第十章
惡意軟件的防護

10.1 學校防範惡意軟件措施

10.1.1 學校須確保伺服器、工作站和流動裝置均採取惡意軟件偵測及修復保護措施。

10.1.2 學校應該設定惡意軟件定義為自動更新，而更新頻率至少每天一次。如無法進行自動更新，技術支援人員應至少每周及在有需要時以手動更新一次。

10.1.3 建議學校購置保安軟件（如惡意程式偵查軟件），以便推行中央管理，即運用指定的控制台管理學校內所有保安軟件。它通常具備遠程更新、政策實施、狀態查詢、報告編製、保安功能等特點，可節省政策／識別碼／更新所需的調配時間、實施統一標準的學校保安政策、協助進行遵行要求評估，以及減輕技術支援人員的工作負擔。

10.1.4 學校應確保所有局部區域網絡伺服器、個人電腦、流動裝置及通過遠程接達連接內部網絡的電腦，都必須開啓抗惡意軟件保護功能。

10.1.5 學校應啓動抗惡意軟件保護程式掃描所有經互聯網輸入的網絡通訊。通訊閘的配置應設定為可阻截、隔離及刪除含有惡意內容的網絡通訊，以及建立審計記錄以供日後參考。

10.1.6 學校應留意如電腦通過抽取式媒體（例如通用串列匯流排閃存盤或硬磁碟、光碟等）啓動，在啓動前必須掃描抽取式媒體是否附帶惡意軟件，這樣可防止伺服器受開機磁區電腦病毒感染。

10.1.7 學校應該考慮使用網頁內容過濾軟件防止人員濫用資源，例如從互聯網下載大量檔案或瀏覽有害網站。這些活動不但消耗頻寬和浪費資源，亦會增加受惡意軟件感染的風險。

10.1.8 技術支援人員和資訊科技負責人應登記接收保安通知／警告訊息，以便盡早取得重要的惡意軟件警報。資訊科技負責人應及時向全體終端用戶轉發保安警報，並採取必要的應變措施。

10.1.9 學校應教導用戶使其明白大規模惡意軟件攻擊的影響、了解惡意軟件的各種感染途徑以免受感染，例如教導用戶一些含有惡意軟件的電子訊息，可能是仿冒其朋友或同事發出的。

10.2 用戶防範惡意軟件措施

10.2.1 用戶應定期更新惡意軟件定義和偵測及修復保護引擎。更新功能應設定為自動更新，而更新頻率至少須為每天一次。如無法進行自動更新（例如不常接達網絡的流動裝置），至少須每周以手動更新一次。

10.2.2 用戶應啓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惡意軟件。此外，根據操作需要定期對系統進行全面掃描。

10.2.3 用戶應避免開啓可疑的電子訊息，不要點擊來源不可信任的劃一資源定位址連結(URL)，以免被引導至惡意網站。用戶在使用前應特別小心檢查附件和下載檔案的檔案類別，包括 “exe”, “bat”, “cmd”, “jar”, “lnk”, “msi”, “inf”, “scf”, “scr”, “pif”, “com” 和 “vbs” 是否附帶惡意軟件。

10.2.4 用戶應在使用前應檢查儲存媒體上及經網絡收到的檔案是否附帶惡意軟件。切勿使用來源不明的儲存媒體和檔案，除非已檢查並清除儲存媒體和檔案中的惡意軟件。

10.3 惡意軟件事故處理和修復

10.3.1 如懷疑電腦感染惡意軟件，用戶應切斷受感染電腦的網絡連線，以免影響網絡磁碟機及其他電腦，並終止一切活動，因為繼續使用懷疑受感染的電腦可能會讓惡意軟件進一步傳播。

10.3.2 用戶應立即向技術支援人員或資訊科技負責人匯報任何懷疑惡意軟件事故。

10.3.3 香港電腦保安事故協調中心（hkcert@hkcert.org）可為學校提供處理惡意軟件事故的技術支援。

10.3.4 用戶亦可在技術支援人員的協助或建議下，使用市面上抗惡意程式的軟件，自行清除惡意軟件。

10.3.5 移除惡意軟件並不代表能夠復原或取回受感染或被刪除的檔案。復原已損壞檔案的最有效方法是以原來的檔案取代已損壞的檔案。因此，檔案應定期備份，而且應保存足夠備份複本，以便在有需要時復原檔案。備份應該處於離線狀態，以確保不會受到惡意軟件的感染。

10.3.6 將電腦中的惡意軟件清除後，用戶應對電腦及其他儲存媒體進行全面掃描，以確保沒有任何惡意軟件。忽略重新掃描電腦這一步驟可能導致電腦再次受惡意軟件感染。

10.4 預防勒索軟件

10.4.1 勒索軟件是一種惡意軟件。電腦罪犯會利用這種軟件把受感染電腦裝置內的檔案鎖上。這些被鎖的檔案就好像人質一樣，受害人如要取回這些資料，便需按照勒索軟件的指示繳付「贖金」，才可把檔案解鎖。

10.4.2 用戶應該留意開啓可疑電郵或當中的附件及超連結、瀏覽包含惡意程式的網站、下載及安裝包含勒索程式的軟件或流動應用程式可能引至感染。

10.4.3 不要開啓可疑的電郵及即時短訊，或當中的附件，例如壓縮檔（zip）或內藏執行檔（exe）和超連結。

10.4.4 用戶不應瀏覽可疑網站，亦不要從可疑網站下載任何檔案。

10.4.5 技術支援人員應該為使用中的軟件安裝最新的修補程式，並檢查及更新抗惡意程式碼軟件及識別碼至最新版本。此外，技術支援人員應該定期全面掃描電腦，以偵測及防預惡意軟件攻擊。

10.4.6 學校應停止或限制使用電腦系統內所有不必要的服務及功能。

10.4.7 技術支援人員應定期把重要資料備份和不要把備份資料連接電腦。

10.5 處理勒索軟件事故和復原

10.5.1 處理受感染的電腦，技術支援人員應：

(a) 切斷受感染電腦的網絡連線，以免影響網絡磁碟機及其他電腦。

(b) 關上電腦的電源，防止勒索軟件把電腦內更多檔案加密。

(c) 記下發現有關事件前曾經進行的電腦操作，例如使用過的程式和檔案、開啓過的電郵及瀏覽過的網站。

(d) 向香港電腦保安事故協調中心和香港警務處舉報有關罪行。

(e) 從備份復原數據至未受感染的電腦裝置。