保護你的個人電腦

Windows 用戶

1. 使用嚴謹的帳戶密碼
2. 設置標準使用者帳戶作日常使用
3. 關閉訪客帳戶
4. 啟用有密碼保護的屏幕保護程式
5. 使用最新的抗惡意程式碼保安軟件
6. 使用個人防火牆
7. 更新作業系統、應用程式和瀏覽器
8. 為瀏覽器作基本保安設定
9. 定期備份數據
10. 棄置或轉售裝置前要徹底刪除數據

目 錄

1 使用嚴謹的帳戶密碼

風險

由於簡單密碼容易被破解，這增加了電腦被未經授權存取的機會。

檢查步驟

可用的工具

功能：幫助用戶學習如何選擇嚴謹的密碼。

- Kaspersky Secure Password Check (只提供英文版)
- Intel Grade My Password

系統設定

目的：建立 / 更改你的電腦登入密碼，及檢查有否執行嚴謹的密碼政策。

- 如何使用密碼保護電腦。

- 如何變更 Windows 密碼。

- 如何變更密碼原則設定。

更多提示

✓ 定期更換密碼並應選取一些自己容易記得但別人難以猜破的密碼。

✓ 不應使用舊密碼，亦不應將寫下來的密碼放在電腦附近。請瀏覽資訊安全網了解更多處理帳戶及密碼的良好守則。

2  設置標準使用者帳戶作日常使用

風險 

惡意軟件可以感染電腦，利用已登入用戶的權限作惡意活動。

檢查步驟

系統設定

目的：為你的電腦建立標準使用者帳戶，及變更使用者帳戶的管理員權限。

- 如何建立使用者帳戶。
- 如何變更使用者的帳戶類型。

更多提示

✓ 應在有需要時才使用系統管理員帳戶，如管理其他使用者帳戶、安裝或移除軟件或更改系統的安全設定等。

✓ 不同的帳戶應使用不同的登入密碼，特別是用於處理私人和敏感資料的帳戶。

3 關閉訪客帳戶

風險

電腦的訪客帳戶提供資訊給攻擊者，因而增加保安風險。

檢查步驟

系統設定

目的：關閉電腦的訪客帳戶。

- 如何開啟或關閉訪客帳戶。

更多提示

✓ 由於訪客帳戶允許用戶進行網絡登入、瀏覽互聯網以及把電腦關閉，使用訪客帳戶前應評估保安風險。

✓ 使用訪客帳戶前應先為帳戶設定密碼，因為預設的訪客帳戶是無需使用密碼登入。

4  啟用有密碼保護的屏幕保護程式

風險 

無人看管的電腦容易被未經授權存取系統。

檢查步驟

系統設定

目的：啟用密碼式屏幕保護。

- 如何開啟或關閉屏幕保護裝置。
- 如何使用您的 Windows 密碼做為屏幕保護裝置密碼。

更多提示

✓ 在任何時候都應該啟動有密碼保護的屏幕保護程式，並不要讓你的電腦變成無人看管，特別是身處於公眾場所。

✓ 屏幕保護程式一般預設在用戶離開電腦15分鐘之後自動啟動，然而將時間設得更短可起更好的保安作用。

5 使用最新的抗惡意程式碼保安軟件

風險

你的電腦會受病毒、木馬程式和其他惡意軟件攻擊，因而導致數據和財務損失。

檢查步驟

可用的工具

功能：偵測惡意軟件攻擊你和為被感染的電腦清除惡意軟件。

- Windows Defender (Windows 8內置軟件)
- Microsoft Security Essentials (Windows 7 and Vista適用)
- BitDefender QuickScan（只提供英文版）
- TrendMicro HouseCall（只提供英文版）
- 其他抗惡意程式碼保安軟件

系統設定

目的：檢查你的電腦是否受最新的抗惡意程式碼保安軟件保護。

- 如何知道我的電腦已安裝抗惡意程式碼保安軟件。（只提供英文版）
- 如何讓 Windows Defender 定義維持在最新狀態。
- 如何設定 Windows Defender 掃描電腦的時間。

注意：請留意設定保安功能的確實步驟會因不同產品而有所不同，因此建議用戶應盡可能按照官方的用戶手冊內的指示進行設定。

更多提示

- ✓ 應為抗惡意程式碼軟件啟動自動更新功能，以確保抗惡意程式碼軟件本身及其定義檔都是最新的版本。
- ✓ 啟動實時保護功能並定期為你的電腦進行全面掃描，如每週一次。
- ✓ 時刻保持警覺，若發現流動裝置的如電池很快耗盡、速度變慢及不尋常地使用大量數據，此等徵兆表示流動裝置可能已被惡意軟件所感染。
- ✓ 要小心提防假冒的防惡意軟件及虛假的彈出保安警告，它們都是誘騙用戶下載惡意軟件到電腦的常見手法。

6 使用個人防火牆

風險

與網絡連接的電腦能被攻擊者遙距探測、掃描、連接並發送用戶數據到外部伺服器，因而容易受到網絡攻擊。

檢查步驟

可用的工具

功能：為你的電腦啟用防火牆保護。

- Windows 防火牆（Windows 內置軟件）
- Comodo Free Firewall（只提供英文版）
- ZoneAlarm Free Firewall（只提供英文版）

系統設定

目的：檢查Windows防火牆是否已被啟用及驗證防火牆規則。

- 如何檢查Windows防火牆是否已被啟用。
- 如何允許程式 / 限制程式通過 Windows 防火牆進行通訊。

更多提示

✓ 在任何時候都應該啟動個人防火牆，特別是當需要連接到互聯網。

✓ 應該啟動家用路由器的內建防火牆功能，以進一步保護你電腦及家用網絡，免受網絡攻擊。

7 更新作業系統、應用程式和瀏覽器

風險

有已知保安漏洞的電腦，特別是與互聯網連接的電腦，更容易遭到惡意軟件感染和網絡攻擊。

檢查步驟

可用的工具

功能：偵測過時的軟件、瀏覽器和插件。

- Check and Secure website（偵測過時的瀏覽器和插件）
- Qualys Browser Check（偵測過時的瀏覽器和插件）
- Windows Baseline Security Analyser（偵測過時的作業系統和應用程式）
- Nessus Vulnerability Scanner（試用版）（偵測過時的作業系統和應用程式）

系統設定

目的：檢查你電腦的Windows作業系統和其他Microsoft產品是否在最新狀態，並取得最新的保安更新程式。

- 驗證你的電腦是否已在最新狀態。
- 如何取得最新的保安更新程式。

更多提示

✓ 為軟件產品啟用自動更新功能，並切記要重啟你的電腦，才能完成整個更新安裝過程。

✓ 移除過時軟件產品，或升級軟件產品以保證繼續有安全更新的支援。應避免使用沒有安全更新的電腦進行涉及敏感資料的活動，例如網上銀行。

8 為瀏覽器作基本保安設定

風險

預設的瀏覽器設定可能導致用戶在不知情的情況下允許執行惡意程式碼及暫存敏感資料和密碼。

檢查步驟

系統設定

目的：檢查瀏覽器是否已採用基本保安設定。

- 如何保護你的 Internet Explorer, Mozilla Firefox 及 Safari 瀏覽器。（只提供英文版）
- 如何保護你的Chrome瀏覽器 – 網絡釣魚與惡意軟體警示、管理你的網站密碼、允許或限制外掛程式, 刪除暫存資料和停用自動填入表單功能。

更多提示

✓ 不要登入可疑網站，或連接這類網站提供的連結。因為這些網站可能會導致電腦被惡意軟件感染，同時瀏覽器亦可能會在用戶不知情的情況下被強制下載檔案。

✓ 使用應用程式後應刪除瀏覽器內的暫存記憶檔，特別是在進行涉及敏感資料的活動之後，例如網上銀行。

9  定期備份數據

風險 

在受惡意軟件感染、硬件故障和裝置遺失的情況下，數據無法復原。

檢查步驟

系統設定

目的：備份和復原檔案和完整的系統。

- 如何備份檔案。
- 如何從備份復原檔案。
- 如何建立系統映像備份。
- 如何從系統映像備份復原電腦。.

更多提示

✓ 定期進行備份，並小心保護備份數據。

✓ 測試復原程序，以確保已備份數據可以復原。

✓ 將資料同步至雲端服務前應評估保安風險，並應避免將敏感資料自動備份至雲端平台上。

✓ 應盡可能使用嚴謹的密碼及認證方式，例如雙重認證，保護你的網上帳戶，特別是用作資料備份的雲端服務帳戶。請瀏覽資訊安全網了解更多處理帳戶及密碼的良好守則。

10 棄置或轉售裝置前要徹底刪除數據

風險

裝置內的數據即使已被刪除，仍有可能透過復原軟件工具將數據復原，以致有資料外泄風險。

檢查步驟

可用的工具

功能：徹底刪除電腦中的硬碟（包括固態硬碟（SSD））內的數據，即使透過復原軟件工具亦不能將已刪除的資料還原。

以下的工具可以徹底刪除磁碟內的數據：

- Darik's Boot and Nuke (DBAN) （只提供英文版）
- Windows Sysinternals – SDelete
- Eraser（只提供英文版）

以下的工具可以徹底刪除固態硬碟內的數據：

- ATA Secure Erase（只提供英文版）
- Secure Erase (HDDErase) （只提供英文版）
- Intel SSD Pro 管理工具（只技援 Intel 固態硬碟）
- SanDisk SSD Dashboard 儀表盤（只技援 SanDisk 固態硬碟）

注意：

- 市場上的一些數據刪除軟件，可以徹底刪除整個或部份硬碟空間。在刪除硬碟前，請詳細閱讀軟件內的授權協議和說明。
- 部份固態硬碟供應商提供了詳細的步驟/工具進行徹底刪除。不同廠商的刪除步驟/工具或會不同，建議你聯絡產品供應商了解技術細節。

更多提示

✓ 硬碟經過徹底刪除後，數據再也不能恢復，如有數據需要保留，在刪除數據前備份資料。

✓ 請瀏覽資訊安全網了解更多棄置處理敏感性資訊的電腦設備的選擇。

✓ 盡快為新的硬碟開啟系統內的全面硬碟加密功能（例如 BitLocker），並選用一個嚴謹的密碼，以保護數據。

✓ 即使Microsoft Windows的版本並不提供全面硬碟加密功能，亦應使用其他合適軟件為敏感數據進行加密，並選用一個嚴謹的密碼，以保護數據。

免責聲明

這部份所提及的保安檢查設定，旨在主動和針對性地提高流動裝置的安全性，但同時可能會改變用戶體驗，亦有可能會影響到一些應用程式的功能和效用。在保安檢查過程當中所提及到的安全設定，其確實的設定步驟會因不同產品而有所不同，因此建議用戶應盡可能按照用戶手冊內的指示進行設定，生產商的官方網站一般都會提供用戶手冊以便用戶下載。

用戶亦應留意網絡安全資訊站中的重要事項。在下載及使用保安軟件或工具前，請細閱相關的用戶協議和私隱政策。