Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

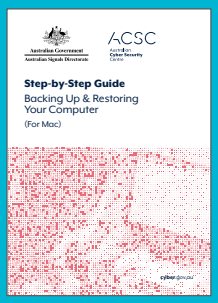
小企业网络安全指南

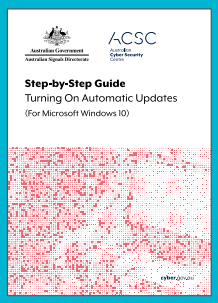
cyber.gov.au

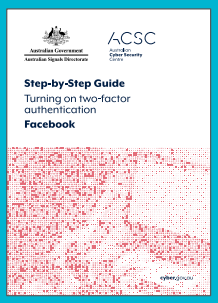
补充指南

更多保护您企业
网络安全的措施，
请访问cyber.gov.au
阅读我们的小
企业**网络安全丛书**

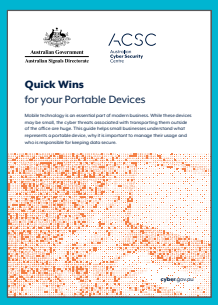
分步指南







快速指南



目录

序言 4

网络威胁：关键领域 5

恶意软件 6

诈骗短讯(网络钓鱼) 7

勒索软件 8

软件因素：关键领域 9

自动更新 10

自动备份 11

多重身份认证 12

人员和程序：关键领域 13

权限控制 14

短语密码 15

员工培训 16

概要核对清单 17

词汇表 18

序言

这一指南旨在帮助小企业保护自己免受最常见网络安全威胁。

网络安全事故有可能给小企业造成灾难性的影响。

不幸的是，我们在澳大利亚网络安全中心(ACSC)每天都会看到网络安全事故对个人、小企业和大公司造成的损害。

我们知道很多小企业的业主和运营者没有时间和资源专注于网络安全。然而，小企业可以采取一些简单的措施来避免常见的网络安全事故。

我们的 *小企业网络安全指南* 旨在帮助小企业理解、采取行动并提高其对不断演变的网络安全威胁的应对能力。指南用词简洁，行动措施简单，指南是为小企业专门设计。

本指南是理解基本网络安全知识的良好出发点。如果你希望进一步提高网络安全知识，可以在ACSC网站找到更多资讯和建议: **cyber.gov.au**

ACSC的目标是帮助澳大利亚成为网络安全度最高的地方。

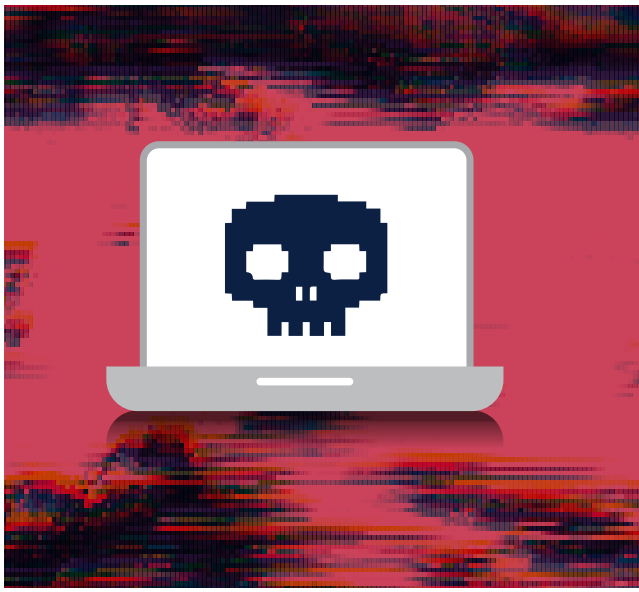
作为Australian Signals Directorate（ASD）的一部分，澳大利亚网络安全中心（ACSC）致力于提供网络安全建议、协助和操作响应措施，以防止、检测和补救对澳大利亚的网络威胁。

网络威胁：关键领域

对于小企业，即使最小的网络安全事故也可能造成灾难性的影响。

本部分旨在帮助小企业保持警惕，做好准备。识别解释最常见的网络威胁种类以及如何保护你的企业。

恶意软件 (恶意软件)



这是什么？ 旨在造成损害的无授权软件

恶意软件是勒索软件、病毒、间谍软件和木马软件等软件的总称。

为什么？ 制造混乱。损害。欺骗。

罪犯们利用恶意软件 盗取重要的资讯例如银行或信用卡号码和密码。

恶意软件也能 **控制或监控** 用户的电脑。罪犯们用这些权限和数据来：

- **欺诈**
- **身份盗窃**
- **干扰** 企业
- **盗取** 敏感数据或知识产权
- **抽取** 电脑资源进行更大范围的犯罪活动

是谁？ 任何人，任何地方

恶意软件制造者可能在世界上任何地方。

他们所需的只是一台电脑，技术和邪恶意图。罪犯们能轻易获得廉价工具使用恶意软件攻击你。

罪犯们大范围撒网，攻击最脆弱的目标。采取网络安全措施，对威胁保持警惕，你可以避免自己的企业成为攻击目标。

阻止恶意软件

- 自动更新 你的操作系统，软件和应用
- 定期备份 你的重要数据
- 培训员工 识别可疑链接和附件

诈骗短讯（网络钓鱼）

这是什么？ ‘狡猾的’电邮、短讯或电话，目的是骗取接收者的钱财和数据

罪犯们经常使用电邮、社交媒体、电话或短讯来尝试诈骗澳大利亚的企业。

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企业采取特定行动，例如：

- **支付伪造的账单** 或更改合法账单的支付资讯
- **披露银行账户资料**，密码和信用卡号码（有时也被称为‘网络钓鱼’诈骗，网络罪犯会仿制银行和网站的官方名称和标志使自己看起来是合法的。）
- **授权你电脑或服务器** 的远程控制权限
- **打开一个附件**，其中可能含有恶意软件
- **购买礼物卡** 并寄给骗子

在哪里？ 电邮、社交媒体、电话或短讯

网络钓鱼诈骗不仅仅限于电邮。它们日益复杂，更加难以识别。

警惕紧急付款和更改银行账户的请求，意外的附件，以及检查或确认登入资讯的要求。

访问 **scamwatch.gov.au** 举报骗局。

谁？ 澳大利亚企业

诈骗短讯可能发给上千人，也可能针对某个特定目标。

然而，罪犯们会用一些常用的伎俩来欺骗你的员工。他们的讯息可能有：

- **权威性：** 该讯息是否自称来自 官方人士或企业高层？
- **紧迫性：** 该讯息是否告诉你出现了问题，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？

如果你认为某短讯或电话可能确实来自你信任的机构(例如你的银行或供应商)，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。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。

勒索软件

这是什么？勒索软件是一种恶意软件，它锁定你的电脑或文件，直到你支付赎金

勒索软件锁定或加密你的文件，使你无法再使用或访问它们。有时甚至能让你的设备无法运行。勒索软件可以用和其他恶意软件一样的方式感染你的设备。例如：

- 访问不安全或可疑的网站
- 打开不明来源的链接、邮件或文件
- 网络或设备(包括服务器)安全度低

为什么？金钱

勒索软件给网络罪犯们提供低风险高回报的收入。它们易于开发和传播。赎金通常通过网上数字货币或加密货币如Bitcoin支付，使其难以被追踪。此外对网络罪犯有利的是，多数小企业没有做好应对勒索软件攻击的准备。

谁？小企业，中型企业和大企业

小企业可能尤其脆弱，因为它们不太可能采取有助于阻止勒索软件并复原系统的网络安全措施。

切勿支付赎金

支付赎金不能保证受害者的文件得到复原，也不能阻止被盗数据被公开或被出售用于其他犯罪活动。这也会增加受害者再次成为攻击目标的可能性。

如果你遇到勒索软件需要支持，致电ACSC 24/7热线 1300 CYBER1 (1300 292 371)

无论是否决定支付赎金，我们都鼓励受害者登录cyber.gov.au向ACSC举报勒索软件事件。分享事件资讯有助于保护其他澳大利亚企业。

阻止勒索软件并复原

- 定期备份你的重要文件
- 自动更新你的操作系统，软件和应用
- 如有可能，要求多重身份认证使用服务(第12页)
- 审查并保护你网络上的设备(包括服务器)和任何连接互联网的服务(远程桌面，文件共享，网页邮件)。如果对此不确定，咨询IT专业人士。

软件因素：关键领域

妥善管理你的软件，数据和网上账户能够大大提高企业对最常见网络威胁的防御能力。

例如，操作系统是电脑上最重要的软件。它管理你电脑的硬件和所有程序，因此需要定期更新，确保你始终在使用最安全的版本。

提高复原力，保持更新，注意这些软件因素，保持小企业长久安全。

自动更新

这是什么？ 软件更新

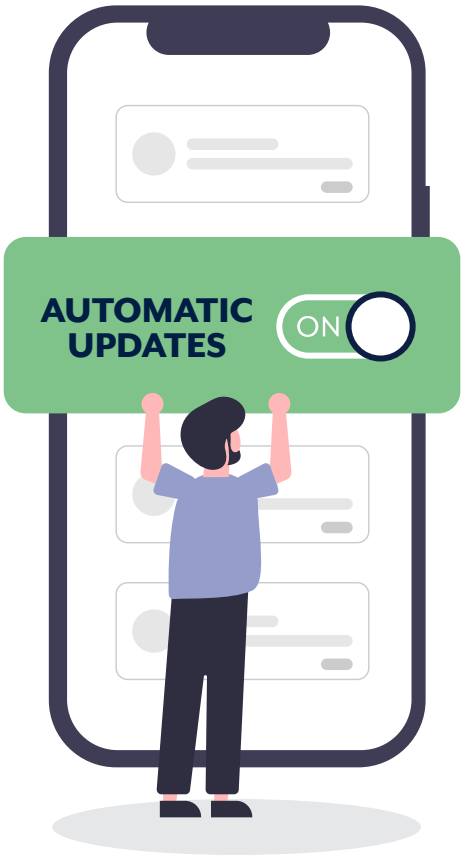
更新 **是** 你安装在服务器、电脑和移动设备上的软件(程序，应用和操作系统)经完善的版本。自动更新 **是** 默认或 **‘设定后忘记’** 系统，有更新时自动更新你的软件。

为什么？ 安全

- 保持操作系统和应用程序更新是 **保护自己免受** 网络攻击的最佳方法之一。
- 定期更新你的软件 **可以减少网络罪犯利用已知漏洞** 运行恶意软件或入侵你电脑的机会。
- **节省时间和顾虑，** 自动更新是保护你的设备和数据安全的重要方法

什么时候？ 今天和每一天

- **开启自动更新**, 尤其是操作系统
- **如果自动更新不可用，** 定期检查是否有更新
- 如果你收到提示更新你的操作系统或其他软件，你应当 **尽快安装更新**
- **设置一个合适的自动更新时间** 以避免对企业正常运营造成干扰。
- 如果你使用 **防病毒软件，确保开启自动更新**



注意：

如果你的软件或硬件过于陈旧，可能无法更新，从而令你的企业易于出现安全问题。

ACSC建议你尽快升级你的设备和软件。

截至2020年，Windows 7, Microsoft Office 2010 和 Windows Server 2008 支持已经终止从而不再安全。

更多资讯请阅读ACSC的支持终止 *快速指南* 手册，访问 cyber.gov.au

自动备份

这是什么？ 数据备份

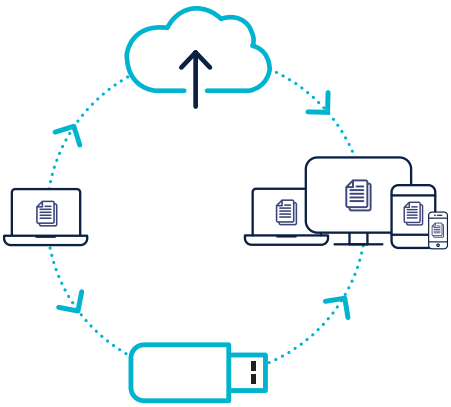
备份 是你企业最重要资讯例如客户资料和财务记录的数码副本。备份可以被保存到外部存储设备或云端上。

自动更新 是默认或‘设定后忘记’系统，无需人力介入自动备份你的数据。

每次备份后安全地移除你的备份存储设备连接，这将保证其在遭到网络攻击时仍然安全。

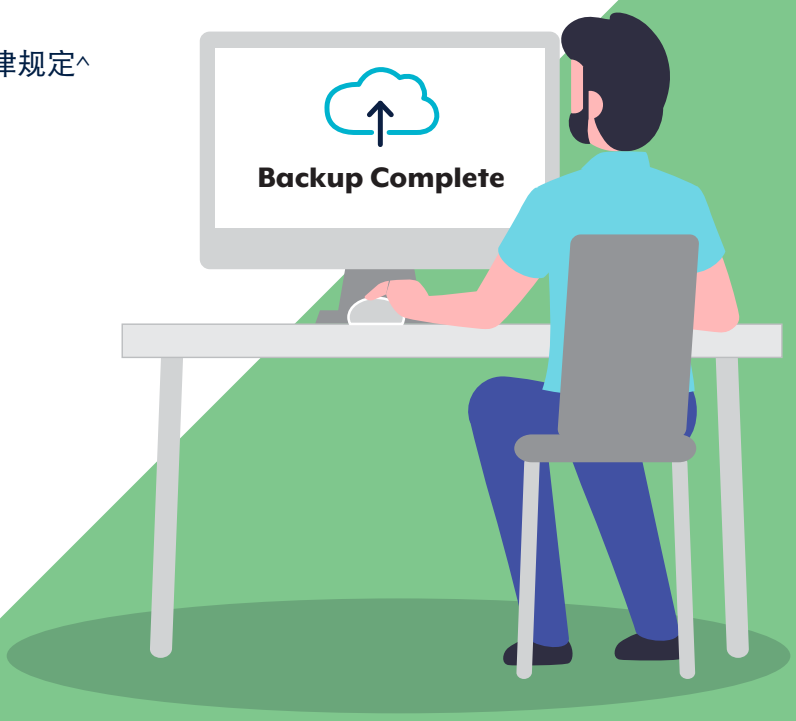
为什么？ 轻松复原

- **备份是一种预防措施，** 以便在你的信息丢失、被盗或受损时， 你仍然可以访问这些数据
- **让你的企业能够在遭受网络攻击(例如勒索软件)后** 复原并尽可能缩短停工时间
- **保护你企业的可信度** 并有助于符合法律规定^



什么时候？ 今天和每一天

- **选择一个适合你企业的备份系统**考虑在最坏情况下你可以承受的损失，这有助于你确定具体需求例如备份数据的频率
- **定期检验备份** 尝试复原数据
- **始终保持至少一个备份不连接你的设备，** 最好是存放在另一个不同的场所以避免自然灾害或盗窃的影响。
- **不要把你的备份连接到感染勒索软件或病毒的设备上**



^某些行业有义务在特定期间保存记录。
确保自己了解你的数据保存要求。

多重身份认证

这是什么？ 一个要求两种或更多身份证明来获得权限的安全措施

多重身份认证 (MFA) 通常要求以下组合：

- **一些你知道的事情** (密码/短语密码,PIN, 保密问题)
- **一些你有的东西** (智能卡，实物令牌，认证应用)
- **一些你的生物特征** (指纹或其他生物识别)

为什么？ 安全防护力大大提高

MFA是防止无授权入侵你重要资讯和账户的最有效方法之一。

多重保护增加了罪犯攻击你企业的难度。罪犯也许能盗取一部分身份如你的密码，但他们仍然需要获得并使用其他身份证明才能进入你的账户。

在哪里应用？ 登入重要账户

小企业应尽可能在重要账户上开启MFA，财务和电邮账户优先。MFA选项包括，但不限于：

- 实物令牌
- 随机PIN
- 生物识别/指纹
- 认证应用
- 电邮
- 短讯

人员和程序：**关键领域**

无论企业规模多小，都需要了解并在各个层面主动实施网络安全措施。

你的内部程序和员工是阻止网络安全威胁的最后也是最重要的防线。

鉴于小企业通常没有足够资源设置专职IT人员，本部分讲解你应如何管理企业的资讯权限，保护你的企业账户，并培训员工防止、识别和举报网络安全事件。

权限控制

这是什么？管理你企业电脑环境里谁能够获得什么资讯

权限控制是一种限制电脑系统进入的方法。它通过限制以下进入权限来保护你的企业：

- 文件和文件夹
- 应用程序
- 数据库
- 邮箱
- 网上账户
- 网络

为什么？尽可能降低无授权获取重要资讯的风险

一般而言，员工不需要获得企业的所有数据、账户和系统权限来做自己的工作。

该权限应尽可能受到限制，这样员工和外部供应商不会无意或有意威胁你的企业。

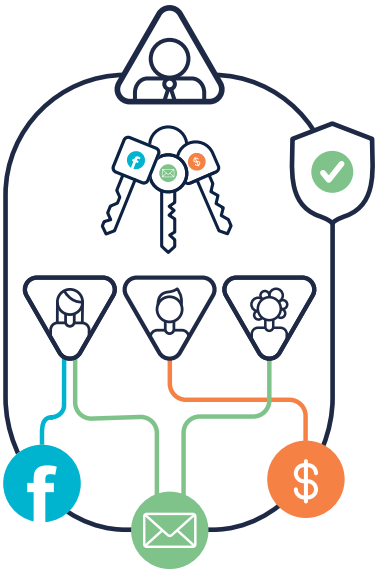
权限控制系统和程序让企业主和运营者能够：

- **决定谁可以有权限获得** 特定文件、数据库和邮箱
- **控制任何赋予外部供应商的权限** 如会计师，网站托管商
- **限制谁有账户权限** 例如供应商网站和社交媒体
- **任何账户、设备或系统被入侵时** 降低潜在的损失
- **当员工更换职位或辞职时** 取消其系统和数据权限

谁？最小权限原则.

取决于企业的性质，最小权限原则对大多数小企业来说是最安全的方法。

该原则仅授予员工完成工作所需的最低权限。这样也能减少‘内部人’无意或有意威胁企业的风险。



权限控制原则

- 把员工在企业设备上从‘管理员’账户过渡到标准账户。
- 复审数码文件和文件夹的权限许可
- 不要在员工之间共享账户或密码/短语密码
- 当员工辞职或你更换供应商时记得取消权限，删除账户并/或更换密码/短语密码

短语密码

这是什么？ 更安全版本的密码

多重身份认证 (MFA,见第12页) 是保护你的账户免受网络罪犯攻击的最有效方法之一。无法采用MFA时，你应当使用短语密码来保护你的账户。

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 onionclay pretzel’

为什么？ 安全且容易记住

这让网络罪犯更难破解而你更容易记住。

创建的短语密码应是：

- **长度足够：** 短语密码越长越好。长度最好在14个字节以上。
- **不可预测：** 使用混合的不相关随机词汇。不使用著名的短语，语录或歌词。
- **独特：** 不要在多个账户上重复使用一个短语密码

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。

在哪里应用？ 你的账户和设备

如果你无法在账户或设备上使用MFA，则应当使用短语密码来保证安全。在此情况下，一个安全的短语密码可能是入侵者和你重要资讯之间仅有的障碍。

记住你的短语密码应该是独特的，因为重复使用密码会让网络罪犯更容易入侵多个账户。

更多创建短语密码的建议，请见ACSC的*创建高保密度短语密码*指南 **cyber.gov.au**

考虑使用密码管理应用

使用密码管理应用(也可以用来存储短语密码)是良好的网络安全习惯。给每个重要账户创建一个独特的短语密码听起来难以做到，但使用密码管理应用储存你的短语密码可以解除你记住哪个短语密码用在哪里的负担。
确保你使用的任何密码管理应用都是来自可信且有良好声誉的来源而且其自身也得到高保密度也易于记住的短语密码保护。

员工培训

这是什么？保护员工和企业免受网络威胁的教育

教育自己和员工如何防止、识别和举报网络犯罪。

给员工基本网络安全培训，包括更新他们的设备，保护他们的账户，以及识别诈骗短讯。

你还应该考虑实施 **网络安全事故应对** 计划，在出现网络事故时指导你的企业和员工如何应对。

这有助于你了解你的关键设备和程序，以及关键联络者以做出应对和复原。

为什么？员工会成为阻止网络安全威胁的第一道和最后一道防线

培训能够改变员工的习惯和行为并产生共享责任来保护企业安全。

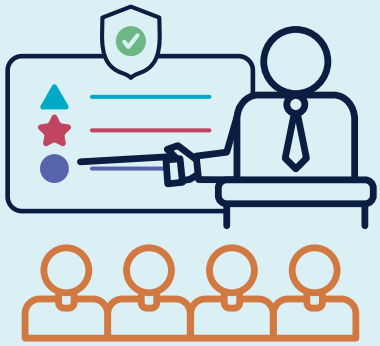
网络安全人人有责。

什么时候？定期网络安全宣传培训

网络安全在不断演变。

让所有人都了解最新网络安全威胁可能事关罪犯是否能够入侵你的资金、账户和数据。

“教育自己和员工如何防止、识别和举报网络犯罪。”



网络安全宣传提示

- 培训员工识别可疑链接和附件
- 定期提供更新的网络安全培训
- 制订网络安全事故应对计划
- 鼓励浓厚的网络安全文化
- 分享诈骗短讯范例，帮助员工识别网络安全威胁

概要核对清单

软件因素

自动更新你的操作系统，软件和应用

- 如果你收到提示更新你的操作系统或其他软件，你应当尽快安装更新
- 设置一个合适的自动更新时间以避免对企业正常运营造成干扰。

定期备份你的重要数据

- 定期检验备份尝试复原数据
- 始终保持至少一个备份不连接你的设备

尽可能在重要账户上开启MFA

- MFA是防止无授权入侵你重要资讯和账户的最有效方法之一
- 优先保护财务和电邮账户以获得最佳效果

人员和程序：

管理你的企业里谁能够获得什么资讯

- 采用最小权限原则
- 当员工辞职或你更换供应商时记得取消权限，删除账户并/或更换密码/短语密码

当MFA不可用时，使用短语密码保护账户和设备

- 短语密码使用4个或更长的随机词汇作为你的密码
- 短语密码需要足够长，不可预测且独特才是最有效的

为员工进行基本网络安全培训

- 包括更新他们的设备，保护他们的账户，以及识别诈骗短讯
- 定期提供更新的网络安全培训

词汇表

防病毒软件
旨在保护你的电脑和网络不受病毒感染的软件程序。

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。

生物识别
通过识别人的生物特性例如指纹或声音验证其身份。

比特币
在互联网上用于多种服务的数码货币(加密货币)。

暴力破解攻击
一种每秒钟产生数百万字节组合的攻击方法。这种方法对破解简短的密码很有效。

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。

数据
数据是各种资讯，包括文件、文字、号码、图片、音频和视频。

默认设置
电脑、操作系统或程序事先为用户设定好的一些设置。

字典攻击
基于规则和数据库每秒进行数百万次潜在尝试的攻击类型。这种攻击对破解不太复杂和常用的短语密码有效率高。

加密
使数据无法被他人读取从而防止他人获取其内容的方法。

网络
一组互相连接，共享数据的电脑、服务器、主机、网络设备、外围设备和其他设备。

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

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 。

间谍软件
用来隐蔽地收集用户在设备上活动资讯的程序。

令牌
多重身份认证时由实物设备或认证应用产生的安全代码。令牌也可以指产生安全代码的实物设备，该设备体积小，可以挂在钥匙扣上，或者像一张信用卡。

特洛伊木马
一种恶意软件，通常伪装成合法软件，但其中含有恶意代码，网络罪犯以此来入侵用户的系统。

病毒
旨在造成损害、盗取个人资讯、更改数据、发送邮件、显示讯息或以上行为组合的程序。

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