



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre



如何安全使用互聯網

年長者指南

cyber.gov.au

序言

上網能讓你同朋友和家人保持聯絡，
瞭解一些話題，甚至能玩遊戲。

就像開車前係好安全帶一樣，在使用互聯網之前你也應該採取幾個步驟保證安全。

澳大利亞網路安全中心(ACSC) 希望確保所有人都能安全上網。本手冊包含一些基本的網路安全措施，你可以在上網時用這些措施保護自己。



作為Australian Signals Directorate (ASD) 的下屬機構，澳大利亞網路安全中心 (ACSC) 提供網路安全建議、協助和操作回應措施，以防止、檢測和補救對澳大利亞的網路威脅。ACSC的目標是幫助澳洲成為網路安全度最高的地方。訪問[cyber.gov.au](https://www.cyber.gov.au)獲取更多網路安全資訊、指南和建議

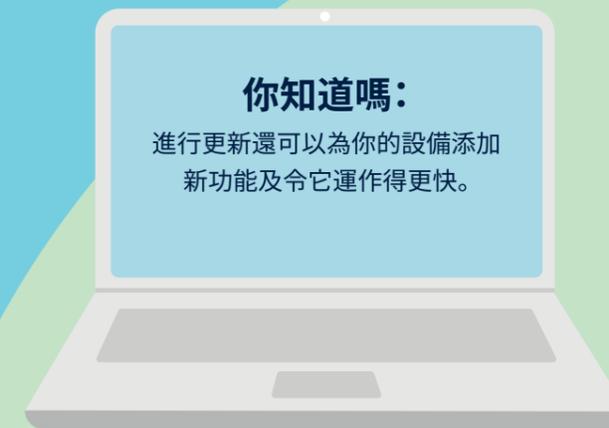
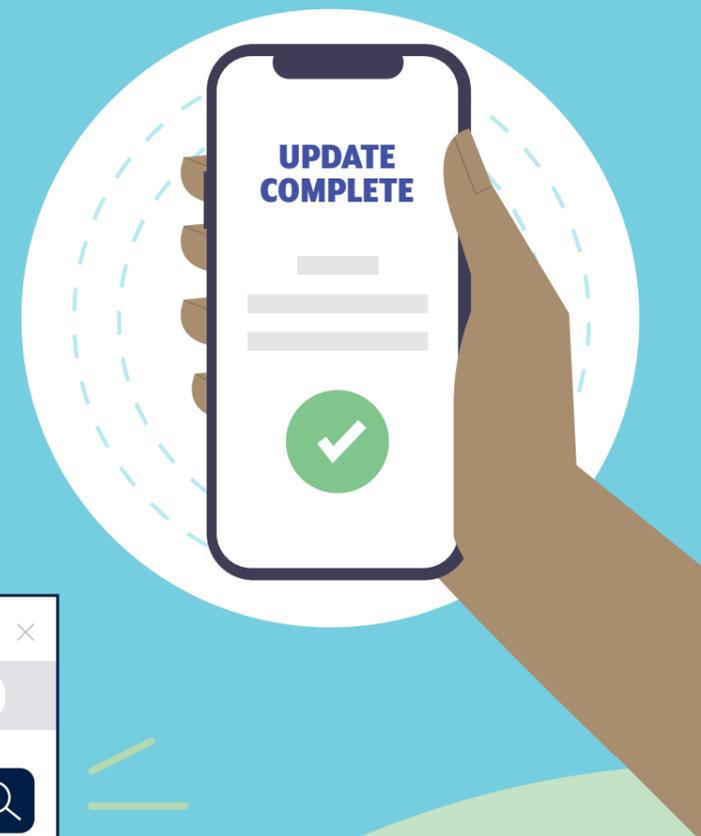
年長者網路安全

▶ 貼士1:更新你的設備

更新您的軟體就像保養你的車輛一樣。它能提高你的設備性能，令其更加安全。

網路罪犯總是在尋找新方法入侵他人的設備。在設備上設置自動安裝更新能夠彌補軟體的任何弱點，讓駭客們無從下手。

若要查找更多資訊，請在 [cyber.gov.au](https://www.cyber.gov.au) 搜尋‘Updates’ (更新)。



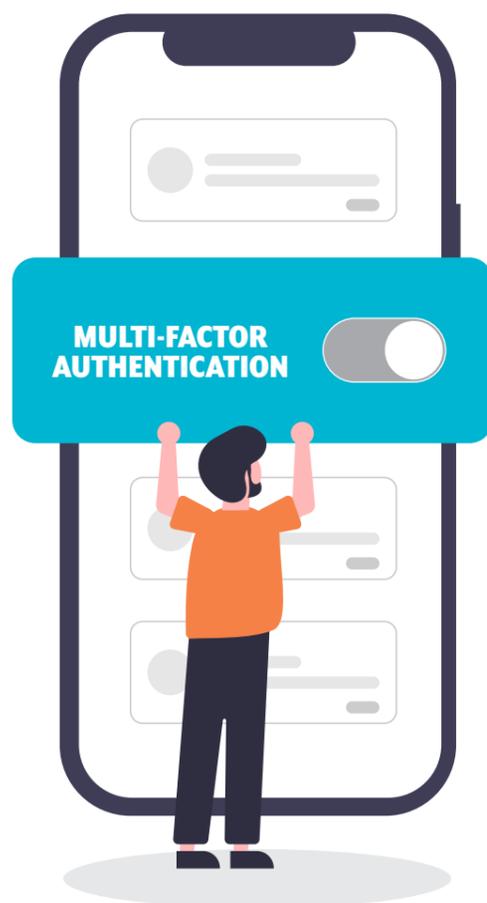
貼士2: 開啟多重身份認證

你賬戶的多重身份認證就像是你家裡的防盜網一樣。它阻止試圖闖入的罪犯從而給你保護。

多重身份驗證開啟後, 你需要提供多種資訊才能登入你的賬戶。例如, 你可能需要一個短訊密碼和你自己的密碼來登入你的社交媒體賬戶。

多重保護增加了罪犯入侵的難度。他們也許能破解一部分, 例如你的密碼, 但他們仍然需要獲得拼圖的其他部分才能進入你的賬戶。

若要查找更多資訊, 請在 [cyber.gov.au](https://www.cyber.gov.au) 搜尋 'Multi-factor authentication' (多重身份認證) 或 'MFA'。



請記住:

如果你需要幫助來開啟多重身份認證, 向家人和朋友求助。

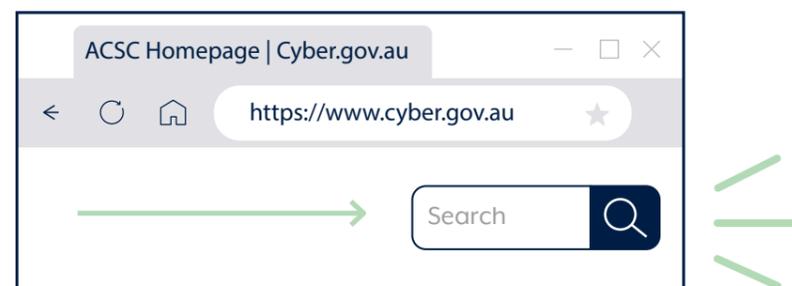
貼士3: 備份你的設備

執行'備份'是製作重要文件的副本並將其存放在安全的地方。這就像是複印珍貴照片後將其存放在保險箱裡, 以免日後原件丟失。

當你備份電腦、手機或平板設備時, 你的文件副本會被存放在網上或另一個設備上。備份重要文件和珍貴照片後你會感到高枕無憂。

如果你的設備出現問題或被駭客入侵, 你能夠輕鬆地從備份中恢復文件。

若要查找更多資訊, 請在 [cyber.gov.au](https://www.cyber.gov.au) 搜尋 'Backups' (備份)。



你知道嗎:

定期備份你的設備 意味著你 始終可以使用你最新的文件

貼士4: 設置短語密碼

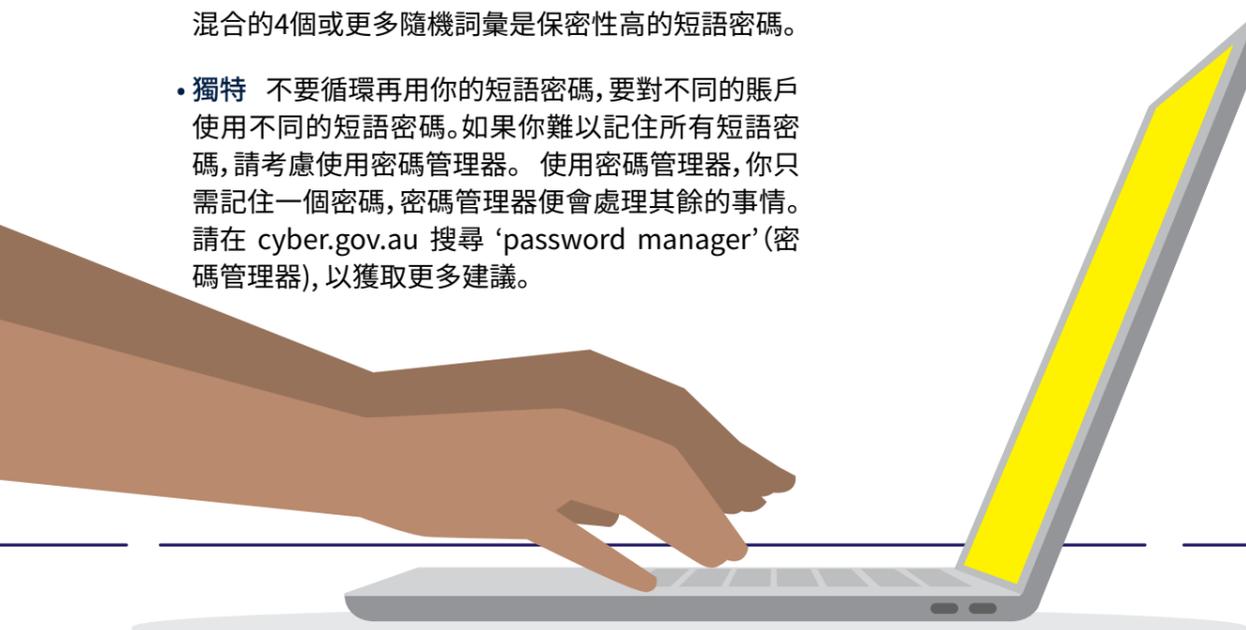
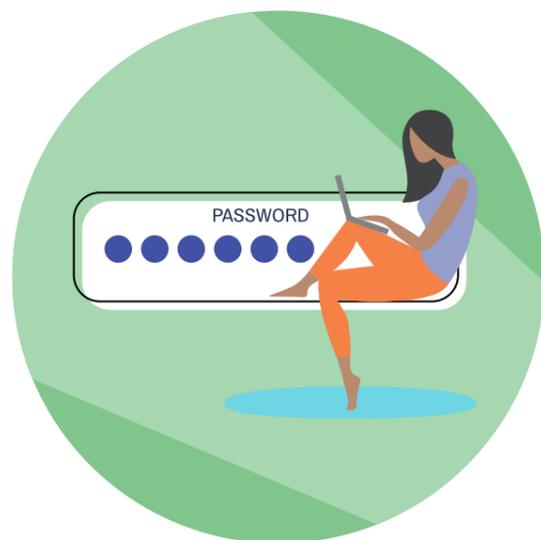


如果說密碼是給你的賬戶加了一把鎖，那麼短語密碼就是給你一套防盜系統！這是更牢固更安全的升級版密碼。

無法開啟MFA時，使用短語密碼保護你的賬戶。短語密碼使用4個或更長的隨機詞彙作為你的密碼。這讓網路罪犯更難猜測而你更容易記住。

你創建的短語密碼應該是：

- 長度足夠 越長越好。長度最好在14個字元以上。4個或更多你能夠記住的隨機詞彙最好。例如，‘purple duck potato boat’。
- 不可預測 短語密碼可預測程度越低越好。句子或許是很好的短語密碼，但太容易被猜到。混合的4個或更多隨機詞彙是保密性高的短語密碼。
- 獨特 不要循環再用你的短語密碼，要對不同的賬戶使用不同的短語密碼。如果你難以記住所有短語密碼，請考慮使用密碼管理器。使用密碼管理器，你只需記住一個密碼，密碼管理器便會處理其餘的事情。請在 cyber.gov.au 搜尋 ‘password manager’ (密碼管理器)，以獲取更多建議。



請在 cyber.gov.au 搜尋‘Passphrases’ (短語密碼)，了解更多關於設立安全密碼的資訊。

貼士5: 發現並舉報騙局



你舉報騙局越早，我們就能越早行動。

如果你相信有人在試圖使用互聯網欺騙你，你最好提前行動保持警惕，以免被人利用。

如果事情聽起來好得令人難以置信，那就很可能不能相信。一條短訊可能說你贏得大獎或你的電腦有病毒，此類短訊並非只有你收到。

它可能來自騙子，他們想利用你。

請記住，騙徒通常會冒充你信任的人或組織。如果你收到一個看似來自你信任的人的訊息，但用的卻是一個新的電話號碼、電郵地址或社交媒體資料，你要保持警覺。在你回覆之前，請通過你可以信賴的渠道與他們聯繫，以驗證他們是否真是向你發送訊息的人或組織。例如，如果你收到一個看似來自你的孩子的短訊，但卻是來自一個新號碼發出，請不要回覆；你可以先通過社交媒體向孩子發送訊息，確認他們是否真的更改了電話號碼。



你知道嗎：

狡猾的網路罪犯可能使用你知道的名字或電郵地址。以下情況要小心：

- 你被要求立即支付賬單
- 你被要求更改個人資訊或密碼
- 你被要求點擊一個鏈接或打開一個文檔。



總結

現在你已經瞭解了安全使用互聯網的知識，你可以更自信地享受網上時光了。

記住，網路罪犯總是能想出新方法來攻擊網路用戶。

定期更新你的網路安全知識，瞭解最新安全措施總是有好處。

獎勵性貼士

想要瞭解更多網路安全的知識嗎？請閱讀以下貼士。

考慮你發佈的內容。

慎重考慮你在網路上共享的資訊以及誰會看到。只接受你在生活中認識的人加好友的請求。

獲取新威脅警示。

訂閱我們的免費警示服務。這樣當我們發現新的網路威脅時你會及時知道。

這樣當攻擊發生時你也會得到應對建議。

同親友討論網路安全。

現在你已經提高了網路安全知識，和家人朋友分享你所學到的。你的知識有可能幫助他們避免日後陷入騙局！

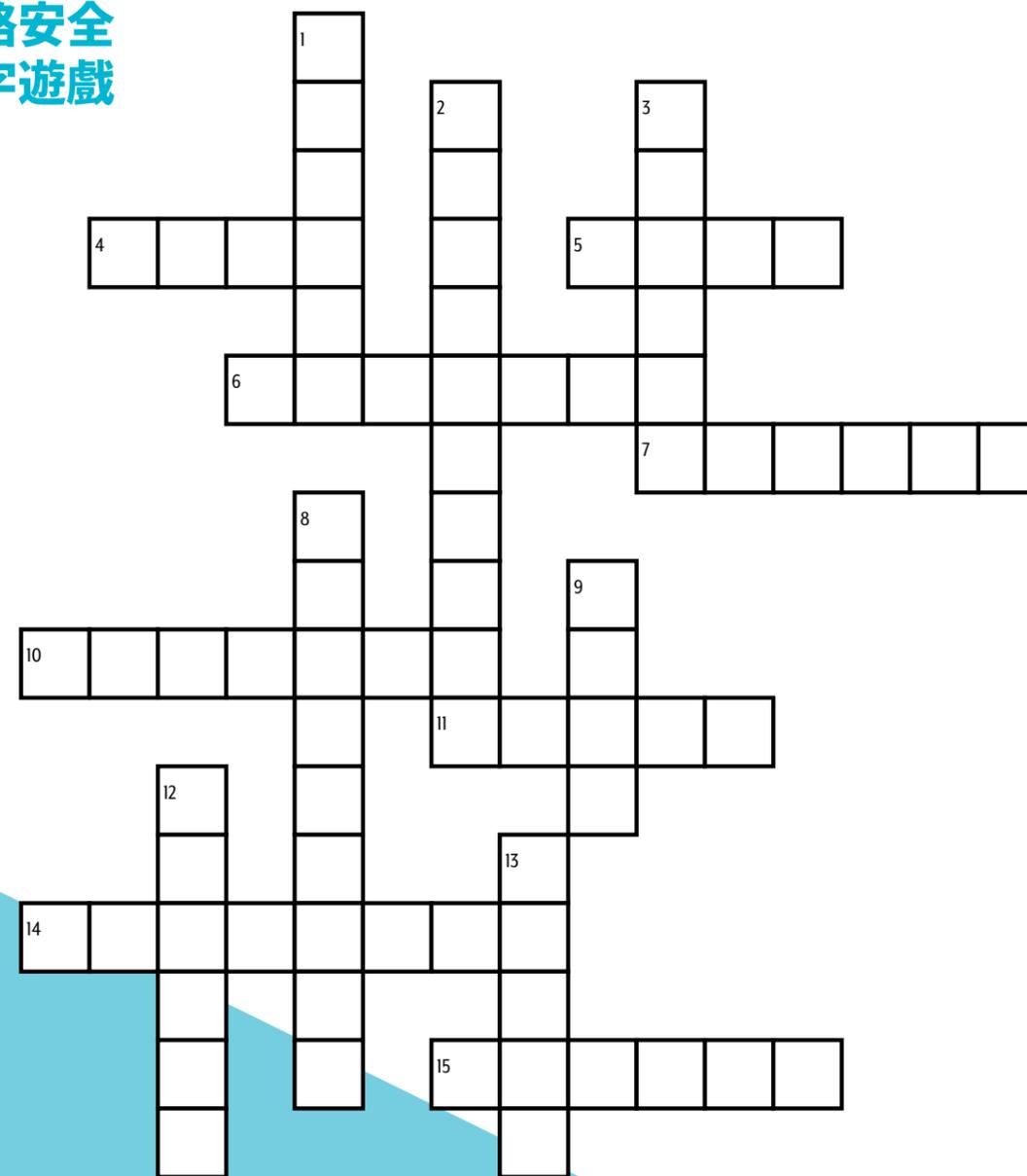
進行銀行業務或網上購物時避免使用公共Wi-Fi。

公共Wi-Fi在看視頻和網頁時很便利，但只使用自己家裡的網路進行任何涉及資金的操作。公共Wi-Fi可能有風險。

舉報網路攻擊事件，保護澳大利亞的安全。

如果你認為自己是網路犯罪的受害者，立刻採取行動。cyber.gov.au有更多建議

網路安全填字遊戲



向下

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

橫向

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

免責聲明

本指南的內容只屬一般性資訊，不應被視為法律意見，也不應在任何特定或緊急情況下，依靠它作為幫助。在任何重要事項上，你都應該根據個人情況，尋求適當的獨立專業意見。

若因依賴本指南的資訊而引致有任何損害、損失或費用，聯邦政府概不承擔任何責任。

版權

© 澳洲聯邦政府 2023

除了國徽(Coat of Arms)和其他已說明出處的地方外，本刊物內所有素材均根據 Creative Commons 署名4.0 國際許可協議提供 (www.creativecommons.org/licenses)。

為了避免有任何疑慮，此許可協議僅適用於這文檔中列出的素材。



你可在 Creative Commons 網站上，找到相關的許可協議條款詳情，以及 CC BY 4.0 許可協議的完整法律條文 (www.creativecommons.org/licenses)。

國徽的使用

在總理和內閣部門網站上，列有使用國徽的條款詳情 (www.pmc.gov.au/government/commonwealth-coat-arms)。

欲瞭解更多資訊，或報告網路安全事件，請聯絡我們。

cyber.gov.au | 1300 CYBER1 (1300 292 371)

此號碼僅適用於澳洲境內。