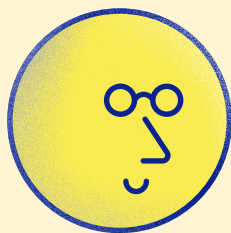


如何识别 并避免 诈骗



保护自己的防诈骗指南



Australian Government



National
Anti-Scam
Centre



ScamWatch
Stop. Better safe than scammed.

承认原住民国家

澳大利亚竞争与消费者委员会 (ACCC) 承认澳大利亚各地原住民国家的传统所有者和监护人，并承认他们与这片土地、海洋和社区的持续联系。我们向他们和他们的文化表示敬意；向他们过去、现在和未来的长者致敬。

Australian Competition and Consumer Commission
Ngunnawal
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

©澳大利亚联邦2023年

本文件受版权保护。除《1968年版权法》允许的任何使用外，本文件中的所有材料均根据知识共享署名4.0澳大利亚许可证 (Creative Commons Attribution 4.0 Australia licence) 提供，但以下内容除外：

- 联邦徽章
- ACCC和AER标志
- 澳大利亚竞争与消费者委员会未拥有版权，但可能是本出版物的一部分或包含在其中的任何插图、图表、照片或图形。

相关许可证条件的详细信息可在知识共享 (Creative Commons) 网站上找到，CC BY 4.0 AU 许可证的完整法律代码也可在该网站上获得。

有关复制和权利的请求以及咨询应寄至ACCC的企业传播总监 (Director, Corporate Communications, ACCC)，邮寄地址：GPO Box 3131, Canberra ACT 2601。

重要通知

本出版物中的信息仅为一般指南。这些信息并不构成法律建议或其他专业建议，且不应作为任何司法管辖区的法律声明而予以依赖。由于本出版物仅为一般指南，因此可能包含概括性内容。如果您有任何疑问，则应寻求专业建议。

ACCC已经尽一切合理努力提供最新且准确的信息，但不对这些信息的准确性、时效性或完整性做出任何保证。

希望再次出版或以其他方式使用本出版物中的信息的各方必须在出版之前检查此信息的时效性和准确性。这应在每一版出版之前进行，因为ACCC的指导和相关过渡立法经常发生变化。各方的任何咨询都应寄至ACCC的企业传播总监 (Director, Corporate Communications, ACCC)，邮寄地址：GPO Box 3131, Canberra ACT 2601。

ACCC 05/24_24-13

www.accc.gov.au

目录

您可以获得帮助	1
什么是诈骗？	3
识别和避免诈骗的简单步骤	4
短信或SMS诈骗	7
电子邮件诈骗	11
电话诈骗	15
网站诈骗	19
社交媒体、应用程序和网络消息诈骗	23
您应该了解的主要诈骗方式	27
在哪里举报诈骗	31
更多帮助和支持	33



本指南由国家反诈骗中心 (National Anti-Scam Centre) 编写, 它将帮助您识别诈骗并保护自己免受诈骗伤害。

诈骗是一种犯罪, 实施诈骗的人是犯罪分子。在澳大利亚, 许多人都遭受过诈骗并失去了他们的钱财, 有时候甚至失去了他们一生的积蓄。诈骗会危害人们的生活。

诈骗正在变得越来越难以识别, 因此我们需要共同努力来阻止诈骗。

国家反诈骗中心致力于保护澳大利亚人免遭诈骗。

我们与政府和行业合作, 寻找新的方法来阻止骗子从澳大利亚人那里窃取钱财和个人信息。以下是我们实现这一目标的一些方式。

我们帮助人们识别和避免诈骗

我们通过Scamwatch分享有关诈骗的最新信息, 以及您可以保护自己免受诈骗的方式。

我们打击骗子

通过在政府和行业之间收集和分享情报, 我们让骗子更难继续犯罪, 也让人们更容易举报诈骗。



您可以获得帮助

如果您正在阅读本指南，那么您或您认识的人可能已经遭到了诈骗。不幸的是，受害者不止您一个人。诈骗手段正在变得日益复杂，这意味着任何人都可能遭到诈骗。

如果您遭遇了诈骗，迅速采取行动很重要。

如果您被骗子骗走了钱，请联系您的银行或发卡机构。

联系IDCARE，电话：[1800 595 160](tel:1800595160)；网址：www.idcare.org。

诈骗之所以会成功，是因为它们看起来像是真的。骗子靠的是您没有注意到警示迹象来实施诈骗，因为您很匆忙，某样东西看起来超级便宜，您不想错过，或者因为诈骗信息看似来自您信任的人。

请遵循以下3个步骤来保护自己免遭诈骗：

停下来

如果不确定，请不要把钱财或个人信息提供给任何人。



骗子会主动提出帮助您或要求您验证自己的身份。他们会假装成来自您知道和信任的机构，例如服务提供商、警察、银行或政府服务机构。

核实

问问自己—这个消息或电话会不会是假的？



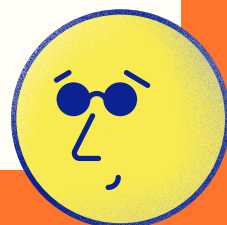
切勿点击消息中的链接。仅使用您自己从企业或政府机构的官方网站或应用程序中找到的联系信息来联系他们。如果您不确定，请说“不”，挂断电话或删除信息。

举报

如果感觉不对劲，请迅速采取行动。



如果您注意到异常活动或骗子获取了您的钱财或信息，请联系您的银行。寻求帮助，并向ReportCyber和Scamwatch举报诈骗。当您举报诈骗时，您就是在帮助所有澳大利亚人建立起对抗诈骗的防线。



什么是诈骗？

诈骗是指有人欺骗您以窃取您的钱财或个人信息。

诈骗是由犯罪分子实施的经济犯罪，他们通常非常有组织，而且诈骗手段严密复杂。

诈骗：

- ✓ 由犯罪分子实施
- ✓ 看起来像是真的
- ✓ 提供可信的故事
- ✓ 向您施加压力，让您采取行动

诈骗不是：

- ✗ 计算机黑客攻击
- ✗ 不公平的合同条款
- ✗ 骚扰性营销手段

重要的是要记住，并非所有负面经历都是诈骗。您可能付款购买了某个产品，却从未收到；或者购买了某样东西，却发现质量很差。虽然这些情况很令人失望，但不一定是诈骗。《澳大利亚消费者法》为澳大利亚消费者就此类问题提供保护。

欲了解更多信息，请访问www.accc.gov.au/consumers

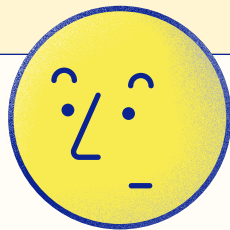
识别和避免诈骗的简单步骤

诈骗可能发生在我们所有人身上。诈骗之所以会成功，是因为骗子会编造可信的故事来窃取您的钱财以及获取您的个人信息。

骗子正在变得越来越聪明，他们会利用新技术、产品、服务和重大事件来说服您，让您相信他们的骗局是真实的。

识别诈骗可能很困难。以下是一些需要留心的情况。有时，骗子会结合使用这些手段。

- 1. 赚钱或省钱的机会：**骗子会欺骗您，让您相信您可以获得令人难以置信的便宜货或优惠。他们会向您施加压力，让您迅速采取行动，以免错过。请记住，如果某个便宜货看起来好得令人难以置信，则通常是假的。
- 2. 悲惨的故事和大声求助：**骗子会试图利用您的善心欺骗您。他们会与您分享悲痛的故事和悲剧，并解释他们为什么需要您的帮助和您的钱财。
- 3. 链接和附件：**骗子会利用链接将您带到诈骗网站，这些网站旨在窃取您的信息和钱财。骗子还可能会要求您打开附件。这些附件可能会安装病毒来窃取您的信息。



4. **施加压力, 让您迅速行动:** 骗子不希望您花时间仔细思考情况。他们希望给您施压, 让您迅速行动。这可能包括威胁说如果您不赶快行动, 就会发生不好的事情。
5. **要求您以不寻常或特殊的方式付款:** 骗子常常会要求您使用不常见的方式付款, 比如预付的借记卡、iTunes 卡或比特币等虚拟货币。这笔钱一旦花出去, 就无法追回。
6. **要求您设立新账户或PayID:** 骗子可能会要求您设立一个新的银行账户或PayID来向他们付款(或接收他们的付款)。他们可能会假装来自您的银行, 并告诉您将钱转入新账户以确保其安全。

如果骗子成功骗走了您的钱, 他们会试图从您那里骗取更多的钱。不幸的是, 三分之一的诈骗受害者被骗的次数不止一次。如果您被骗子骗走了钱, 请留意那些主动提出帮您追回钱款的骗子。这是另一种跟进诈骗。



短信或SMS诈骗

骗子会假装自己来自政府、执法部门、值得信赖的企业，甚至假装成您自己的家人或朋友，向您发送短信。

这些短信会听起来很紧急，试图让您迅速行动。它们通常会附带一个链接，这会将您带到诈骗网站。骗子可以窃取在这些诈骗网站上输入的任何个人信息，并利用这些信息窃取您的钱财或以您的名义实施欺诈。

为了使这些短信看起来真实，骗子会复制或伪装他们的电话号码，使其看起来是合法企业或您认识的人的电话号码和来电显示。

诈骗短信甚至可能与来自某个机构的真实短信出现在同一消息链中，这使它们更难以识别。

某一条短信可能是诈骗的迹象

这条短信：



要求您立即采取行动，进行付款或转账。



要求您点击短信中的链接或拨打消息中提供的电话。



要求您用自己的用户名和密码登录一个在线账户或提供其它个人信息。



来自家人或朋友，并称其联系方式已更改。



威胁说如果您不采取行动，就会停止某个服务或向您收费。



称您或您的账户已被黑客入侵或涉及欺诈。



称您的付款或包裹送达存在问题。

保护自己免受短信诈骗的步骤



1. 如果您认识的人发短信说他们有了一个新的电话号码：

- a. 尝试拨打您已有的他们的旧号码，并且
 - b. 向新号码发送一个只有他们才会知道答案的问题，以核实他们确实是他们所说的那个人。
-



2. 切勿点击短信中的链接。
-



3. 如果短信中有某个网站的链接，请不要点击该链接。相反，您可以自己在网上搜索该网站，或使用官方应用程序。
-



4. 请不要使用所提供的电话号码对短信做出回复。
-



5. 使用您自己找到的电话号码（例如从该机构网站上找到的号码）给该机构或个人回电。
-



电子邮件诈骗

骗子会假装成来自政府、执法部门和企业，给您发送电子邮件。他们会使情况听起来很紧急，迫使您迅速行动。

骗子会使用与真实机构相同的标志和类似的电子邮件地址。骗子还可能会复制机构或企业的电子邮件地址，或将他们的电子邮件地址伪装在机构或企业的电子邮件地址后面，从而让诈骗电子邮件看起来更真实。

某一封电子邮件可能是诈骗的迹象

这封电子邮件：



要求付款，但账户信息是新的或者自从您上次付款以来已发生更改。



要求您用自己的用户名和密码登录一个在线账户或提供其它个人信息。



是意料之外的电子邮件，并且包含一个附件，还邀请您打开该附件。



要求您确认自己的银行详细信息以接收您意料之外的退款或钱财。



声称拥有关于您的信息或图像，并威胁要将它们公开。



主动提出为数据泄露或身份盗窃而帮助您追回钱款或获得赔偿。

您可以采取以下步骤来保护自己 免遭电子邮件诈骗

1. 通过以下任一方式核实电子邮件是否真实：



- a. 使用您自己找到的联系方式（例如从该机构网站上找到的联系方式）直接联系该人或机构，或
 - b. 通过其官方应用程序访问机构（切勿通过链接访问）。
-



2. 立即停止与任何试图威胁或恐吓您的人联系。



3. 切勿将个人信息透露给任何提出给您以下好处的人，也不要向这个人付款：

- a. 帮助您就之前的诈骗或数据泄露获得补偿或追回损失，或，
 - b. 获奖奖金、奖品或遗产。
-



4. 在可能的情况下使用多重身份验证。这提供了一层额外的保护，意味着骗子必须知道您的电子邮件密码以及发送到您手机的 PIN 码才能访问您的电子邮件账户。



电话诈骗

骗子会打电话称自己来自知名的机构。这包括政府机构、执法部门、投资公司和法律事务所、银行以及电信服务提供商。

他们会使情况听起来很紧急，迫使您迅速行动。他们可能会试图说服您提供个人或银行账户详情，或者访问您的计算机。

来电者可能已经掌握了一些关于您的信息，比如您的姓名或住址，使这通电话显得很真实。

某一通电话可能是诈骗的迹象

来电者：



要求付款或要求您将钱转到一个新账户。



要求您提供密码、PIN码、一次性代码或一些其它的安全信息。



要求您提供财务详细信息，比如信用卡或银行详细信息。



要求您在手机或计算机上完成某项操作，比如安装软件或访问安全账户。



声称来自执法部门，并威胁立即逮捕您或将您驱逐出境。



称您的银行或其它线上账户已被黑客入侵或涉及欺诈。

您可以采取以下步骤来保护自己免遭电话诈骗

1. 通过以下任一方式核实来电者是否真实：



- a. 使用您自己找到的联系方式（例如从该机构网站上找到的联系方式）直接联系该人或机构，或
- b. 通过其官方应用程序访问机构（切勿通过链接访问）。



2. 如果您不确定来电者的身份，或者他们威胁或恐吓您，请立即挂断电话。



3. 切勿安装允许他人访问您的计算机或设备的软件。



4. 您可以忽略来自您不认识的号码的电话，或者让电话转到语音信箱。



有用的信息！

即使您拥有私人号码或者已在谢绝来电登记册（Do Not Call）上登记，您仍可能收到诈骗电话。



网站诈骗

骗子可能会在网上假装成任何人，包括政府、真实企业、名人或您的朋友或家人。

他们可能会创建虚假的网站，让其看起来像知名品牌。他们可能会冒充名人，让他们看起来像是在认可商品或服务。这些网站可能包含虚假评论，使您信任他们。

您可能会在网上看到虚假广告横幅或弹出窗口，其中包含虚假警告或错误消息。

某一个网站可能是诈骗的迹象

这个网站：



以大大低于平时或其他网站的价格销售商品。



告诉您一种只需很少风险或努力就能快速、轻松赚钱的方法。



包含紧急警告或错误消息，要求您点击链接。



要求您用不寻常或特殊的方式付款，比如礼品卡或比特币等加密货币。



只包含正面评价。

您可以采取以下步骤避免网站诈骗



1. 对比价格。如果某个优惠看起来好得令人难以置信，那么它很可能就是假的。



2. 在付款或提供个人信息之前，研究一下您所打交道的机构或个人。



3. 不要依赖这个网站上的评价。搜索该网站或企业名，在搜索时加上“诈骗”或“评价”一词。



4. 如果您的屏幕上弹出警告或错误消息，不要点击它，而是直接前往它所指的应用程序，以核实它是否真实。



5. 为您的操作系统和应用程序启用“自动更新”，确保您用于网上购物的设备保持最新状态。



有用的信息！

可访问www.cyber.gov.au了解在网上保护自己的实用方法



社交媒体、应用程序和网络消息诈骗

如果您不认识的人在社交媒体、WhatsApp、微信等消息平台或应用程序上联系您，则可能是诈骗。

骗子假装成别人时，常常会使用该人的真实照片或该机构的官方标志，以使骗局更难以识破。

社交媒体上的骗子会设立虚假的个人资料，假装来自政府、真实企业、雇主、投资公司，甚至假装成您的朋友、家人或者浪漫对象。

他们可能会冒充名人，使这些名人看起来像是在推广商品或服务。

骗子还可能从您在社交媒体账号上分享的详情中了解许多关于您的信息。他们可能会利用这些信息猜测您的账号密码或开展针对您的其它诈骗。

某个社交媒体或应用程序是诈骗的迹象

这个社交媒体上的个人资料或应用程序：



告诉您一种只需很少风险或努力就能快速、轻松赚钱的方法。



邀请您参与竞赛或限时优惠。



要求将对话从应用程序（如约会应用程序）转移到私聊或电子邮件。



称某位名人认可或支持某一产品或服务。



称有人要以高价购买您正在出售的东西，且不用事先查看实物。



威胁说要公开您的私照，除非您向他们付款。



联系您并向您提供工作。



有用的信息！

欲了解如何在不同社交媒体平台上保持安全的信息，请访问www.esafety.gov.au

您可以采取以下步骤来避免社交媒体和应用程序诈骗。



1. 核实这个个人资料是否可能是假的。这个账号是否活跃？他们有多少朋友/关注者，以及他们在网上发表了多少内容？



2. 在网上搜索这个个人资料的姓名，搜索时加上“诈骗”一词。



3. 切勿在没有面试或讨论您的经验、适合性和推荐人的情况下就接受提供给您工作。研究一下提供该工作岗位的招聘人员和企业或个人。通过在互联网独立搜索获得的电话号码联系该招聘机构。

不要支付预付款来保证获得工作。



4. 只接受持有澳大利亚金融服务执照 (Australian Financial Services license) 的人士提供的投资建议，并检查一个公司或网站是否在国际证监会组织 (IOSCO) 投资者警示门户网站上列出。



5. 切勿将钱转给仅在网上认识的人。骗子常常会说他们住在国外，无法与您见面。



6. 切勿将自己的私密照片发送给仅在网上认识的人。

欲了解有关诈骗的更多信息，包括骗子可能与您联系的其它方式，例如亲自联系和通过信件联系，请访问[Scamwatch](https://www.scamwatch.gov.au)。



您应该了解的主要诈骗方式

以下是一些您需要注意的最常见的诈骗类型。您可以在[Scamwatch](#)网站上找到关于每种诈骗类型的更多信息，包括警示迹象和保护自己的步骤。

冒充诈骗

骗子会欺骗您，让您以为他们来自值得信赖的机构，例如警察、政府、银行和知名企业。他们甚至可能假装成您的朋友或家人。骗子会通过发送钓鱼电子邮件或短信来搜寻关于您的信息。这些都是为了窃取您的信息。他们通过假装自己来自官方机构或是您认识和信任的人，试图说服您向他们提供个人信息。

骗子会利用技术手段使他们的来电或短信看起来像是来自正当的电话号码。他们可以使短信与来自某机构的真实消息显示在同一对话线程中。

投资诈骗

骗子会使用令人信服的营销和新技术，使他们的投资提案听起来好得不容错过。他们承诺给您高额的红利，但风险很小，甚至没有风险。他们经常使用向您施压的手段，迫使您快速行动，以便他们可以窃取您的钱财。

工作和就业诈骗

骗子会提供只需付出很少努力就能获得高薪的工作。他们假装自己代表知名公司和网上购物平台进行招聘。有时，他们列出的工作甚至不存在。骗子还会冒充知名的招聘机构。他们的目标是窃取您的钱财和个人信息。他们可能会要求您预付款才能为他们工作。

产品和服务诈骗

骗子会假装成买家或卖家来窃取您的钱财。他们会设立虚假网站，或在合法的零售商网站上设立个人资料，以低得令人难以置信的价格提供产品或服务。他们会发布虚假广告和虚假评论。他们可能使用盗窃的标志、“.com.au”的域名和盗窃的澳大利亚商业编号（ABN）。这些诈骗很难识别。

骗子还会冒充您知道和信任的企业，给您发送虚假账单。他们甚至可能更改合法发票上的详细信息，以便客户最终向骗子付款，而不是向您付款。

浪漫诈骗

骗子会利用对爱情、约会或友谊的承诺来窃取您的钱财。他们会竭尽全力让您相信这段关系是真实的，并操纵您，让您给他们钱。

骗子会在社交媒体、约会或游戏应用程序和网站上找到您。他们也可能给您发短信或电子邮件。他们隐藏在虚假的个人资料和身份背后，有时假扮成名人。一旦您信任了他们，他们就会遇到“紧急情况”，并请求您的帮助。这通常是要求您给钱或其它产品。

威胁和勒索诈骗

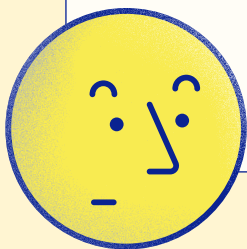
骗子会假装成来自值得信赖的机构，并声称您需要付钱，否则会发生不好的事情。如果您不同意立即付钱，他们可能会威胁说要将您逮捕、驱逐出境，甚至给您造成身体伤害。

他们还可能对您进行勒索，威胁要分享您发送给他们的裸照或视频，除非您给他们钱。

意外之财诈骗

骗子会试图让您相信有人欠您钱，或者您有资格得到意料之外的钱或奖金。

骗子会要求您在领钱或奖金之前支付费用或提供您的银行或身份详情。遗憾的是，天上不会掉馅饼。





在哪里举报诈骗

我们正在努力提高人们对如何识别、避免和举报诈骗的意识，从而使骗子更难在澳大利亚行骗。

我们分享举报的诈骗信息，并与政府、执法部门和私营部门合作，以打击和预防诈骗。

帮助他人谨防诈骗，向Scamwatch举报。在Scamwatch网站上填写举报单，举报您遭遇的诈骗经历，

网址：www.scamwatch.gov.au

请记住，如果您是诈骗的受害者，迅速采取行动很重要。

- 如果您被骗子骗走了钱，请联系您的银行或发卡机构。
- 联系IDCARE，电话：1800 595 160 | idcare.org



更多帮助和支持

成为诈骗的受害者可能会让人感到难以承受。重要的是要记住，任何人都可能遭遇诈骗，并且您可以获得帮助。

如果您或您认识的人遭遇了诈骗，请与他人谈一谈。您可以向家人、朋友、家庭医生或以下支持服务寻求帮助。

生命线 (Lifeline) : 13 11 14 | lifeline.org.au
或在线危机支持聊天（一天24小时，一周7天）

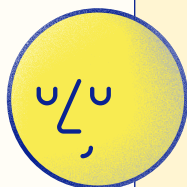
跨越忧郁 (Beyond Blue) : 1300 22 4636 | beyondblue.org.au
或在线聊天（一天24小时，一周7天）

儿童帮助热线 (Kids Helpline) : 1800 55 1800 | kidshelpline.com.au
（一天24小时，一周7天）

诈骗的财务影响可能是毁灭性的，并且会改变人们的生活。

如果您正在经历财务困境，可以通过[国家债务帮助热线 \(National Debt Helpline\)](#) 与财务顾问交谈：

[1800 007 007](#) 周一至周五上午9点30分至下午4点30分
或者于周一至周五上午9点至晚上8点使用实时聊天



scamwatch.gov.au