诈骗人员会利用掌握的技术和编造的故事不断改变他们的诈骗手段。他们的目的是骗取您的财物或个人信息。所有人都有可能遭遇诈骗，因此保护自己的最佳方式是时刻保持警惕。

请继续阅读本手册，了解辨别诈骗的实用技巧。

Spark nz

举报

scamhelp@spark.co.nz

0800 168 168 (星期一 - 星期五：8.30am – 6pm，法定假日除外)

如果收到诈骗短信，请将该短信转发至 **7726**，从而向新西兰内务部 **(Department of Internal Affairs)** 举报

通过 **netsafe.org.nz/report** 向新西兰网络安全公司Netsafe举报

如需了解诈骗的更多信息和示例，请访问 **spark.co.nz/scams**

SPA4227

Spark nz | netsafe
netsafe.org.nz

保护自我 谨防电信诈骗

辨别诈骗

- 诈骗人员可以通过他们所选的号码 (如新西兰本地号码) 掩盖真实来电者的ID。这种手段称为号码欺诈—— 电话其实是从海外打来，但诈骗人员想要通过隐藏海外电话ID，以显得更真实可信。
- 诈骗人员可能会声称他们发现您的调制解调器/电脑存在问题，并提出可以通过远程访问控制您家里的电脑。如果您最近真的遇到一些技术问题，这可能就更有说服力了。
- 他们可能知道您的全名、地址和出生日期。这些信息可以通过在线搜索找到或从黑市上买到，因此不应凭这些细节便认为他们是真实合法的。
- 诈骗人员可能是从国际电话中心来电，周围有很多工作人员——通常环境非常嘈杂。
- 一些诈骗电话可能会在响铃之后，您接听之前挂断。这些电话通常来自海外号码。这类诈骗称为“一响即挂 (Wangiri)”诈骗。目的是让您回电，以便他们收取高额的通话费。
- 告知您中奖了，可领取奖品或奖金，但其实您并没有参加过该活动。

如何保障安全

- 请注意您提供个人信息的地方和对象。
- 确保您的软件和杀毒程序实时更新。
- 所有在线账户都使用不同的密码。
- 经常更改密码，不要重复使用旧密码。
- 在线账户尽可能采用双重验证 (2FA)。
- 如果您无法判断来电者是否真的是与您有业务往来的公司，请挂断电话，然后直接按照电话簿或其官网所列的电话号码致电该公司。
- 如果您收到陌生号码的未接来电，请忽略此号码，不要回拨。这可能是一个专门引诱您回电，然后收取高额通话费的诈骗手段。
- 请对陌生联系人保持警惕，即便他们来自合法组织。
- 请访问 **spark.co.nz/scams**，以了解辨别诈骗的最新技巧。

认为自己已经受骗

- 如果您已按照他们的要求在电脑 (或其他设备) 上执行了任何操作，请立即让电脑断网。
- 如果您已提供银行或信用卡的详细信息，请立即联系您的银行。
- 更改所有设备的在线帐户密码，如果您已授权他们访问您的电脑，请向电脑服务公司求助。
- 向您的电信运营商和新西兰网络安全公司Netsafe举报这一诈骗行为。
- 将诈骗的详情告知您的亲朋好友，以便他们也留意警惕。
- 访问 **spark.co.nz/scams**，了解最新的诈骗信息 。