保安資訊有限公司 408 台中市南屯區三和街 150 號 1 樓
http://www.savetime.com.tw/ 電話：886-4-23815000 傳真：886-4-23813000

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊-資訊安全考題-端點安全篇(含解答)

壹、選擇題：

（ ）1. 請問以下那一種居家安全防護方式較安全?

(A) 門窗都沒鎖，任由所有人進出。等到壞人嘗試要破壞或偷竊時才叫家人一起來抓壞人。

(B) 門窗上鎖，只有有鑰匙的人才能進來。

(C) 門窗上鎖、加上鐵窗並加裝保全系統，即使有鑰匙及磁卡，也未必能進來。並且在室內也裝監視器，以監視所有的狀況，並且在鄰近的所有進出道路都設有檢查哨，所有進出的人車都需符合安全規定(例如，不能是通緝犯、車上不能載有危險物品、甚至只有特定的人車才能進出)。

【解析】正確答案是(C)。答案A可以說是只有在陶淵明的桃花源記才存在的情形，現實生活中也有，像居住在孤島或人煙稀少的深山中但畢竟是少數。答案B是有比A安全，但現在的小偷或強盜，所使用的破壞工具已進步到屋主在屋內都發現不到壞人已經進來了。答案C是非常安全的，比總統府還安全。除了人車管制外，多重的檢查哨，讓壞人跟本一點機會都沒有。而且所有人員的一舉一動都被監控，就是要發生荊軻刺秦王的事件也不可能。

（ ）2. 請問以下電腦安全防護較安全？

(A) 在所有的端點電腦安裝防毒系統並隨時更新病毒定義檔及掃描引擎。

(B) 在所有的端點電腦安裝防毒系統並隨時更新病毒定義檔及掃描引擎、安裝個人防火牆並隨時保持最新的作業系統的修正更新。

(C) 在所有的端點電腦安裝防毒系統並隨時更新病毒定義檔及掃描引擎、安裝最先進的個人防火牆、端點的入侵防禦系統及網路存取控制技術並隨時保持最新的作業系統的修正更新。並且執行『安全政策保證系統』-以提供作業系統、記憶體威脅、周邊裝置控管、檔案及登錄檔保護、應用程式控管過濾….等多項保護，讓只有安全的端點電腦才能存取網路以避免產生內部/對外攻擊。

【解析】正確答案是(C)。答案A可以提供最基本的安全保護，只要您的電腦不要上到惡意網站、不要接收惡意的郵件、不要存取不安全的隨身碟/光碟/磁碟片、不要下載不安全的檔案，這樣A的方案，一定是夠安全的。現實社會中，不上網的電腦很少、有能力判斷問題網站的人非常少、不與人交換檔案的更少。防毒軟體的運作原理是透過病毒定義檔的更新以偵測已經被發現的已知病毒及透過掃描引擎的啟發性技術(行為模式)來偵測未知的病毒，但後者較易產生誤判而產生副作用(如誤刪檔案或無法開機)、前者需要有人中毒並把病毒樣本遞交給防毒公司，防毒公司才能透過自動化或專業人員的分析來遞交解藥(也就是病毒定義檔的更新)。現在病毒變種及擴散的速度比防毒公司提供解藥的速度還要快，所以只安裝防毒軟體是不夠的，單獨的防毒軟體

只能清除已經進入電腦系統的病毒並不能防止病毒進入電腦系統。答案B當然比A要安全許多，它不但可以清除病毒也能防止病毒不要進來電腦系統內。但使用者的疏忽行為，例如使用簡單的密碼或根本就沒有密碼，就如同把鑰匙插在門鎖上。瀏覽有問題的網站或接收到有問題的郵件而被植入木馬程式、後門程式、間諜程式或成爲殭屍網路的一員，隨時啟動沒有設定或薄弱的密碼遠端遙控軟體(如VNC)。就如同鐵門深鎖但被挖空了一個隱形的後門而不自知。答案C是最安全的解決方案。除有A與B的入門級與中階的防護外，更能保護並自我強制電腦系統的完整性，規範電腦系統內可以執行的程式與可接受的行為、周邊裝置的存取控制，即使病毒進來也不讓它發作，即使被植入木馬或後門也能阻檔對外的網路存取。所以它的運作原理是-只有安全的電腦才能存取被規範的安全網路存取。

（　　）3. 下列的解決方案中。那幾種組合可以提供電腦最高的安全防護等級？-複選題。

(A) 賽門鐵克企業防毒系統-工作站及伺服主機版本(Symantec Antivirus Corporate Edition –Workstation & Server-台灣地區稱企業防毒完整組合 B)。

(B) 賽門鐵克用戶安全解決方案(Symantec™ Client Security-台灣地區也有人稱網路安全大師企業版)。

(C) 賽門鐵克企業安全防護解決方案(Symantec™ Sygate™ Enterprise Protection)與網路存取控制(Symantec™ Network Access Control)及隨選安全解決方案(Symantec™ On-Demand Protection Solution)。

【解析】正確答案是(A+C)或(B+C)。但考量建置成本-(A+C)應該是比較有利的。因為A與B的防毒系統與管控機制及介面完全一樣，B內建的防火牆及入侵防護屬於中階功能，C在這兩個元件都屬於業界最高級的。當然C還包含政策強制執行與自我強化的功能。簡單而言，A可以偵測並清除已經進來電腦系統的病毒，B除有A的功能外，更能防護病毒不要進入電腦系統，C則是防護病毒不能進入網路。許多電腦在單機模式完全掃描不到病毒，但只要一啟動網路功能或上網，防毒系統就馬上彈跳出偵測到病毒，而且無法清除，有很高的比例是來是網路芳鄰或遠端電腦的攻擊(或下載)。此時只要啟動設定個人防火牆的規則，都能降低這個威脅。

賽門鐵克的企業防毒系統的市佔率是全世界第一名的，技術也是最先進的。例如，它是最早導入人工智慧的啟發性偵測專利技術- Blood-hound 的廠商，擁有全世界最多的病毒研究及回應中心-遍及多數地區，能提供全天24小時最快速的威脅回應及因應地區型的攻擊。主動偵測收集散佈於網際網路上的不正常網路行為，能先行取得抑制病毒發作的先機。透過為數最多的用戶後送的病毒樣本，並來自於全球最大的垃圾郵件監控網(BLOC)可以最快獲得新型病毒及釣魚郵件的樣

本。由於能最快取得真實病毒的樣本，所以賽門鐵克的防毒系統以誤判率最低並能偵測到最多真實環境的病毒而廣受企業用戶歡迎，其它業者由於規模較小，無法像賽門鐵克一樣有這麼強的後端收集樣本與快速研發回應的能力，所以採用較高比例的啟發性偵測技術(行為模式偵測)，號稱能偵測到最新的病毒，然因誤判率較高，往往將正常的檔案清除而讓電腦無法開機或刪除重要的檔案，同時也佔用較多的資源而影響電腦的效能。

以上的A方案，適合於清除一般的電腦病毒，如果是漏洞型的病毒則建議採用選項B的方案，近來所有防毒軟體都束手無策的目標型攻擊、間諜程式、後門程式、殭屍病毒則需要由前二者搭配C方案來解決，都有令人非常滿意的效益。

在併購Sygate後，更擁有全世界最好的端點防火牆及入侵防禦技術，更是網路存取控制的技術制定者，安全政策的強制，自我防禦機制，更把電腦的安全等級有被動回應提升為真正的主動防禦。

如果您面臨一直無法徹底解決的電腦病毒(PCVirus)問題，可以尋求保安資訊的協助。他們有最豐富的病毒危機化險為夷的成功經驗，他們有完整的成功導入不同防護層級及因環境不同的最佳化經驗，專業於病毒防護有十年以上的經驗。是台灣地區商譽卓越的績優服務廠商。相關資訊可上網:www.savetime.com.tw(好記:幫您節省時間.的公司.在台灣)。