Hong Leong Bank

DUITSMART

A Better Future for all Malaysians

普遍的  金融诈骗

我们大多数人在新闻或社交媒体上都遇到过金融诈骗案

但是你真的知道多少呢?

这里提供一个迷你指南

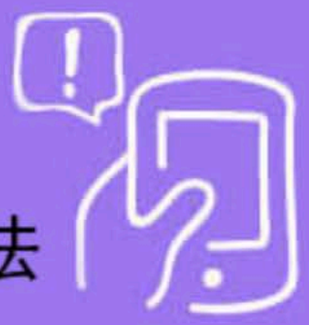
采用最新策略，以帮助您做好准备并保护自己。

澳门骗局法

重要迹象

- 您接到某人的电话，该人声称自己是银行/警察/其他机构的管理人员
- 呼叫者有“证据”表明您实施了犯罪例如，洗黑钱，毒品贩运，交通事故逃逸等。
- 要求您对调查保密，不要告知银行或其他人，包括您的家人。
- 指示您将钱存入当局以调查非法交易，并确保在案子结清后将退还所有资金。
- 如果您不配合，则有可能冻结您的帐户，逮捕或对您提起诉讼。

TAC骗局法



重要迹象

- 您收到某人的电话，该人声称其 TAC 短信被错误地发送给您的电话号码。
- 来电者听起来可能很有礼貌或表示非常抱歉，并要求您提供收到的 TAC 代码以完成紧急交易。
- 作为借口，来电者可能声称最近因为切换了手机号码，或者他们的家人错误地使用了错误的号码而照成TA短信错误发送的意外。
- 并向您保证交易完成后会对其错误发送讯息进行改正。

网络钓鱼诈骗法

重要迹象

- 您收到声称来自您的银行/其他机构的 SMS /电子邮件。
- 消息指示您单击打开假网站的链接。
- 并要求您更新您的个人信息或银行/在线登录详细信息。
- 如果您未按照指示，则有可能威胁到您的银行户口被关闭或冻结。

请记住

- 指示您将钱存入当局以调查非法交易，并确保在案子结清后将退还所有资金。
- 如果系统告知您您的银行帐户与犯罪有关，请直接到银行进行确认。
- 您应该时刻保持警惕，即使来电者的电话号码显示正确，或是来电者向您保证会提供交易"收据"。

请记住

- TAC 只会发送到在与您的银行帐户链接并注册的手机号码，因此不会有“错误”发送的机会。请切勿与任何人分享您的 TAC。

请记住

- 银行绝不会通过短信，短信应用程序，电子邮件或社交媒体要求个人/银行信息或确认详细信息。
- 当您单击从未经请求的 SMS/电子邮件收到的链接时，请当心。
- 在浏览器中输入网上银行的网址 (www.hongleongconnect.my) 以进入银行的官方平台，并且确保仅在看到注册过程中选择的安全图片后才输入密码/登录。

维持良好的 安全习惯

切勿与任何人共享您的网上银行登录详细信息(即用户名和密码)或 TAC，即使要求此类信息的一方声称来自银行，马来西亚国家银行或其他当局，也切勿分享。

创建一个结合字母，数字和符号的强大在线银行密码，并定期进行更改。

及时检查您的交易警报，并定期审查帐户余额和对帐单。

如果您发现未经授权的交易或差异，请立即将其报告给您的银行。

如果您想了解更多使用 DuitSmart 的方法并获得更好的财务状况，请浏览 www.hlb.com.my/duitsmart