警惕诈骗

CommBank把信任和安全放在首位。我们看到顾客受骗子的压力或欺骗而给他们转钱的例子越来越多。这些骗局经过精心策划而且形式多样。重要的是要保持警惕，觉得什么地方不对就告诉我们。要进一步了解如何保护自己以及如何举报诈骗，请访问：**commbank.com.au/safe**。

验证及核实

- 在CommBank app里完成安全检查。
- 启用多重身份验证功能，加一道证明你身份的检查。
- 使用**CallerCheck**核实自称银行来电者的身份。
- 在分行使用**CustomerCheck**向职员证明你的身份。
- 首次付款账户细节看似可疑的话，**NameCheck**会给你提示。

设备及支付安全

- 使用最新的杀毒软件，保护你的电脑抵御常见威胁。
- 使用安全的支付办法，比如触卡或插卡付款。
- 不要共享能够使用数字钱包的设备。

密码和个人资料

- 不要共享密码或PIN，共享个人资料时要谨慎。
- 不要把NetCode给任何人，包括CommBank的职员。
- 你可以随时在NetBank和CommBank app里改密码。
- 设定保密强度高的密码并定期换密码。要了解设定密码的建议，请访问：commbank.com.au/password-security。

电子邮件、短信以及在网上

- 不要点击可疑电子邮件或短信里的链接。
- 如果你对一条信息感到怀疑，问你信任的人或直接用官方联系方式联系该机构。
- 挂掉第三方自动、可疑或威胁性的来电。
- 警惕社交媒体和线上平台不明身份的联系人。

停。检查。拒绝。

停。什么地方不对劲？如果有疑问，最好停下来。吸一口气。
检查。问你信任的人或直接用官方联系方式联系该机构。
拒绝。挂掉来电、删除电子邮件、屏蔽电话号码。更换密码。

如果你认为受到诈骗，应立刻联系CommBank，电话：**13 22 21**，
从海外可以致电：**+61 2 9999 3283**。

如果英语不是你的第一语言，政府免费提供150多种语言的笔译和口译服务，可以帮助你与我们沟通，你给我们打电话或来我们分行时我们可以安排这项服务。

请记住：我们永远不会给你发电子邮件或发短信询问NetBank Client ID、密码或NetCode等银行资料，或发送一个链接让你直接从电子邮件或短信登录。务必在浏览器里输入commbank.com.au或用CommBank app安全地登录你的银行账户。如果怀疑是否来自CommBank，把它转发到hoax@cba.com.au并删除它。澳大利亚联邦银行 ABN 48 123 123 124 AFSL 澳大利亚信贷许可234945。

Commonwealth Bank

2024年6月1日出版

有关常见骗局的重要信息



投资（包括加密货币）

骗子用高回报的承诺引诱个人，高回报通常涉及加密货币或其它投资机会。骗子会尝试通过电话、电子邮件或社交媒体平台联系你。

保护自己的提示：

- 如果听起来太好、不像是真的，那很可能就不是真的。
- 警惕不请自来的要约以及从速投资或行动的压力。
- 先在ASIC网站上核实公司或经纪人的合法性。



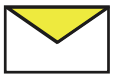
远程访问

骗子假冒来自受信赖的公司或机构给你打电话，并试图访问你的账户或设备。

保护自己的提示：

- 切勿在第三方来电者的要求下或迫于其压力下载远程访问软件。
- 你总能用官方网站上找到的正当联系方式给一个机构回电。
- 如果你接到自称来自CommBank的电话，你总能叫我们用app里的CallerCheck功能核实来电。

商务电子邮件盗用



骗子用盗用地址给企业发电子邮件，或把电子邮件伪装成来自一个受信赖的联系人，比如你的助理、顾客、律师、经理或供货商。

保护自己的提示：

- 在首次付款或修改支付细节之前，先用官方联系号码给机构打电话确认细节。
- 付款时使用NameCheck功能，看户名是否吻合所提供的BSB和账号。
- 训练员工识别并举报网络钓鱼企图。

网络钓鱼和短信钓鱼



骗子使用的欺骗性电子邮件或短信有可能包括一个链接，把你引向一个假的网站或索取敏感私人信息。

保护自己的提示：

- 不要点击可疑电子邮件或短信里的链接。
- 你可以用现有官方联系方式直接联系机构确认信息的真实性。
- 举报可疑的CommBank信息：hoax@cba.com.au

有关常见骗局的重要信息

约会交友诈骗

骗子用假的个人资料约会交友，骗受害人汇钱或发私人信息。

保护自己的提示：

- 切勿汇钱或把密码、信用卡或账户资料交给你不信任的人。
- 在网上用谷歌或社交媒体app调查你的潜在伴侣。尝试反向搜图，确定给你发的照片是不是别人的照片。
- 和家人朋友谈你在网上结识的人。他们或许能给些意见并识别你可能忽视的危险信号。

网上购物

骗子用网店或网上广告引诱购物者购买不存在或假的产品。

保护自己的提示：

- 仅在有信誉、安全的网站上购物，警惕看上去太好、不像是真的优惠。
- 使用安全的支付方式，避免直接给卖家转账。
- 不要仓促下单，不要理会“优惠有限”或“促销结束倒计时”的压力。

工作机会诈骗



所给的工作机会似乎不需要花什么力气就能得到丰厚的回报，或保证能快速赚钱。

保护自己的提示：

- 通过官方渠道核实公司和工作机会信息，对公司进行调查，确保他们是合法的而且目前正在营业。
- 警惕来自以下渠道的工作机会：社交媒体、加密聊天群、来自你不认识的人或你不知道的公司的电子邮件、电话或信函。
- 一个正当的公司永远不会要求你提前付款或用你的私人银行信息来促成公司的资金运作或交易。

威胁及惩罚



骗子假冒主管部门或受信赖的机构勒索钱，不然就威胁罚款或采取法律行动。

保护自己的提示：

- 挂掉威胁性的电话，直接联系机构。
- 一个正当的机构永远不会要你用不寻常的方式付钱，比如用礼品卡或店卡、iTunes券、电汇或比特币。
- 如果你担心安全问题，联系警务求助线。