

保护您的线上个人信息 (Protecting your personal information online)

几乎每个应用程序、社交媒体平台或网站多少都会要求您提供部分个人信息。您的个人信息包括任何可用于识别您身份的详细信息或数据，例如定位您的位置或详细住址，以及其他独特的详细信息。在分享个人信息之前一定要三思而行，这一点很重要。



保护您的个人信息很重要

保护您的个人信息非常重要，因为骗子和身份窃贼可以利用这些信息冒充您。他们可以以您的名义创建虚假账户，并可能采取现在或将来会对您造成不良影响的行动。这可能包括欺诈，例如从您的银行账户中窃取资金，或以您的名义贷款。

骗子可能会单独或结合其他信息来使用您的个人信息。可能包括您特有的日常信息，例如：

个人信息

- 姓名
- 家庭住址
- 电话号码
- 出生日期
- 驾驶执照号码
- 银行账户详细信息
- 邮箱地址
- 账户用户名和密码

身份证明文件

- 驾驶执照
- 护照
- 出生证明
- Medicare 卡
- 澳大利亚签证或公民身份证明
- 移民卡 (ImmiCard)



请注意您分享的内容

社交媒体

最好避免在社交媒体账户上分享个人信息。骗子可以通过您在网上分享的详细信息了解您。有时他们会创建测验或问答帖，诱骗您分享个人信息。他们利用这些信息猜测您的账户密码，或针对您设计其他骗局。

请谨记：只接受现实生活中认识的人的好友请求，将您的社交媒体帐户设置为私人帐户，并确认哪些人可以看到您分享的内容。

使用应用程序

仅从官方应用商店下载应用程序，在下载任何应用之前都需阅读隐私政策和用户评价。您还可以限制应用程序可以访问的信息。有些应用程序会请求不必要的权限，如访问您的联系人列表、相机、存储、位置和麦克风。在智能设备的设置菜单中查看并调整应用程序权限。

确保您的信息安全

使用设备安全功能

在计算机上安装安全软件是保护您自己和隐私的最简单的方法之一。好的计算机安全功能包括：安装信誉良好的反间谍软件、杀毒软件和防火墙软件。您还应该启用自动更新功能，以保持在线安全工具和应用程序的更新。您可以使用自动定时屏幕锁定或需要密码才能打开的屏幕保护程序，并在多次登录尝试失败时自动锁定屏幕。

提示：密码管理器应用程序还可以帮助您创建和存储难以猜到或破解的复杂密码。您可以在**密码管理器**应用程序中了解相关信息，在 Be Connected 网站上了解如何进行设置。

密码

使用强密码保证您的帐户安全。密码口令是更安全的密码版本，由至少四个随机单词组成。

尝试为每个帐户设定不同的密码，并且不要重复使用任何旧密码的部分。

设定密码时，请将其设置为：

- **长密码** – 至少 14 个字符
- **难预测** – 使用至少 4 个包含数字、符号和大小写字母的随机单词
- **独特的** – 不要重复使用密码

例：Yellow So Hey Plant > Yell*w-S0heyPl@nt!

提示：您可以使用新南威尔士州政府的密码强度测试器确认您的密码强度：nsw.gov.au/id-support-nsw/be-prepared/passwords

多重身份验证

启用账户的多重身份验证始终是一个安全的做法。多重身份验证（也称为两步身份验证）额外增加了一层安全性。这意味着当您使用密码登录帐户时，可能会要求您执行额外步骤来确认您的身份，例如输入短信即时发送的代码或使用面部识别。

使用安全连接

当您需要访问重要帐户、发送敏感信息或输入密码时，请连接到受信任的互联网连接（例如在家中或工作场所），或者使用您自己的移动数据流量（如果可用）。公共 Wi-Fi 不如家里或工作场所的 Wi-Fi 安全。

诈骗和数据泄露

保护自己免受诈骗

了解骗局及其运作方式是避免陷入骗局的重要步骤之一。骗子会假装成您认识的组织或个人，试图诱骗您交出个人信息。这些骗局被称为“冒充诈骗”。

请谨记：

停下来——如果不确定对方的身份，不要向任何人支付金钱或提供个人信息

骗子经常要求您验证您的身份，或要求您付款。

思考——问问自己这条信息或电话可能是假的吗？

警惕意外的电话、信息和电子邮件。如果您不确定某条消息是否可信，请直接致电该组织官方网站上的电话号码。

保护措施——一旦感觉到不对劲，请立即采取行动

如果发现任何异常活动，或是骗子骗取了您的钱或信息，请联系银行。

安全地网购

网购时，请确保使您在和可信赖的卖家交易，并记得浏览客户返评。在输入您的个人信息之前，请检查该网站的域名是否以“https”开头，或该网站在浏览器上是否有安全图标（通常是一个小小的、锁定的挂锁图标），表明它是一个更安全的网站。网购时，请使用安全的付款方式，例如 PayPal、BPAY 或信用卡。



提示：您可以浏览 Be Connected 网站，获取我们与 Scamwatch 合作开发的免费模拟[诈骗指南](#)。

数据泄露

当组织持有的个人信息在未经授权的情况下被访问、披露，或者丢失时，就会发生数据泄露。如果您的个人信息涉及到可能对您造成严重伤害的数据泄露事件，许多组织和政府机构都有法律责任告知您。

如果您的信息涉及数据泄露，请务必迅速采取行动，并咨询[澳大利亚信息专员办公室（Office of the Australian Information Commissioner）](#)的建议。您采取的行动取决于数据泄露所涉及的信息。记录您所做的事情。您还可以从 [IDCARE](#) 获得免费支持和建议。

如需了解您使用的网站或应用程序是否发生过数据泄露事件，您可以使用 [haveibeenpwned.com](#) 等服务进行查询。如果发生了数据泄露，请立即更改您的账户密码。

身份欺诈

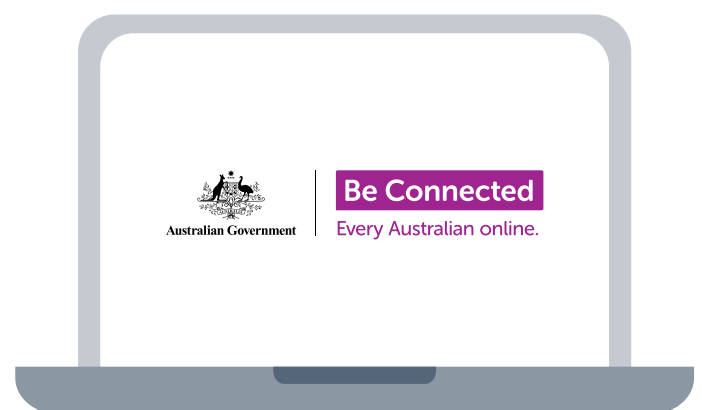
如果您知道或怀疑您的身份已被盗用：

- 请通过 [ReportCyber](#) 向澳大利亚信号局（Australian Signals Directorate）的澳大利亚网络安全中心（Australian Cyber Security Centre）举报。
- 请拨打 131 444 联系警方。要求提供警方报告或参考编号作为您已报案的证据。
- 如果您知道或有怀疑被盗的个人信息类型，请联系相关机构或组织告知他们。
- 请尽快通知您的金融机构。
- 如果这是骗局的一部分，请通过 [Scamwatch](#) 向国家反诈骗中心（National Anti-Scam Centre）举报。

花时间探索 Be Connected

Be Connected 是一个综合性网站，提供免费资源，专门用于支持澳大利亚的老年人们安全地上网，自信地探索数字世界。对于想要帮助老年社区成员享受互联网好处的家庭和社区组织来说，此网站也非常有用。

访问 [beconnected.esafety.gov.au](#)



本计划由 eSafety 作为 Be Connected 计划的一部分进行开发。

[beconnected.esafety.gov.au](#)