孩童與家庭網路安全

# 網路威脅安全指南

## 網路威脅

所謂網路威脅是指在使用者不知情或未經授權的情況下自行安裝至使用者電腦上的一些惡意程式，其中包括間諜程式、廣告軟體、木馬程式、殭屍程式、電腦病毒及蠕蟲等。這些程式除了利用網路作為其散播、藏匿、自我更新及將所竊取的資料供不法人士使用的工具外，還可以集結在一起從事非法活動，比如說，木馬程式可從網路下載間諜程式，而電腦蠕蟲可利用殭屍程式讓使用者的電腦受到感染。

以下是關於網路威脅的基本定義及其相關安全須知：

| 威脅種類 | 定義 |
|---|---|
| 惡意程式 | 藏匿在用戶端中並在未提示用戶或未經用戶授意的情況下執行惡意運作的程式。 |
| 電腦病毒 | 電腦病毒是一種會進行自我複製的可執行程式，和真實的病毒一樣，其散佈速度非常快。病毒不但會損害用戶電腦、在用戶不知悉的情況下隨意張貼訊息和圖片、損毀電腦檔案、重新格式化硬碟，或是佔據電腦儲存空間及記憶體讓電腦運作速度變慢。 |
| 網路蠕蟲 | 網路蠕蟲是一種具備獨立運作能力的電腦程式，可將其自行複製的程式透過網路連線、電子郵件附加檔或即時通訊(透過檔案分享應用程式)散播至其他電腦系統中與其他惡意程式結合運作。<br>蠕蟲可能阻擋用戶對某些網站的連結，或是竊取用戶電腦中的應用軟體授權碼。 |
| 木馬程式 | 木馬是一種會執行惡意運作但本身並不會進行自我複製的程式。通常它會以看似無害的檔案或應用程式而暗地隱藏惡意程式碼的形式入侵用戶電腦。當木馬被執行後，用戶可能會遭遇電腦系統出現問題，甚至有時候會遺失儲存在電腦中的訊息。 |
| 垃圾郵件 | 垃圾郵件意指任何不請自來、透過電子郵件或即時通訊方式傳送的訊息—為廣告收益用途使用。 |
| 網路釣魚 | 利用電話、電子郵件、即時通訊或傳真獲取用戶個人資料以竊取用戶身分(或錢財)的一種手法。<br>多數的網路釣魚看似具備合法用途，但實際上是設計用來從事不法。 |
| 網址嫁接 | 透過劫持合法網站的網址或是URL連結 - 如www.mybank.com - 將用戶重新導向看似原本正規網站的惡意網站;<br>當使用者連結到該偽網站後，在其不知情的狀況下將被竊取相關個資且可能被用作不法使用。 |
| 間諜程式 | 間諜程式是一種被安裝或執行於用戶端(在使用者不知情的狀況下)以監視、追蹤並提供用戶一切電子活動狀況的程式。<br>通常被夾帶在木馬程式裡或是被當作用戶授權下載的合法軟體的一部分而被安裝於用戶電腦中。<br>間諜程式透過下列方式蒐集用戶資訊:<br>• 鍵盤側錄程式(Keylogger)—該程式可以追蹤使用者鍵盤輸入動作以登錄使用者曾經拜訪過的網站或是竊取帳號密碼。<br>• 螢幕擷取技術(Screen-capture technology)—一種可以定期擷取用戶電腦螢幕畫面並記錄如使用帳號資訊的軟體。<br>• 事件記錄器(Event logger)—用來追蹤用戶所造訪過的網頁或其網路行為。(該資訊通常被當作未來吸引用戶的廣告內容參考) |
| 廣告軟體 | 是一種未經用戶同意主動提供如彈出式廣告或是網頁連結等廣告內容的程式軟體。通常被秘密地夾帶在木馬程式裡或是被當作用戶授權下載的合法軟體之一部分被安裝於用戶電腦中。透過安裝間諜程式於現有用戶端以追蹤用戶上網習慣，廣告軟體可根據所蒐集的資料呈現特別符合該用戶需求的廣告內容。 |
| 殭屍程式/傀儡網路 | Bot為robot機器人的簡稱，藉由木馬程式被秘密的植入用戶電腦中。殭屍操控者(botmaster)可在任何時間內集中操控多個殭屍程式，進行垃圾郵件的散播、啟動網路釣魚或執行拒絕服務程式(DoS)的攻擊，並造成網站運作停擺。傀儡網路乃殭屍程式所組成的網絡，它們通常被用作散發垃圾郵件及發動網路釣魚攻擊的工具。 |
| 商業勒索 | 專為破解加密檔案以進行敲詐的軟體。為取回原有檔案文件，受害者需支付贖金購買解密密碼—他們可以透過如PayPal等網路第三方支付系統支付或是在網路上購買東西(售貨單據將附上密碼) |

Childnet International　commonsense media　ConnectSafely Smart Socializing Starts Here™　TREND MICRO™

以下是確保電腦安全及保護家人免受網路威脅的相關網路安全須知：

## 網路安全須知總覽

1. 保持資安防毒軟體的運作並定期更新，特別是當你在機場、咖啡廳等不安全的無線網路環境中使用筆記型電腦的時候。
2. 不管是上網或是直接下載檔案到電腦中，請務必安裝可提供電腦防護的產品或解決方案，並確保除了電子郵件外，你的網路防護軟體還能提供涵蓋點對點網路及所有家用電腦應用的防護，並且可以提供網路進出流量的即時警告。
3. 採用如網頁信譽評等服務(Web reputation)等最新技術，該技術可在你瀏覽網頁前針對該網頁進行可信度與安全的評量。Web reputation技術結合現有URL網站過濾機制及不間斷的掃描技術。
4. 使用最新的網路瀏覽器版本並安裝最新的安全性修補程式。使用外掛NoScript附加元件的網路瀏覽器。
5. 向網際網路服務供應商(ISP)詢問目前其所提供的網路防護機制。
6. 如果你使用的是微軟視窗作業系統，請啟動自動更新(Automatic Update)功能並執行更新的安裝內容。
7. 隨時安裝、更新並維持防火牆及入侵偵測軟體(包括惡意程式/間諜程式安全防護軟體)的運作。

## 針對電子郵件

1. 確保所有的電子郵件帳號都受到垃圾郵件防護產品的保護。
2. 不管寄件者是誰，請留意那些突如其來或是看似來路不明的電子郵件。千萬不要打開那些電子郵件裡所附加的檔案或連結。
3. 向有關當局呈報可疑的電子郵件活動。
4. 如果寄件者為可信賴的對象，在開啟電子郵件附加檔之前先利用資安產品進行掃描。如果是收到URL連結而該連結不長的話，請在瀏覽器中另行輸入URL字串而不是直接從電子郵件中點取。
5. 當收到電子郵件訊問帳戶資料時(金融機構通常不會透過電子郵件索取相關資訊)要特別留意。
6. 千萬不要利用電子郵件將個人財務資料寄給任何人。

## 關於上網及下載線上程式

1. 利用網頁信譽評等服務以確保所要瀏覽的網頁是不受網路威脅而安全無虞的。
2. 對那些要求下載軟體的網頁須格外當心。利用最新資安軟體針對從網路上所下載的程式進行掃描。
3. 詳讀使用者授權合約(End User License Agreement); 如果除了所需要的軟體外還有其他程式將一起被安裝的話，取消安裝程序。
4. 不要理會未經主動索取而要求個人資料的網頁。只有在瀏覽器下方出現鎖定圖標(lock icon)的網站才可以提供個人資訊。

Childnet International
commonsense media
ConnectSafely Smart Socializing Starts Here
TREND MICRO