

互聯網安全介紹

讓我們確保您能夠安全地使用互聯網。

電腦和電郵保安

一些主要網絡風險包括：

- **病毒**，通過互聯網從電腦傳播到另一部電腦，有些病毒只是普通的滋擾，其他則可能會刪除您的數據。
- **木馬病毒**，偽裝成正常的程式，意圖欺騙您安裝。
- **間諜軟體**，竊取密碼或銀行賬戶資料等程式。

您可以採取以下步驟來保護自己和您的電腦抵禦線上威脅的攻擊。

1. 使用**防病毒軟件**，有助於找出、中止和刪除病毒。
2. 使用**反間諜軟件**，有助於阻止您的數據被盜。
3. 使用**防火牆**，有助於保護您的電腦免受互聯網上未經授權的網站入侵。
4. 不時更新您的互聯網保安軟件。
5. 如果您新買的電腦內設置了防病毒軟件，請在試用期完畢後進行更新，或下載AVG 等免費軟件。Windows 10 一般附帶了防病毒軟件Windows Defender。因此，Windows 會為您保持更新。
6. 如果您不肯定，請登入<https://www.staysmartonline.gov.au/> 網站尋找建議。

互聯網安全介紹

您應該格外小心，留意您的電腦是否受惡意軟體攻擊。

1. 在打開電郵之前，請先考慮一下，特別是那些由您不認識的人寄出的電郵附件。
2. 在網上購物之前，最好先了解有關該公司的資料，與那些有良好聲譽的網絡商店交易比較安心。
3. 定期備份您電腦上的所有資料，要是您的電腦受到病毒感染，您仍然可以找回所有重要數據。



保護自己和您的電腦抵禦線上威脅的攻擊

在互聯網上提供個人資料

當您需要在網上提供個人資料，您應當知道分享資料的限制，並要清楚自己的權利。

- 只能在正當合法的公司要求下驗證您的身份時才提供資料。
- 避免把將個人資料（出生日期，住址等）張貼在 Facebook 等社交網站的公共論壇上。犯罪分子會使用您的個人資料進行身份盜用。
- 澳洲的《1988年私隱法》管制私營公司使用個人資料的程序。
- 《資訊自由法》適用於您向政府機構提供的資料。
- 有信譽的公司均有處理個人資料的政策。請登入他們的網站閱讀私隱政策。
- 有關消費者權益的更多資料或有關保護您免受詐騙的最新信息，請瀏覽 ACCC 的網頁：<https://www.accc.gov.au/consumers>。



法律管制私營公司使用個人資料的程序

互聯網安全介紹

在線付款和安全區域

網上購物可以很方便，以下有一些快捷檢測步驟來確保您安全地付款。

1. 您所交易的公司是否有良好的聲譽？在其網站上查核該公司的私隱和退貨政策。並使用搜尋引擎去了解更多有關該公司的資料。
2. 使用信用卡或PayPal購物，兩者均有提供一些對買家的保障。
3. 在輸入您的信用卡資料前，請查看瀏覽器的網址欄。安全的網站應有顯示一個掛鎖符號，網站應該以**https:** 開頭，而不是**http :**。



上網分享資料時請小心

兒童上網安全

兒童經歷淺，因此存在的風險較大：

- 看色情網站。
- 披露個人資料。
- 受到欺凌和騷擾。

互聯網聊天室和社交媒體是別人可接近您的地方。不要讓您的孩子與任何在網上認識‘見面’的人會面，除非有成人的陪同下。

這些保護措施可以讓您幫助孩子安全地上網。

1. 為孩子設立自己的用戶賬戶。
2. 開啟該用戶賬戶的家長監控模式。
3. 在Google網絡瀏覽器中把**安全搜尋**設置啟動，在Bing或Yahoo網絡瀏覽器中把安全搜尋設置轉為‘嚴格’。
4. 將YouTube的設置設為‘限制’，其他的視頻網絡也同樣。
5. 與您的孩子談及他們可能在網上遇到的危險。

如果發現有兒童在網上遇到危險時，請登入

<https://www.esafety.gov.au/complaints-and-reporting>向eSafety專員辦公室報告。