Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

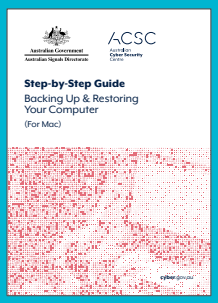
小企業網路安全指南

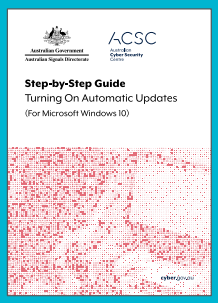
cyber.gov.au

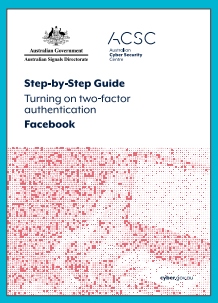
補充指南

更多保護您企業網路安全的措施，請訪問cyber.gov.au閱讀我們的小企業**網路安全叢書**

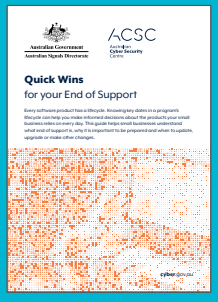
分步指南

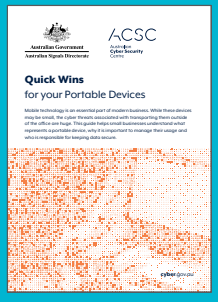


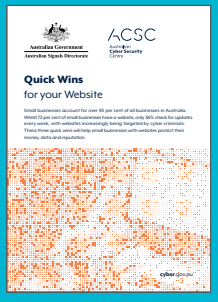




快速指南







目錄

序言 4

網路威脅：關鍵領域 5

惡意軟體 6

詐騙短訊 (網路釣魚) 7

勒索軟體 8

軟體因素：關鍵領域 9

自動更新 10

自動備份 11

多重身份驗證 12

人員和程序關鍵領域 13

權限控制 14

短語密碼 15

員工培訓 16

概要核對清單 17

詞彙表 18

序言

這一指南旨在幫助小企業保護自己免受最常見網路安全威脅。

網路安全事故有可能給小企業造成災難性的影響。

不幸的是，我們在澳大利亞網路安全中心(ACSC)每天都會看到網路安全事故對個人、小企業和大公司造成的損害。

我們知道很多小企業的業主和運營者沒有時間和資源專注於網路安全。然而，小企業可以採取一些簡單的措施來避免常見的網路安全事故。

我們的*小企業網路安全指南*旨在幫助小企業理解、採取行動並提高其對不斷演變的網路安全威脅的應對能力。指南用詞簡潔，行動措施簡單，指南是為小企業專門設計。

本指南是理解基本網路安全知識的良好出發點。如果你希望進一步提高網路安全知識，可以在ACSC網站找到更多資訊和建議：
cyber.gov.au

ACSC的目標是幫助澳洲成為網路安全度最高的地方。

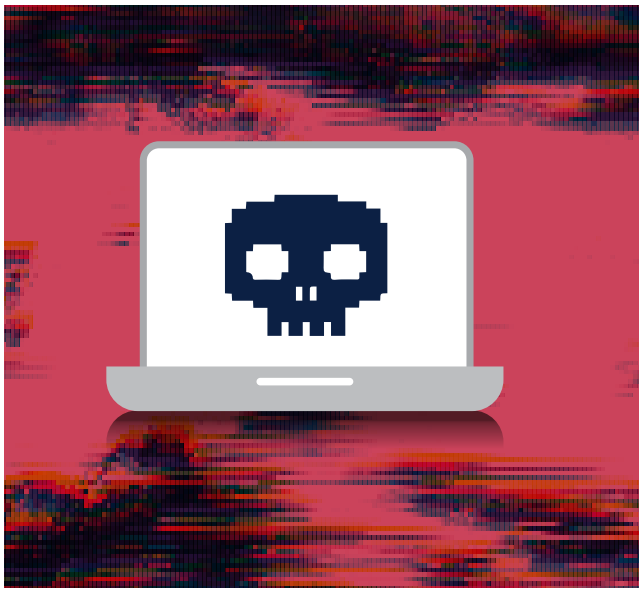
作為Australian Signals Directorate（ASD）的一部分，澳洲網路安全中心（ACSC）致力於提供網路安全建議、協助和操作回應措施，以防止、檢測和補救對澳洲的網路威脅。

網路威脅
關鍵領域

對於小企業，即使最小的網路安全事故也可能造成災難性的影響。

本部分旨在幫助小企業保持警惕，做好準備。識別解釋最常見的網路威脅種類以及如何保護你的企業。

惡意軟體 (惡意軟體)



這是什麼？ 旨在造成損害的無授權軟體

惡意軟體是勒索軟體、病毒、間諜軟體和木馬軟體等軟體的總稱。

為什麼？ 製造混亂。 損害。 欺騙。

罪犯們利用惡意軟體 盜取重要的資訊例如銀行或信用卡號碼和密碼。

惡意軟體 **也能控制或監控** 用戶的電腦。罪犯們用這些權限和數據來：

- **欺詐**
- **身份盜竊**
- **干擾** 企業
- **盜取** 敏感數據或智慧產權
- **抽取** 電腦資源進行更大範圍的犯罪活動

是誰？ 任何人，任何地方

惡意軟體製造者可能在世界上任何地方。

他們所需的只是一台電腦，技術和邪惡意圖。罪犯們能輕易獲得廉價工具使用惡意軟體攻擊你。

罪犯們大範圍撒網，攻擊最脆弱的目標。採取網路安全措施，對威脅保持警惕，你可以避免自己的企業成為攻擊目標。

阻止惡意軟體

- 自動更新 你的操作系統，軟體和應用程式
- 定期備份 你的重要數據
- 培訓員工 識別可疑鏈接和附件

詐騙短訊 (網路釣魚)

這是什麼？ ‘狡猾的’電郵、短訊或電話，目的是騙取接收者的錢財和數據

罪犯們經常使用電郵、社交媒體、電話或短訊來嘗試詐騙澳大利亞的企業。

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企業採取特定行動，例如：

- **支付偽造的賬單**或更改合法賬單的支付資訊
- **披露銀行賬戶資料，**密碼和信用卡號碼(有時也被稱為‘網路釣魚’詐騙，網路罪犯會仿製銀行和網站的官方名稱和標誌使自己看起來是合法的。)
- **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
- **購買禮物卡**並寄給騙子

在哪裡？ 電郵、社交媒體、電話或短訊

網路釣魚詐騙不僅僅限於電郵。它們日益複雜， 更加難以識別。

警惕緊急付款和更改銀行賬戶的請求，意外的附件，以及檢查或確認登入資訊的要求。

訪問 **scamwatch.gov.au** 舉報騙局。

誰？ 澳大利亞企業

詐騙短訊可能發給上千人，也可能針對某個特定目標。

然而， 罪犯們會用一些常用的伎倆來欺騙你的員工。他們的訊息可能有：

- **權威性：**該訊息是否自稱來自 官方人士或企業高層？
- **緊迫性：**該訊息是否告訴你出現了問題，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：** 該資訊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？

如果你認為某短訊或電話可能確實來自你信任的機構(例如你的銀行或供應商)，找到一個你能夠信任的聯絡方法。

訪問官方網站，或撥打它們公示的電話號碼。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。

勒索軟體

這是什麼？ 勒索軟體是一種惡意軟體，它鎖定你的電腦或文檔，直到你支付贖金

勒索軟體鎖定或加密你的文檔，使你無法再訪問或使用它們。有時甚至能讓你的設備無法運行。勒索軟體可以用和其他惡意軟體一樣的方式感染你的設備。例如：

- 訪問不安全或可疑的網站
- 打開不明來源的鏈接、郵件或文檔
- 網路設備(包括伺服器)安全度低

為什麼？ 金錢

勒索軟體給網路罪犯們提供低風險高回報的收入。它們易於開發和傳播。贖金通常通過線上數位貨幣或加密貨幣如Bitcoin支付，使其難以被追蹤。此外對網路罪犯有利的是，多數小企業沒有做好應對勒索軟體攻擊的準備。

誰？ 小企業，中型企業和大企業

小企業可能尤其脆弱，因為它們不太可能採取有助於阻止勒索軟體並恢復系統的網路安全措施。

切勿支付贖金

支付贖金不能保證受害者的文檔得到復原，也不能阻止被盜取數據被公開或被出售用於其他犯罪活動。這也會增加受害者再次成為攻擊目標的可能性。

如果你遇到勒索軟體需要支持，致電ACSC 24/7 熱線1300 CYBER1 (1300 292 371)

無論是否決定支付贖金，ov.au向ACSC舉報勒索軟體事件。分享事件資訊有助於保護其他澳大利亞企業。

阻止勒索軟體並復原

- 定期備份你的重要數據
- 自動更新你的操作系統，軟體和應用程式
- 如有可能，要求多重身份認證使用服務 (第12頁)
- 審查並保護你網路上的設備(包括你的伺服器)和任何連接互聯網的服務(遠程桌面，文檔共享，網頁郵件)。如果對此不確定，咨詢IT專業人士。

軟體因素
關鍵領域

妥善管理你的軟體、數據和線上賬戶能夠大大提高企業對最常見網路威脅的防禦能力。

例如，操作系統是電腦上最重要的軟體。它管理你電腦的硬體和所有程式，因此需要定期更新，確保你始終在使用最安全的版本。

提高恢復力，保持更新，注意這些軟體因素，保持小企業長久安全。

自動更新

這是什麼？ 軟體更新

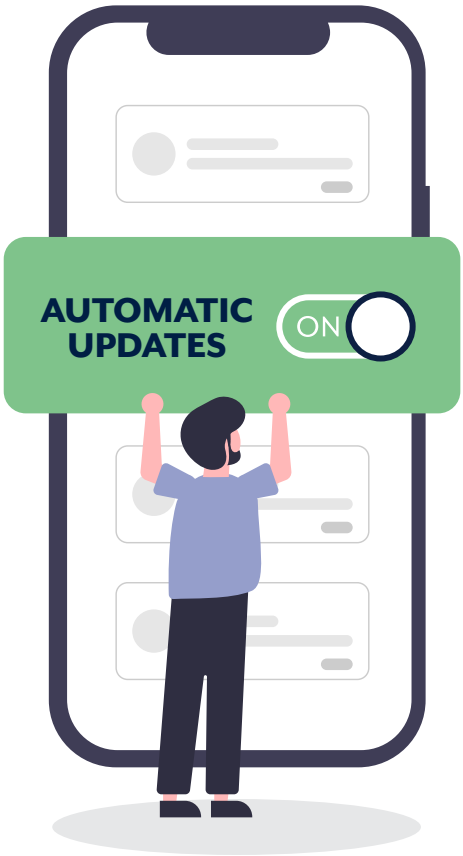
更新 **是** 妳安裝在伺服器、電腦和移動設備設備上的軟體(程式、應用和操作系統)經完善的版本。自動更新 **是** 缺省或 **'設定後忘記'** 系統，有更新時自動更新你的軟體。

為什麼？ 安全

- 保持操作系統和應用程式更新是 **保護自己免受** 網絡攻擊的最佳方法之一。
- 定期更新你的軟體 **可以減少網路罪犯利用已知漏洞** 運行惡意軟體或入侵你電腦的機會
- **節省時間和顧慮，** 自動更新是保護你的設備和數據安全的重要方法

什麼時候？ 今天和每一天

- **開啟自動更新，** 尤其是操作系統
- **如果自動更新不可用，** 定期檢查是否有更新
- 如果你收到提示更新你的操作系統或其他軟體，你應當 **盡快安裝更新**
- **設置一個合適的自動更新時間**以避免對企業運營造成干擾
- 如果你使用 **防病毒軟體，確保開啟自動更新**



注意：

如果你的硬體或軟體過於陳舊，可能無法更新，從而令你的企業易於出現安全問題。

ACSC建議你盡快升級你的設備和軟體

截至2020年，Windows 7, Microsoft Office 2010和Windows Server 2008支持已經終止從而不再安全。

更多資訊請閱讀ACSC的支持終止*快速指南*手冊，訪問 cyber.gov.au

自動備份

這是什麼？ 數據備份

備份 是你企業最重要資訊如客戶資料和財務記錄的數位副本。備份可以被保存到外部設備或雲端上。

自動更新 是缺省或 ‘設定後忘記’ 系統，無需人力介入自動備份你的數據。

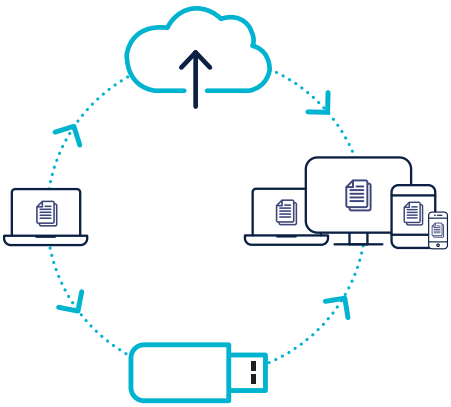
每次備份後安全地移除你的備份存儲設備連接，這將保證其在遭到網路攻擊時仍然安全。

為什麼？ 輕鬆復原

- **備份是一種預防措施，** 以便在你的資訊丟失，被盜或受損時 你仍然可以訪問這些數據
- **讓你的企業能夠在遭受網路攻擊(例如勒索軟體)後** 復原並盡可能縮短停工時間
- **保護你企業的可信度** 並有助於符合法律規定^

什麼時候？ 今天和每一天

- **選擇一個適合你企業的備份系統**考慮在最壞情況下你可以承受的損失，這有助於你確定具體需求例如備份數據的頻率
- **定期檢驗備份** 嘗試復原數據
- **始終保持至少一個備份不連接你的設備，** 最好是存放在另一個不同的場所以避免自然災害或盜竊的影響
- **不要把你的備份連接到感染勒索軟體或病毒** 的設備上



^某些行業有義務在特定期間保存記錄。確保自己了解你的數據保存要求。

多重身份驗證

這是什麼？ 一個要求兩種或更多身份證明來獲得權限的安全措施

多重身份認證 (MFA) 通常要求以下組合：

- **一些你知道的事情** (密碼/短語密碼,PIN,安全問題)
- **一些你有的東西** (智慧卡，實物令牌，認證應用)
- **一些你的生物特征** (指紋或其他生物識別)

為什麼？ 安全防護力大大提高

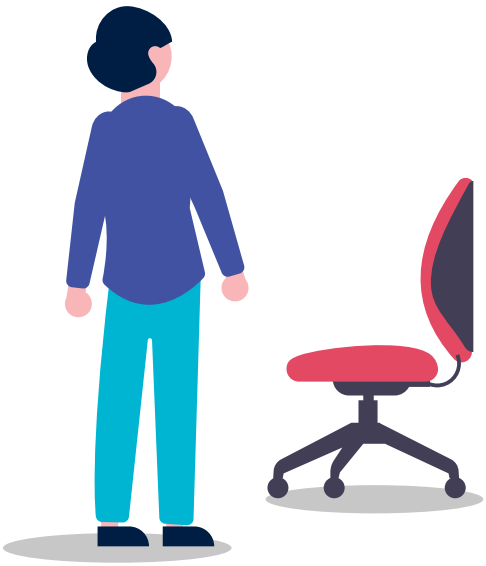
MFA是防止無授權入侵你重要資訊和賬戶的最有效方法之一。

多重保護增加了罪犯攻擊你企業的難度。罪犯也許能盜取一部分身份如你的密碼，但他們仍然需要獲得並使用其他身份證明才能進入你的賬戶。

在哪裡應用？ 登入重要賬戶

小企業應盡可能在重要賬戶上開啟MFA，財務和電郵賬戶優先。MFA選項包括，但不限於：

- 實物令牌
- 隨機PIN
- 生物識別/指紋
- 認證應用
- 電郵
- 短訊



人員和程序
關鍵領域

無論企業規模多小，都需要了解並在各個層面主動實施網路安全措施。

你的內部程序和員工是阻止網路安全威脅的最後也是最重要的防線。

鑒於小企業通常沒有足夠資源設置專職IT人員，本部分講解你應如何管理企業的資訊權限，保護你的企業賬戶，並培訓員工防止、識別和舉報網路安全事件。

權限控制

這是什麼？ 管理你企業的電腦環境裡誰能夠獲得什麼資訊

權限控制是一種限制電腦系統進入的方法。它通過限制以下進入權限來保護你的企業：

- 文檔和文件夾
- 應用程式
- 數據庫
- 郵箱
- 線上賬戶
- 網路

為什麼？ 盡可能降低無授權獲取重要資訊的風險

一般而言，員工不需要獲得企業的所有數據、賬戶和系統權限來做自己的工作。

該權限應盡可能受到限制，這樣員工和外部供應商不會無意或有意威脅你的企業。

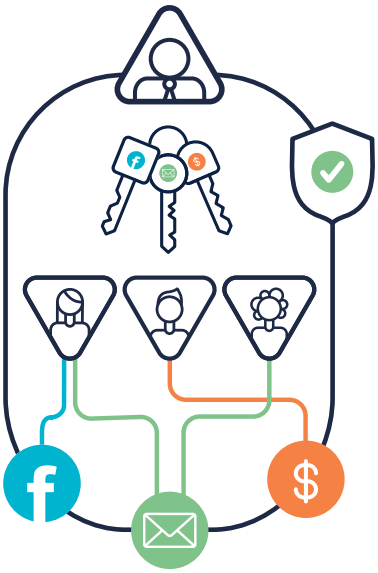
權限控制系統和程序讓企業主和運營者能夠：

- **決定誰可以有權限獲得** 特定文檔、數據庫和郵箱
- **控制任何賦予外部供應商的權限** 如會計師、網站託管商
- **限制誰有賬戶權限** 例如供應商網站和社交媒體
- **任何賬戶、設備或系統被入侵時** 降低潛在的損失
- **當員工更換職位或辭職時** 取消其系統和數據權限

誰？ 最小權限原則

取決於企業的性質，最小權限原則對大多數小企業來說是最安全的方法。

該原則僅授予員工完成工作所需的最低權限。這樣也能減少‘內部人’無意或有意威脅企業的風險。



權限控制原則

- 把員工在企業設備上從‘管理員’賬戶過渡到標準賬戶
- 複審數位文檔和文件夾的權限許可
- 不要在員工之間共享賬戶或密碼/短語密碼
- 當員工辭職或你更換供應商時記得取消權限，刪除賬戶並/或更換密碼/短語密碼

短語密碼

這是什麼？ 更安全版本的密碼

多重身份認證(MFA，見第12頁)是保護你的賬戶免受網路罪犯攻擊的最有效方法之一。無法採用MFA時，你應當使用短語密碼來保護你的賬戶。

短語密碼使用4個或更長的隨機詞彙作為你的密碼。例如，‘crystal onionclay pretzel’

為什麼？ 安全且容易記住

這讓網路罪犯更難破解而你更容易記住。

創建的短語密碼應是：

- **長度足夠**短語密碼越長越好。長度至少在14個字元以上。
- **不可預測:** 使用混合的不相關隨機詞彙。不使用著名的短語，語錄或歌詞。
- **獨特：**不要在多個賬戶上重複使用一個短語密碼。

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。

在哪裡應用？ 你的賬戶和設備

如果你無法在設備或賬戶上使用MFA，則應當使用短語密碼來保證安全。在此情況下，一個安全的短語密碼可能是入侵者和你重要資訊之間僅有的障礙。

記住你的短語密碼應該是獨特的，因為重複使用密碼會讓網路罪犯更容易入侵多個賬戶。

更多創建短語密碼的建議，請見ACSC的*創建高保密度短語密碼*指南 **cyber.gov.au**

考慮使用密碼管理應用

使用密碼管理應用(也可以用來存儲短語密碼)是良好的網路安全習慣 給每個重要賬戶創建一個獨特的短語密碼聽起來難以做到，但使用密碼管理應用儲存你的短語密碼可以解除你記住哪個短語密碼用在哪裡的負擔。
確保你使用的任何密碼管理應用都是來自可信且有良好聲譽的來源 而且其自身也得到高保密度也易於記住的短語密碼保護。

員工培訓

這是什麼？保護員工和企業免受網路威脅的教育

教育自己和員工如何防止、識別和舉報網路犯罪。

給員工基本網路安全培訓，包括更新他們的設備，保護他們的賬戶，以及識別詐騙短訊。

你還應該考慮實施**網路安全事故應對**計劃，在出現網路事故時指導你的企業和員工如何應對。

這有助於你了解你的關鍵設備和程序，以及關鍵聯絡人以做出應對和復原。

為什麼？員工會成為阻止網路安全威脅的第一道和最後一道防線

培訓能夠改變員工的習慣和行為並生共享責任來保護企業安全。

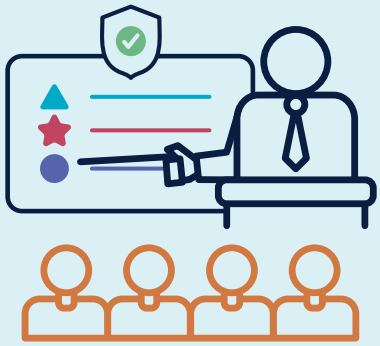
網路安全人人有責

什麼時候？定期網路安全宣傳培訓

網路安全在不斷演變。

讓所有人都了解最新網路安全威脅可能事關罪犯是否能夠入侵你的資金、賬戶和數據。

“教育自己和員工如何防止、識別和舉報網路犯罪。”



網路安全宣傳貼士

- 培訓員工識別可疑鏈接和附件
- 定期提供更新的網路安全培訓
- 製訂網路安全事故應對計劃
- 鼓勵濃厚的網路安全文化
- 分享詐騙短訊範例，幫助員工識別網絡安全威脅

概要核對清單

軟體因素

自動更新你的操作系統，軟體和應用程式

- 如果你收到提示更新你的操作系統或其軟體，你應當盡快安裝更新
- 設置一個合適的自動更新時間以避免對業正常運營造成干擾

定期備份你的重要數據

- 定期檢驗備份嘗試復原數據
- 始終保持至少一個備份不連接你的設備

盡可能在重要賬戶上開啟MFA

- MFA是保護你重要資訊和賬戶的最有效法之一
- 優先保護財務和電郵賬戶以獲得最佳效果

人員和程序

管理你企業的電腦環境裡誰能夠獲得什麼資訊

- 採用最小權限原則
- 當員工辭職時記得取消權限，刪除賬並/或更換密碼/短語密碼

當MFA不可用時，使用短語密碼保護賬和設備

- 短語密碼使用4個或更長的隨機詞彙作你的密碼。
- 短語密碼需要足夠長，不可預測而且獨特才是最有效的

為員工進行基本網路安全培訓

- 包括更新他們的設備，保護他們的賬戶，以及識別詐騙短訊。
- 定期提供更新的網路安全培訓

詞彙表

防病毒軟體
旨在保護你電腦和網路不受病毒感染的軟體程式。

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。

生物識別
透過識別人的生物特性如指紋或聲音驗證其身份。

比特幣
在互聯網上用於多種服務的數位貨幣(加密貨幣)

暴力破解攻擊
一種每秒鐘產生數百萬字節組合的攻擊方法這種方法對破解簡短的密碼很有效。

雲端
提供大容量分配儲存和處理能力的遠程服務器網路。

網路罪犯
任何非法入侵電腦系統損壞或盜取資訊的人。

數據
數據是各種資訊，包括文檔、文字、號碼、圖片、音頻和視頻。

缺省設置
電腦、操作系統或程式事先為用戶設定好的一些設置。

字典攻擊
基於規則和數據庫每秒進行數百萬次潛在嘗試的攻擊類型。這種攻擊對破解不太複雜和常用的短語密碼有效率高。

加密
使數據無法被他人讀取從而防止他人獲取其內容的方法。

網路
一組互相連接可共享數據的電腦、伺服器、主機、網路設備、外接設備和其他設備。

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

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。

間諜軟體
用來隱蔽地收集用戶在設備上活動資訊的程式。

令牌
多重身份認證時由實物設備或認證應用產生的安全代碼。令牌也可以指產生安全代碼的實物設備，該設備體積小，可以掛在鑰匙扣上，或者像一張信用卡。

特洛伊木馬
一種惡意軟體，通常偽裝成合法軟體，但其中含有惡意代碼，網路罪犯以此來入侵用戶的系統。

病毒
旨在造成損害，盜取個人資訊、更改數據、發送郵件、顯示訊息或以上行為組合的程式。

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。

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)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre