在线展示汇总

Australian Government

Be Connected
Every Australian online.

您能识别诈骗吗?

留意诈骗和诈骗方法是预防诈骗的重要步骤之一。每年都有澳大利亚老年人因为诈骗而损失几百万澳元。虽然互联网是探索世界、与他人联系的好地方，但我们无法总能确定在网上认识的人的身份。您知道骗子的伎俩后就会更容易识别诈骗。

网络钓鱼诈骗

网络钓鱼诈骗指骗子让您认为他们来自可信任的机构或您认识的个人，以便向您套取银行账户、密码和信用卡号码等个人信息。

网络钓鱼信息看起来像是真实的，骗子常常会复制他们要假扮的机构所使用的格式，其中包括机构的品牌和图标。这类诈骗以多种形式出现，包括电子邮件、短信息或电话。例如，您可能会收到：

- 银行发给您的短信，要求您确认密码。
- 互联网提供商发给您的电子邮件，要求您更新信息。
- 家人用新号码给您发的短信，告诉您他们遗失了手机，需要您紧急给他们汇钱。
- 金融机构打给您的电话，提醒您账户有“未经授权或可疑的活动”，或者如果您不更新自己的信息，账户将被关闭。
- 您在Facebook上认识的某个人发来的通知，推荐某个网站。

税务和Medicare诈骗

骗子假扮成澳大利亚税务局（ATO）、Medicare和其它政府机构的工作人员，骗您付款和透露个人信息。这类骗子创建虚假网站，给您发电子邮件、短信和打电话，谎称自己来自政府机构。

ATO绝不会通过电子邮件、短信或电话，要求您做以下操作：

- 提供税务编号、信用卡或银行账户等个人信息。
- 支付费用才能收到退税或者免于因逃税而被逮捕。
- 点击链接输入您的个人信息。
- 下载文件或安装软件。

如果您不确定沟通信息是否来自ATO，可以致电ATO的防诈骗热线1800 008 540或访问网站ato.gov.au/scams查询。

如何保护自己

- 不要着急。再读一次信息。问自己，这个消息或电话是假的吗？
- 它使用了官方电子邮件地址吗？还是有点不对劲？
- 收件人是谁？如果它称呼的是“尊敬的顾客”而不是您的名字，那就要提高警惕。
- 其中有拼写错误或语法错误吗？这可能是它来自骗子的征兆。
- 不要使用信息中提供的联系方式，它们可能是虚假的。在网上搜索机构的电话和官方网站。
- 不要点击任何链接或打开附件，这么做可能会将病毒下载到您的设备上——点击删除即可。
- 不要透露您的税务编号（TFN）、生日、银行账户或信用卡信息。

请记住：骗子可能会玩弄您的感情，让您没有时间仔细考虑就做出回应。他们的伎俩可能包括威胁或罚款，说您账户上有未经授权的消费，或者假扮成需要帮助的家人。

交友和恋爱诈骗

骗子会利用人们寻找朋友或恋爱伴侣的机会，常常通过约会网站、应用程序、社交媒体、甚至是网络游戏，假扮成人们要找的潜在对象。他们的目的是获得您的信任，让您提供金钱、礼物、私密照片或个人信息。

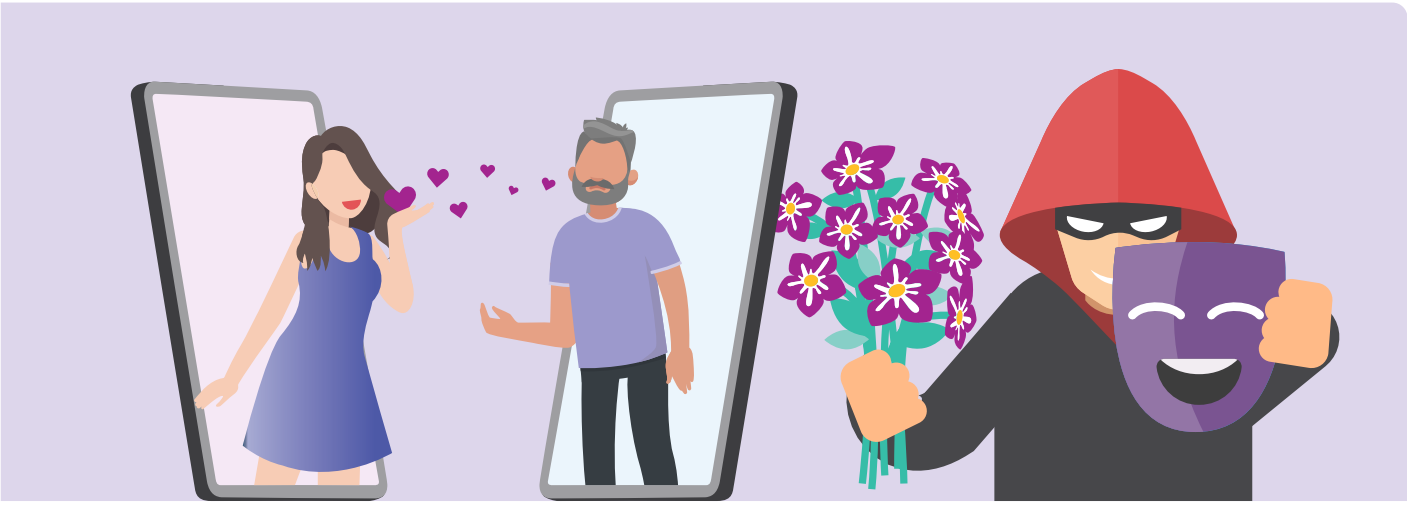
如何防范诈骗和保障安全?

留意这类人：

- 迅速表达深深爱意。
- 获得您的信任后（常常等待几周、几个月甚至几年），告诉您一个细节丰富的故事，向您索要金钱或借钱、索要礼物或您的银行账户/信用卡信息。
- 避免见面和找借口声称自己没法去见您。
- 网上个人档案与他们告诉您的细节不一致。

如何保护自己

- 绝对不要将金钱、信用卡信息、网上账户信息、重要个人文件的副本交给您没有见过面的个人。
- 在Google上搜索个人图片，确定他们是否是声称的那个人，还是图片是从网上其它地方找的。前往网站 images.google.com，然后点击相机图标。
- 当他们提及金钱问题或因为紧急情况需要金钱时提高警惕。
- 警惕拼写和语法错误且前后矛盾的故事。
- 不要分享私密照片或视频。骗子很善于利用泄露的资料来勒索诈骗目标。



技术支持诈骗

此类诈骗的惯用伎俩是，一开始声称是大型电信公司或电脑公司的电话或电子邮件，例如，Telstra、NBN或Microsoft，他们说您的电脑或网络出了问题，然后他们可以解决问题。他们然后要求远程接入您的电脑，“找到问题所在”，或者劝说您购买无用的软件或服务以便“修复”电脑。

如何保护自己

- 如果您接到陌生来电，声称电脑有问题和需要远程连接，那就挂断电话。
- 不要允许陌生的来电者远程接入您的电脑。
- 不要提供您的银行账户或信用卡信息等个人资料。
- 不要购买陌生来电或电子邮件兜售的软件。
- 忽略那些告诉您拨打技术支持的弹出信息。

避免诈骗的有用技巧

停下来

- 向别人汇钱或提供个人信息前，三思而后行。
- 骗子会声称要帮助您或者让您验证自己的身份。他们会假扮来自您熟悉和信任的机构，比如您使用过的商户、或者警察、政府、或虚构的服务机构。

想一想

- 问自己，这个消息或电话是假的吗?
- 绝对不要点击信息中的链接，询问您信任的亲友他们会怎么做。在联系商户或政府机构时，仅使用他们的官方网站或安全有保障的应用程序上列出的联系信息。如果您不确定，直接拒绝、挂断电话或删除信息。

保护措施

- 如果发生什么差错迅速行动。
- 如果您丢失了金钱或个人信息，或者您发现银行卡或账户上有异常活动，应立即联系银行。从IDCARE之类的机构寻求帮助， 并向ReportCyber举报网络犯罪。帮助其他人向Scamwatch举报诈骗。

求助，我怀疑自己被骗了

如果您觉得自己被骗了，不要觉得难为情和不敢说出来。您接下来可以这么做：

- 联系银行并阻止向骗子继续付款。
- 如果您经历网络犯罪，并且在网上损失金钱，您可以通过ReportCyber或者访问cyber.gov.au报警。
- 如果您担心自己的个人信息已泄露或被滥用，请联系澳大利亚全国身份和网络支持服务IDCARE，电话号码是1300 432 273，网址是idcare.org。
- 通过网页scamwatch.gov.au/report-a-scam向ACCC举报诈骗。这有助于提醒人们当前有哪些诈骗、关注诈骗趋势，以及尽可能阻止诈骗。
- 将诈骗信息告诉您的亲友以保护他们。

请谨记：您的身边总有人能提供帮助——cyber.gov.au或scamwatch.gov.au的工作人员、熟悉技术知识的亲友，或本地的电脑俱乐部。

如需获取防骗的最新信息，请订阅**Scamwatch的电子邮件提醒**。

花时间了解 Be Connected指引

Be Connected是一个综合性网站，上面提供了免费资源，尤其可对澳大利亚的老年人提供支持，以帮助他们安全上网和放心使用数字技术。该网站还支持了家庭和社区机构，以便帮助社区老年人享受网络带来的各种便利。

访问beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

本课程由eSafety为Be Connected项目编制。