

預防病毒與惡性程式碼

1. 什麼是 EICAR ？

EICAR是「歐洲電腦抗毒研究機構」(European Institute for Computer Anti-virus Research)的簡稱。它在科學、研究、發展、實施和管理的領域，為IT保安專家提供一個獨立而公平的平台。它利用一系列的知識資料庫，來制訂最佳做法步驟和說明指南。EICAR的官方網站是 < <http://www.eicar.org> >。

2. 什麼是 WildList ？

肆意傳播表 (Wild List) 是指全球流行的電腦病毒清單。這個清單刊載在肆意傳播表國際組織 (WildList Organisation International)的網站內。這個組織由 Joe Wells 和 Sarah Gordon 在1996年建立。他們與全球抗毒研發隊伍和自願者緊密合作，定期更新清單內容，目的是提供準確、及時和全面的電腦病毒最新的資訊。該組織免費向公眾提供這個肆意傳播表。

3. 有沒有CMOS種類的電腦病毒？

雖然電腦病毒可寫入(及破壞)個人電腦的 CMOS 記憶體，但電腦病毒卻不能「藏」在那裡。惡性程式碼或可會更改 CMOS 的資料，因而導致電腦無法啟動，但它卻無法感染 CMOS 或匿藏在該處。病毒可利用 CMOS 記憶體貯存部分編碼，但貯存在該處的可執行編碼必須先移往電腦的主要記憶體才可執行。迄今尚未發現可把編碼貯存在 CMOS 記憶體內的電腦病毒。有報告稱 AMI BIOS 曾受木馬程式病毒感染。其實，它不是一種病毒；它只是一種不會複製的「惡作劇程式」。這種有害的程式並不是在磁碟上，也不是在 CMOS 內；它只是直接寫入系統上的 BIOS 唯讀記憶體晶片內的編碼。到了每年的十一月十三日，這個程式會終止電腦的啟動過程，並且透過揚聲器播出「Happy Birthday」(生日快樂) 的聲音。

4. 有沒有 BIOS 種類的病毒？

理論上，BIOS 內有可能藏有電腦病毒，並且可在該處被執行。現有的技術已可協助程式把編碼寫入 BIOS 內。當啟動個人電腦時所執行的程式的最初步編碼，便是貯存在基本輸入輸出系內。

有些病毒是可以在BIOS內發作，典型的例子就是 CIH 病毒，又稱為 Chernobyl 或 Spacefiller。

5. 有沒有專門針對流動裝置，比如說手機，的病毒和惡性程式碼？

有的，事實上專門針對流動裝置的病毒和惡性程式碼正在以驚人的速度增長。

可以安裝應用程式的手機很可能遭到病毒或惡性程式碼攻擊。現在已經有少數關於病毒攻擊流動裝置的報導，其中的一個例子就是 Cabir。

在2007年，針對流動裝置的惡性程式碼發展的趨勢的複雜性，抵得上桌面電腦20年來發展的病毒。比如說，已經有木馬程式和病毒可以通過手機來傳播。原因是現有的流動裝置及其操作平台並不支援現有的抗電腦病毒軟件。

6. 資料檔案會受到病毒感染嗎？

純資料檔案是不受病毒和惡性程式碼感染的，但是它們可以感染含有可執行程式碼的資料檔案。例如：有些病毒和惡性程式碼通過文字處理軟件，如 Microsoft Word 和 Adobe PDF 文檔來傳播。

7. 什麼是巨集病毒，它是如何傳播的？

巨集病毒是一種由巨集語言寫的程式，使用在一些軟件應用程式裡（如文字處理軟件、報表等）。巨集病毒為了繁殖，會利用巨集語言的能力把自己從一個受感染的檔轉移到另一個檔。例如，當打開感染巨集病毒的 Word 檔時，通常病毒會複製到 Word 通用範本（典型的是 NORMAL.DOT）中，之後打開或創建的所有檔都將一一遭到感染。巨集病毒由於成爲受感染檔的一個組成部分，所以可以隨文檔轉移，甚至感染其他的文檔。

8. 巨集病毒會造成什麼破壞力？

如所有的電腦病毒一樣，巨集病毒可以破壞資料和文檔。有些案例中，巨集病毒可以重新格式化電腦的硬碟。雖然已知巨集病毒多數沒有很大破壞力，但卻浪費用戶的生產力和時間。

9. 如何減少Word巨集病毒對硬碟及檔案造成的破壞？

你應該定時備份你所有的資料，安裝並啓動即時進行掃描的抗電腦病毒軟件，及使用最新的病毒識別碼和相應的偵測修復軟件，並定期掃描整個系統。

10. Microsoft Access 資料庫也會感染電腦病毒和惡性程式碼嗎？

會，第一隻Access檔巨集病毒JETDB_ACCESS-1會感染Microsoft Access 97 資料庫。當你打開一個受感染的資料庫檔案時，此病毒會開始搜尋並逐一感染現行目錄下，及其父目錄和根目錄下的所有.MDB檔案。

11. 我的電腦會不會因接駁互聯網瀏覽網頁／下載程式而受到電腦病毒和惡性程式碼感染？

如果你有部份的保安修補程式還未安裝，或執行 ActiveX、active scripting 及 JAVA 應用程式，或執行從互聯網下載的程式而這些程式可能已感染病毒，因此，你的電腦也有可能受到感染。

電腦用戶在瀏覽互聯網時，應注意採取以下措施：

- 確保已經為作業系統及電腦上的軟件安裝了最新的保安修補程式。
- 啓動即時進行掃描的抗電腦病毒軟件，及使用最新的病毒識別碼和相應的偵測修復引擎。
- 避免瀏覽可疑／不可信賴的網站。
- 不執行未經辨識的以 ActiveX 技術編寫的指令，或從不可信賴的來源取得的以 ActiveX 技術編寫的指令。
- 可能的話，在瀏覽器的設定中關閉執行 Script 的選項。
- 避免從不可信賴的網站下載程式，因為這樣做電腦會很易受到病毒感染。

12. 電子郵件內容會受病毒感染嗎？

普通電子郵件的內容，如果只有純文字而不含可執行程式碼的話，是不會受到感染的。但嵌入了可執行的HTML格式的電郵，和附加在郵件中的附件都可能受病毒感染。現時大部份抗電腦病毒軟件都可掃描電子郵件及附件。

13. 我收到一個電子郵件，看起來象虛假的新病毒通告，或是一個看起來好得不太真實的促銷廣告，我該怎麼辦？

惡作劇電子郵件是由惡意的個體發出的不真實的謠言、警告、或警報，意圖就是欺騙接收人信以為真的電郵。這些電郵的典型例子包括與新電腦病毒有關的，促銷，或者其它熱門的、吸引他人注意的相關的惡作劇郵件。惡作劇電子郵件通常有以下一個或多個特徵：

- 它們使用技術專業術語和複雜的技術描述；
- 它們要求收信人發送或轉發郵件給他們認識的每個人；
- 它們不包含發信人的資訊，或者使用偽造的發信人資訊。

雖然惡作劇電子郵件不直接傷害電腦，但它們包含不真實的資訊而誤導接收者，甚至引起恐慌。轉發惡作劇電子郵件會消耗網絡和系統資源，並且浪費接收者的時間。

處理互聯網惡作劇電子郵件的適當的方式就是不理會它們。爲了減少傳播互聯網惡作劇電子郵件，請不要：

- 傳播來源不明的消息，除非先確認他們是否可靠的、具有權威性的資訊來源；
- 轉發任何惡作劇電子郵件。

14. 防火牆可否偵測電腦病毒？

防火牆本身不能偵測出電腦病毒和惡性程式碼。但是，因爲防火牆在網絡上的位置是偵測病毒的理想地點，部分防火牆已經設有插入的掃描病毒的程式。此外，亦有部分程式可在防火牆之前或之後的位置偵測病毒。請注意，掃描 FTP 或 HTTP 檔案的工作會耗用大量網絡資源而。防火牆只是其中一個病毒入侵點，病毒還可經由軟磁碟、移動記憶體和電子郵件感染內聯網。

15. 什麼是掃描引擎(Scan Engine)?爲什麼抗電腦病毒軟件除了更新病毒識別碼，還需要更新掃描引擎？

病毒掃描引擎是實際執行掃描工作及偵測病毒的程式，而病毒識別碼是掃描引擎用以識別病毒的「指紋」。推出新版本的掃描引擎有著不同的原因。舊的掃描引擎可能偵測不出新種類的病毒。新版本的掃描引擎會提高掃描表現及偵測率。部分抗電腦病毒軟件製造商在一個檔案裡提供掃描引擎及病毒識別碼的更新程式，另一些則以分開的檔案提供。

16. 在多台電腦的網絡環境中，什麼是最有效的方法去更新病毒識別碼？

替電腦系統和網絡定期地更新最新的病毒識別碼對於有效地偵測和阻擋最新的病毒和它們的變種是非常重要的，特別是在高危害病毒爆發的時候。爲增強病毒識別碼的更新過程，應該考慮在電腦運行時或登錄到網絡伺服器時，自動地更新所有連接網絡的電腦的病毒識別碼。亦可以考慮使用抗電腦病毒軟件製造商的自動更新病毒識別碼系統去進行自動更新。

17. 爲什麼我不能成功清除某些受感染電腦病毒或惡性程式碼感染的檔案？

很可能作業系統或其它程式正在使用你想清除病毒的檔案。最好是以安全模式重新開機，然後用抗電腦病毒軟件或別的清除工具清除病毒。

18. 爲什麼抗電腦病毒軟件能偵測到某些病毒和惡性程式碼，但卻不能清除它們？

抗電腦病毒軟件不單能偵測病毒，亦能偵測其他可能無法清除的惡性程式碼。例如，特洛伊木馬就是應該刪除的，而非嘗試清除的惡性程式碼。在另一些情況下，病毒可能損毀檔案而令它無法復原。不過，這裡有一些指引，可以提高你成功復原檔案的機率：

- 使用最新的病毒識別碼和掃描引擎
- 確保磁碟有足夠的空間
- 參考抗電腦病毒軟件製造商官方網站提供的相關指示，或下載適用的病毒移除工具
- 若果仍告失敗，可獲取病毒樣本及送往抗電腦病毒軟件製造商，以便其作出指引。

19. 在我的部門裏，作為互聯網通訊閘的電腦已經裝了最新的抗電腦病毒軟件。為什麼有些部門電腦還是感染了病毒？

根據以往的經驗，病毒感染大多數與處理電郵時的操作方式，或與資訊科技保安管理方式相關。例如，不難看見一個用戶直接利用辦公室的電腦來存取由外部互聯網供應商或電子郵件服務提供的私人的電郵帳戶。這樣私人的電郵服務可能未通過互聯網集中管理或電郵通訊閘的病毒偵查過程。因此，強烈建議用戶不要在工作時使用私人電子郵件服務。請看相關問題[如果必須在工作環境中使用私人電子郵件，我應該怎麼做?]，以瞭解更多關於在工作環境中使用個人電郵的細節。

另一個原因是直接連接到了辦公室的互聯網服務，例如為個別職員安排的寬頻或撥號調制解調器接入的互聯網服務。這樣病毒就會繞過中央互聯網通訊閘提供的周邊防護措施。職員的筆記本電腦在辦公室之外時感染了病毒，然後回到辦公室環境繼續使用，也是另一個感染源。

另外，有些病毒會利用軟件漏洞，除非應用了對應的最新的保安修正檔才能有效地阻止它。除了上述之外，用戶應時刻保持保安意識，採取最佳的操作方式。當用戶處理文件和電子郵件時，應該保持警惕，不要打開或轉發可疑電郵或他們的附件，這樣就可以減低電腦感染病毒的機會。

20. 從防護病毒的觀點來看，使用中央互聯網通訊閘有什麼優點？

如果從外部互聯網供應商下載的電子郵件內包含病毒，而用戶的工作站並沒有適當的病毒保護措施(即沒有啓動已安裝最新病毒識別碼抗電腦病毒軟件的自動保護功能)，工作站便會容易地受病毒感染。受感染的電腦可能會進一步繼續感染其他網絡上連接的伺服器的檔案和目錄，病毒通過內部網絡傳播，並觸發大規模的電腦病毒感染。部署一個中央互聯網通訊閘是一種有效的解決方案，它能提供額外的病毒防護層，阻攔危險的電子郵件及其附件，例如那些副檔名為.EXE附件。而且，及時和定期的更新最新的病毒識別碼到中央互聯網通訊閘，比設法更新所有用戶的電腦相對更容易，因此它更為可靠和安全。

21. 如果必須在工作環境中使用私人電子郵件，我應該怎麼做？

有時，我們會在辦公室裡的使用私人電子郵件服務。然而這時，最好安裝一台單獨的、沒有連接上網絡的電腦，並使用專門的互聯網去讀取私人電子郵件。另外，這台單獨的電腦應該由安裝了最新的病毒識別碼的抗電腦病毒軟件進行保護。並且先檢查接受到的電子郵件和附件，才讓它們進入到內部系統和網絡。

22. 何謂“仿冒詐騙攻擊”？

仿冒詐騙是是一種社交工程的攻擊，犯罪者利用電子郵件或欺詐網站，引誘毫無戒心的網絡用戶透露私人資料，例如網上銀行之登入名稱和密碼。

23. 什麼是惡性程式碼？

惡性程式碼是會在資訊系統中導致不良結果的程式。**惡性程式碼**的例子包括電腦病毒、網絡蠕蟲、特洛伊木馬、邏輯炸彈、間諜軟件、廣告軟件和後門程式。由於他們對軟件和資訊處理的設施造成嚴重的威脅，必須採取防備措施防止和查出**惡性程式碼**。

24. 什麼是蠕蟲？

蠕蟲是另一種能自行複製和經由網絡擴散的程式。它跟電腦病毒有些不同，電腦病毒通常會專注感染其它程式，但蠕蟲是專注于利用網絡去擴散。從定義上，電腦病毒和蠕蟲是非不可並存的。隨著互聯網的普及，蠕蟲利用電郵系統去複製，例如把自己隱藏於附件並於短時間內電郵予多個用戶。有些蠕蟲(如CodeRed)，更會利用軟件上的漏洞去擴散和進行破壞。

25. 什麼是特洛伊木馬？

特洛伊木馬是一個假裝提供正常功能的程式，但事實上當執行時會進行一些惡性及不正當的活動。特洛伊可用作黑客工具去竊取使用者的密碼資料或破壞硬碟內的程式或資料。與電腦病毒不同，特洛伊並不會複製自己。它的傳播技術通常是誘騙電腦用家把特洛伊木馬植入電腦內，例如通過電郵上的遊戲附件等。

26. 什麼是間諜軟件？

「間諜軟件」是指在未經用戶允許的情況下，就將用戶網上活動的資料秘密地轉送至別人的軟件。這些資料通常被用作市場推廣用途，例如針對用戶的上網習慣和喜好，以彈

出式視窗或垃圾郵件等形式，向用戶發送個人化的廣告。一些間諜軟件也能竊取受害者的文件，甚至獲取敏感和個人資訊。

27. 什麼是廣告軟件？

廣告軟件則會於運行時在螢幕顯示廣告標語，很多廣告軟件同時也是間諜軟件。在許多情況下，免費軟件開發商為用戶免費提供他們的產品時，接受廣告軟件市場贊助，把廣告軟件加入到免費軟件產品中。您應該在安裝任何免費軟件或共用軟件之前仔細地閱讀使用條款。安裝免費軟件和共用軟件時，有可能暗示您同意安裝廣告軟件。

28. 什麼是後門程式？

後門程式是在某一網絡埠聽候命令的惡性程式碼的總稱。多數後門程式包括客戶端和伺服器端。客戶端寄居在攻擊者的遠程電腦裡，伺服器端在受感染的電腦系統中。當客戶端和服務器之間的連接建立時，攻擊者就可控制受感染的電腦。例如，後門程式允許攻擊者監測或從一台受感染的電腦竊取資料，上傳和啟動的病毒或者刪掉用戶資料等等。

29. 什麼是 rootkit？

Rootkit是一種程式／工具，用作奪取系統的根本目錄或管理員身份接達權。Rootkit亦指沒有通過正常授權及／或認證過程的惡意入侵。Rookit可包含後門程式，和攻擊者用來隱藏自己的蹤跡的工具。

30. 什麼是殭屍電腦？

殭屍電腦是指連接互聯網而已經受入侵者、電腦病毒或木馬程式影響的電腦。一般而言，擁有者並不知道該等入侵。該等電腦通常被用作惡意用途，例如在接收遠程指令後作出拒絕服務攻擊。

31. 什麼是殭屍網絡？

殭屍網絡即主機遙距控制殭屍電腦所組成的網絡。

32. 為什麼抗電腦病毒軟件不能修復特洛伊木馬或蠕蟲感染的檔案？

嚴格來說，並沒有「被特洛伊或蠕蟲感染的檔案」。病毒和特洛伊或者蠕蟲之間的一個區別就是病毒將複製自己到一個乾淨的檔案，當受病毒感染的乾淨檔案被執行或被打開時，病毒將感染其他乾淨的檔案。

特洛伊木馬是一種惡性程式碼安裝在受感染的電腦中但並不附在任何檔案上。橫跨網絡傳播的蠕蟲也是一種惡性程式碼，但它並不會複製到一個乾淨的檔案。所以當電腦感染特洛伊或蠕蟲時，沒有可修復的檔案。

33. 什麼是防範仿冒詐騙最好的工具？

為避免被捲入網絡詐騙，請採用以下的一些最佳做法：

- 不要回應電子郵件要求輸入個人資料（如密碼），不要點擊不可信來源和可疑的電子郵件提供的URL連結，這樣，你才能避免被重新定向至看似合法的惡意網站。
- 通過傳統的電子郵件或電話來聯絡網站所屬的組織，如銀行，來驗證該網站的真確性。
- 手動鍵入網址，以到達預期的網站，或使用你之前保存的曾經去過的重要或關鍵網站的書籤。
- 登錄到任何網站，你應定期檢查帳戶狀態和上次登錄時間，確定是否有任何可疑活動。
- 遞交敏感的個人或帳戶資訊給網站時，必須保持警惕。銀行及金融機構很少利用電子郵件問及你的個人或戶口資料。如果有疑問，要諮詢有關的組織。
- 必須確保你的電腦安裝有最新的抗電腦病毒軟件和病毒識別碼。這將減少被受欺詐性電子郵件或攻擊軟件漏洞的網站的影響。這也有助於保護您的電腦機免遭其他安全或病毒攻擊。
- 考慮使用濫發郵件過濾產品，以發現和阻止欺詐性電子郵件，但需要提防假警報。
- 發送任何你收到的網絡仿冒詐騙電子郵件給關組織和/或警方作進一步調查。

34. 怎樣防範電腦變成僵屍電腦？

以下最佳做法可以幫助保護您的電腦避免成爲一部殭屍電腦：

- 在你的電腦裡安裝和使用抗電腦病毒和個人防火牆軟件。
- 更新您的抗電腦病毒軟件，經常更新病毒識別碼。
- 及時更新你的抗電腦病毒軟件，因爲過時的抗電腦病毒軟件對新發現的病毒無效。
- 給你使用的軟件安裝最新的保安修補程式。
- 當你不使用互聯網的時候，斷開你的電腦互聯網接駁。已接駁上互聯網的電腦時刻都有感染病毒的風險，它們被攻擊的可能性更大。

35. 怎樣防範我的電腦感染病毒和惡性程式碼？

必須安裝和使用抗電腦病毒軟件或惡性程式碼的檢測和維修工具。您也可以考慮採取類似的產品應付間諜軟件和廣告軟件。用戶應定期更新病毒識別碼及惡性程式碼定義。更新功能應設置為自動更新，而更新頻率至少須為每日一次。如無法進行自動更新，至少須每週手動更新一次。

此外，用戶應：

- 啟動即時偵測以掃描現行程式、執行程式及正在處理的檔案是否附帶電腦病毒及惡性程式碼。
- 定期對系統進行全面掃描。
- 定期檢討並為作業系統及應用程式安裝最新的保安修補程式。
- 在安裝任何軟件之前，核查軟件是否完整（例如比較校驗和）及確保軟件並無附帶電腦病毒和惡性程式碼。
- 因個人互聯網電子郵件較容易受電腦病毒感染，應避免使用。倘若因業務需要而必須使用個人互聯網電子郵件服務，則應在獨立設置的專用互聯網連接電腦處理這些郵件。
- 應使用主硬磁碟啟動工作站。未經允許不得透過抽取式儲存裝置啟動工作站。
- 定期備份你的電腦資料。

如果你懷疑自己的電腦感染了病毒，你應該停止使用它，因為這可能會散播電腦病毒或惡性程式碼。如果這是你的辦公室的電腦或手提裝置，你要立即向上司和局部區域網/系統管理員通報。

雖然你可以使用抗電腦病毒軟件清除惡性程式碼，它可能無法完全恢復受感染的檔案。你應該從原來的備份系統更換任何受感染的檔案。恢復後，完整的掃描自己的電腦和其他可移動存儲媒介，確保一切病毒或惡性程式碼不再存在。

36. 局部區域網絡／系統管理員應該如何防範電腦網絡感染電腦病毒和惡性程式碼？

局部區域網絡／系統管理員應確保伺服器及工作站均安裝抗電腦病毒軟件或惡性程式碼偵測及修復軟件。電腦病毒識別碼及惡性程式碼定義應配置為自動更新，而更新頻率至少須為每日更新一次。如無法進行自動更新，局部區域網絡／系統管理員應至少每週人手進行更新。

亦應考慮實施以下：

關於網絡方面：

- 安裝抗電腦病毒及內容過濾通訊閘，以掃描所有輸入或輸出的信息／檔案是否含有惡意內容。通訊閘應配置為可阻截、隔離及刪除含有惡意內容的信息或檔案，有關信息或檔案，以及建立審計記錄以供日後參考。
- 定期檢討並為網絡作業系統及通訊閘安裝最新的保安修補程式。
- 就電腦設備及發展中或用以測試的軟件均應採用相同的資訊保安考慮事項及程序。
- 所有電腦須進行全面掃描後，方可接達網絡。

- 於每安裝一台新機器，服務維修和安裝新的軟件後進行全面的系統掃描。

對伺服器端：

- 透過主硬磁碟啟動伺服器。如電腦須透過抽取式儲存媒體啟動（例如 USB Thumbdrive、USB 硬磁碟、唯讀光碟、數碼影像光碟等），在啟動前必須掃描抽取式儲存媒體是否附帶電腦病毒。
- 定期檢討，並從產品供應商的作業系統及應用程式下載最新的保安修補程式。
- 使用接達控制功能保護伺服器的，例如儲存應用程式的目錄應設定為“唯讀”。此外，應按照“需要賦予”原則賦予接達權，尤其是“寫入”及“修改”權。
- 運用文件管理解決方案共用文件，從而減低受感染檔案在不受控制下傳播的機會。
- 在供用戶使用前，應先將所有新安裝的軟件，進行病毒掃描。
- 定期執行全面病毒掃描。
- 定期備份電腦資料。

此外，管理員應透過登記接收保安通知／警告信息取得最新的安全警告信息。他們應該立即向全體用戶轉達關鍵和主要的電腦病毒警報，教導用戶以令其明白大規模的惡性程式碼攻擊的影響，並確保用戶採取最佳的做法以免他們的電腦感染電腦病毒和惡性程式碼。

37. 帶有欺騙特點的群發郵件病毒

37-1. 我聽說過群發郵件病毒和它的欺騙能力，它有什麼特性？

某些電腦病毒能大規模發送感染了病毒的電子郵件。這種病毒通常從受感染的電腦偷取電郵地址（如電郵程式中的地址簿），然後隨機選擇某些電郵地址發送感染了病毒電子郵件。它也能偽裝寄件人和收件人地址。

因此，電子郵件上的寄件人可能不是真正的寄件人。這可以使電子郵件看起來是由另一人發送的，而事實上並非如此。這是一個常見的手法以圖欺騙收件人，並掩飾病毒的來源。

如果你收到此類病毒感染的電子郵件，它意味著你的電郵地址可能是在別人受感染的電腦中被偷取，並且已經在這個過程中傳播受感染的電子郵件。遇到這種情況時，你的電郵地址也可能被利用為偽裝寄件人地址，並發送更多病毒感染的電子郵件到其他用戶。

37-2. 如果我收到群發郵件病毒生成的受病毒感染的電郵，我該怎麼辦？

你應該拒收和刪除這種郵件，不要打開其附件。你應該確保你的電腦有完善的抗電腦病毒保護機制，同時抗電腦病毒軟件安裝了最新的病毒識別碼和偵查修復引擎。除非可以確認受病毒感染的寄件者的電郵地址是真實的，否則不要寄發任何詢問郵件給寄件者，

因為寄件者的地址大多是偽裝的，並且寄件者和受病毒感染的電郵無關。這樣可以避免進一步混亂和多餘的投訴。