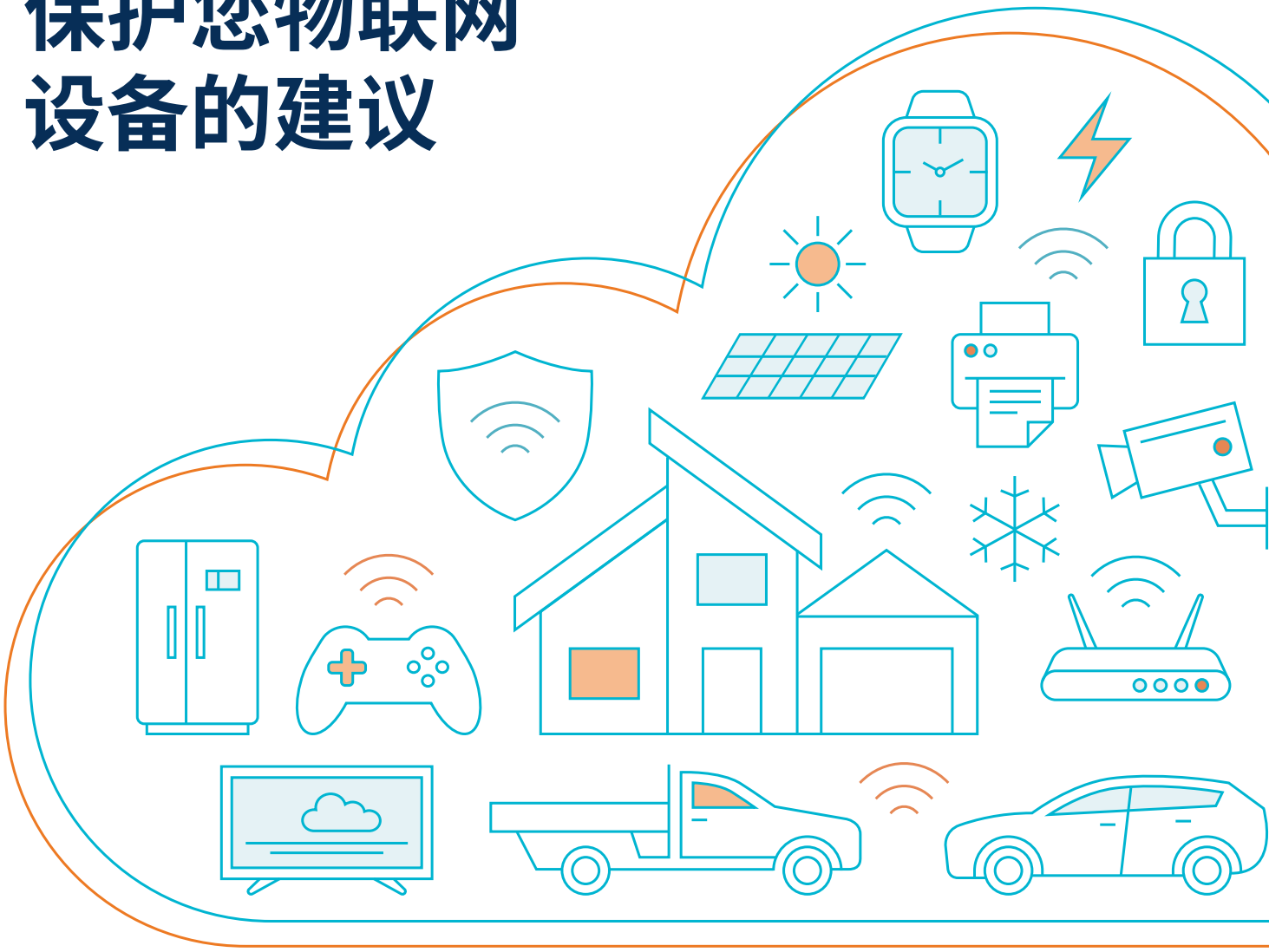
保护您物联网设备的建议



澳大利亚网络安全中心制定了此信息，旨在帮助社区安全地购买和使用物联网 (IoT) 设备。物联网设备是指已添加联网功能的日常用品。物联网设备的例子包括婴儿监控、无人机、安全摄像头、智能电视和太阳能逆变器。家庭和企业中的物联网设备通常使用 Wi-Fi 或蜂窝网络（如 4G 或 5G）连接到互联网。

许多常见于澳大利亚家庭和企业中的物联网设备在设计时并未考虑到安全性。这导致设备容易通过互联网受到入侵。此类事件可能会让网络犯罪分子未经授权访问您的设备和个人数据，以达到恶意目的。

购买物联网设备前

在购买设备前进行研究很重要，因为制造商提供的安全级别各不相同。在购买设备之前，请比较不同制造商销售的同类设备。需要考虑的因素包括：

1. **该设备是否由知名且信誉良好的公司制造，并由知名且信誉良好的商店销售？**知名且信誉良好的公司更有可能在设计产品时考虑其安全性。知名且信誉良好的商店更有可能只销售来自知名且信誉良好的公司的设备，并且拥有更严格的供应链，确保设备按制造商预期的方式到达您手中。

2. **是否可以更改密码？**更改密码总是一个好的办法。尤其是，如果设备出厂时带有强度较弱的默认密码，这一点就变得更加重要。具有良好安全性的设备应具有唯一、不可预测、复杂且难以猜测的密码，因为强度较弱的默认密码是攻击设备最简单的途径。

3. **制造商是否提供更新？**公司在发现设备漏洞时及时提供更新修复非常重要。例如，如果设备上的软件包含已知漏洞，或者黑客开发了新的入侵方式，则需要更新来提供修复。

4. **设备将收集哪些数据以及数据将与谁共享？**有关被收集数据类型以及数据使用场景的信息应在制造商的网站或其隐私政策中可见。始终考虑在线或移动应用程序收集的信息非常重要。

5. **该设备是否只做您想让它做的事情？**购买功能超出您需求的设备，包括联网功能，可能会降低您的安全性。您不会使用的设备功能会让设备更容易被攻破，而不会为您带来任何好处。

物联网设备

在设置设备时，请记住一些简单的问题，以帮助您保持网络和数据更安全。

1. **设备是否需要连接到互联网？**能联网并不意味着应该联网。未连接到互联网的设备被入侵的可能性要小得多。如果您不打算使用需要联网的功能，那么您应该考虑是否需要把它接入互联网。

2. **设备是否在安全位置？**如果设备不需要安装在不安全的区域，将其安装在安全位置可以降低物理入侵的风险。

3. **我是否更改了默认用户名和密码？**使用强密码或密码短语很重要。如果您的设备出厂时没有唯一、不可预测、复杂且难以猜测的密码，则需要更改此密码。默认用户名和密码会被收集并发布到网上，使您的设备容易受到攻击。

4. **我的Wi-Fi网络是否已安全设置，并且是否有安全密码？**保护您的Wi-Fi网络和路由器，使攻击者更难访问您的设备和网络。

更进一步

在您的路由器上专门为物联网设备设置一个额外的Wi-Fi网络。这在您的 Wi-Fi 路由器上可能被称为“访客”网络。如果您的物联网设备之间不需要相互通信，请启用“客户端隔离”功能。将您的物联网设备与您的敏感数据隔离，可确保物联网设备被入侵后不会授予（入侵者）对您的其他设备或数据的访问权限。

5. **不需要的设备功能是否已关闭？**如果您的设备具有不需要或不必要的功能（例如摄像头或麦克风），应尽可能禁用这些功能。

更进一步

查找提及允许从本地局域网 (LAN) 或广域网/互联网远程访问设备网页管理界面的配置设置。除非您自己需要远程访问，否则请确保将其设置为本地局域网。

维护物联网设备

您的物联网设备设置并投入使用后，有一些重要事项需要记住。这些包括：

1. **定期重启设备**如果物联网设备开始变慢或无法操作，则可能存在病毒。大多数恶意软件存储在内存中，可以通过设备重启（即关闭再打开设备）轻松删除。如果设备在重启后仍然缓慢或无法操作，请尝试恢复出厂设置，但请注意这可能会清除您的所有用户数据和个性化设置。

2. **定期更新。**有些设备会自动更新。对于那些不自动更新的设备，请定期与制造商核实并在更新可用时应用。当您的设备不再有可用更新时，请考虑升级到有可用更新的新款设备。无法获取安全更新的设备在发现新漏洞时将无法受到保护，这些设备可能会对您的网络、隐私和数据造成风险。

3. **不使用设备时请将其关闭。**长时间让不使用和未受监控的设备通电并连接到您的 Wi-Fi 网络，可能会增加您的设备受到攻击的可能性。可以自动实现该做法的一个选项是使用电源插座计时器，仅在指定时间内为设备供电。

4. **注意您每月的互联网流量使用量或账单金额的显著增加。**互联网使用量或账单费用的显著增加可能表明您的设备已被入侵。除非您企业内部的 IT 部门将对此进行调查，否则应恢复出厂设置（但请注意这可能会清除您的所有用户数据和个性化设置），然后更改密码。

处置物联网设备

处置设备（通过丢弃或出售）可能会让其他人轻松访问您的个人信息或数据。防止这种情况发生的方法包括：

1. **擦除所有数据和个人信息。**制造商应提供一种方法来清除设备和相关应用程序中的数据和个人信息。擦除您的个人信息可确保在您处置设备后，没有人能访问它。处理物联网设备后，如果您已不再需要其在线账户，请注销它。

2. **执行设备恢复出厂设置。**恢复出厂设置旨在清除本地存储的数据并将密码、用户名和设置恢复为默认值。请查阅设备的用户手册或制造商的网站，了解如何执行恢复出厂设置。

3. **将设备与手机和其他设备解除关联。**若设备仍可访问您的其他设备、网络或在线账户，处置它可能会导致其他人获得访问权限。确保您检查其他设备并移除其与您正在处置的设备的任何配对。任何授予移动应用的权限，如若不再需要，应及时移除。

4. **移除任何连接到设备的可移动媒体（例如 USB 闪存驱动器、存储卡等）。**可移动媒体可能包含在恢复出厂设置中未删除的个人数据，应从设备中物理移除、物理销毁并单独处置。

帮助

受信息窃取器入侵影响或需要协助的澳大利亚组织，可以通过电子邮件asd.assist@defence.gov.au 或拨打 24/7 紧急帮助热线 **1300 CYBER1 (1300 292 371)** 联系澳大利亚信号局网络安全中心。

向 ReportCyber 报告网络犯罪：www.cyber.gov.au/report

如果您遭受了身份盗窃，请通过他们的网站 www.idcare.org 联系 IDCARE。

访问 www.cyber.gov.au 获取为您和您的家人提供的建议。注册免费的 ACSC 警报服务，获取最新在线威胁信息。

让我们把澳大利亚打造成最安全的在线连接之地。

有关网络安全建议，请访问 www.cyber.gov.au

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。

版权所有

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。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre