



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre



個人網路安全 首要步驟

cyber.gov.au

個人網路安全系列

個人網路安全系列

個人 **網路安全:首要步驟** 是3冊指南系列的第1冊，旨在幫助澳大利亞民眾瞭解基本網路安全知識以及如何採取行動保護自己免受常見網路威脅的攻擊。



首要步驟



進階步驟



高階步驟

目錄

簡介	1
開啟自動更新	2
開啟多重身份認證 (MFA)	4
定期備份你的設備	5
使用短語密碼保護你的重要帳戶	6
保護你的移動設備	7
養成你的網路安全思維	8
概要核對清單	11
詞彙表	12

簡介

什麼是個人網路安全？

在日益受技術驅動的世界裡，我們每天使用的設備和帳戶易於遭受網路威脅：

- 你的設備可能包括電腦、手機、平板設備和其他連接網路的設備。
- 你也可能使用網路帳戶如電子郵件、網路銀行、網上購物、社交媒體、網路遊戲等等。

個人網路安全是你採取的一些持續步驟以保護你的帳戶和設備免遭網路威脅。

什麼是網路威脅？

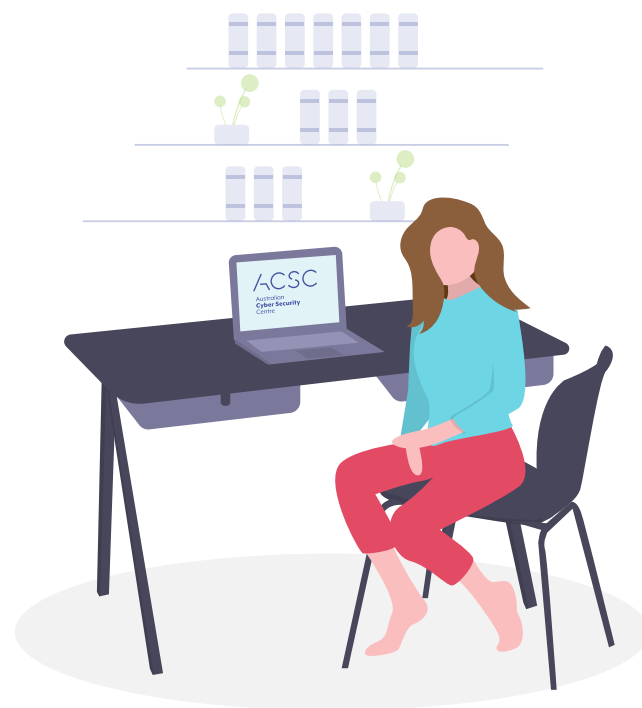
影響澳大利亞民眾的主要網路威脅是**網路騙局**和**惡意軟體**。

- **惡意軟體是各種企圖造成損害的惡意軟體的總稱**，包括病毒、蠕蟲、間諜軟體、木馬和勒索軟體。網路罪犯使用惡意軟體盜取你的資訊和金錢，控制你的設備和帳戶。
- **網路騙局是網路罪犯們發送的訊息**，目的是操縱你披露敏感資訊或在你的設備上激活惡意軟體。

這些攻擊會給受害者造成嚴重的個人和財務損失，而且日益頻繁複雜。

本手冊如何幫助我免遭網路威脅？

無論你是首次學習還是更新網路安全知識，本手冊都是極佳的出發點。個人網路安全：首要步驟是3冊指南系列的第1冊，旨在幫助澳大利亞民眾瞭解基本網路安全知識以及如何採取行動保護自己免受常見網路威脅的攻擊。



開啟自動更新

什麼是更新？

更新是你安裝在伺服器、電腦和移動設備上的軟體（程式、應用和操作系統）經完善的版本。

軟體更新能修復軟體‘缺陷’（代碼錯誤或漏洞），保護你的設備。網路罪犯和惡意軟體利用這些缺陷入侵你的設備，盜取你的個人資料、帳戶、財務資訊和身份。

網路罪犯們不斷地發現並利用新的軟體缺陷，因此更新你設備上的軟體有助於保護你免遭網路攻擊。

如何設置自動更新？

自動更新是缺省或‘設置後忘記’設置，當有新的更新可用時自動安裝。

- ✓ 在所有軟體和設備上開啟並確認自動更新。
- ✓ 如何開啟自動更新取決於你的設備和軟體。
- ✓ 盡可能設置一個方便的自動更新時間，例如當你睡覺或通常不使用設備的時間。



你的設備必須連接電源，打開並且有可用存儲空間。

提示：如果你收到更新設備軟件的提示，你便應該盡快更新。



請在 cyber.gov.au 搜尋‘Updates’（更新），便可找到更多有關如何開啟自動更新的資訊。



沒有自動更新設置該怎麼辦？

如果沒有自動更新功能，你應當透過軟體或設備的設置菜單定期檢查並安裝更新。

我的舊設備和軟體沒有收到任何更新該怎麼辦？

如果你的設備、操作系統或軟體過於陳舊，則可能無法繼續得到製造商或開發者的支持。

當產品到了‘支持終止’階段時，將無法繼續得到更新，從而使你易於因已知軟體‘缺陷’遭到網絡攻擊。支持終止的產品包括Windows 7 操作系統和iPhone 6。

如果你的設備、操作系統或軟體技術支持已經終止，ACSC建議你盡快升級以保證安全。

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



開啟多重身份認證 (MFA)

什麼是MFA？

你可以使用多重身份認證(MFA)來提高你最重要賬戶的安全性。MFA要求你提供以下認證方式中兩種或以上的組合才能登入賬戶：

- **你知道的一些事情** (例如PIN、密碼或短語密碼)；
- **一些你有的東西** (例如智慧卡，實物令牌，認證應用、短訊或電郵)；
- **你的一些個人特性** (例如指紋、面部識別或虹膜掃描)。

MFA給你的賬戶增加認證保護層，使網路罪犯更難獲得對你賬戶的初始訪問，因為破解賬戶需要更多時間、精力和資源。



如何開啟2FA來保護我最重要的賬戶？

你應當現在就開啟2FA，從你最重要的賬戶開始：

- ✓ 所有網上銀行和財務賬戶 (例如銀行，PayPal)
- ✓ 所有電子郵件賬戶 (例如 Gmail, Outlook, Hotmail, Yahoo!)

如果你有很多電子郵件賬戶，優先保護那些和你網上銀行或其他重要服務相連接的賬戶。

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’。

個人網路安全：首要步驟

定期備份你的設備

什麼是備份？

備份是你儲存在外部存儲設備或雲端上的最重要資訊(例如照片、財務資訊或記錄)的數碼副本。

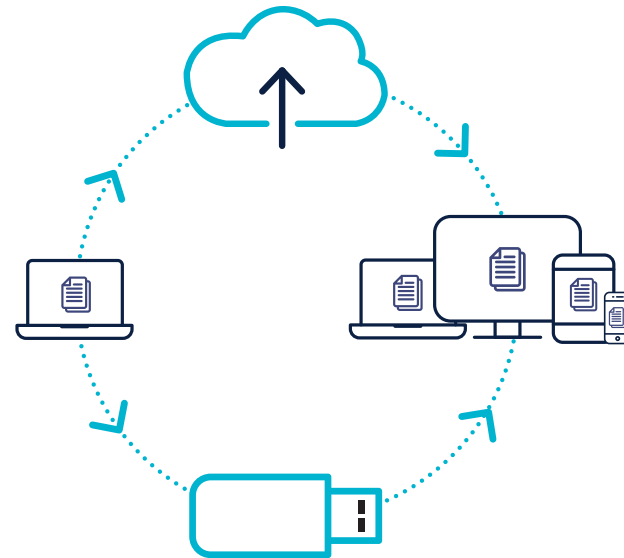
備份是一種預防措施，以便在你的資訊丟失、被盜或受損時你仍然可以恢復這些資訊。

如何備份我的設備和文檔？

你應該定期為你的文件和設備做備份，無論是每天、每周或每月，最終都是由你作出決定。備份的頻密次數可能取決於：

- 你加載到設備上的新文件數量。
- 你對文件做了多少次更改。

提示：定期檢查備份，以便熟悉恢復過程，經常確保你的備份工作妥善完成。



請在 [cyber.gov.au](https://www.cyber.gov.au) 搜尋 'Backups' (備份)，以獲取更多有關如何將資料備份的資訊。

個人網路安全：首要步驟

使用短語密碼保護你的重要帳戶

多重身份認證(MFA, 見第4頁)是保護你的帳戶免受網路罪犯攻擊的最有效方法之一。**如果MFA不可用**，和簡單密碼相比，獨特的高保密度短語密碼能更好地保護你的帳戶。

什麼是短語密碼？

短語密碼使用4個或更長的隨機詞彙作為你的密碼。

例如，'crystal onion clay pretzel'

- **短語密碼比普通密碼** 更安全。

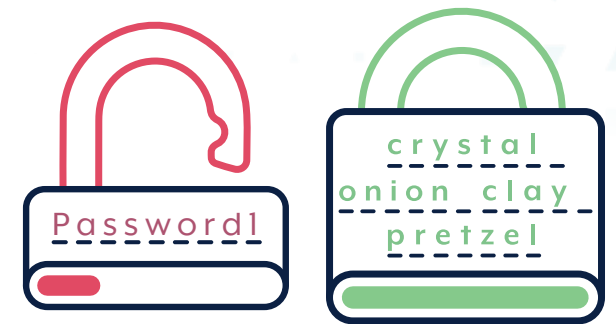
短語密碼讓網路罪犯更難破解而你更容易記住。

如何創建短語密碼？

創建的短語密碼應是：

- **足夠長：**至少14個字節，使用4個或更多隨機詞彙。短語密碼越長越安全。
- **不可預測：**使用4個或更多不相關隨機詞彙組合。不使用著名的短語、語錄或歌詞。
- **獨特：**不要在多個帳戶重複使用。

如果網站或服務要求複雜的密碼包括符號、大寫字母或數字，你可以將其包括在短語密碼中。你的短語密碼仍然需要足夠長，不可預測而且獨特以達到最佳的安全性。



我應該用短語密碼保護哪些帳戶？

如果你最重要的帳戶無法得到MFA(見第4頁)的保護，把你的密碼改成獨特的高保密度的短語密碼，從以下帳戶開始：

- ✓ 網上銀行和財務帳戶
- ✓ 電子郵件帳戶

如果你有很多電子郵件帳戶，優先保護那些和你網上銀行或其他重要服務相連接的帳戶。

你通常可以在你的帳戶設置菜單裡把密碼改成獨特的高保密度的短語密碼。

提示：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，密碼管理器會處理其餘的事情。請在 [cyber.gov.au](https://www.cyber.gov.au) 上搜尋 'password manager' (密碼管理器)，以獲取更多建議。

請在 [cyber.gov.au](https://www.cyber.gov.au) 搜尋 'Passphrases' (短語密碼)，以獲取更多有關如何設立安全的短語密碼的資訊。

保護你的移動設備

如今人們使用智慧手機和平板設備隨時隨地連接網路、購物、工作、進行銀行業務、研究、追蹤運動健身，完成上百種其他任務。

如果我的手機被破解、丟失或被盜會發生什麼？

- 網路罪犯會利用你設備上存儲的資訊，包括社交媒體和電子郵件帳戶，盜取你的金錢或身份。
- 你可能失去無法替代的數據例如照片、記事或訊息(如果沒有備份)。
- 網路罪犯可能使用你的電話號碼欺騙其他人。



如何保護好我的移動設備？

設備安全：

- ✓ **使用** 短語密碼、密碼、PIN或口令鎖定你的設備。使其難以被猜測 - 你的生日和圖形鎖很容易被網絡罪犯猜到。使用短語密碼獲得最佳安全保護(見第6頁)。你也可以考慮使用面部識別或指紋來解鎖你的設備。
- ✓ **確保** 你的設備靜止一小段時間後自動鎖屏。
- ✓ **切勿** 在公共充電點給你的設備充電，避免使用第三方充電器。
- ✓ **對待** 你的手機像對待錢包一樣。始終隨身攜帶並妥善保管。

軟體和應用安全：

- ✓ **使用** 設備的自從更新功能，當有應用和操作系統更新可用時盡快安裝(見第5頁)。

- ✓ **設置** 設備要求短語密碼/密碼才能安裝應用。家長監控也可用於這一目的。
- ✓ **檢查** 在設備上安裝新應用尤其是免費應用時仔細檢查其隱私許可。只安裝來自良好聲譽開發者的應用。

數據安全：

- ✓ **開啟** 遠程鎖定和刪除功能，如果你的設備支持這些功能。
- ✓ **確保** 在出售或丟棄你的設備之前徹底刪除個人數據。

連接安全：

- ✓ **關閉** 藍牙和Wi-Fi，在你不使用它們時。
- ✓ **確保** 你的設備不會自動連接新的Wi-Fi網路。

請在 cyber.gov.au 搜尋 'Secure your mobile phone' (保護你的手機)，以獲取更多有關如何保護你的手機的資訊。

養成你的網路安全思維

個人網路安全不僅僅是更改設置，它也涉及你的思維和行為。

警惕網路詐騙

眾所周知，網路罪犯使用電郵、訊息、社交媒體或電話嘗試欺騙澳大利亞民眾。這些罪犯們偽裝成你認為你認識的或應該信任的個人或組織。

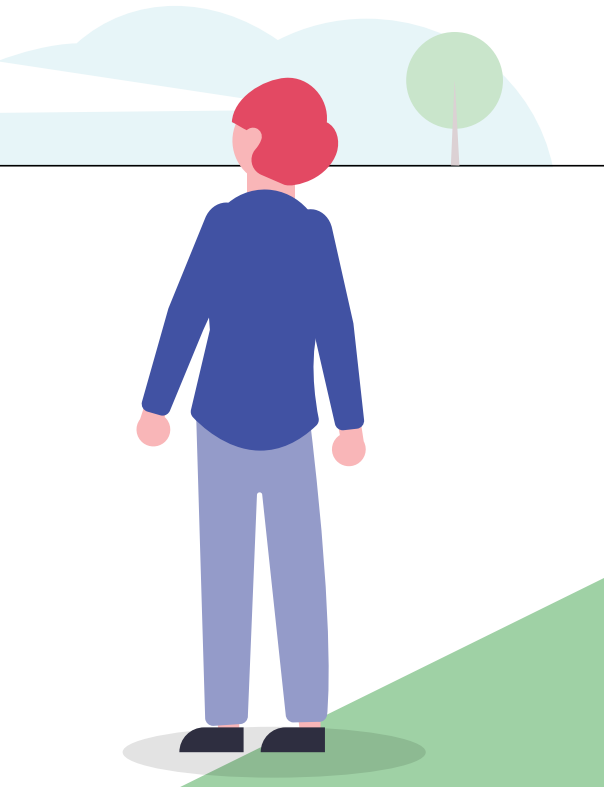
他們的訊息或電話試圖誘騙你採取特定行動，例如：

- 披露銀行帳戶資料，密碼和信用卡號碼
- 授權你電腦或伺服器的遠程控制權限
- 打開一個附件，其中可能含有惡意軟體
- 匯款或送出禮物卡

我該如何識別詐騙訊息？

識別詐騙訊息並不容易。網絡罪犯們通常使用一些特定的伎倆來欺騙你。他們的訊息可能有：

- **權威性** – 該訊息是否聲稱由某個官方機構、例如銀行發出？
- **緊迫性** – 該訊息是否告訴你出現了問題，或你必須在限定時間內回復或付款？
- **情緒性** – 該訊息是否讓您感到恐慌、充滿希望或好奇？
- **稀缺性** – 該訊息是否提供了某種稀缺的東西，或承諾划算的交易？
- **實時事件性** – 該訊息是否有關突發的新聞或重大事件？



請在 cyber.gov.au 瀏覽 'Learn the basics' (了解基礎知識)，以了解如何察覺網路釣魚或詐騙訊息。

個人網路安全：首要步驟

收到詐騙訊息時我該怎麼辦？

如果你收到詐騙訊息或電話，你應該置之不理，刪除或向ACCC Scamwatch舉報 scamwatch.gov.au

如果你擔心自己的網路安全，也可以聯絡ACSC的網路安全專線**1300 CYBER1** (1300 292 371)

如果你遭受詐騙，並認為自己的銀行帳戶、信用卡或借記卡可能有風險，請立即聯繫你的財務機構，它們可能會凍結你的帳戶或制止一項轉帳。

我不確定一個訊息是否是詐騙訊息時怎麼辦？

如果你認為某短訊或電話可能確實來自你信任的機構(例如你的銀行)，找到一個你能夠信任的聯絡方法。訪問官方網站，撥打它們公示的電話號碼。或親身前往實體店或分行。切勿使用你收到的訊息中或通過電話獲得的任何鏈接或聯繫方式，這些可能是偽造的。

點擊前三思

- ✓ 點擊打開電郵、網站、和短訊鏈接時要三思。
- ✓ 始終對 收到的附件保持警惕。
- ✓ 如果你的瀏覽器提醒你某個網站不安全，立刻將其關閉。
- ✓ 請記住：任何IT人員、政府部門或企業都不會聯絡你要求擬披露登入訊息。

如果你認為自己是網路犯罪的受害者，請在 cyber.gov.au/report 網站上向ACSC ReportCyber舉報，或致電網路安全專線 **1300 CYBER1** (1300 292 371)

你也可以通過訂閱 ACSC 的免費警示服務，了解最新的威脅。請在 cyber.gov.au 搜尋 ‘Subscribe to the ACSC alert service’ (訂閱 ACSC 警示服務)，當我們發現新的網路威脅時，便會向你發出警示。

個人網路安全：首要步驟

在社交媒體上分享前慎重考慮

網路罪犯在實施網路詐騙和網路攻擊時可能使用你在社交媒體上公開發佈的資訊。

切記互聯網是永久性的，你永遠無法完全清除所發佈的內容。

發佈前如何慎重考慮？

- **考慮：**網路罪犯會如何使用這些資訊來攻擊我或我的帳戶？
- **考慮：**我能否把這些資訊或圖片坦然地出示給線下的陌生人？

我應該避免分享哪些資訊？

避免在網上分享有可能被網路罪犯用來：識別你，透過騙局操縱你或推斷出你帳戶恢復問題答案的資訊(包括圖片)。這可能包括你的：

- 出生地和生日
- 地址和電話
- 僱主和工作經歷
- 曾上過的學校
- 其他任何可能被用來針對你的個人資訊。



概要核對清單



你完成了本指南的所有內容嗎？

使用這個簡便的核對單來追蹤你的進度：

- ✓ **我已經在所有設備上都開啟了自動更新：**
 - 電腦 (台式機和筆記本)
 - 手機
 - 平板電腦
- ✓ **我已經在最重要帳戶上開啟了多重身份認證：**
 - 所有網上銀行和財務帳戶 (例如 銀行, PayPal)
 - 所有電子郵件帳戶 (例如 Gmail, Outlook, Hotmail, Yahoo!)
- ✓ **我定期備份我的設備：**
 - 電腦 (台式機和筆記本)
 - 手機
 - 平板電腦
- ✓ **我在最重要而且無法開啟MFA的帳戶上使用獨特高保密度的短語密碼：**
 - 網上銀行和財務帳戶
 - 電子郵件帳戶
- ✓ **我已經妥善保護好我的移動設備：**
 - 筆記本
 - 手機
 - 平板電腦
- ✓ **每天都使用網路安全思維**
 - 我能夠識別詐騙訊息
 - 收到詐騙訊息時我知道該怎麼做
 - 如果不確定時我知道如何檢查一個訊息是否是詐騙訊息
 - 我點擊鏈接打開附件前會慎重考慮
 - 我在社交媒體上分享任何內容前會慎重考慮
- ✓ **如果我是網路犯罪或騙局的受害者我知道該如何得到幫助**



詞彙表

- 帳戶恢復**
用一組問題或其他認證方法來復原或重新獲得帳戶權限或更改帳戶短語密碼/密碼。
- 應用**
也被稱為移動應用，是通常用於智慧手機或平板設備上的軟體。
- 附件**
隨電子郵件發送的文檔
- 認證應用**
用於透過多重身份認證(MFA)證實電腦用戶身份賦予其進入權限的應用。
- 雲端**
提供大容量分配儲存和處理能力的遠程伺服器網路。
- 網路罪犯**
任何非法入侵電腦系統損壞或盜取資訊的人。
- 設備**
電腦或通訊設備。例如，一台電腦、筆記本、手機或平板電腦。
- 支持終止**
支持終止是指一家公司停止對其產品或服務的支持。這通常是針對硬體和軟體產品，當一家公司發佈一個新版本時停止對之前版本的支持。
- 惡意軟體**
無授權入侵控制用戶電腦、盜取資訊、擾亂或癱瘓網路的軟體。
- 操作系統**
安裝在電腦硬盤上的軟體，使電腦硬體運行電腦程式並同其進行通訊。例如：Microsoft Windows, Apple macOS, iOS, Android
- 實物令牌**
通常可掛在鑰匙環上的實物設備，可以產生安全代碼用於MFA電腦用戶身份認證。
- 遠程接入**
從其他地方獲得設備和網路的進入和控制權限。
- 軟體**
通常稱為程式，一組使用戶和電腦及硬體互動或執行任務的指令。

免責聲明

本指南中的資料具有普遍性，不應被視為法律建議或任何特定情況下或緊急情況下的協助依據。在任何重要問題上，您應該根據自己的情況尋求適當的獨立專業意見。

對於因依據本指南中的資訊而產生的任何損害、損失或費用，澳洲聯邦不承擔任何責任或義務。

版權所有

© Commonwealth of Australia 2023.

除澳洲國徽和另有說明的部分外，本指南中的所有資料均依據知識共享 (Creative Commons) 署名 4.0 公共授權合約國際版 (www.creativecommons.org/licenses) 提供。

為免生疑義，這意味著該授權合約僅適用於本指南中所列的資料。



有關授權條件的詳情及 CC BY 4.0 授權的完整法律條文均可在 Creative Commons 網站 (www.creativecommons.org/licenses) 上查閱。 (www.creativecommons.org/licenses).

澳洲國徽的使用

有關澳洲國徽使用的條款在澳洲總理內閣部的網站上有詳細介紹 (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。