其他常见的诈骗攻击方式

语音钓鱼和电话诈骗

电话诈骗，或称语音钓鱼，是指诈骗者假冒成您的银行或其他可信任的机构来进行电话诈骗。以现时的人工智能技术(例如:深度伪造技术)，骗徒能从图像撷取你的容貌伪造成影片。此外，深度伪造技术还可透过声音模仿，只需撷取你五秒钟的对话，骗徒便能使用此技术模拟你的声音来创造不同的对话。因此，骗徒可以借助深度伪造影像和声音制作出根本不存在的影片。骗徒甚至可能让来电显示成您认识且信任的号码或伪冒您的认识的声音以要求将资金转移到另一个账户。此被称为改号欺诈，其对话内容听起来可能非常真实可信，诈骗者甚至可能已经掌握了一些有关您的个人资讯，如账户号码或地址。如果您觉得有任何不妥，或察觉有异，请不要犹疑，立即挂断电话。您可以反过来致电您所知的机构电话号码，例如您银行卡背面的电话号码，以核实来电的真伪。

但请留意，骗徒可能继续保持通话线路连通，甚至伪造拨号的音效，让您误以为真。因此，请使用另一部手机，或相隔至少30秒后才致电。
常见的例子包括：

- 「您的银行」通知您的账户出现风险，需要将您的资金转移到另一个账户，以确保安全。
- 「您的银行」需要您的协助来调查诈欺事件。
- 您的网络或电讯供应商致电给您，替您解决您从没有报告过的问题。

银行可以根据您的要求转账，但绝不会因此索取您的密码、PIN码、任何一次性密码或安全代码。