



交通部公路總局臺中區監理所政風室 公務機密維護宣導

近期偽冒政府機關網域發送勒索用戶之詐騙郵件

台灣電腦網路危機處理暨協調中心（下稱 TWCERT/CC）接獲民眾收到勒索郵件的通報，該郵件來源為駭客偽冒政府機關網域發送詐騙郵件。郵件內宣稱駭客已取得用戶電子郵件的訪問權限、於用戶的電子設備植入惡意軟體，並取得用戶所有的通訊與活動紀錄。接著表明擁有用戶的私密影片，若不希望影片外流必須支付特定數量的比特幣，否則將會公開用戶的私密影片至其親友。

提醒民眾，收到此類詐騙郵件請勿匯款，建議先聯繫相關單位進行求證，或是至 TWCERT/CC 官網進行通報。

郵件特徵：

1. 郵件來源為偽冒政府機關網域
2. 郵件內容表示已在用戶的設備植入惡意軟體、取得用戶的電子郵件，以及所有在電腦網路上的活動紀錄。
3. 要求支付特定數量的比特幣至指定帳戶，否則會將私密影片外流。

TWCERT/CC 提供以下防護建議：

1. 建議立即將郵件中提到密碼的系統進行密碼更改，並且定期更換密碼（使用 12 個字元以上之英文、數字與符號混合之密碼）。
2. 不隨意點擊信件中的任意連結、附件或檔案，以避免遭植入惡意軟體。
3. 收到偽冒政府機關網域發送之郵件，建議聯繫相關單位求證，或是撥打 165 反詐騙諮詢專線尋求協助。
4. 至 TWCERT/CC 官網進行資安通報。

資料來源：【台灣電腦網路危機處理暨協調中心】

<https://www.twcert.org.tw/tw/cp-15-6468-eff9b-1.html>