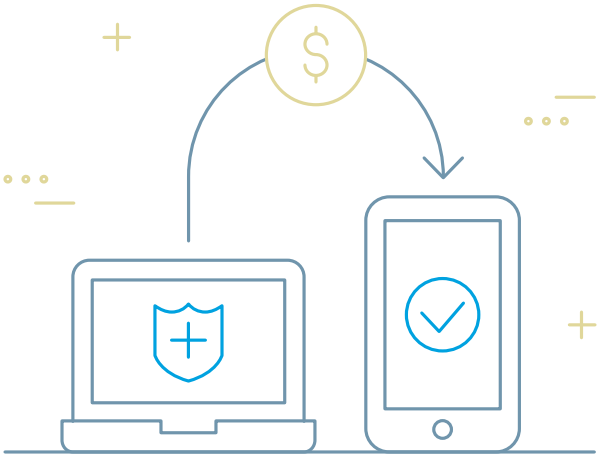
ANZ银行业务安全指南

我们致力于保护您和您银行业务的安全，而您也要尽到您的职责。在我们的共同努力下，我们会让您更安全。本指南会告诉您我们已经采取了哪些安全措施、有哪些可以让您自己和您的银行业务保持安全的小提示，以及要注意的诈骗类型。把它打印出来，放在一个您可以随时看到以作参考的地方，比如放在冰箱上、家里的电话旁边，或者办公室里。如果您认为您的朋友或家庭成员会受益于此信息，请与他们分享。

去哪里寻求建议和帮助

- **cert.govt.nz** – 新西兰致力于提高网络安全的政府机构。
- **police.govt.nz**
- **netsafe.org.nz** – 提供实用工具、支持和建议，确保在线安全。

如需任何帮助，请拨打**0800 269 296**，或者登录**www.anz.co.nz/banksafe**，查找更多有帮助的信息。



办理银行业务的方式

我们为您提供多种方式来办理日常银行业务。

除了前往分行或致电我们的客户服务中心，您还可以在方便的时间和地点使用电话或电脑办理银行业务。

这些选择具有灵活性，也是办理银行业务非常安全的方式。每种方式都可以用来查看账户余额和转账历史、在账户之间转账以及向其他人或企业付款(例如：支付账单)。

- **ANZ网上银行业务**
  通过一个安全的、用密码加以保护的互联网站点随时随地访问您的银行账户。
- **ANZ goMoney手机应用程序**
  将我们的手机银行应用程序下载到您的iPhone、iPad或Android设备，在PIN(个人身份识别码)、您的指纹或Face ID的保护下，您可以随时访问您的所有银行账户。
- **ANZ电话银行业务**
  使用您专属的客户编号和安全的个人身份识别码(PIN)，或者注册可以为您提供额外安全保护的语音ID，这样您可以通过电话访问您的银行账户。

银行与安全措施

我们采取一系列的安全措施来帮助保护您的个人信息：

- **线上转账码**可在您通过网上银行业务和goMoney软件进行某些转账时为您提供额外的保护。设置完此验证码后，我们将向您发送一条短信，其中包含一个用来在进行某些转账前输入的唯一验证码。
- **VISA身份验证服务**有助于防止未经授权在线使用您的信用卡。多数情况下，该验证服务都可以自动完成，但有些时候可能会向您的手机发送一个唯一的验证码，您需要输入此验证码来继续您的转账。
- **语音ID**使您能够登录到ANZ电话银行业务，或者通过我们的客户服务中心使用您自己独特且安全的声纹验证您的身份。
- **诈骗监控系统**使我们能够识别您账户上潜在的诈骗活动。如果我们怀疑有诈骗行为，我们会联系您，并且可能会暂停您的银行业务或阻止您的银行卡业务，以防止进一步的诈骗转账的发生。

切记，ANZ从不通过电话或电子邮件询问您的密码、PIN或安全码。我们也不会要求远程访问您的电脑或电话或留下预先录制好的带有说明的信息。
请不要将您的密码、PIN或安全码告诉任何人，甚至ANZ员工或警方。

ANZ Bank New Zealand Limited 06/21 21799

安全办理银行业务提示

以下提示将有助于确保您和您的银行业务安全。

网上银行业务

- 通过输入完整的地址(例如: anz.co.nz)访问网上银行，而不要点击您在电子邮件中收到的链接。ANZ银行不会向您发送要求您点击其中的链接来登录到您的网上银行的电子邮件。
- 如果您怀疑您的密码被泄露，请拨打**0800 269 296**联系我们，我们可以帮助您快速安全地更改密码。
- 确保您所有软件和应用程序均为最新版本。同时，确保您安装了最新的防病毒软件。
- 确保您注册获取线上转账验证码，它是我们的双重身份验证手段，以便您在线办理银行业务时得到第二重保护。
- 切勿将您的客户编号、密码或PIN保存在您的浏览器或设备上。
- 切勿向任何人泄露您的密码、PIN或安全验证码，即使这些人声称是银行工作人员或警方。

手机银行业务

- 对您的PIN保密，使它不易被猜到，并且切勿将同一PIN用于其它方面。
- 不使用时将手机锁屏，完成操作后始终从ANZ银行goMoney登出。
- 将软件、操作系统和应用程序设置为自动更新，以确保获得最新安全功能。
- 切勿下载不熟悉的应用程序，或者让任何人远程访问您的设备。

电话银行业务

- 对您的PIN保密 – 确保您的PIN不易被猜到，切勿将其写下来和透露给任何人。
- 如果使用语音ID – 切勿录制语音识别短语，或者让其他人用您的客户编号录制他们的声纹。
- 不要使用与您的银行卡、goMoney或与其它公司身份验证相同的PIN。

保护您的个人信息

- 将您的个人详细信息，如法律文件和银行对账单，放在安全的地方。像对待您的钱财一样对待这些详细信息 – 不要把它们泄露出去!
- 确保您的所有设备均通过PIN、密码或者FaceID或TouchID之类的生物识别功能加以保护，以便即使设备丢失，您的信息也始终得到保护。
- 切勿在您的浏览器中保存您的客户编号或网上银行密码或PIN。
- 如果您发现任何可疑的事情，请立即查看对账单并立即致电银行。
- 在扔掉上面有您个人信息的文件之前，先将其销毁(能撕毁切碎最好)。
- 您的个人信息非常有价值，可用于实施诈骗。无论是在网上，还是在电话中，提供您的信息时都要小心谨慎。

使用您的银行卡

- 收到您的银行卡后，一定要用墨水笔在背面签名。
- 您所有的银行卡都要使用不同的PIN，不要让其他人轻易能够猜出它(如您的出生日期)。记住您的PIN(切勿写下来)，并定期更改。
- 即便有人声称是您的开户行的工作人员或警方，也要将您的PIN保密。
- 将您的银行卡放在安全的地方，不要让其他人使用。不要让它离开您的视线，例如在餐馆中。
- 在ATM或EFTPOS机上输入您的PIN时，要用手遮挡。

ANZ Bank New Zealand Limited 06/21 21799

自己要时刻保持警惕，了解都有哪些骗局并及时发现危险信号

任何人，包括您，都可能成为骗局的受害者。那是因为骗子不会区别对待，而是会以任何性别、年龄段或社会经济背景的人为下手目标。重要的是您要熟悉可能以您为目标的诈骗手法。

了解有哪些骗局

- 技术支持/远程访问电话诈骗
- 抓捕黑客骗局
- 爱情骗局
- 投资骗局
- 虚假慈善机构
- 虚假的就业机会
- 恐吓及勒索诈骗
- 彩票诈骗
- 意想不到的快速致富计划
- 未偿债务诈骗
- 电话诈骗
- 政府补助金诈骗
- 商业电邮欺诈/发票诈骗

发现危险信号

- 您是否认识您要向其汇款的人?
- 您是否曾被要求下载软件来远程访问您的电脑或移动设备?
- 您是否曾被要求以第三方的名义收发资金?
- 您是否接到过要求您汇款的电话?
- 您是否被要求提供过多的个人信息，或者来电方应该已经知道的信息?
- 您是否被告之必须马上行动或者对此事保密?

您是否收到过不同寻常的请求?

骗子试图使用无法追踪的付款，如先存款后使用的借记卡、礼品卡、比特币、iTunes卡或转账系统。他们可能会要求您将资金转账到新西兰或离岸账户，以协助调查或"抓捕黑客/诈骗犯"。

您是否曾被要求下载远程访问软件?

不要让任何突然给您打电话的人说服您安装软件以便访问您的电脑或移动设备，即使这些人声称是警方、您的电话公司或银行的工作人员。立即挂断，然后用其公开的电话号码给该公司回电话核实其合法性。

您是否核实了您的付款详细信息?

确保您核实了有关付款说明的所有更改，尤其是通过电邮收到的此类相关变动。通过公开的详细联系信息与相关机构取得联系，使您能够确认相关更改是真实的，而不是诈骗犯截获通信内容的结果。

三思而后行

- 您了解您汇款的原因吗?
- 您收到此次付款或汇款的发票了吗?
- 您为何要向新西兰境外的国家汇款?
- 他们说的话听起来像真的吗?

自己要时刻保持警惕，了解都有哪些骗局并及时发现危险信号

有人需要您的紧急经济援助吗?

骗子会充分利用人们寻找浪漫伴侣的心理，试图以此让他们提供金钱、礼物或个人详细信息。

他们可能会使用假名或者冒充真实可信的人的身份，并且经常声称来自新西兰但在海外工作。向您不熟悉或未见过面的人汇款前要三思而后行。

好得令人难以置信?

您应该自己进行合理的查询，并在网上查询某个财务顾问是否是注册财务顾问 – 如果不是，请不要和他们打交道。在网上搜索公司名称通常可以很快知道这是否是一场诈财骗局。

在向不请自来的来电者提供详细信息或者回复提供财务建议或紧急投资机会的电邮之前，请确保进行了充分的核实。

注意网络钓鱼技俩

诈骗犯惯用的伎俩是冒充银行或其他声誉良好的机构的工作人员，妄图窃取您的个人信息或获得您的银行账户的访问权限。

网络钓鱼攻击的可能方式:

- 电邮
- 短信(有时称作“短信诈骗”)
- 电话。

需要警惕的事情:

- 被要求点击下载恶意软件的附件。
- 被要求提供您的个人信息，如安全详细信息、信用卡详细信息、密码、PIN或安全验证码。
- 被要求点击链接以访问您的网上银行。
- 被要求下载允许远程访问您的设备的软件。

如何保护自己不受骗子的伤害

对意想不到的电话要非常小心

不要让从未谋面的来电人远程访问您的手机或电脑。分享个人信息时要小心，并且如果您不确定，就先挂断，然后再按公开的电话回电该机构进行核实。务必向电话公司和银行举报诈骗电话。

点击电邮和短信中的链接或附件要小心。

将鼠标悬停在链接上看看它指向哪个网站，如果有疑虑，就不要点击。在手机设备上，您可以按住链接，它所指向的网址将弹出来，可以先查看一下。

只在您信任的网站上购物

当心您和您认识的其他人从未听说过或使用过的网站。切勿将电脑设置为自动保存密码或其他个人信息。

始终直接输入URL(网址)

访问购物网站或登录到您的网上银行时，直接输入URL。这样，您会知道您在正确的网站上，而不是一个“假”网站。

迅速行动

如果您认为下载了可疑的附件或者点击了以ANZ名义的电邮或短信中的链接，请立即联系ANZ。

ANZ Bank New Zealand Limited 06/21 21799