AUSTRALIAN COMPETITION & CONSUMER COMMISSION

防诈骗小黑皮书

袖珍指南，助您识别诈骗，免受诈骗，保护自己

AUSTRALIAN
COMPETITION
& CONSUMER
COMMISSION

防诈骗小黑皮书

袖珍指南，助您识别诈骗，免受诈骗，保护自己

ISBN 978 1 920702 00 7

澳大利亚竞争和消费者委员会(Australian Competition and Consumer Commission)
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 12/16_1129

www.accc.gov.au

内容

介绍

每年，诈骗都使澳大利亚人、企业和经济蒙受数以亿计澳元的损失，并对受害者及其家人造成情感伤害。

保护自己的最佳方式是通过了解和教育。新版*“防诈骗小黑皮书”(The Little Black Book of Scams)*是由全国消费者保护机构澳大利亚竞争和消费者委员会(ACCC)提供。防诈骗小黑皮书得到国际公认，是消费者和小企业了解诈骗的重要工具，包括：

- 需要注意的最常见骗局
- 诈骗者可以与您联系的不同方式
- 诈骗者用来欺骗您的办法
- 警告标志
- 如何保护自己，及
- 在哪里获得帮助。

*防诈骗小黑皮书*可以在上网获取，地址是www.accc.gov.au/littleblackbookofscams。

保护自己—在诈骗监察(Scamwatch)网站登记

要比诈骗者领先一步，通过访问ACCC的骗局监督网站www.scamwatch.gov.au了解更多信息，您可以在这里登记针对消费者和小企业的新骗局的免费电子邮件提醒。
您也可以在Twitter上关注诈骗监察@scamwatch_gov或http://twitter.com/scamwatch_gov。

需要防范的最常见骗局

每个人都有可能受到诈骗，所以每个人都需要了解有关如何识别和避免被骗的信息。有些人认为只有轻信和贪婪才会成为骗局的受害者。事实是诈骗者很聪明，如果您不知道需要注意什么，任何人都可能成为骗局的牺牲品。

您是否收到过好得难以置信的提议，可能是打电话来帮助修理您的电脑，也可能是威胁您支付子虚乌有的欠款、银行或电信提供商发出的关于您帐户问题的提醒，甚至是邀请 “加好友” 或上网连线？诈骗者知道如何打动您以获得他们想要的东西。

他们变得越来越高明，与时俱进，利用新技术、新产品或服务以及发生的重大事件来创造可信的故事，取得您的信任，然后说服您将自己的资金或个人信息发送给他们。

然而，根据每年收到的成千上万的诈骗报告，ACCC已经准备了一份常见诈骗清单，以揭示诈骗者不希望您知道的诈骗秘密和策略。

约会和浪漫骗局

约会和浪漫骗局每年使澳大利亚人损失数以百万计的澳元，并可能会毁掉个人和家庭生活。

这种诈骗的运作方式

约会和浪漫诈骗者在合法的约会网站、移动应用程序或脸书等社交媒体平台上创建虚假个人资料，并且使用往往是从其他人窃取的照片和身份信息。他们使用这些个人资料试图与您建立长达数月甚至数年的关系，这样做的目的是为了获得您的金钱。诈骗者会提出要钱来帮助解决看病、伤害、旅行费用或家庭危机等问题。他们是无情的，会对您撒谎，利用您善良的本性。

诈骗者通常会在海外，并编造借口解释他们为什么在那里，例如服兵役、做工程师工作或照顾朋友或亲戚。他们的真实身份永远不是自己声称的那样，一些狡猾的诈骗者甚至可能会送小礼物给您。这样做是因为他们有更加宏伟的计划，晚些时候从您那里获得更多的钱。

保护自己

- 永远不要把金钱和个人信息交给您只在网上见过的人。
- 如果一个网上崇拜者在仅联系过几次或者有过几次对话之后，就要求在约会网站或社交媒体平台之外进行交流，那么需要注意，这可能是一个诈骗者。
- 对您的崇拜者进行图像搜索，以帮助确定他们是否名副其实。您可以使用Google或TinEye等图片搜索服务。
- 在线分享私密照片或视频时要小心谨慎。众所周知，骗子会使用您不希望任何其他人看到的图片或视频来敲诈他们的目标。

投资骗局

“无风险投资” 还是可能会遭遇不幸?

这种诈骗的运作方式

投资骗局有多种形式，包括加密货币购买、二元期权交易、商业投资、退休金计划、管理基金以及股票或财产的买卖。诈骗者使用看上去很专业的小册子和网站来美化“机会”，从而掩盖其欺诈行为。通常，诈骗者开始会突然打来一个电话或发来一封电子邮件，提供“不容错过”、“高回报”或“保证”机会。诈骗者通常在海外经营，不会具有澳大利亚金融服务许可。

电脑预测软件骗局承诺能够准确预测股市走势、赛马、体育赛事或彩票的结果。这只是一种伪装成投资的赌博形式。大多数计划或安排都没有任何用处，最终买家也无法收回他们的钱。在许多情况下，供应商会消失得无影无踪。

退休金骗局承诺让您可以提前提取退休金基金，往往是通过自我管理的退休金基金或收取一笔手续费。诈骗者可能会要求您附和一个故事，以便尽早释放您的资金，然后，作为您的财务顾问，他们将欺骗您的退休金公司直接把您的退休金福利向他们支付。一旦他们得到了您的钱，诈骗者可能会收取大笔“手续费”，或者让您一无所有。

保护自己

- 不要让任何人强迫您做出有关您的资金或投资的决定 — 特别是如果突然出现的出乎意料的承诺。
- 在您交出自己的钱之前，请自行对投资公司进行调查，并查看www.moneysmart.gov.au，了解他们是否拥有澳大利亚金融服务许可证。问问自己：如果一个陌生人知道赚钱的秘诀，他们为什么要与您分享？

如果您还不到退休年龄，请当心那些声称可以帮助您轻松提取预留退休金福利的宣传。如果您提前非法提取退休金，可能会受到税法的处罚。

威胁和惩罚骗局

如果政府机构或可以信任的公司告诉您付钱，请先止步，仔细思考，小心核查。

这种诈骗的运作方式

这些骗局不是通过提供奖品、金钱或回扣，而是使用威胁手段来吓唬您交出自己的钱。诈骗者可能会打电话给您并威胁要**逮捕**您，或者发送一封电子邮件，声称您有尚未偿付的**超速罚款**、**欠税务局债务**或有**未付账单**。

在通话过程中，骗子会迫使您立即付款，并告诉您，如果您拒绝，就会派遣警察到您家。众所周知，骗子会针对社区中的弱势群体，例如新来的移民。他们假装成移民局的官员，威胁受害者支付费用以纠正他们的签证错误，否则会将他们**驱逐出境**。还有一个非常类似的骗局，骗子假装来自澳大利亚税务局，告诉受害者说他们有一笔未付税款。

诈骗者还会假装是可以**信任的公司**，如您的银行、天然气、电力、水或电话提供商。他们会威胁说如果您不立即支付账单，将取消服务或向您收取相当高额的罚款。有时，他们可能冒充像澳大利亚邮政这样的企业，通知您去提取一件物品，否则每天都需要支付手续费。无论具体情况如何，他们都会试图让您担心，然后不经过思考，也不去检查故事是否属实就采取行动。

如果骗局通过电子邮件发送，则可能包含附件或链接到虚假网站，在那里您将被要求下载“账单”、“罚款”或“交付详细信息”的证明。一旦打开附件或下载文件就会导致您的电脑感染恶意软件(请参阅第16页)。

保护自己

- 不要理会打电话的人给您施加压力。先停顿一下，思考清楚，核查他们的故事是否属实。
- 政府机构或可以信赖的公司绝不会要求您通过礼品卡、电汇或比特币等不寻常的方式付款。
- 验证联系人的身份，可以通过直接打电话到相关组织 — 通过电话簿、过去账单或网上搜索等独立来源找到这些机构。
- 请勿使用他们的电子邮件中所提供的或在通话期间提供给您的联系方式。重复一次，一定要通过独立的来源去查找他们。

出乎意料的金钱骗局

如果要求您在收到货物或金钱之前提供付款，请三思而后行。

这种诈骗的运作方式

诈骗者有一天突然告诉您，您有资格领取金钱、宝石、黄金或价值不菲的股票，但您需要**预先付款**才可以。他们所承诺的东西您永远也不会收到，并且他们总还会有一个借口告诉您为什么还需要再支付一笔钱。如果您支付了这样的费用，就不要再想要回您的钱了。

回扣或退款骗局是有骗子告诉您，由于您多缴了税款、银行手续费或某种补偿等原因，有一笔钱要退给您。但是，在获得这笔资金之前，您需要支付少许手续费。

遗产继承诈骗，诈骗者可以扮演律师、银行家或外国官员的角色，并告诉您，您有权获得大额继承权，或者主动提出让您分享某种方案，因为您的姓名与死亡者的姓名相同。他们会经常使用貌似冠冕堂皇的文件，并要求您在收到遗产之前支付费用和税款。他们还可以要求您提供个人信息以填写 “官方文件”。这意味着您不仅会丢钱，个人身份的资料也会被盗取。

有一种骗局通常称为**尼日利亚骗局**，或许起源于西非，但现在可能来自世界任何地方。会有骗子告诉您，他们有一笔很大财富，拼命想要从他们国家转出来，需要您的帮助来达到这个目的。他们可能会声称财富是腐败的政府或官员所抛弃的隐秘的金钱、黄金或资产，如果您同意接收，他们会在安全的情况下给予您很大

的份额。像所有这些骗局一样，他们会说您需要首先缴纳税款、银行费用或反恐和洗钱支票的费用，然后他们才能给您汇款。

这些骗局通常来自海外，并要求通过电汇付款，但也可能要求银行转账或其它付款方式。

如果您不慎陷入这些骗局，将永远不会从骗子那里收到任何东西，而且会损失您所发送的任何金钱。

保护自己

- 请记住，没有快速致富的办法：如果听起来好得令人难以置信，那可能就不是真的 。
- 如果陌生人要求通过汇票、电汇、国际资金转账、预付卡或电子货币进行预付款，应避免这样做，以这种方式发送出去的钱极少能收回。
- 如果莫名发来的电子邮件看起来可疑，请将其直接删除。不要点击任何链接。
- 政府部门、银行或公用事业部门绝不会联系您，并要求您预付款项以安排退费或回扣。
- 如果您不确定，请以独立方式核查联系人的身份。请勿使用发送给您的邮件中提供的联系信息— 可以通过电话簿或网上搜索等独立来源获取正确的联系详细信息。
- 使用其信息的确切措辞在网上进行搜索 — 可以通过这种方式识别许多骗局。

奖品和彩票骗局

不要被意外的赢奖所诱惑 — 最终赢得意外之财的只有诈骗者。

这种诈骗的运作方式

这些骗局试图欺骗您提前付款，或提供您的个人信息，以便从您从未报名参加的彩票、赌金独赢活动或竞赛中获得奖品。诈骗者声称您需要在 “奖金” 或奖品发放之前支付费用或税款。您可能还必须致电或发送短信到收费率很高的一个电话号码才能领取奖品。

刮奖诈骗是指收到装有光鲜的小册子和几张刮奖卡的邮件，其中一张卡会中奖。为了让人觉得更可信，它通常会中二等奖或三等奖。当您打电话领取奖金时，诈骗者会要求您先支付费用或税款，然后才能获得奖金。

彩票骗局可能会使用真实海外彩票的名称声称您已赢得现金，即使您从未参加过抽奖。诈骗者通常要求收取费用或税款然后才能释放资金。他们还会告诉您需要提供个人信息来证明您是正确的赢家。但是他们会使用此信息盗用您的身份，或从您的银行帐户中窃取金钱。

假礼券和礼品卡是指诈骗者向您发送电子邮件或短信或社交媒体消息，声称您已经赢得了知名零售商的礼品卡，但您需要提供一些个人资料才能获取。这是为了获取个人信息，以盗用身份，或向您展开另一场骗局。据了解，这些邮件骗局也会向您的电脑或手机发送勒索软件（请参阅第17页）。

旅行奖骗局是指诈骗者声称您赢得了免费假期或机票。事实上，实际获得的是购买住宿或航班代金券的机会。这些旅行券通常有隐藏的费用和条件，或者可能是假的，毫无价值。同样，诈骗者可能会为您提供子虚乌有的惊人折扣的假期套餐。

保护自己

- 记住：除非您已经参加彩票抽奖或比赛，否则不会赢钱。
- 抽奖和彩票不需要您另外付费来领取奖金 — 使用其信息的确切措辞在网上进行搜索，可能有助于确认这是一个骗局。
- 在拨打电话或发短信至以“19”开头的电话号码之前请三思而后行 — 那些电话或短信都按高价收费。

网上购物、分类广告和拍卖骗局

诈骗者也非常喜欢网上购物的便利性。

这种诈骗的运作方式

越来越多的消费者和企业在网上购买和销售物品。不幸的是，诈骗者喜欢在网上寻找受害者。

诈骗者可以创建非常有说服力的**假零售网站**，看起来像真实的东西，包括脸书等社交媒体。辨别零售网站是否是骗局的最大窍门是看他们的付款方式 — 如果要求您通过电汇或其他不寻常的方式付款，请谨慎行事。

网上拍卖骗局是指诈骗者声称您有第二次机会购买您出价的物品，因为获胜者退出了。诈骗者会要求您在拍卖网站的安全支付系统之外付款；如果您这样做，钱将会丢失，您将无法得到您所支付的物品，拍卖网站也无法帮助您。

网上分类广告诈骗是针对买家和卖家的常见骗局。买家应该小心那些在合法分类广告网站上发布虚假广告的诈骗者。广告范围很广，涉及从出租物业到宠物，二手车或相机的任何物品，并且通常价格便宜。如果您对该项目表现出兴趣，则诈骗者可能声称他们正在旅行或已经移居海外，并且代理人将在收到付款后交付货物。付款后，您将无法收到货物，也无法联系卖家。

对于卖家，分类广告诈骗者会以慷慨的报价回复您的广告。如果您接受，诈骗者将通过支票或汇票支付。但是，您收到的金额会远远超过约定的价格。在这种**多付款骗局**中，“买方” 可能会告诉您这是一个错误，并会要求您通过汇款退还多余的金额。诈骗者希望您在发现他们的支票出现跳票或者汇票是虚假的之前汇出这笔钱。如果您已经发出了钱，那么这些钱以及您所销售的物品就都回不来了。

保护自己

- 准确了解您在与谁打交道。如果是澳大利亚零售商，一旦出现问题，解决问题更容易。
- 检查卖家是否有信誉，是否有退款政策和投诉处理服务。
- 应该避免接受任何通过汇票、电汇、国际资金转账、预付卡或电子货币要求预付款的安排。以这种方式发送的钱很少能够退回。切勿通过电子邮件向任何您不了解或不信任的人发送资金，或在网上提供信用卡或网上交易账户详细信息。
- 只能通过网站的安全付款方式付款 — 查找并使用以”https”开头、以及有封闭的挂锁符号的网址。
- 永远不要接受支付金额超过您的约定金额的支票或汇票，永远不要替任何人转钱。

针对电脑和移动电子设备的骗局

请记住: 任何连接到互联网的电子设备都易受到攻击。

这种诈骗的运作方式

远程存取诈骗者通过电话呼叫您，声称您的电脑已被病毒感染。如果您按照他们的说明操作，就会允许他们进入并控制您的电脑，窃取信息或安装恶意软件。他们也可能试图说服您购买“反病毒” 软件，这种软件通常被证明价格过高或在互联网上可以免费提供。

恶意软件是指可以安装在您的电脑或其它设备上的任何恶意软件，包括病毒、间谍软件、勒索软件、特洛伊木马和击键记录程序。

击键记录器和间谍软件允许诈骗者准确记录您在键盘上键入的内容，以查找您的密码和银行信息，或存取个人信息并将其发送到任何他们想要的地方。安装后，诈骗者可以控制您的电子邮件和社交媒体帐户，并获取设备上的任何信息，包括密码。他们还可以使用您的帐户向您的朋友和家人发送更多诈骗信息。

勒索软件是另一种类型的恶意软件，它会加密或锁定您的设备，不向他们付款解锁就不能再使用。但支付款项并不能保证它将被解锁或免于隐藏病毒，这些病毒也可能传播并感染网络上的其他电脑或设备。

恶意软件通常通过电子邮件发送，可能貌似来自合法来源，例如您的公用事业服务商、政府机构甚至是声称要发出罚款的警察。请勿点击链接或打开不是完全放心的任何附件，否则您可能就会下载恶意软件。这些骗局既针对个人也针对企业。

保护自己

- 警惕免费下载服务，包括音乐、游戏、电影和浏览成人网站。他们可能在您不知情的情况下安装有害程序。
- 确保您的办公室网络、电脑和移动设备安全。定期更新安全软件、更改密码并备份数据。场外和离线存储备份。www.staysmartonline.gov.au介绍了如何备份数据和保护移动设备。
- 不要打开陌生人发来的附件或点击电子邮件或社交媒体消息中的链接 — 只要按删除键即可。

身份盗窃

所有骗局都有可能导致身份信息被盗用。保护自己免受诈骗也意味着保护您的个人信息安全。

每种骗局都有身份盗窃的危险

大多数人会将骗局与骗钱联系在一起。但是，您的信息对诈骗者也很有价值。诈骗者窃取您的个人信息以进行欺诈性活动，例如使用您的信用卡进行未经授权的购买，或使用您的身份开设银行或电话帐户。他们可能会以您的名义贷款或进行其它非法业务。他们甚至可能会将您的信息出售给其他诈骗者，以便其进一步非法使用。

身份被盗在财务上和情感上都可能是毁灭性的。可能需要很多个月的时间才能回收您的身份，而且身份被盗的影响可能会持续多年。

网络钓鱼 — 诈骗者通过电子邮件、电话、脸书或短信突然与您联系，假装来自合法的企业，如银行、电话公司或互联网服务商。他们会引导您访问该企业网站的虚假版本，要求您提供个人详细信息，借口说出现技术错误需要验证客户记录。他们可能会打电话模仿奢侈品零售商声称有人正在尝试使用您的信用卡。他们建议您联系您的银行，但他们不会挂断电话并保持连线状态。当您尝试致电银行时，您仍然在与模拟真实电话的诈骗者交谈，他们模仿银行工作人员并询问您的帐户和安全信息。在任何一种情况下，诈骗者都会记录您提供给他们的任何信息，然后使用它来进入您的帐户。

假冒调查 — 诈骗者需要您完成网上调查，作为交换，他们会提供知名零售商礼品卡等奖品或奖励。调查会要求您回答一系列问题，包括披露重要身份证明或银行详细信息。

作为任何骗局的一部分 — 诈骗者经常在其它诈骗活动中询问个人信息。在彩票诈骗中，诈骗者经常要求提供驾驶执照或护照“证明您的身份才能发放奖金”。在约会和浪漫诈骗中，他们可能会要求提供信息以 “赞助他们的签证申请，来澳大利亚探访您”。

请记住：向诈骗者提供个人信息与给钱一样糟糕。请妥善保留个人信息并确保其安全。

保护自己

- **在网络环境中，无论讲什么话，或做什么事，都要三思而后行**
  在网上分享自己的信息应当心，包括社交媒体、博客和其它网上论坛。在填写调查、参加抽奖、点击链接或附件，甚至“加好友”、“点赞”或“分享” 某些内容之前，请先停下来，思考妥当之后再做。
- **警惕任何索取您的个人信息或金钱的请求**
  诈骗者会试图通过使用知名公司或政府部门的名称来欺骗您透露自己的信息。如果您认为这是一个骗局，请不要回应。使用电话簿或在网上搜索来查找该组织的联系信息。切勿使用他们在原始电邮中提供的联系信息。

如果您向诈骗者提供了个人身份信息，请致电1300 432 273联系IDCARE。

慈善和医疗骗局

高收入 — 保证？不可能！

这种诈骗的运作方式

就业和就业骗局是指在家工作或建立和投资“商业机会”的提议。诈骗者承诺在您支付初始预付款后会获得工作，高薪或大量投资回报。这些付款可能用于“商业计划”，培训课程、软件、制服、安全许可，税金或费用。如果您支付费用，可能也无法收到任何东西，或不是您所预期或他们所承诺的东西。

一些工作机会可能是为了掩护**非法洗钱活动**，在那里他们要求您担任“账户经理”或“个人助理”，用您的银行账户接受汇款以获得佣金，然后把钱汇到外国公司。

工作诈骗通常通过垃圾邮件或知名分类广告和求职者网站 — 甚至政府求职者网站进行宣传。

这些工作骗局的一大风险是，您可能会被要求提供许多您不应提供的个人信息，包括税号和护照或驾驶执照的副本。此信息可能在以后会被用于身份盗用。

保护自己

- 警惕那些声称会保证收入或需要预付款的说法或计划。
- 永远不要同意为其他人转账 — 这是洗钱，属于非法行为。
- 申请工作时，请勿提供税务档案号码、驾照或护照。您可能需要提供此类信息，但只有在开始工作之后才需要。

洗钱是刑事犯罪：不要同意为陌生人转账。

工作和就业骗局

诈骗者是无情的，可能在您生活绝望而有需要的时候出手。

这种诈骗的运作方式

当人们希望对某一慈善事业进行捐赠或想解决某一健康问题时，骗子就会乘虚而入。

慈善骗局是指骗子通过假装为合法的事业或慈善事业或他们创造的虚构事业工作来筹集资金。诈骗者通常会利用新闻中最近报道的自然灾害或危机。

这些骗局会将急需的捐款从合法慈善机构转移出去。慈善机构必须在政府注册 — 请先核查他们的注册资质然后再放心地捐款。

奇迹治疗骗局提供一系列看上去像合法的替代医疗产品和服务，通常承诺对严重疾病可以尽快有效地提供救治办法。通常使用虚假的已经“治愈”的人的虚假证词来进行宣传。

减肥骗局承诺通过少许努力或者无需努力即可有效减肥。这种类型的骗局可能涉及不寻常或限制性饮食、革命性的健身运动、彻底减脂的装置、突破性药丸、膏药或软膏。 您可能需要支付大笔预付款或签订长期供货合同。

虚假网上药店以非常便宜的价格提供假药和药品，有时在没有医生处方的情况下提供。 这些药物可能含有有限的活性成分或根本没有活性成分，这会对使用者产生致命的后果。

保护自己

- 如果在街道上遇到慈善捐献收集者，请要求查看他们的身份证明。如果您对他们的身份有任何疑问，请不要付钱。
- 查看澳大利亚慈善机构非营利协会的注册慈善机构名单。
- 如果您正在考虑有关药物、保健品或其它治疗方法的“奇迹”或“即刻有效”的宣传，请咨询您的医疗保健专业人士。
- 问问自己：如果这真的是一种神药，您的医疗保健专业人员难道不会告诉您这件事吗？

商业骗局

许多企业工作性质繁忙，诈骗者利用这一特点来骗取他们的钱财。

这种诈骗的运作方式

针对企业的诈骗伪装花样繁多，可能会在最繁忙的时候出现，例如财政年度末。

虚假账单骗局是骗子用来对付企业的最常见技巧。诈骗者发出不需要的或未经授权的生意列表、广告、产品或服务的虚假账单。**业务目录骗局**是一个众所周知的示例，您会收到在一个所谓著名的目录中列表的账单。诈骗者通过伪装的未结发票或免费列表来欺骗您进行登记，但在细则中隐藏订阅协议。

域名诈骗是诈骗者使用的另一种策略，您被欺骗注册一个非常类似于您自己的未经请求的互联网域名注册。您可能还会收到有关您的实际域名的虚假续订通知，并在没有意识到的情况下付款。

办公用品供应骗局是指您接收未曾订购的产品并被要求付款。这些骗局通常是您经常订购的产品或服务，如文具和清洁用品。诈骗者通常会给您的公司打电话，假装您已经订购了服务或产品。

付款转向诈骗是指诈骗者使用他们通过黑客攻击您的电脑系统而获得的信息，然后装扮成您的常规供应商之一，并告诉您他们的银行详细信息已经更改。他们可能会告诉您他们最近更换了银行，并可能使用复制的信头和品牌来说服您他们是真的。 他们会为您提供新的银行帐号，并要求将所有未来的付款支付到新的帐号。这种骗局通常只有当您的常规供应商询问为什么还没有给他们付款时，才会被发现。

勒索软件对任何企业都是极具破坏性的。最好的防御措施是定期备份数据并将备份存储在异地和离线状态。请参见第17页的更多细节。

保护自己

- 不要立刻同意提议或交易 — 如果交易涉及金钱、时间或长期承诺，请一定要求对方以书面形式提供，并寻求独立咨询。
- 切勿向突然与您联系且您不了解、也不信任的人提供您企业的银行、财务和会计信息。
- 有效的管理程序对防止诈骗会非常有效 — 制定明确定义的流程来验证帐户和支付账单，并且在收到要求更改银行信息的请求时仔细查看。
- 培训员工识别诈骗。
- 业务数据应异地和离线备份。
- 小心查看要求更改付款信息的电子邮件。每次都直接与对方公司或个人核查付款明细的更改。

诈骗如何运作 — 骗局的解析

大多数诈骗都遵循相同的模式，一旦理解了这一点，就会更容易辨识骗局。

如果仔细查看本书中列出的所有不同类型的诈骗，您很快就会注意到大多数骗局都包括三个阶段：(1)接近；(2)沟通；(3)付款。

了解诈骗的基本组成部分会帮助您避免当前常见的诈骗形式，并防范未来出现的新诈骗。

1. 接近：交付方法

当诈骗者接近您时，总会带着一个编造出来让您相信的谎言故事。诈骗者总会冒充其他人，政府官员、专家投资者、彩票官员甚至是浪漫的崇拜者。

为了向您提供这些谎言，诈骗者将使用一系列不同的沟通方法。

上网

诈骗者潜伏在互联网的匿名环境中。

电子邮件是一种受欢迎的骗局传递方法，提供了一种廉价而简单的大规模通信方式。针对您的个人信息“钓鱼”的网络钓鱼电子邮件是最常见的电子邮件诈骗类型。

社交网络平台，约会网站和网上论坛允许诈骗者“加好友”并进入您的个人生活以获取您的个人信息，然后用这些信息来对付您或您的家人和朋友。

诈骗者使用**网上购物、分类广告和拍卖网站**来定位买家和卖家，最初的联系通常是通过信誉良好且值得信赖的网站或看似真实的虚假网站进行的。注意查看是否有安全的支付选项，并注意不寻常的支付方式，如电汇、比特币或预付钱卡。信用卡通常会提供一些保护。

打电话

诈骗者也会打电话和发短信。

诈骗者通过**打电话**对家庭和企业进行各种各样的诈骗，从威胁税务诈骗到提供奖品或“帮助”处理电脑病毒。因为可以通过成本低廉的互联网协议语音(VOIP)来打电话，所以呼叫中心可以在海外运营，其电话号码看起来像是本地号码。电话呼叫者的身份很容易被伪装，诈骗者用它来让您相信他们的身份，这是许多诈骗技巧中的一种。

诈骗者使用**短信**发送一系列诈骗，包括抽奖或奖品诈骗。如果您回复，可能会被收取高额费用或发现自己已注册订阅服务。除非您知道短信来自哪个人，否则不要回复或点击短信中的链接，这样会更安全。它们还可以用照片、歌曲、游戏或应用程序的形式包含附件或链接到恶意软件。

上门

小心 — 些诈骗者会来到您家门口试图欺骗您。

挨家挨户诈骗通常是指欺诈者推销根本不会送货的或品质很差的商品或服务。甚至您不想要或不同意的工作，他们也会向您收费。一个常见的挨家挨户骗局是由欺诈的技术维修工人进行的，他们从一个地方转到另一个地方，进行劣质的房屋维修或只是拿走您的钱然后跑掉。

合法的企业可以挨家挨户销售，但必须明确表明自己的身份和公司的名称，并遵守其它规则。在门到门销售实践方面，您有特定的权利，包括改变主意的机会 — 请访问网站 www.accc.gov.au/doortodoor了解更多信息。

诈骗者可以扮成**假慈善工作者**来收集捐款。他们会利用洪水和森林大火等近期事件。您在捐赠之前应该要求他们出示身份证明，并查看他们的正式收据簿。

大宗邮件仍然用于发送**彩票和抽奖诈骗**，**投资机会**、**尼日利亚诈骗和假遗产继承信件**。光鲜的小册子并不保证他们的做法是正当的。

无论他们使用何种方式，他们讲的故事总是诱饵，如果您信服了，骗子会试图让您走下一步。

2.沟通与诱骗

如果您给他们一个与您交谈的机会，他们就会开始用他们的诈骗工具箱中所有的伎俩来说服您把自己的钱给他们。

诈骗者的伎俩可能包括以下方面：

- 诈骗者会精心编造**令人信服的故事**来获得他们想要的东西。
- 通过使用您的**个人信息**，他们让您觉得自己以前已经与他们打过交道，这样使该骗局看起来是正当的。
- 诈骗者可能会**定期与您联系**以建立信任并使您确信他们是您的朋友、合作伙伴或浪漫的对象。
- 他们通过利用您对赢奖的兴奋，对永恒之爱的承诺，对不幸事故的同情，对没有能够提供帮助的内疚，或对被逮捕或被罚款焦虑和恐惧来**玩弄您的情绪。**
- 诈骗者喜欢创造一种**紧迫感**，因此您没有时间考虑清楚，从而做出感性的反应而不是理性的反应。
- 同样，他们使用**高压销售策略**，声称优惠是有时间限制的，价格会上涨或市场会改变，机会将会丧失。
- 骗局会使用**光鲜的小册子**和技术行业术语，使用办公室前台、呼叫中心和专业网站，拥有真实业务的所有特征。
- 通过访问互联网和聪明的软件，诈骗者很容易制作**赝品和貌似官方真品的假文件**。一份似乎得到政府批准或充满法律术语的文件可能会让骗局显得冠冕堂皇，看似很有权威。

诈骗者的具体手段都是为了让您降低防御能力，建立对他们的故事的信任，从而快速或非理性地采取行动，并进入最后阶段 — 付钱。

3.付钱

有时您能够判断诈骗的最大线索就是诈骗者要求您用方式什么付钱。

在骗局的几分钟内或经过几个月的感情培养之后，就会开始要钱。至于您如何汇款，诈骗者也有他们喜欢的方式。

有时候，诈骗者会将受害者引导至最近的**汇款**地点(邮局、电汇服务、甚至银行)汇款。也有时候，他们会保持手机连线，一步一步地给出具体的指示，甚至可能会给您派一辆出租车来帮助解决这个问题。诈骗者愿意以任何方式接受资金，这可能包括**直接银行转账**、**预付借记卡**、**礼品卡**、**Google Play**、**Steam**或**iTunes**卡或虚拟货币(如**比特币**)。任何不寻常的付款方式的要求都使他们露出马脚，表明是一场骗局。

信用卡通常可以提供一些保护，您还应该查看安全的付款方式，如网址中出现“https”字样，并且网站上有一个封闭的挂锁符号。

不要向在网上或通过电话认识的人汇款 — 特别是如果他们在海外。

请注意，诈骗者还可以要求以贵重物品和贵重礼品(如珠宝或电子产品)的形式付款。向诈骗者付钱并不是您应该担心的唯一问题 — 如果您帮助为陌生人转账，就可能会无意中卷入**非法洗钱**活动。

保护自己的黄金法则

警惕诈骗存在的事实。当处理来自个人或企业的不速之客的联系时，无论是通过电话、邮件、电子邮件、面对面还是在社交网站上，总是要警惕这种方法可能是骗局。请记住，如果看起来好得令人难以置信，那可能就是骗局。

知道您在和谁打交道。如果您只是在网上认识某人或不确定某项业务的合法性，请花一些时间再做一些调查研究。将照片进行Google图片搜索，或在互联网上搜索可能曾经与他们打过交道的其他人。

不要打开可疑文本、弹出的窗口或电子邮件 — 直接删除即可。如果不确定，请通过电话簿或上网搜索等独立来源验证联系人的身份。请勿使用发送给您的邮件中所提供的联系信息。

确保您的个人信息安全。请给信箱上锁。在丢弃账单和其他重要文件之前，请先将其撕碎。将密码和个人识别码保存在安全的地方。请注意您在社交媒体网站上分享的个人信息量。诈骗者可以使用您的信息和图片来创建虚假身份或实施针对您的骗局。

谨防不寻常的付款方式。诈骗者经常要求通过电汇、预付卡甚至Google Play、Steam或iTunes卡和比特币付款。这几乎总是可以表明这是骗局的一部分。

确保移动设备和计算机的安全。始终使用密码保护，不与他人共享使用(包括远程)，更新安全软件和备份内容。使用密码保护自己的WiFi网络，避免使用公共电脑或WiFi热点访问网上银行或提供个人信息。

仔细选择密码。选择其他人难以猜测的密码并定期更新。保密性强的密码应既包括大写也包括小写字母，还有数字和符号的混合。不要为每个帐户/个人资料使用相同的密码，也不要与任何人分享您的密码。

当心对您的个人信息或金钱进行索取的任何要求。切勿向您不认识或信任的任何人汇款或提供信用卡号码，网上帐户详细信息或个人文件副本。不要同意为他人转移金钱或货物：洗钱是一种刑事犯罪。

上网购物时要小心。谨防那些看起来好得令人难以置信的优惠，并只使用您了解并信任的网上购物服务。在使用虚拟货币(比如比特币)之前要三思而后行 — 他们没有与其他交易方法相同的保护措施，这意味着钱一旦发送出去，就无法回收。

在哪里可以寻求帮助或支持

如果您因为受骗而损失金钱，或将您的个人信息泄露给了诈骗者，那就无法收回你的金钱。但是，您可以立即采取措施限制损失的程度，保护自己免受进一步损失。

联系您的银行或信用合作社

如果您已向诈骗者汇款或提供个人银行信息，请立即联系您的银行或信用合作社。如果诈骗者有您的帐户详细信息，银行可能会停止转帐或停止兑现支票，或关闭您的帐户。如果您的信用卡被欺诈性收费，您的信用卡提供商可能会执行“退款”（将交易反转）。

恢复被盗身份

如果您怀疑自己是身份盗用的受害者，请务必迅速采取行动，以降低财务损失或其他损失的风险。

请联系**IDCARE**。这是一项由政府资助的免费服务，为身份犯罪的受害者提供支持。IDCARE可以帮助您制定相应计划，以采取适当的措施来修复对您的声誉、信用记录和身份造成的损害。浏览IDCARE网站www.idcare.org 或致电1300 432 273。

申请**联邦政府受害者证书** — 证书有助于支持您声称自己是身份犯罪的受害者，并可用于帮助您与政府或金融机构重新建立您的信誉。请浏览总检察长办公室网站www.ag.gov.au（或致电02 6141 6666），了解有关保护和恢复身份的更多信息。

联系辅导或支持服务

如果您自己或您认识的人被骗，可能因此而患有情绪紧张或抑郁症，请咨询您的全科医生，当地健康专家或您信任的人。您也可以考虑联系辅导或支持服务，例如：

生命热线(Lifeline) — 当您在危机中需要支持时，请致电13 1114(7天24小时全天候)联系生命热线或访问www.lifeline.org.au。

Beyondblue — 有关抑郁或焦虑的信息，请致电1300 224 636联系beyondblue或访问www.beyondblue.org.au。

儿童帮助热线(Kids helpline) — 为5至25岁的年轻人提供热线电话和网上辅导及支持服务。请致电 1800 551 800 联系儿童帮助热线，或访问www.kidshelpline.com.au。

澳大利亚财务辅导(Financial Counselling Australia) — 如果您遇到财务困境，请致电1800 007 007 与免费的财务辅导员交谈，或浏览www.financialcounsellingaustralia.org.au。

在哪里举报骗局

向有关当局举报诈骗，您就可以帮助他人。您的信息将帮助这些组织更好地了解最新的骗局，并提醒其他人应该注意什么。

以下组织会接受有关特定类型的诈骗的情况的举报。

诈骗监察(Scamwatch)

通过Scamwatch向澳大利亚竞争及消费者委员会(ACCC)报告诈骗行为 — 请浏览网站www.scamwatch.gov.au。

比诈骗者领先一步

比诈骗者领先一步 — 访问Scamwatch网站，了解针对澳大利亚消费者和小企业的骗局。详细了解诈骗如何运作，如何保护自己，以及如果被骗，应该怎么办。

在Scamwatch登记订阅服务，即可收到有关新一轮诈骗手段的免费电子邮件提醒。

www.scamwatch.gov.au

在Twitter上关注Scamwatch@scamwatch_gov或http://twitter.com/Scamwatch_gov。

如果您在网站或社交媒体平台上遇到骗局，请将其报告给网站，以便对其进行调查和删除。如果诈骗者冒充政府部门或银行这样的合法组织，也让他们知道，以便他们可以警告他人。

其它机构

您还应该考虑将您遇到的骗局报告给其它专门处理特定类型骗局的机构。

骗局的类型	机构
网络犯罪	澳大利亚网络犯罪在线举报网络 (Australian Cybercrime Online Reporting Network, ACORN) — 浏览www.acorn.gov.au
金融和投资骗局	澳大利亚证券和投资委员会(Australian Securities and Investments Commission, ASIC) — 浏览www.moneysmart.gov.au或致电ASIC资讯热线1300 300 630
欺诈和盗窃	您当地的警察 — 电话13 1444
垃圾邮件和短信	澳大利亚通信和媒体管理局(Australian Communications and Media Authority, ACMA) — 访问www.acma.gov.au或致电ACMA客户服务中心1300 850 115
与税务相关的骗局	澳大利亚税务局(Australian Taxation Office, ATO) — 报告税务骗局或验证声称来自ATO与您联系的人是否属实: • 致电1800 008 540 或将您的税务骗局的电子邮件转发至ReportEmailFraud@ato.gov.au
银行业	您的银行或金融机构

联系当地的消费者保护机构

虽然ACCC是处理一般消费者保护事务的国家机构，但州和地区机构也可以为您提供帮助。

澳大利亚首都地区监管服务办公室 (Australian Capital Territory Office of Regulatory Services)	www.accesscanberra.act.gov.au 13 2281
维多利亚州消费者事务办公室 (Consumer Affairs Victoria)	www.consumer.vic.gov.au 1300 558 181
新南威尔士州公平交易办公室(New South Wales Fair Trading)	www.fairtrading.nsw.gov.au 13 3220
北领地消费者事务办公室(Northern Territory Consumer Affairs)	www.consumeraffairs.nt.gov.au 1800 019 319
昆士兰州公平交易办公室 (Queensland Office of Fair Trading)	www.fairtrading.qld.gov.au 13 7468
南澳大利亚州消费者和商业服务办公室(South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
塔斯马尼亚州消费者、建筑和职业服务办公室(Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
西澳大利亚州矿业部、工业监管和安全办公室(Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

更多信息

澳大利亚政府在如何保持上网安全和可靠方面拥有一些非常好的资源。

- Stay Smart 网络服务 — www.staysmartonline.gov.au
- CyberSmart网站 — www.cybersmart.gov.au
- Stay Smart网上指南 — 请浏览 www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au