Australian Banking Association

保证你自己的安全：
警惕诈骗

以新冠病毒疫情为由的诈骗活动有可能在未来数月里越来越多。

诈骗犯用虚假的电子邮件、电话或短信试图窃取个人资料。他们假装来自你的银行、世界卫生组织、政府部门、慈善机构或合法的商业机构，比如旅行社、供电公司、电话或网络公司、或你本地的超市。

保护你自己

你的银行永远不会发电子邮件或短信询问任何账户或财务细节，包括更新你的住址或电话/手机/网上银行的登录细节。

政府部门及其它合法机构永远不会要你点击一个链接来更新资料。如果可疑，请教朋友或家人，或直接联系相关机构进行询问。

如果陌生人给你打电话索要个人资料，马上挂电话。直接给有关公司打电话，问他们是否给你打过电话。

永远不要打开陌生人或机构发的附件。永远要警惕听起来好得难以置信的提议或索要太多资料的提议。

银行会给予帮助，以下情况应马上联络银行：

- 你在接诈骗电话、回复诈骗电子邮件或短信时透露了你的银行资料
- 你不小心点击了任何链接或下载了任何附件
- 你注意到账户里出现不寻常交易。

如何识别诈骗

- 叫你更新或确认个人资料，包括地址、出生日期、银行账户资料、税号、个人识别号或密码。
- 电子邮件或短信包含可疑链接。如果你不确定，请朋友或家人帮忙。
- 叫你马上付钱或付押金。
- 如果一种提议听起来好得难以置信，那很可能就是假的。
- 电子邮件地址与公司名称不吻合。
- 打电话的人要求远程进入你电脑。

Australian Banking Association

www.ausbanking.org.au

保护财务资料不被骗取的重要提示

- 挂掉可疑电话，代之去公司网站或找出他们的电话号码，直接给他们打电话。
- 永远不要把密码或个人识别号告诉别人。用密码保护你的设备。如果你和别人共用一台电脑，永远不要保存密码，永远要记得退出你的账户。
- 定期检查你的银行账户，以便及时发现可疑交易。
- 避免在购物时刷卡。轻敲或插入卡片通常更安全。
- 取消信用卡提现功能。
- 请教银行保护你账户的最好方法。
- 如果你认为受到诈骗，马上向银行报告。

骗子有很多行窃方法，主要包括：

Phishing（网络钓鱼）– 假装来自一个可信渠道（比如银行、慈善机构或政府部门），用电子邮件或短信窃取你的个人资料。讯息看上去像真的，通常叫你在假网站上输入个人资料或叫你点击一个链接 – 这会让骗子进入你的电脑窃取你的个人资料。

网上购物诈骗 – 诈骗犯装成真实的网店，要么通过一个假网站、要么通过一个真的零售网站上的一条假广告。假的网店网址通常会要求异常付款方式，比如要求通过汇票、电汇、国际转账或礼品卡立即付款。

投资诈骗 – 诈骗犯自称是股票经纪人或投资经理，提供财务或投资咨询服务。他们会叫你交钱投资一个可能是真的、也可能是假的项目，然后骗走你的钱。

远程登录诈骗 – 诈骗犯谎称你的电脑或网路连接有问题或感染了恶意软件。他们会试图说服你安装一种应用软件或让他们进入你的电脑。然后他们会窃取你的个人资料或要求你“付费”解决问题。

交友约会诈骗 – 诈骗犯与你形成某种关系，勒索钱财。他们长期与你发展关系，然后会叫你把财产转到他们名下或要求成为你遗嘱的受益人。他们还经常问你要钱，以解决某种健康、旅行或家庭问题。

有用链接：

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/