次數據洩露事件，影響了超過 2450 萬筆紀錄，其中加州和紐約是最大的受害熱門攻擊點。在大學裡，有 43% 的入侵是由於網絡犯罪分子造成的，而另外 27% 的入侵則是在機構意外洩漏訊息時發生的。網絡保險公司 Beazley 負責美國違規回應小組的負責人弗蘭克·奎因 (Frank Quinn) 表示這個問題在去年疫情開始後嚴重更加嚴重，疫情讓這些駭客能夠更輕易的發動網路攻擊。

網絡犯罪分子通過發送看起來非常真實可信的電子郵件，宣傳疫苗或獲得新冠肺炎相關援助的步驟，利用人們對健康和財務的諮訊誘因。奎因說，就算是經過網路安全嚴格訓練的人，當他們在瀏覽手機

上的電子郵件時也並不總是那麼小心。自疫情開始以來，他的客戶的網絡安全保護保險費率已飆升 30% 至 65%。為了馬上就買到保險，大學必須證明他們採取更多的預防措施。

專家提供了一系列技巧及建議，幫助學校防止駭客：

1. 專家說學校應確保對網絡遠距登錄有嚴格保護，詐騙者會不斷掃描網絡，只要一有空隙極有可能遭到入侵。
2. 虛擬專用網絡是阻止入侵者進入的一種方式。
3. 遵循 3-2-1 備份策略：在兩個不同的媒介平台上具有三個資料數據備份，其中一個副本需位於異地媒介平台以進行恢復，並且在平時練習數據恢復。
4. 不要僅僅依靠帳號和密碼，必須使用多重的身份驗證，至少需要兩種身份驗證形式才能登錄。
5. 減少具敏感訊息網站中具高階管理安全權限的人員人數。
6. 持續培訓學生和員工，避免點擊任何疑似網絡攻擊電子郵件

撰稿人/譯稿人：**Katherine Mangan/ Alison Lang**

資料來源：**The Chronicle of Higher Education**