诈骗与欺诈

保护您的资金安全的方法指南

Simplified Chinese

本指南介绍了一些最常见的骗局以及保护您和您的资金安全的方法。

内容

您遭遇过诈骗吗?	02
保护您的资金的最佳建议	03
推销电话诈骗	04
远程访问诈骗	05
网络钓鱼诈骗	06
银行卡诈骗	07
投资骗局	08
婚恋/交友诈骗	09
防范建议总结	10

您遭遇过诈骗吗？

须采取这些行动

1. 立即致电 0800 269 296（国际 +64 4 440 3142 通话可能产生费用 。
2. 停止与骗子继续通信。屏蔽他们的电话号码或电子邮件地址。
3. 如果您认为您的银行卡信息遭到泄露，请立即通过 ANZ 网上银行或 ANZ goMoney 应用程序或致电我行来冻结或取消您的银行卡。检查您的账户交易记录以确保每笔交易都是您进行的。
4. 更改您的密码。改用其他没有被诈骗者侵入风险的电子设备进行操作，或者如果您的账户被锁定，请联系相关公司寻求帮助。

同时确保您：

- 向您信任的家庭成员或朋友寻求帮助和支持。
- 向您使用的任何其他金融提供商或银行以及警方报告诈骗或欺诈行为，或者如果相关的话向CertNZ报告。

我们的最佳建议可帮助您保护

您的资金

1. 警惕接到的意外电话，因为诈骗者会假扮为一些合法机构。通过该组织对外公开的电话号码与其联系，核实电话的真实性。
2. 切勿点击意外收到的电子邮件、短信或社交媒体短信中的链接或下载其中的附件。
   - 如果您有一张付款账单将要寄到，请注意当心，因为骗子有可能会截获付款账单。防止诈骗的最佳操作方式是联系相关公司或个人，确认账单的真实性，并确保银行账户信息正确无误。
   - 删除陌生的人或组织的意料之外的电子邮件或信息。
3. 切勿通过点击链接访问您的网上银行。务必在网络浏览器中输入完整网址(www.anz.co.nz)来访问。
4. 切勿向意外来电泄露您的密码、信用卡信息、网银或 goMoney 登录信息、或两步身份验证码（即短信验证码），同时注意切勿点开带有链接的电子邮件或短信，以防泄露以上信息。
5. 切勿允许他人远程访问您的设备或被诱导下载或安装软件。

访问 ANZ 银行安全中心了解最新的诈骗情况，
ANZ.CO.NZ/BANKSAFE

推销电话诈骗

当接到意外来电被要求提供个人信息时，警惕受骗遭受资金损失。

此骗局的常见迹象

诈骗者可能会声称，为了保证您的账户和资金安全，要求您：

- 将钱转移到另一个账户。
- 将个人或银行信息提供给他们，例如信用卡信息或 Visa Secure 代码。
- 对您账户上出现的一笔可疑交易进行验证，或者他们会通知您说有一笔退款。
- 准备好现金、银行卡和密码，以便他们来您家取这些东西。
- 将资金转移到其它新西兰账户或离岸账户，以帮助抓捕黑客或参与欺诈活动的银行工作人员。
- 设立一个加密货币账户或其他类型的账户。

最佳建议

- 如果是陌生来电要求您提供个人信息，马上挂断电话。
- 如果您不确定来电的真实性，可以拨打该机构公布的官方电话号码以便确认。
- 如果您被要求购买预付借记卡、礼品卡、加密货币、iTunes 卡或使用第三方汇款机构，一定要拒绝。

远程访问诈骗

当有人获得您的设备（即智能手机、平板电脑或计算机）的访问权时，他们就可以未经许可使用您的网上银行或 goMoney 应用程序、窃取您的个人信息或保存在该设备上的任何数据，或假冒您。

此骗局的常见迹象

诈骗者会打电话、发短信或发送电子邮件声称：

- 您的互联网连接有问题。
- 您的设备有问题或需要维护。
- 有黑客在攻击您，他们可以帮助阻止黑客攻击。
- 他们发现了未经授权的交易并可以帮助阻止它。诈骗者甚至可能会提供一步步的指示或提出要引导您完成整个操作，包括登录您的网上银行或 goMoney。

最佳建议

- 切勿将您的设备的访问权交给陌生人。
- 切勿将您的网上银行密码或登录信息保存到浏览器中。

网络钓鱼诈骗

这是有人试图诱骗您向他们提供信息或资金，
通常是通过短信或电子邮件。

此骗局的常见迹象

- 点击链接，例如通过点击链接来“支付过路费”。
- 制造紧迫感或压力，要求您迅速采取行动，例如声称“您的账户已被冻结”。
- 拼写和语法都错误迭出，包括打字错误。
- 发件人电子邮件地址不正确，或电子邮件地址看起来有些可疑。
- 短信是从海外电话号码发来的。
- 声称您的账户信息“被盗”、“丢失”，或需要“更新”，要求您“确认”或“验证”账户信息的短信。
- 指向虚假网站的链接，而这些网站看起来像真的一样，以及带有可能会将病毒下载到您的设备上的附件。

最佳建议

- 不要点击陌生的短信或电子邮件中的链接。
- 如果您不确定，请向一位您信任的家庭成员或朋友询问，或者拨打该公司对外公开的电话号码以核实是否为真。

银行卡诈骗

即有人窃取并使用您的银行卡或卡上的信息。请注意，诈骗者不需要实际持有您的银行卡即可进行欺诈交易。

您可能会注意到：

- 收到陌生的电子邮件、短信或陌生来电，要求您提供您的银行卡信息。
- 您的交易记录中显示有发生在您不熟悉的商店或地点的异常或您不记得发生过的交易。

最佳建议

- 时常检查您的账户交易记录以确保每笔交易都是您完成的。
- 使用 goMoney 中的 ANZ Card Tracker 功能查看哪些商家有可能存储了您的银行卡信息。
- 对您的密码保密。切勿将其记在什么地方并确保别人难以猜到。
- 不要提供您的信用卡号、有效期、CVV 码，和/或 Visa Secure 码给那些向您打电话、发送电子邮件、发送信息（包括通过社交媒体）或短信的人。这包括自动语音消息，声称您的账户上出现意外收费或退款。
- 为您所有的银行卡、goMoney 和电话银行设置不同的密码。
- 如果您的卡丢失或被盗，请立即在网上银行或 goMoney 冻结或取消该卡，或致电我们。

在网上银行或 GOMONEY 冻结或取消您的卡。
访问 **ANZ.CO.NZ/GUIDES** 了解如何操作

投资诈骗

通常是您被邀请投资一个虚假的赚钱机会或您正在积极寻求机会投资。

此骗局的常见迹象

有人提供给您一个机会来：

- 购买某个公司的股份。
- 将钱投资于一笔定期存款。
- 投资外汇。
- 投资黄金或其他贵金属。
- 投资房地产。
- 购买加密货币。

诈骗者提供这些机会时通常会敦促您迅速采取行动，以免错过机会。

最佳建议

- 在投资之前，请彻底调查一下该公司、该投资机会，及其背后是什么人。从独立来源寻找信息，包括监管机构、金融分析师和信誉良好的新闻媒体。
- 在做出任何决定之前，先咨询有执照的财务顾问或投资专业人士。
- 请记住，如果某个投资机会听起来好得令人难以置信，那么它可能就是假的。

保护您的资金

如果投资机会来自于以下渠道，请非常谨慎小心：

- 一家未在监管机构注册或未提供清晰透明信息的公司。
- 一个意外接到的电话、社交媒体帖子或社交媒体上聊天交友找对象，并最终索要钱财或请您参与投资的。

如果有人和您联系，声称要帮助您收回之前投资中投出去的资金，请务必警惕。

婚恋和交友诈骗

诈骗者会试图获得您的信任从而骗取钱财。

此骗局的常见迹象

如果您在网上结识的一个人，他们：

- 很快地表达他们对您的钦佩或爱慕。
- 有一个令人心碎的故事或令人信服的借钱理由——通常开始的金额很小。
- 总是有各种借口告诉您他们为什么不能与您亲自见面。
- 声称是在海外工作。
- 如果您进行视频通话，他们会将相机关闭或者您只能看到模糊的图像。

最佳建议

- 任何人都可能会遇到婚恋骗局，因此在网上与人交往时要小心谨慎。
- 如果在网上认识的人或对象向您提出的请求令您感到不安或不知道该怎么办，请找您信赖的家人或朋友商量。

防范建议总结

您可以将这份防范建议贴在冰箱上或电脑旁。

建议一

询问您信赖的家庭成员或朋友的意见

建议二

如果陌生来电要您提供个人信息，马上挂断电话

建议三

切勿点击陌生的短信或电子邮件中的链接

建议四

切勿将您的设备的访问权交给陌生人

建议五

约定好一个秘密的家庭密码来核查这是否真的是您的亲人

建议六

不要迫于压力而仓促做决定

建议七

使用独一无二的密码 来保护您的银行信息和设备。切勿将您的客户号码、密码保存到您的浏览器或设备中。

建议八

如果对方要求提供个人信息或资金，可通过拨打该公司的官方电话来验证真伪

建议九

使用额外的银行安全措施，例如 ANZ OnlineCode 或语音 ID

建议十

定期检查您的交易记录

您是否遭遇过诈骗，或者想了解有关诈骗的更多信息以及如何保护您的资金？

访问 anz.co.nz/banksafe

致电 0800 269 296　前往任何分行