

# 做足防護措施

## 降低電子郵件安全風險



資訊科技辦公室 (ITO) 定期提醒同事們注意資訊科技保安，並頒布了一系列資訊科技相關的政策，亦錄影了相關的培訓視頻。

ITO 過去兩年在不同時間給同事安排了釣魚郵件的測試，每次結果都有進步，這表示同事對釣魚郵件已提高了警覺。

今期將再次提醒大家電子郵件安全的重要性！



電子郵件常被用於傳播惡意軟件、垃圾郵件和網絡釣魚攻擊。大家必須採取安全措施以降低風險。



大家要假設電子郵件不安全，因為可能會被截取。發送敏感信息時，建議將其放入文件中並加密，然後再通過電子郵件發送。一種加密方法是使用 7-Zip 壓縮並加密文件。確保不要將加密密碼與加密文件一起發送，因為密碼也可能被截取。



大家在發送包含敏感信息的電子郵件時應格外小心，以確保目標收件人的電子郵件地址正確無誤。



留意可疑和偽造的電子郵件地址或姓名。確保發件人的電子郵件地址與公司名稱和格式完全匹配。不要點擊電子郵件中嵌入的鏈接。這些鏈接可能指向惡意網站。



掃描所有電子郵件附件以防當中隱藏惡意軟件。



使用複雜的電子郵件帳戶密碼。

### 不要個人化

請勿包含易於猜測的個人信息  
例如姓名和生日，例如：Peter0413

### 多樣化

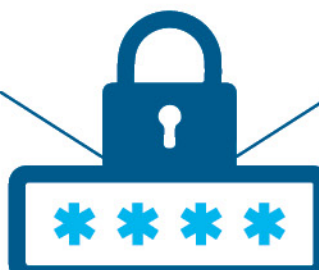
混合大寫字母、小寫字母、數字和符號  
例如：StrOngPa\$\$w@rd3

### 要夠長

建議的最小密碼長度至少  
為 8 個字符

### 特別

每個網站使用不同密碼  
例如：123\_Site.Name\_456



\*\*\*\*