Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

小型企业网络安全指南

内容复杂度
简单 ●○○

cyber.gov.au

简介

对于小型企业，即使轻微的网络安全事件也可能带来毁灭性的影响。本指南包含可帮助保护您的企业免受常见网络安全威胁的基本安全措施。首先，我们建议采取以下三项措施：

- 开启多重身份验证
- 更新您的软件
- 备份您的信息

本指南可能包含与您的企业无关的措施，或者您的企业可能有更复杂的需求。完成本指南后，我们建议小型企业实施基本八项（Essential Eight）缓解策略的一级成熟度。如果您对此建议或更广泛的网络安全有疑问，我们建议您咨询IT专业人士或值得信赖的顾问。

请访问 cyber.gov.au 阅读我们的完整指南，其中包括每项措施的操作建议。

目录

小型企业面临的威胁 4
诈骗消息 4
电子邮件攻击 5
恶意软件 6
保护您的账号 7
开启多重身份验证 7
使用强密码或密码短语 7
管理共用账号 7
实施访问控制 7
保护您的设备和信息 8
更新您的软件 8
备份您的信息 8
使用安全软件 8
保护您的网络和外部服务 9
加固您的网站 9
在出售或丢弃设备之前重置设备 9
保持设备锁定并确保设备物理安全 10
保护您的企业数据 10
让员工做好准备 11
对员工进行科普 11
制定应急计划 11
随时了解最新动态 11

小型企业面临的威胁

诈骗消息

网络犯罪分子常常将小型企业当成诈骗的目标。他们的目标是欺骗您或您的员工，让您或员工：

- 汇款或寄送礼品卡
- 点击恶意链接或附件
- 泄露密码等敏感信息。

网络犯罪分子可能会尝试通过电子邮件、短信、电话和社交媒体来对您的企业实施诈骗。他们通常会假装成您信任的个人或组织。

网络钓鱼攻击

网络钓鱼攻击是小型企业特别需要注意的问题。这些诈骗通常包含虚假网站的链接，鼓励您登录账号或输入机密信息。

网络钓鱼攻击通常会泄露您的账号密码。网络犯罪分子经常利用这种方法来“控制”小型企业的社交媒体账号，并用其勒索钱财。

降低风险的方法

如果消息来自一个已知实体并且看起来很可疑，请谨慎行事。单独联系该个人或企业，以检查该消息是否属实。使用您通过真实来源（例如通过访问该企业的官方网站）找到的联系方式，而不是可疑消息中包含的联系方式。

使用以下资源了解识别诈骗和网络钓鱼攻击的更多信息：

- 识别并举报诈骗
- 了解如何识别网络钓鱼诈骗
- 识破社交工程诈骗消息。

案例研究：

一家快递公司的员工收到了一封来自本公司高管的电子邮件，要求她购买6张面值500澳元的万事达预付礼品卡。这位高管告诉她要保密，这些卡片将作为给员工的礼品券。购买后，该员工被要求拍摄卡片的正反两面并将其发给这位高管，作为购买证明。

该员工按照指示前往邮局并使用她的个人信用卡购买了礼品卡。她回复了高管的电子邮件，发送了礼品卡的照片作为证据。

从邮局回来后，该员工将实体卡片交给了这位高管，而高管对此事并不知情。经审查，**所有有关礼品卡的电子邮件都来自一个陌生的电子邮件地址，而非来自该高管的真实电子邮件账户。之前的一切其实都是诈骗。**

电子邮件攻击

除了网络钓鱼等诈骗之外，针对小型企业的常见的电子邮件攻击是**商务电子邮件泄露** (BEC)。犯罪分子可以通过使用泄露的电子邮件账户或其他方式（例如使用与真实企业类似的域名）来冒充企业代表。除了窃取信息之外，这些攻击的目标通常是欺骗受害者将资金汇款到诈骗者运营的银行账户。

降低风险的方法

对电子邮件攻击的最佳防范措施是对员工进行培训并提高他们的防范意识。确保您的员工知道要时刻对包含以下内容的电子邮件提高警惕：

- 付款请求，特别是紧急或逾期的付款请求
- 更改银行信息
- 电子邮件地址看起来不太对，例如域名与供应商的公司名称不完全匹配。

虽然这些攻击可能是毁灭性的，但降低风险的措施很简单，而且几乎不需要任何花费。**当员工收到此类电子邮件时，降低风险的最有效措施是向发件人致电，确认对方是否真的发送了邮件。**请勿使用邮件里留的联系方式，因为这些联系方式可能是假的。引入正式流程，以便员工在收到付款请求或银行信息更改时可以遵循该正式流程操作。

了解如何使用以下资源来保护您的企业，防范BEC诈骗和电子邮件泄露：

- 商务电子邮件泄露
- 保护您的企业，防范电子邮件欺诈和泄露
- 如果您的企业成为电子邮件欺诈或电子邮件泄露的目标，该怎么办?

案例研究：

一家小型建筑企业收到了供应商发来的一封电子邮件，称他们已更换银行。这家供应商提供了新账户信息，用于支付发票款项。由于该电子邮件看起来很真实，**因此该建筑企业没有致电供应商确认银行账户信息的更改是否属实。**

该企业向供应商支付了超过7万澳元的发票。第二天，另一名员工又错误地再次对同一张发票付款，额外支付了超过7万澳元的金额。总共向新银行账户支付了超过15万澳元。

当该企业向供应商致电询问是否可以退还重付的款项时，供应商告知说这些银行信息不正确。有关方面立即展开调查，供应商发现黑客入侵了他们的一个电子邮件账号，并发送了欺诈性的银行账户信息。**各方没能追回任何钱。**

恶意软件

恶意软件是意在造成危害的恶意软件的总称，例如勒索软件、病毒、间谍软件和木马软件。恶意软件可能会：

- 窃取或锁住您设备上的文件
- 窃取您的银行信息或信用卡卡号
- 窃取您的用户名和密码
- 控制或监视您的计算机。

恶意软件可能会让您的设备无法正常工作、删除或损坏您的文件，或者让其他人访问您的个人或企业信息。如果设备感染了恶意软件，您可能很容易受到其它攻击。该恶意软件还可能传给连在您网络上的其它设备。

有多种方式使您的设备遭到恶意软件感染，包括：

- 访问被恶意软件感染的网站
- 从互联网下载被感染的文件或软件
- 打开被感染的电子邮件附件。

勒索软件

勒索软件是一种常见且危险的恶意软件。它的工作原理是将您的文件锁定或加密，使您无法再访问这些文件。需要支付赎金（通常以加密货币的形式）才能恢复对文件的访问权限。网络犯罪分子还可能威胁说除非支付赎金，否则要在网上公开或出售数据。

降低风险的方法

虽然防病毒软件或安全软件可以帮助您防范恶意软件，但没有任何软件是100%有效的。员工必须对电子邮件、网站和文件下载保持警惕，并定期更新设备以确保安全。

请参阅以下资源，了解防范勒索软件侵害您的企业的更多信息：

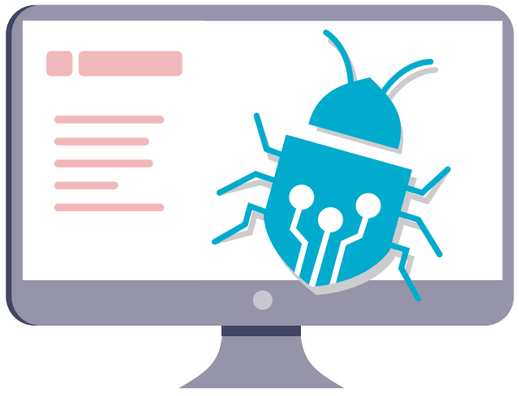
- 勒索软件
- 防范勒索软件的攻击
- 如果您被勒索赎金，该怎么办？

案例研究：

某一天早晨，一家汽车配件商店的员工来上班时发现无法启动他们的服务器计算机。当其IT提供商访问服务器时，他们发现了一个打开的窗口，其内容称所有计算机数据都已被加密。这条信息要求他们支付比特币赎金以解锁文件。

该计算机上插入了一个备份驱动器，该驱动器也已被加密。他们尝试连接更多的备份驱动器，但文件在几秒钟内就被自动加密。**他们在尝试恢复数据之前未能删除勒索软件，而且丢失了所有备份文件。**

剩下的唯一选择是将服务器恢复出厂设置并使用新系统重新开始。他们的业务丢失了多年的数据，不得不重新开始。



保护您的账号

开启多重身份验证

多重身份验证 (MFA) 让网络犯罪分子更难访问您的账号。

多重身份验证为您的账号增添了一重安全保障。这是防止他人访问您的账号的最有效方法之一，因此您应该尽可能使用多重身份验证。任何登录您账户的人都需要提供除了您的用户名和密码之外的其它信息。这可以是短信或身份验证应用程序中包含的唯一代码。如需了解更多信息，请阅读有关多重身份验证（MFA）的建议，可在**cyber.gov.au/mfa**上浏览。

✓ **从最重要的账号开始，尽可能启用多重身份验证。**

实施访问控制

限制用户访问可以降低网络安全事件的危害。

访问控制是一种限制访问某些文件和系统的方法。通常，员工不需要拥有企业所有数据、账号和系统的完全的访问权限。只应允许他们访问履行自己职责所需的内容。

限制访问有助于降低网络安全事件造成的危害。例如，如果某一员工的计算机感染了勒索软件，在有适当访问控制的情况下，这可能只会影响少量文件，而不是整个企业。

✓ **确保每个用户只能访问履行自己职责所需的内容。**

使用强密码或密码短语

使用安全密码或密码短语保护您的账户，防范网络犯罪分子的入侵。

许多小型企业因为设密码的方式不当而面临网络攻击。例如，在多个账户上重复使用相同的密码。您可以使用密码管理器和密码短语来创建强密码。

密码管理器就像密码的虚拟保险箱。您可以用它为每个账号创建和存储**独一无二**的强密码。如果您有许多账号，这将帮您免除记住独一无二密码的负担。您不必记住各个密码或它们所属的账号，因为这些都记录在您的密码管理器中。

对于您定期登录的账号，或者您不想将密码存储在密码管理器中的账号，请考虑使用密码短语作为密码。密码短语是随机单词的组合，例如“crystal onion clay pretzel”。当您想要一个易于记住的安全密码时，密码短语非常有用。使用四个或四个以上单词的随机组合，并保持其唯一性——**不要在多个账号上重复使用一个密码短语**。如需了解更多信息，请阅读我们对密码短语和密码管理器的建议，可在**cyber.gov.au/passphrases**上浏览。

✓ **使用密码管理器为您的每个重要账号创建和存储独一无二的密码。**

管理共用账号

共用账号可能会危及安全性，并使跟踪恶意活动变得困难。

在小型企业中，员工可能有合理的理由需要共用账号，但应尽可能避免这种做法。当多名员工使用同一账号时，可能很难追踪某个特定员工的活动，也更难追踪入侵的网络犯罪分子。除非您更改密码，否则员工在离职后也可以继续访问账号。

✓ **限制共用账号的使用，并保护您的企业所使用的任何账号。**

保护您的设备和信息

更新您的软件

始终将软件更新到最新版本是保护您的企业免受网络攻击的最佳方式之一。

更新可以修复操作系统和其它软件中的安全缺陷，让网络犯罪分子更难入侵。新的漏洞一直被人发现，因此不要忽略让您更新的提示。定期更新软件将降低网络犯罪分子利用已知弱点运行恶意软件或侵入您设备的几率。如果您需要帮助，ACSC已就软件更新发布指南。

如果您的设备或软件太旧，可能无法进行更新。如果制造商已停止支持产品更新，您应考虑升级到更新的产品以确保安全。举例而言，**iPhone 7**和**Microsoft Windows 7**等系统已不再接收重大更新。

如需了解更多信息，请阅读我们对软件更新的指南，可在**cyber.gov.au/updates**上浏览。

✓ **为您的设备和软件启用自动更新。**

使用安全软件

防病毒软件和勒索软件防护工具等安全软件可以帮助保护您的设备。

使用安全软件检测并删除您设备中的恶意软件。可以将防病毒软件设置成定期扫描可疑文件和程序。发现威胁时，您将收到警报，可疑文件将被隔离或删除。

许多小型企业可以**使用Windows安全中心（Windows Security）**来防范病毒和恶意软件。Windows 10和Windows 11设备中内置有Windows安全中心，包括免费的病毒和威胁防护。您还可以用安全中心来打开设备上的勒索软件防护功能。

如需替代产品和选项，请阅读我们关于防病毒软件的建议，在cyber.gov.au上搜索*antivirus*（防病毒）。

✓ **将安全软件设置成在设备上定期进行扫描。**

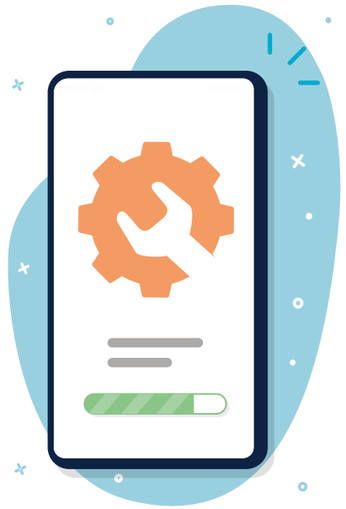
备份您的信息

定期备份可以帮助您在信息丢失或泄露时进行恢复。

备份重要信息应该成为您企业的常规操作或自动操作。如果没有定期备份，您可能无法在网络攻击后恢复信息。

您可以使用多种方法和产品来备份信息。关于对您的业务进行信息备份的详细建议，请阅读我们对信息备份的建议，可在**cyber.gov.au/backups**上浏览。每家企业的最佳选择都不同，因此如果您不确定，请咨询IT专业人士。

✓ **创建定期备份您信息的计划并实施该计划。**



保护您的网络和外部服务

通过解决您网络中的潜在漏洞，保护您的企业免受网络攻击。

您网络中的设备和服务可能成为网络犯罪分子的主要目标。许多这些系统的安全保护可能很复杂，因此请与IT专业人员讨论以下建议。

- **保护您的服务器：**如果您在家或企业使用NAS或其它服务器，请格外小心确保其安全。这些设备是网络犯罪分子的常见目标，因为它们通常存储重要文件或执行重要功能。保护这些设备需要采取许多降低风险的策略。例如，请务必确保定期更新所有服务器或NAS设备。应使用强密码短语或多重身份验证来保护管理员账号。
- **尽可能减少对外暴露的足迹：**审核并保护您网络上任何暴露于互联网的服务。这可能包括远程桌面、文件共享、网络邮件和远程管理服务。
- **迁移至云服务：**考虑使用提供内置安全性的在线服务或云服务，而不是自行管理。例如，使用在线服务来处理电子邮件或网站托管等事务，而不是自己运行和保护这些服务。
- **提高路由器的安全性：**请遵循我们关于保护路由器的方法的指南，包括更新默认密码、为顾客或访客打开“访客”Wi-Fi，以及使用最强的加密协议。在**cyber.gov.au**上搜索*router*（路由器）了解更多信息。
- **了解您的网络供应链：**现代企业经常外包多项服务。例如，使用托管服务提供商来维护其IT。这些服务或提供商的安全问题可能会对您的业务产生重大影响。了解网络供应链风险管理的详细建议，请在 **cyber.gov.au** 上阅读我们的网络供应链指南。

✓ **咨询IT专业人士，以了解保护网络安全的各种方法。**

加固您的网站

网站是网络攻击的主要目标。

通过以下一些基本的安全措施来保护您的网站，防范遭到劫持：

- 使用多重身份验证或强密码保护您的网站登录
- 定期更新网站的内容管理系统和插件
- 定期备份您的网站，以便在遭受网络攻击后可以将其恢复。

ACSC为网站所有者提供了额外的资源。请在**cyber.gov.au**上搜索这些资源：

- 帮您的网站实现速赢
- 实施证书、TLS、HTTPS和机会TLS
- 域名所有者的域名系统安全
- 准备和应对拒绝服务（DoS）攻击

✓ **通读ACSC有关网站安全的资源。**

在出售或丢弃设备之前重置设备

旧设备上的数据可能会被陌生人访问。

如果您不安全地丢弃设备，网络犯罪分子可能会访问其中的信息。这可能包括电子邮件、文件和其他企业数据。在出售、交易或丢弃企业设备之前，请删除上面的所有信息。例如，恢复出厂设置。这将有助于抹去所有信息并将设备恢复到原始设置。

了解重置设备的建议，请阅读我们对如何安全丢弃设备的指南。请在**cyber.gov.au**上搜索*dispose*（丢弃）。

✓ **在出售或丢弃企业设备之前对其恢复出厂设置。**

保持设备锁定并确保设备物理安全

限制对企业设备的访问将可以降低恶意活动的几率。

限制对企业设备的物理访问是防止数据被盗或其它恶意活动的一种简便方法。企业设备不应存放在未经授权的员工或公众可以访问的地方。

使用安全控制措施来进一步保护您的企业设备。至少应使用密码短语、PIN码或生物识别技术来锁定设备。确保将这些设备设置为在短时间内没有操作后自动锁定。

✓ **将设备配置为在短时间内没有操作后自动锁定。**

保护您的企业数据

您的企业保存的数据对于网络犯罪分子来说是很有吸引力的目标。

数据泄露事件呈上升趋势——不要让您的企业成为受害者。请务必了解您的企业保存了哪些数据以及保存的位置。了解了这些之后，请使用本指南中的建议来帮助保护您的数据，以免网络犯罪分子访问它们。一些小型企业可能还有额外的法律义务。

- **统一管理企业数据。**您可能将数据存储在许多设备或服务中。当数据分散存储时，会增加您需要保护和备份的系统数量。大量系统还会为网络犯罪分子创造更多的攻击机会。如果可能，请将您的企业数据存储在一个安全并定期备份的集中位置。集中存储数据可能会在系统遭受入侵时造成更大的数据泄露，因此请确保通过安全配置和限制访问来充分保护该集中位置。请向IT或网络安全专业人士寻求建议。
- **了解您保护数据的义务。**一些小型企业可能对他们收集的个人信息的处理方式负有法律义务。请阅读澳大利亚信息专员办公室（Office of the Australian Information Commissioner）针对小型企业的指南以了解更多信息，其网址为**oaic.gov.au**。如果您不确定，咨询法律专业人士。

✓ **了解您的企业保存的数据以及您对保护这些数据负有哪些责任。**

让员工做好准备

对员工进行科普

具备良好网络安全实践的员工是您抵御网络攻击的第一道防线。

员工应具备网络安全意识，包括以下主题：

- 常见的网络安全威胁，例如商务电子邮件泄露和勒索软件
- 保护措施，包括强密码或密码短语、多重身份验证（MFA）和软件更新
- 如何识别诈骗和网络钓鱼攻击
- 企业特定政策（例如，报告可疑电子邮件或在付款前验证发票真实性的流程）
- 紧急情况下该怎么做。

ACSC网站上提供了大部分主题的资源，请浏览cyber.gov.au/learn。您可以考虑用其它方式对员工进行科普，例如正式课程或内部培训。无论您如何决定，请记住，网络安全培训不是一次性的要求，应该定期温故知新。

✓ **确定如何在企业中教授网络安全意识。**

制定应急计划

应急计划可以降低网络攻击对您的企业造成的影响。

在应对网络安全事件时，每一分钟都很重要。制定应急计划意味着您的员工可以花更少的时间弄清楚该做什么，因而有更多的时间来采取行动。

制定应急计划时请考虑以下问题：

- 员工报告潜在网络安全事件的流程是什么？
- 您应该联系谁以寻求帮助？例如，IT专业人员和您的银行。
- 如何将该事件告知您的员工、利益相关者或客户？
- 如果任何关键系统处于离线状态，您将如何照常管理业务？

确保您的员工熟悉应急计划，包括他们可能要承担的任何职责或责任。保留一份应急计划的实体副本，以防您需要它的时候系统处于离线状态。

✓ **为网络安全事件制定应急计划。**

随时了解最新动态

成为ACSC的合作伙伴，接收来自ACSC的最新信息。

成为ACSC的合作伙伴，随时了解最新的网络威胁和漏洞。该服务将每月向您发送新闻通讯，并在发现新的网络威胁时向您发送警报。

网络安全是一个快速发展的领域。网络犯罪分子在发现漏洞后几分钟内就会积极利用漏洞。随时了解网络安全形势将有助于您的企业了解可能面临的威胁以及如何防范这些威胁。

✓ **为您的企业注册登记ACSC合作伙伴计划。**

免责声明

本指南中的材料具有一般性，不应被视为法律建议或在任何特定情况或紧急情况下可依赖的帮助材料。在任何重要事项上，您都应该根据自己的情况寻求恰当的独立专业建议。

对于因依赖本指南中包含的信息而导致的任何损害、损失或费用，联邦政府不承担任何责任或义务。

如需了解更多信息或报告网络安全事件，请联系我们：

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

该号码仅可在澳大利亚境内拨打。

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre