

如何安全管理您的电子邮件 (Managing your emails safely)

邮箱是您进入网络世界的门户。它让您能与家人和朋友保持联系，并使用网购和银行等服务。使用强密码和多重身份验证，确保您的邮箱帐户尽可能安全非常重要。



查看电子邮件的方法

您可以通过以下不同的操作方式查看电子邮件：

手机应用程序

- 使用邮箱服务提供商的应用程序，您可以从苹果设备的 App Store 或安卓设备的 Play Store 下载该应用程序
- 将您的邮箱帐户链接到：
 - 您的智能设备上预装的邮件应用程序
 - 计算机上的邮件或 Outlook 应用程序。

网站

- 通过计算机或智能设备上的浏览器，登录您邮箱服务提供商的网站。

电子邮件服务提供商

许多邮箱电子服务提供商都提供免费和付费邮箱帐户的选项，其中包括：

-  **Gmail** 谷歌
-  **Outlook** 微软
-  **雅虎邮箱** 雅虎
-  **iCloud** 苹果
-  **ProntonMail** 普腾公司

访问 Be Connected 网站，阅读关于如何设置和使用 Gmail、Outlook 和雅虎的[逐步指南 \(step-by-step guides\)](#)。

提示：您可能需要设置一个仅用于银行业务、或仅用于网购的电子邮箱帐户，以帮助管理垃圾邮件。

管理您的邮箱

设置文件夹和标签

在收件箱中创建文件夹是保持帐户井然有序的好方法，可以帮助您更轻松找到重要的电子邮件。根据您使用的邮箱服务，文件夹有时也称为“标签”。

整理和归档您的电子邮件

您的电子邮件服务有使用便利的控件，可帮助您以各种方式归档电子邮件，并将垃圾邮件和垃圾数量降至最低。当您收到新邮件并打开阅读时，屏幕顶部会出现一些控件。您可以单击这些控件来执行以下操作：

- **删除：**将邮件移至垃圾箱 / 垃圾文件夹
- **归档：**将电子邮件移至归档文件夹
- **标记为未读：**让电子邮件再次显示为未读邮件
- **标签 / 文件夹：**标记电子邮件或移动它到文件夹中。

管理垃圾邮件

您的电子邮件服务会自动检测并转移已知的垃圾邮件，但有些垃圾邮件可能仍未被检测到。

如果您认为收件箱中的电子邮件是垃圾邮件，您可以：

- **举报垃圾邮件：**告知您的邮箱服务提供商，该电子邮件是垃圾邮件
- **屏蔽电子邮件：**停止接收来自特定发件人的电子邮件
- **取消订阅：**停止接收您订阅的新闻通讯或营销电子邮件。

如果您认为自己已经取消订阅但仍收到垃圾邮件，可以向[澳大利亚通信和媒体管理局 \(Australian Communications and Media Authority\)](#) 投诉。

提示：为了避免收到垃圾邮件，在参加抽奖活动时请谨慎提供个人信息，并留意购买产品或服务时默认勾选的营销邮件订阅选项。

确保您的邮箱帐户安全

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
- **难以预测** – 使用至少四个包含数字、符号、大小写字母的随机单词
- **独特的** – 请勿重复使用密码。

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

提示：密码管理器应用程序还可以帮助您创建和存储他人难以猜到或破解的复杂密码。您可以在 [密码管理器](#) 中找到查询信息，以及在 Be Connected 网站上了解如何进行设置。

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。

使用设备安全功能

在您的计算机上使用安全软件是保护您的帐户和设备的最简单方法之一。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。您还应启用自动更新，这可以使您的在线安全工具和应用程序保持最新状态。

使用安全连接

当您需要访问您的帐户、发送敏感信息或输入密码时，请连接到可信任的互联网连接，例如在家里、在工作场所或使用您自己的移动数据流量（如果可用）。公共 Wi-Fi 不如家庭或办公室 Wi-Fi 安全。

恢复帐户选项

确保为您的所有邮箱帐户设置了恢复账号的电话号码，或备用邮箱地址。如果您无法访问邮箱帐户，或者帐户遭到入侵，您可以使用恢复选项重置密码。

诈骗邮件

诈骗邮件会伪装成来自您认识的合法组织。他们看上去可能是真的，使用伪造的组织徽标和类似的邮箱地址。诈骗电子邮件可能看起来像是来自您的银行、互联网服务提供商、政府机构、零售商，甚至是假扮成朋友或家人的骗子。骗子会假扮成您信任的人，利用某种紧迫感诱骗您付款或提供个人信息，例如重要的密码、信用卡或银行详细信息。

这些类型的诈骗被称为“冒充诈骗”或“网络钓鱼”。

避免诈骗邮件的技巧

- 留意诈骗邮件的迹象。诈骗邮件可能会：
 - 营造紧迫感或使用恐吓策略，要求您付款或确认您的个人信息
 - 使用通用问候语，如“尊敬的客户”、“尊敬的用户”，或者根本不使用问候语
 - 要求您点击链接或下载文件，这可能会将您引导至虚假网站，又或是其包含病毒或恶意软件。
- 始终记得确认发件人的邮箱地址是否合法，并通过查找官方网站和电话号码直接联系该组织。
- 切勿通过电子邮件中的链接登录您的网上帐户或验证详细信息，也不要点击来自未知发件人或可疑邮件中的链接或附件。
- 删除可疑或可能的诈骗电子邮件，使用“报告垃圾邮件”选项将其归类为垃圾邮件。

提示：如果您不确认某封电子邮件，请与可信赖的朋友或家人沟通，并使用其网站上的电话号码联系该组织。

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**。

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。