Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

个人网络安全
首要步骤

cyber.gov.au

个人网络安全系列

个人网络安全丛书

个人 ***网络安全首要步骤*** 是3册指南丛书的第1册，旨在帮助澳大利亚民众了解基本网络安全知识以及如何采取行动保护自己免受常见网络威胁的攻击。

你可以在 **cyber.gov.au**上阅读另外两册指南

首要步骤

进阶步骤

高阶步骤

目录

简介 1
提升个人网络安全 2
开启自动更新 2
开启多重身份验证（MFA） 4
定期备份你的设备 5
使用短语密码保护你的重要账户 6
保护你的移动设备 7
养成你的网络安全思维 8
概要核对清单 11
词汇表 12

简介

什么是个人网络安全？

在日益受技术驱动的世界里，我们每天使用的设备和账户易于遭受网络威胁：

- 你的设备可能包括电脑、手机、平板设备和其他连接网络的设备。
- 你也可能使用网络账户如电子邮件、网络银行、网上购物、社交媒体、网络游戏等等。

个人网络安全是你可以采取的一些持续步骤以保护你的账户和设备免遭网络威胁。

什么是网络威胁？

影响澳大利亚民众的主要网络威胁是 **网络骗局和恶意软件**。

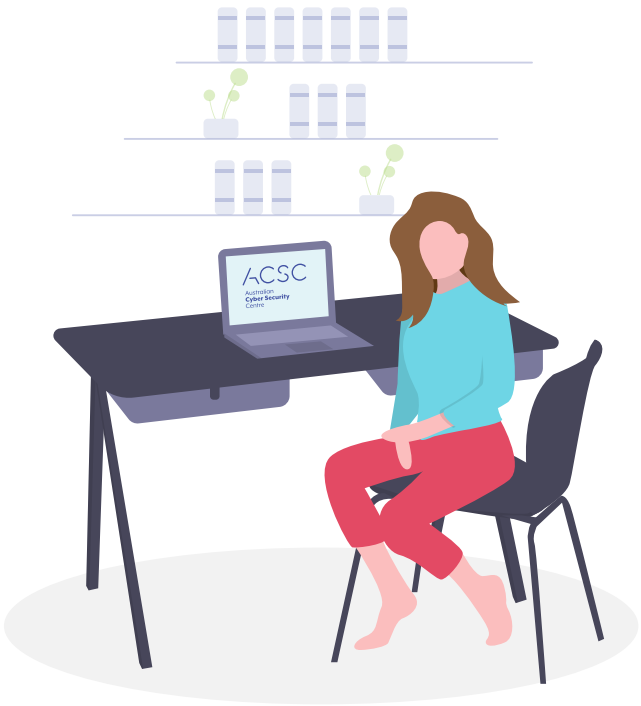
- **恶意软件是各种企图造成损害的恶意软件的总称，** 包括病毒、蠕虫、间谍软件、木马和勒索软件。网络罪犯使用恶意软件盗取你的资讯和金钱，控制你的设备和账户。
- **网络骗局是网络罪犯们发送的讯息，** 目的是操纵你披露敏感资讯或在你的设备上激活恶意软件。

这些攻击会给受害者造成严重的个人和财务损失，而且日益频繁复杂。

本手册如何帮助我免遭网络威胁？

个人*网络安全：首要步骤*是3册指南丛书的第1册，旨在帮助澳洲澳大利亚民众了解基本网络安全知识以及如何采取行动保护自己免受常见网络威胁的攻击。

无论你是首次学习还是更新网络安全知识，本手册都是极佳的出发点。



作为Australian Signals Directorate（ASD）的一部分，澳大利亚网络安全中心（ACSC）致力于提供网络安全建议、协助和操作响应措施，以防止、检测和补救对澳大利亚的网络威胁。ACSC的目标是帮助澳大利亚成为网络安全度最高的地方。

获取更多网络安全资讯、指南和建议，请访问ACSC网站cyber.gov.au

如果你认为自己是网络犯罪的受害者，请在cyber.gov.au
网站上向ACSC ReportCyber举报，或致电网络安全专线 1300 CYBER1 (1300 292 371)

了解最新的网络威胁：订阅ACSC的免费警示服务cyber.gov.au

提升个人网络安全

开启自动更新

什么是更新?

更新是你安装在服务器、电脑和移动设备上的软件(程序，应用和操作系统)经完善的版本。

软件更新能修复软件‘缺陷’(代码错误或漏洞)，保护你的设备。网络罪犯和恶意软件利用这些缺陷入侵你的设备，盗取你的个人数据、账户、财务资讯和身份。

网络罪犯们不断地发现并利用新的软件缺陷，因此更新你设备上的软件有助于保护你免遭网络攻击。

如何设置自动更新?

自动更新是默认或‘设置后忘记’设置，当有新的更新可用时自动安装。

- **在所有软件和设备上**开启并确认自动更新。
- **如何开启自动更新**取决于你的软件和设备。
- **尽可能设置一个方便的**自动更新时间，例如当你睡觉或通常不使用设备的时间。
- **你的设备必须连接电源，**打开并且有可用存储空间。

如果你收到提示更新你设备的软件，你应当尽快安装更新。

没有自动更新设置该怎么办？

如果没有自动更新设置，你应当通过软件或设备的设置菜单定期检查并安装更新。

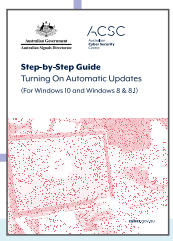
我的旧设备和软件没有收到任何更新该怎么办？

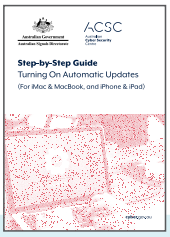
如果你的设备、操作系统或软件过于陈旧，则可能无法继续得到制造商或开发者的支持。

当产品到了‘支持终止’阶段时，将无法继续得到更新，从而使你易于因已知软件‘缺陷’遭到网络攻击。支持终止的产品包括Windows 7操作系统和iPhone 6。

如果你的设备、操作系统或软件技术支持已经终止，ACSC建议你 尽快升级以保证安全。

更多资讯请访问 **cyber.gov.au** *阅读ACSC的*支持终止快速指南手册。





有关如何开启自动更新功能的更多资讯，请参阅ACSC的*分步指南*，访问cyber.gov.au:

开启自动更新（适用于Microsoft Windows 10 和Windows 8 & 8.1）

开启自动更新（适用于iMac和MacBook，以及iPhone和iPad）

开启多重身份验证（MFA）

MFA是什么？

你可以使用多重身份认证(MFA)来提高你最重要账户的安全性。MFA要求你提供以下认证方式中两种或以上的组合才能登入账户：

- **你知道的一些事情**(例如PIN、密码或短语密码)；
- **一些你有的东西**(例如智能卡、实物令牌、认证应用、短讯或电邮)；
- **你的一些个人特性**(例如指纹、面部识别或虹膜扫描)

MFA给你的账户增加认证保护层，使网络罪犯更难获得对你账户的初始访问，因为破解账户需要更多时间、精力和资源。

双重身份验证（2FA）是最常见的MFA类型，要求两种不同的认证方式。

如何开启2FA来保护我最重要的账户？

你应当现在就开启2FA，从你最重要的账户开始：

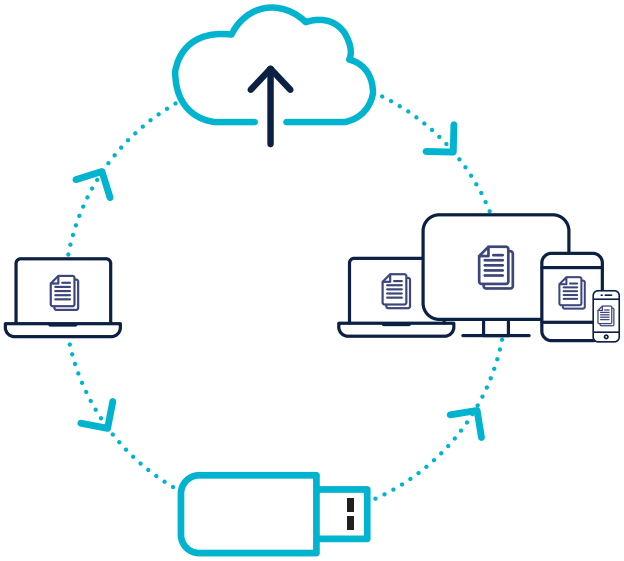
- 所有网上银行和财务账户(例如银行, PayPal)
- 所有电子邮件账户 (例如 Gmail, Outlook, Hotmail, Yahoo!)

如果你有很多电子邮件账户，优先保护那些和你网上银行或其他重要服务相连接的账户。

开启2FA的步骤根据不同的账户、设备或软件应用而有所不同。

有关如何在重要账户上开启2FA的更多资讯，请阅读ACSC的*分步指南*，访问cyber.gov.au，或访问你账户提供者的网站。

定期备份你的设备



MFA是什么？

备份是你储存在外部存储设备或云端上的最重要资讯(例如照片、财务信息或记录)的数码副本。

备份是一种预防措施， 以便在你的信息丢失、被盗或受损时， 你仍然可以恢复这些信息。

如何备份我的设备和文件？

你应该定期备份你的文件和设备。

如何备份，是每天、每周还是每月，最终由你自己决定。备份的频率可能取决于：

- **你在设备上** 传输的新文件的数量，
- **你** 对文件的修改次数，和
- 你能够承受的 **文件损失的数量**

ACSC建议你定期检查你的备份，以便熟悉恢复过程，并确保你的备份是有效的。

有关向外部存储设备和云端备份的更多详细资讯，
请参阅ACSC的*分步指南*，访问cyber.gov.au

PC个人电脑：

- *备份和恢复你的文件*
  - *PC (向云端备份)*
- *备份和恢复你的文件*
  - *PC (使用外部存储设备)*

MAC：

- *备份和恢复你的文件*
  - *Mac (向云端备份)*
- *备份和恢复你的文件*
  - *Mac (使用外部存储设备)*

IOS：

- *备份和恢复你的文件*
  - *iPhone (向云端备份)*

使用短语密码保护你的重要账户

多重身份认证 (MFA)(见第4页) 是保护你的账户免受网络罪犯攻击的最有效方法之一。**如果MFA不可用时**，和简单密码相比，独特的高保密度短语密码能更好地保护你的账户。

什么是短语密码?

短语密码使用4个或更长的随机词汇作为你的密码。

例如：‘crystal onion clay pretzel’

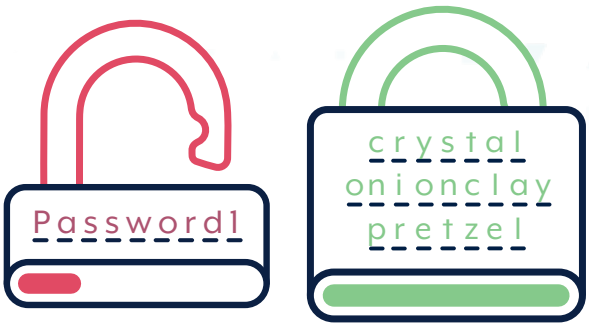
- **短语密码比普通密码** 更安全。
- 短语密码**让网络罪犯更难**破解而**你更容易**记住。

如何创建短语密码?

创建的短语密码应是：

- **足够长:** 至少14个字节，使用4个或更多随机词汇。短语密码越长越安全。
- **不可预测:** 使用4个或更多的不相关随机词汇组合。不使用著名的短语，语录或歌词。
- **独特:** 不要在多个账户重复使用。

如果网站或服务要求复杂的密码包括符号、大写字母或数字，你可以将其包括在短语密码中。你的短语密码仍然需要足够长，不可预测而且独特，以达到最佳的安全性。



我应该用短语密码保护哪些账户?

如果你最重要的账户无法得到MFA(见第4页)的保护，把你的密码改成独特的高保密度短语密码，从以下账户开始：

- ✓ **网上银行和财务账户**
- ✓ **电子邮件帐户**

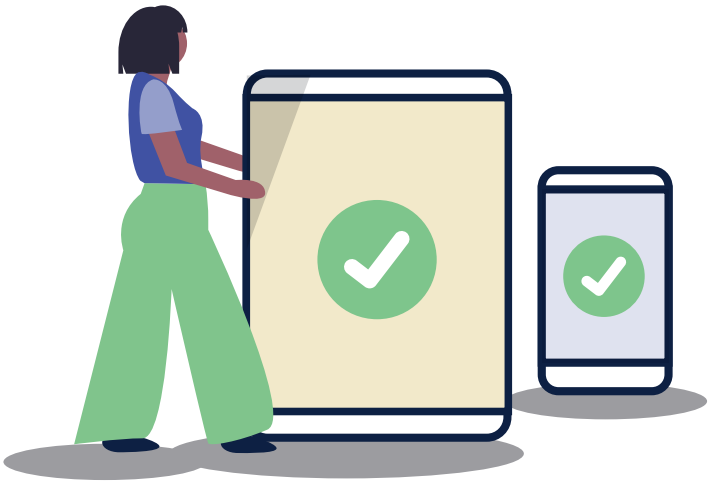
如果你有很多电子邮件账户，优先保护那些和你网上银行或其他重要服务相连接的账户。

你通常可以在你的账户设置菜单里把密码改成独特的高保密度短语密码。

“请记住：切勿在多个账户重复使用一个短语密码。”

更多如何创建高保密度短语密码的建议，请参阅ACSC的
***创建高保密度短语密码*指南** cyber.gov.au

保护你的移动设备



如今人们使用智能手机和平板设备随时随地连接网络、购物、工作、进行银行业务、研究、追踪运动健身，完成上百种其他任务。

如果我的手机被破解、丢失或被盗会发生什么？

- 网络罪犯会用你设备上存储的资讯，包括社交媒体和电子邮件账户，盗取你的金钱或身份。
- 你可能失去无法替代的数据例如照片、记事或讯息(如果没有备份)。
- 网络罪犯可能使用你的电话号码欺骗其他人。

如何保护好我的移动设备？

设备安全：

- **使用** 短语密码、密码、PIN或口令锁定你的设备。使其难以被猜测 - 你的生日和图形锁很容易被网络罪犯猜到。使用短语密码获得最佳安全保护(见第6页)。你也可以考虑使用面部识别或指纹来解锁你的设备。
- **确保** 你的设备静止一小段时间后自动锁屏。
- **切勿** 在公共充电点给你的设备充电，避免使用第三方充电器。
- **对待** 你的手机像对待钱包一样。始终随身携带并妥善保管。

软件和应用安全：

- **使用** 设备的自动更新功能，当有应用和操作系统更新可用时尽快安装(见第5页)。
- **设置** 设备要求短语密码/密码才能安装应用。家长监控也可用于这一目的。
- **检查** 在设备上安装新应用尤其是免费应用时仔细检查其隐私许可。只安装来自良好声誉开发者的应用。

数据安全：

- **开启** 远程锁定和删除功能，如果你的设备支持这些功能。
- **确保** 在出售或丢弃你的设备之前彻底删除个人数据。

连接安全：

- **关闭** 蓝牙和Wi-Fi，在你不使用它们时。
- **确保** 你的设备不会自动连接新的Wi-Fi网络。

养成你的网络安全思维

个人网络安全不仅仅是更改设置，它也涉及你的思维和行为。

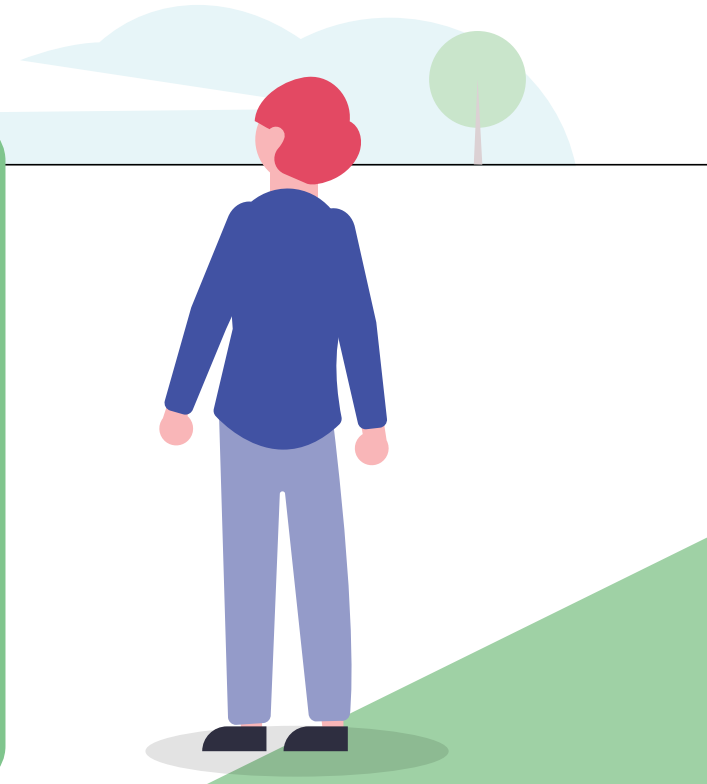
警惕网络诈骗

众所周知，网络罪犯使用电邮、讯息、社交媒体或电话尝试欺骗澳大利亚民众。这些罪犯们伪装成你认为你认识的或应该信任的个人或组织。

他们的讯息或电话试图诱骗你采取特定行动，例如：

- **披露银行账户资料，密码和信用卡号码**
- **授权你电脑的远程控制权限**
- **打开一个附件，其中可能含有恶意软件**
- **汇款或送出礼物卡**

“诈骗短讯可能发给上千人，也可能针对某个特定目标。”



我该如何识别诈骗讯息？

识别诈骗讯息并不容易。网络罪犯们通常使用一些特定的伎俩来欺骗你。他们的讯息可能有：

- **权威性**－该讯息是否声称由某个官方机构，例如银行发出？
- **紧迫性**－该讯息是否告诉你出现了问题，或你必须在限定时间内回复或付款？
- **情绪性**－该讯息是否让您感到恐慌、充满希望或好奇？
- **稀缺性**－ 该讯息是否提供了某种稀缺的东西，或承诺划算的交易？
- **实时事件性**－该讯息是否有关突发的新闻或重大事件？

了解更多如何识别网络钓鱼或诈骗讯息的知识，在ACSC网站上进行小测验cyber.gov.au

收到诈骗讯息时我该怎么做？

如果你收到诈骗讯息或电话，你应该置之不理、删除或向ACCC Scamwatch举报
scamwatch.gov.au

如果你担心自己的网络安全，也可以联络ACSC的网络安全专线 **1300 CYBER1** (1300 292 371)

如果你已经陷入了骗局并认为你的银行账户、信用卡或借记卡面临风险，应立刻联络你的金融机构。他们或许能中断交易或暂时停用你的账户。

我不确定一个讯息是否是诈骗讯息时怎么办？

如果你认为某短讯或电话可能确实来自你信任的机构(例如你的银行)，找到一个你能够信任的联络方法。访问官方网站，或拨打它们公示的电话号码，或亲自前往实体店或分行。切勿使用你收到的讯息中或通过电话获得的任何链接或联系方式，这些可能是伪造的。

如果你认为自己是网络犯罪的受害者，请在cyber.gov.au
网站上向ACSC ReportCyber举报，或致电网络安全专线 1300 CYBER1 (1300 292 371)

了解最新的网络威胁：订阅ACSC的免费警示服务cyber.gov.au
当我们发现新的网络威胁时会向你发出警示通知。

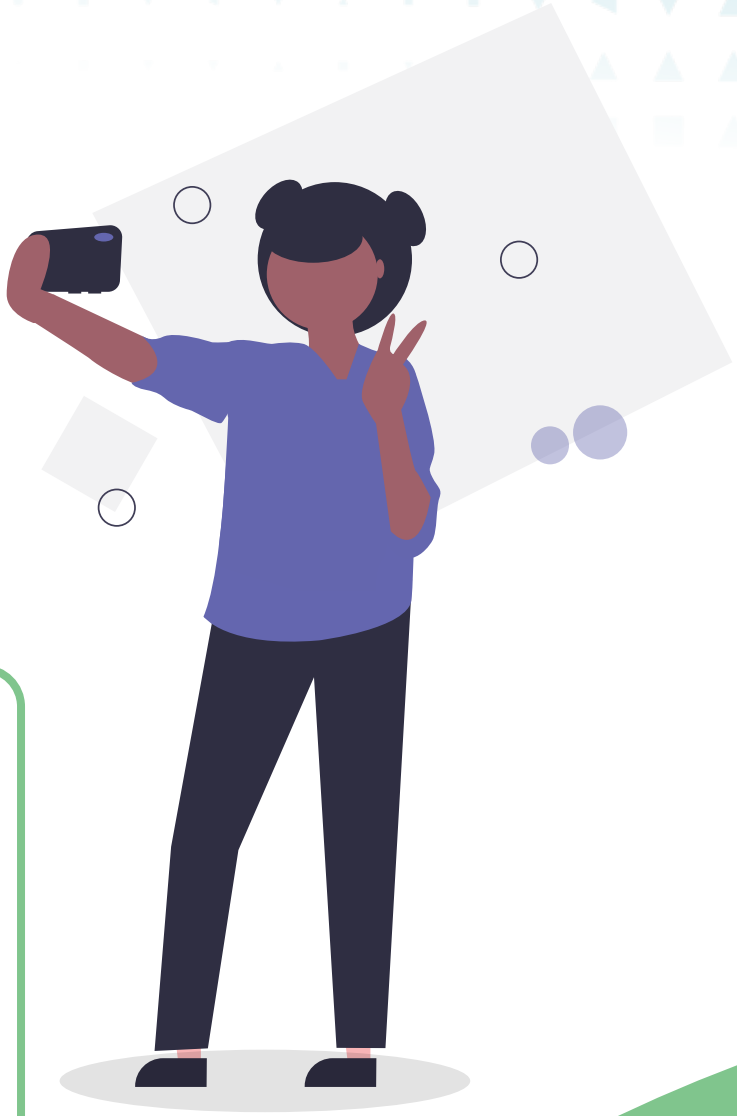
在社交媒体上分享之前慎重考虑

分享前三思而后行！网络罪犯在实施网络诈骗和网络攻击时可能使用你在社交媒体上公开发布的资讯。

切记互联网是永久性的，你永远无法完全清除所发布的内容。

发布前如何慎重考虑?

- **考虑:** 网络罪犯会如何使用这些资讯来攻击我或我的账户?
- **考虑:** 我是否能把这些资讯或图片坦然地出示给线下的陌生人?



我应该避免分享哪些资讯?

避免在网上分享有可能被网络罪犯用来:
识别你，通过骗局操纵你或推断出你账户恢复问题答案的资讯(包括图片)。这可能包括你的:

- **出生地和生日**
- **地址和电话号码**
- **雇主和工作经历**
- **曾上过的学校**
- **其他任何可能被**用来针对你的个人资讯

概要核对清单

你完成了本指南的所有内容吗？

使用这个简便的核对单来追踪你的进度：

- **我已经在所有设备上都开启了自动更新：**
  - 电脑（台式机和笔记本）
  - 手机
  - 平板电脑
- **我已经在最重要的账户上开启了多重身份认证：**
  - 我所有的网上银行和财务账户(例如银行, PayPal
  - 我所有的电子邮件账户（例如 Gmail, Outlook, Hotmail, Yahoo!）
- **我定期备份我的设备：**
  - 电脑（台式机和笔记本）
  - 手机
  - 平板电脑
- **我在最重要而且无法开启多重身份认证的账户上使用独特的高保密度的短语密码：**
  - 网上银行和财务账户
  - 电子邮件帐户
- **我已经妥善保护好我的移动设备：**
  - 笔记本电脑
  - 手机
  - 平板电脑
- **每天都使用网络安全思维：**
  - 我能够识别诈骗讯息
  - 收到诈骗讯息时我知道该怎么做
  - 如果不确定时我知道如何检查一个讯息是否是诈骗讯息
  - 我点击链接打开附件前会慎重考虑
  - 我在社交媒体上分享任何内容前会慎重考虑
- **如果我是网络犯罪或骗局的受害者我知道该如何得到帮助**

词汇表

账户恢复
用一组问题或其他认证方法来复原或重新获得账户权限或更改账户短语密码/密码。

应用
也被称为移动应用，是通常用于智能手机或平板设备上的软件。

附件
随电子邮件发送的文件。

认证应用
用于通过多重身份认证(MFA)证实电脑用户身份赋予其进入权限的应用。

云端
提供大容量分配储存和处理能力的远程服务器网络。

网络罪犯
任何非法入侵电脑系统损坏或盗取资讯的人。

设备
电脑或通讯设备。例如，一台电脑、笔记本、手机或平板电脑。

支持终止
支持终止是指一家公司停止对其产品或服务的支持。这通常是针对硬件和软件产品，当一家公司发布一个新版本时停止对之前版本的支持。

恶意软件
无授权入侵控制用户电脑，盗取资讯、扰乱或瘫痪网络的软件。

操作系统
安装在电脑硬盘上的软件，使电脑硬件运行电脑程序并同其进行通讯。例如：Microsoft Windows, Apple macOS,iOS, Android。

实物令牌
通常可挂在钥匙环上的实物设备，可以产生安全代码用于MFA电脑用户身份认证。

远程接入
从其他地方获得设备和网络的进入和控制权限。

软件
通常称为程序，一组使用户和电脑及硬件互动或执行任务的指令 。

个人
网络安全丛书下一册

现在你已经完成了ACSC的个人*网络安全:首要步骤*指南，你应该继续阅读*个人网络安全：进阶步骤*指南，请访问 cyber.gov.au

个人*网络安全：进阶步骤*指南列明了你现在可以采取的行动以进一步增强你的网络安全。

免责声明

本指南中的资料具有普遍性，不应被视为法律建议或任何特定情况下或紧急情况下的协助依据。在任何重要问题上，你应该根据自己的情况寻求适当的独立专业意见。

对于因依据本指南中的资讯而产生的任何损害、损失或费用，澳大利亚联邦不承担任何责任或义务。

版权所有

© Commonwealth of Australia 2021.

除澳大利亚国徽和另有说明的部分外，本指南中的所有资料均依据知识共享（Creative Commons）署名4.0公共许可协议国际版（www.creativecommons.org/licenses）提供。

为免生疑义，这意味着该许可协议仅适用于本指南中所列的资料。

有关许可条件的详情及CC BY 4.0许可的完整法律条文均可在CreativeCommons网站（www.creativecommons.org/licenses）上查阅。(www.creativecommons.org/licenses)

澳大利亚国徽的使用

有关澳大利亚国徽使用的条款在澳大利亚总理内阁部的网站上有详细介绍(www.pmc.gov.au/government/commonwealth-coat-arms)

欲了解更多资讯，或报告网络安全事件，请联系我们。

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

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre