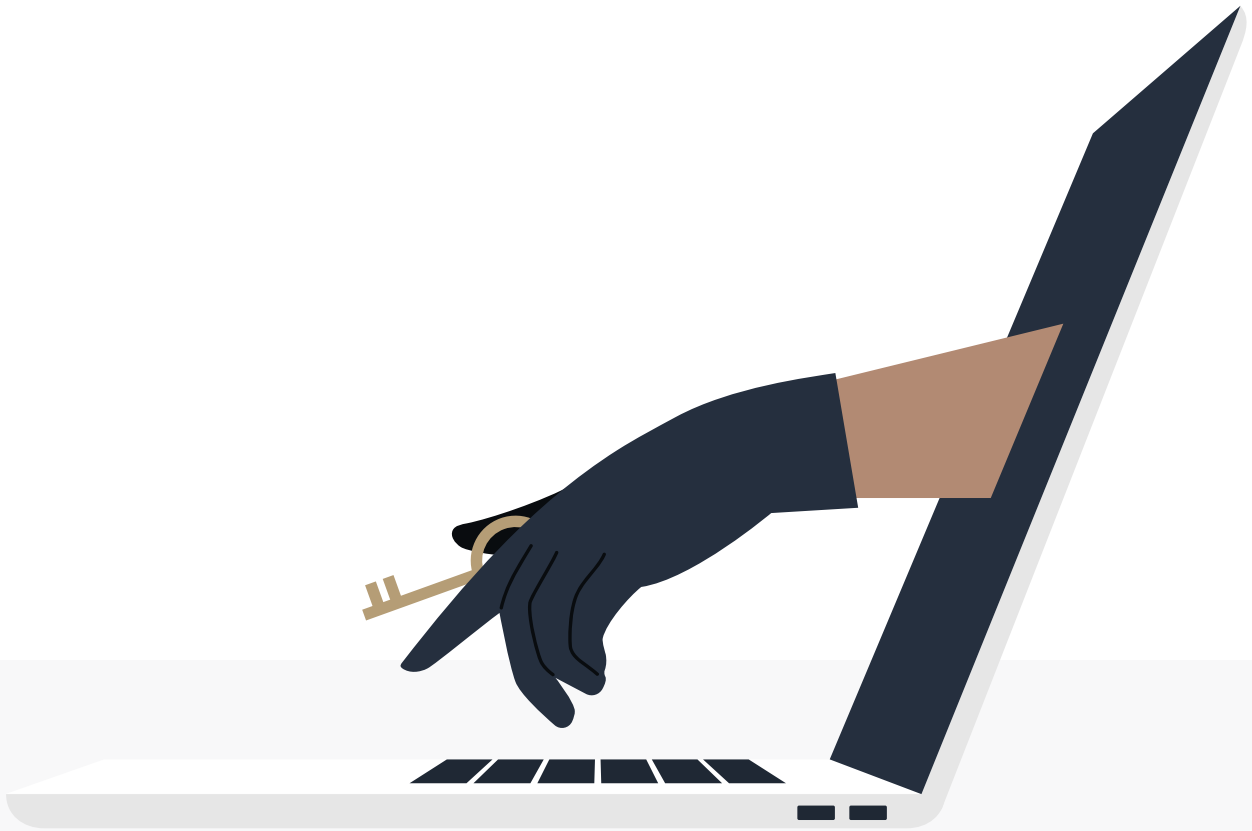
十大技巧保护您免受

冒充诈骗

Chinese (Simplified) | 简体中文



Australian Government | Be Connected
Every Australian online.

Australian Government | National Anti-Scam Centre

SCAMWATCH

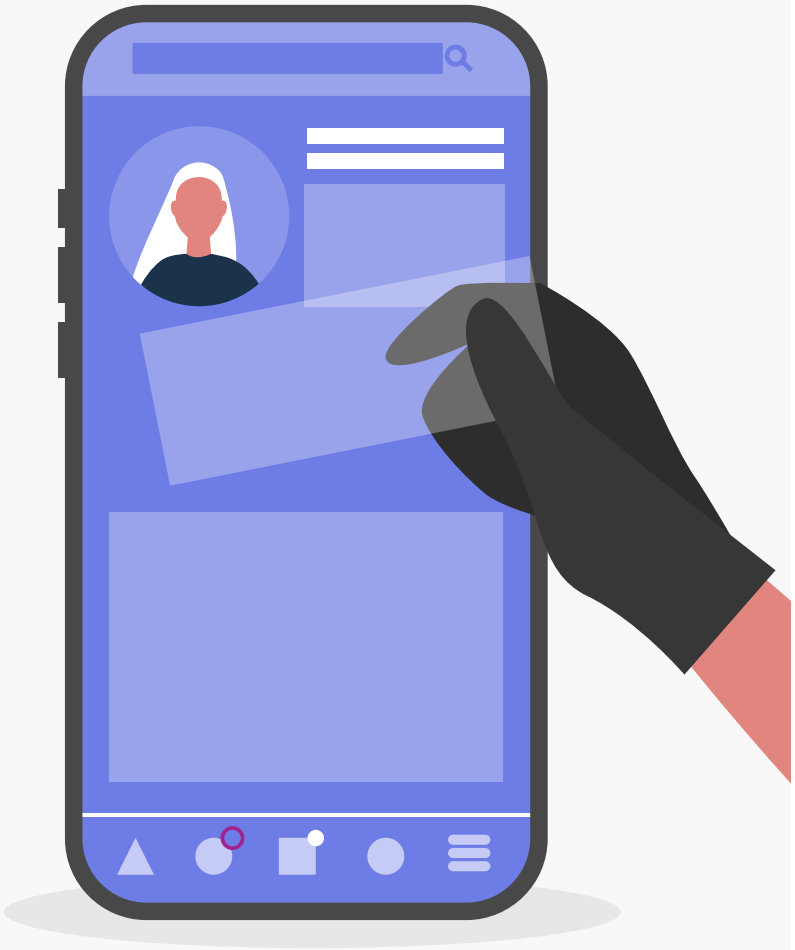
如今的诈骗手段越来越高明。以前，诈骗信息中的错误拼写和语法很容易被发现，但新技术让诈骗行为变得越来越难以发现。

国家反诈骗中心（National Anti-Scam Centre）已与政府、行业专家、执法机构和社区组织联手打击诈骗。同时您也可以采取一些措施来保护自己免受诈骗侵害。最好的保护措施之一是及时了解新出现的骗局，以便您能识别出骗局的迹象。

Be Connected 与国家反诈骗中心的 Scamwatch 合作，为您编撰本指南，帮助您识别冒充诈骗、保护自己免受诈骗侵害，并了解如果您受诈骗侵害，能去哪里寻求帮助。

本指南中提供的所有示例都是真实的骗局。

本指南内容



什么是冒充诈骗?

冒充诈骗旨在让诈骗看起来好像来自您认识的正规组织。诈骗者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，甚至会假装是您的朋友或家人。

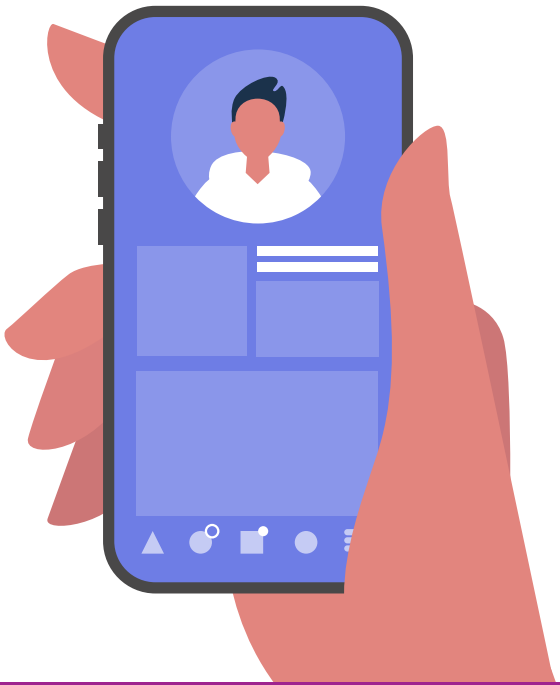
他们会假装成您信任的人，利用您的紧迫感来诱骗您付款或提供个人信息，例如重要的密码、信用卡 或银行账户的详细信息。

诈骗者会使用各种方法与您联系，包括短信、电话、电子邮件、社交媒体帖子以及看起来与官方网站相同的假网站。

什么是伪装诈骗?

诈骗者可以利用技术手段使他们的电话或信息看起来来自可信来源，从而伪装成您了解的机构。这就是“伪装诈骗”。

警惕诈骗，质疑那些要求提供个人信息（如密码或以某种方式付款）的陌生联系人。直接联系其声称所属的组织进行确认。



伪装诈骗有多种类型，包括：

01. **来电显示欺骗：**诈骗者会更改来电显示，让您看到的电话号码与实际号码不同，看起来像是正规的机构来电。

02. **短信欺骗（或伪造发件人显示名称）：**诈骗者会将他们的电话号码修改为某公司的名称（例如修改成 AusPost）。这能让假短信出现在您和某个机构之前的短信记录里，看起来就像真的是官方发送的。

03. **电子邮件欺骗：**诈骗者会更改他们的电子邮件地址或发件人姓名，让电子邮件看起来像是可信发件人发送的。他们可能会伪造“发件人”名字或电子邮件地址，通常是对合法域名进行更改或添加一个字母或数字（例如，将 @amazon.com 更改为 @amaz0n.com）。

常见的冒充诈骗

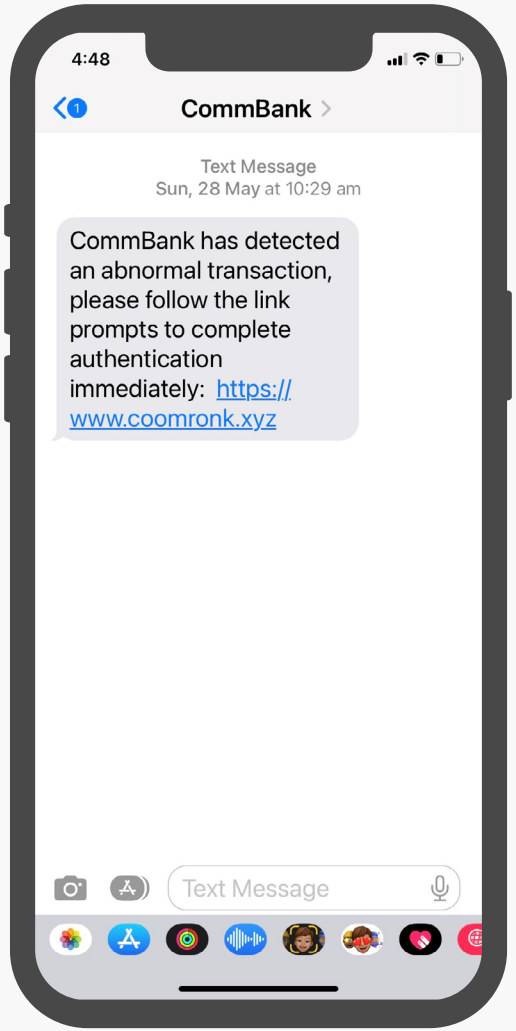
银行冒充诈骗

- 您接到自称是银行安全部门人员打来的电话或发来的短信。他们通知您有可疑交易，并声称您的银行帐户已被盗用。他们会敦促您将钱转到其他账户以“保证资金安全”或“需要进行进一步调查”。
- 您会收到一条短信或电子邮件，要求您点击链接，验证您帐户的详细信息。该链接会让您进入一个虚假网站，旨在获取您的网络银行用户名、密码和其他个人信息。

您要如何确认这是诈骗?

如果您的银行账户出现可疑活动，银行可能会与您联系，但绝不会要求您将资金转移到另一个账户。银行也不会通过陌生短信、电子邮件或电话向您索取任何帐户或个人信息，包括您的密码、PIN 码或一次性密码。

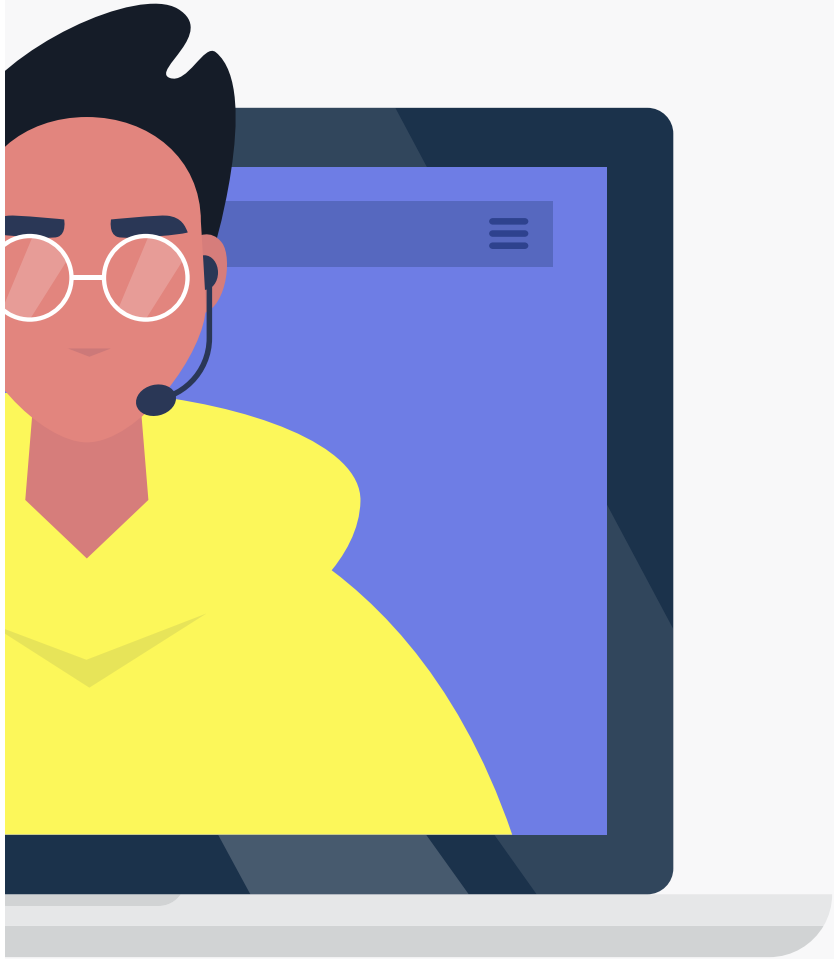
诈骗者可能会将电话号码伪装成您银行的来电显示，请不要以来电显示作为与您通话人身份的证明。他们可能看起来掌握了您的信息，但他们掌握的任何详细信息很可能都是通过欺诈手段获得的。



一条来自伪装号码冒充银行短信的示例，
它要求您点击链接验证您的详细信息。

技术支持服务诈骗

- 一个声称来自您互联网服务提供商、电信或电脑公司的来电者告知您，您的互联网或电脑出现了问题。他们可能会说您的网络或电脑被黑客入侵了、感染了病毒、运行缓慢或者即将断开连接。他们会指导您下载某些应用程序或软件，以便他们远程访问您的电脑，从而可以“修复它”。
- 您的电脑屏幕上会出现一条警告信息，敦促您立即拨打屏幕上显示的电话号码寻求帮助，以解决检测到的某个问题。



您要如何确认这是诈骗?

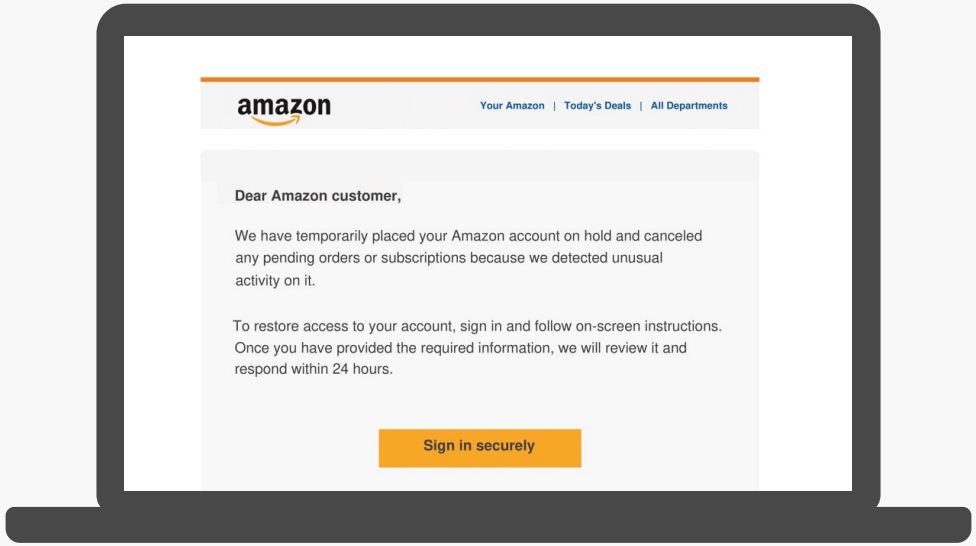
正规公司永远不会打电话告诉您互联网连接或电脑存在问题（他们期望您在出现问题时联系他们）。他们绝不会要求您下载任何类型的软件或应用程序以允许他们访问您的设备。

单击弹出窗口右上角的“x”，关闭可疑的弹出消息。如果这不起作用，请尝试单击弹出窗口外部或关闭弹出窗口的网页。如果弹出窗口仍未消失，请尝试按住 Windows 电脑上的 ALT 和 F4 键关闭网络浏览器。在苹果电脑上，从菜单中点击“强制退出”，然后选择要关闭的浏览器。

账户暂停诈骗

您收到了一封电子邮件或短信，声称来自您熟悉的机构，例如 Amazon、PayPal 或 Netflix。它通知您由于您的帐户存在可疑活动已被暂停，您需要点击提供给您的链接来确认身份，以便他们确认是您本人。

诈骗者使用恐吓手段让您进入虚假网站，获取您的个人信息，例如网站的用户名、密码以及银行或信用卡详细信息。



一封声称来自 Amazon 的诈骗电子邮件示例，它敦促您点击链接提供您的个人信息。

您要如何确认这是诈骗?

Amazon、PayPal 和 Netflix 绝不会通过陌生的电子邮件或短信中的链接要求您提供密码、银行或信用卡详细信息等个人信息。虽然各个机构联系客户的方式有所不同，但最好还是谨慎行事，始终谨慎对待这类电子邮件、短信或电话。

如果您不确定某条消息是否确实来自其声称的机构，请在网上搜索该机构的联系方式直接联系他们。切勿使用短信、电子邮件或电话中提供的联系方式。

警惕诈骗者的恐吓手段

诈骗者使用恐吓手段制造紧迫感，迫使您采取行动。他们可能会用以下的话术引起您的注意：

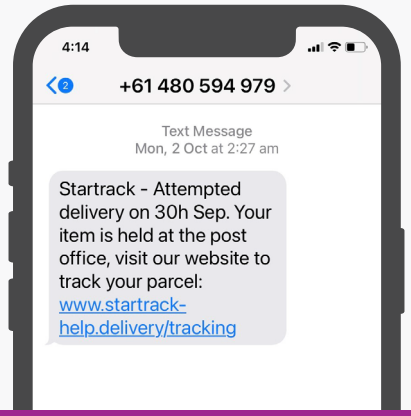
- 检测到异常帐户活动
- 未经授权的登录尝试
- 您的帐户已被封锁 / 锁定
- 您的付款被拒绝
- 我们无法验证您的账单信息

快递投递失败诈骗

您会收到一封声称来自澳大利亚邮政或联邦快递等快递公司的电子邮件或短信，通知您的包裹投递出现问题或延期投递。如果您想收到包裹，则需要支付运费或“更新您的详细信息”。

您要如何确认这是诈骗?

澳大利亚邮政（Australia Post）、联邦快递（FedEx）和其他正规快递公司绝不会通过短信、电子邮件或电话索要您的个人信息或让您付款。如果您正在等待快递送货，最好在快递公司的安全应用程序上，或通过订单的电子邮件中的实时快递追踪服务查询快递状态。如果您没有以上这些查询方式，请直接致电快递公司询问包裹的状态。



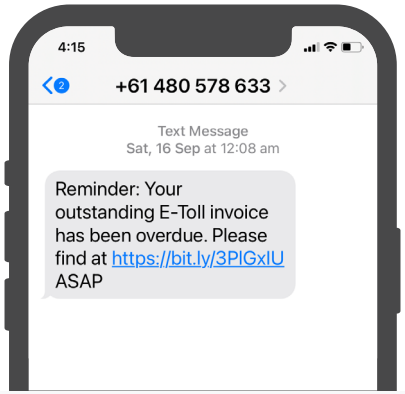
一条声称来自快递公司的假短信示例。

路费诈骗

您收到了一条收费公路运营商发来的短信，通知您路费已逾期。您需要立即采取行动，避免出现罚款。因此他们会提供一个链接让您安排付款，但它实际上会让您进入一个虚假网站，旨在窃取您财务的详细信息。

您要如何确认这是诈骗?

如果您收到的短信声称您有未缴的路费或账户余额不足，那可能是诈骗。访问收费运营商的官网或应用程序，登录您的帐户核实近期的活动记录。



一条路费诈骗短信的示例。

虚假投资诈骗

您看到了一个极佳的投资机会，而且似乎得到了名人或财经网红的认可。它承诺您高回报率且几乎没有风险。当您进行咨询时，就会进入一个看起来很专业的网站，并收到精心制作的宣传材料。

您要如何确认这是诈骗?

如果一桩交易听起来划算得难以置信，那么它很可能就是诈骗。诈骗者会使用高压手段逼您迅速做决定，以免“错失良机”。谨防有用户好评和夸大高额回报承诺的电子邮件、网站或广告。

为您提供服务的“顾问”可能会声称他们不需要澳大利亚金融服务（AFS）执照。即便他们向您提供了执照，请务必确认与您联系的人是否是执照的持有人本人。

虚假网站诈骗

您在 Facebook 上看到一个知名烧烤品牌产品的广告，其售价为 $100，而正常价格为 $900。您点击该零售商网站的链接，发现信用卡付款需支付 2.99% 的手续费，因此您选择通过银行直接转账付款获得另外 5% 的折扣。您收到了一封确认邮件，但是没有收到产品。

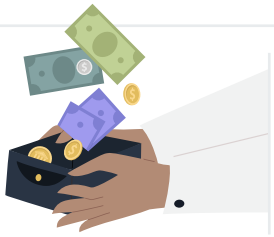
您要如何确认这是诈骗?

虚假网站标出的价格便宜得令人难以置信，付款方式也不常见，还有其他可疑信号，例如伪装成官方网站的网址（例如用 webberbbqs.com 冒充真正的 weber.com）。

诈骗者还可能付费在社交媒体和 Google 等搜索引擎上投放广告（也称为赞助商广告），因此在点击此类广告时要谨慎。

保护自己的十大秘诀

01. 警惕陌生电话。将您不认识的电话号码来电转到语音信箱。



02. 在接到陌生来电或短信时，不要急着提供个人或财务信息，先停下来想一想。问问自己：这可能是假消息吗？

03. 警惕使用恐吓手段的电子邮件。检查邮件上显示的发件人姓名及邮件地址。它们是一致的吗？例如，“发件人”栏目显示“Amazon Support”，但电子邮件地址是 amazonsupport830@gmail.com

04. 不要因为一条短信出现在你与某个认识的机构的对话记录中，就轻易相信它。那仍有可能是一条诈骗短信。

05. 如果您对收到的消息或电话有疑问，请联系其声称来自的机构进行核实。请直接访问相关机构的官方网站，或通过智能手机或平板电脑上的安全应用程序联系他们。

06. 接听电话时，即使通话者声称是您的银行或政府机构工作人员，甚至能报出您帐户的相关信息，切勿通过电话向任何人提供您的密码、PIN 码或一次性代码。

07. 切勿点击短信中的链接。尽管有些链接可能是安全的，但最好还是谨慎行事。除非您能确认发件人的身份，否则请以相同的谨慎态度对待电子邮件中的附件和链接。

08. 切勿听从陌生来电者的指示下载应用程序或安装能让他们访问您设备的软件。立即挂断电话。

09. 切勿点击电子邮件或短信中的链接登录您的网上帐户。请在您的网络浏览器中输入公司的网址，或使用他们的安全应用程序登入您的帐户。

10. 线上付款前请务必检查网站的网址，确认是否是官方网站，在网站底部的“关于我们”、“送货和退货”和其他部分中查看是否有不常见的付款方式、措辞不当或缺失信息。

如果您有任何疑问，请直接在网上搜索，输入相关机构或网站的名称以及“诈骗”（scam）一词。

您认为自己被诈骗了吗?

去哪里寻求帮助

被诈骗会造成经济和精神上的损失，因此请立即寻求帮助并迅速采取行动。有几个您可以采取的步骤：

1. 立即联系您的银行，阻止任何进一步的转账。
2. 联系 IDCARE，他们为受到诈骗或身份盗窃影响的人们提供免费支持服务。拨打 1800 595 160，或访问 idcare.org
3. 请立即将您的密码更改为强密码。
4. 向 Scamwatch 举报诈骗行为，警告其他人：scamwatch.gov.au/report-a-scam
5. 获得支持服务。如果您不方便与朋友或家人沟通这个问题，请联系 Lifeline 或 Beyond Blue 进行保密聊天。如果您损失了大量金钱，请拨打全国债务帮助热线（National Debt Helpline）。

   Beyond Blue：1300 22 4636（全天候服务）或访问 beyondblue.org.au

   Lifeline：13 11 14（全天候服务）或访问 lifeline.org.au

   全国债务帮助热线（National Debt Helpline）：1800 007 007（工作日上午 9:30 至下午 4:30）或访问 ndh.org.au

了解更多信息

请点击下面的图块探索：

《防骗手册》(Little Book of Scams）是国际公认的工具，能帮助您了解一系列常见的骗局以及如何保护自己免受骗局的侵害。

访问 Scamwatch 网站，了解最新的诈骗行为以及如何保护自己免受诈骗侵害的建议。

关于 Be Connected

Be Connected 是澳大利亚政府的一项举措，致力于通过提供一系列不同主题的免费电脑课程、短期在线课程等，培养澳大利亚老年人的网络技能及信心，提高他们的网络安全意识。Be Connected 网站和学习内容由电子安全专员办公室（eSafety Commissioner）负责管理。

关于 Scamwatch

Scamwatch 由国家反诈骗中心管理运营，该中心旨在让澳大利亚人更难成为诈骗分子的目标。它通过教育社区如何识别、避免和举报诈骗来提高人们对诈骗的认知。反诈骗中心会分享诈骗报告内的信息，并与政府、执法部门和私营部门合作，以阻止和防止人们受到诈骗。