DIGITAL FOR LIFE

保持安全上网

4 种常见骗局

与银行相关的网络钓鱼诈骗

- 骗子冒充银行职员；
- 询问您的网上银行用户名、个人密码（PIN）和一次性密码（OTP）。

诈骗信息示例：

您的“银行”户头交易
已被暂停，请在 12 月 28 日
更新，否则您的帐户将被冻结。
请浏览 **bit.ly/abc123**

贷款骗局

- 骗子假装是持牌放债公司的职员；
- 一般通过短信或 WhatsApp 发送借贷服务信息。

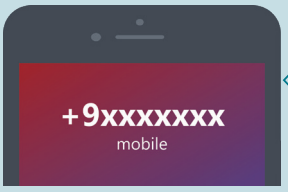
诈骗信息示例：

促销！每月只需分期还款：
8.88-10.88% (公司)
6.88-8.88% (个人)
5000 到 30 万新元贷款，长达 60个月
无隐藏费用
发送短信/WSAPP 信息到 xxx1231

社交媒体假冒骗局

- 骗子冒充您的家人，朋友；政府或企业的科技支援。
- 他们会：
  - 询问您的个人信息，或
  - 让您下载能让他们控制您的设备和信息的软件，或
  - 在接下来的 24 小时内，请您不要查看您的手机简讯、电邮或银行账号。

带有‘+’符号前缀的诈骗电话示例：



你好，我是 XX 公司的
技术支持人员，您的电脑已经通知我们它已经**感染了病毒和间谍软件**。
请**立即下载本软件**，
以免您的电脑在**未来5分钟内**被锁上。

电子商务骗局

- 骗子以低价吸引您；
- 要求您预先付款或要求您提前付款。

诈骗信息示例：

我已为您的商品付款，但这笔钱**已锁定在您的帐户中**。您需要**打开**我发送给您的**电子邮件**来**收款**。

网络钓鱼是网络犯罪分子用欺诈手段诱骗受害者泄露其个人资料和财务信息的一种方法，例如密码、一次性密码（OTP）或银行帐号。

了解网络钓鱼的 6 个迹象：

1. 

使用紧急或威胁性语言

2. 

承诺诱人的奖励

3. 

要求提供私密信息

4. 

错配和误导性信息

5. 
收到出乎意料的电子邮件

6. 
可疑的附件

https://go.gov.sg/csa-spotssignsofphishing

免受网络诈骗的自我保护注意事项

1. 在可行的情况下，启用双重身份验证（2FA）。不仅在网上银行，2FA 还适用于社交媒体、电邮、购物和政府服务等帐户。
2. 请随时拨打政府/企业官方热线或官方应用程序/网站，核实可疑的来电或留言。
3. 如果发现来自您的家人或朋友的信息很可疑，请使用可靠的联系方式直接联络他们，以确认他们是否发送了该信息。
4. 使用大写和小写的字母、数字和符号设置强密码。使用与记忆相关的单词构成短语例 **IhadKAYAtoastAT8AM!**
5. 从 Apple App Store 下载并安 ScamShield 应用程序。*(安卓系统很快就会出现)*。
https://go.gov.sg/scamshield-setupguide

可在 **www.gov.sg/trusted-sites** 找到可信赖的政府相关网站列表。

请浏览 **www.scamalert.sg** 了解更多信息，或拨打防诈骗咨询热线 **1800-722-6688**，以获取预防诈骗的相关建议。

1. **不要**在收到自称来自政府或合法企业的邮件或电邮时，立即点击其中的链接。
2. **绝对不要**分享您的个人或财务信息、密码和一次性密码给他人。
3. **不要**通过电子邮件或短信中提供的联系方式直接联络发件人，先查看官方网站上列出的联系方式进行联络。
4. 当您收到来路不明的紧急广告或信息并要求您遵循某些指示时，**不要**惊慌。删除和屏蔽该用户，并在平台上举报该信息。

鸣谢： *Singapore Police Force and Cyber Security Agency of Singapore*

An initiative by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Supported by:

SG :DIGITAL OFFICE