安全使用网络　避免憾事发生

网络钓鱼和网上诈骗的类型

1 冒充骗局

犯罪分子会冒充是政府部门、银行或电信公司等信誉良好机构的职员，试图通过电话、WhatsApp或短信骗取钱财。

他们会要求您：

- 遵照紧急指示以解决问题。谎称您的电子设备感染病毒、遭入侵或有技术上的问题
- 提供个人资料、网络银行的资料或一次性密码来解决您银行账户的问题或诱导您加入虚假不实的优惠、折扣或抽奖

来自XYZ银行：
我们侦测到您的账户有可疑的活动，请点击以下链接以确认这是您的电子设备：XYZ-bank.-com/sg/online-banking/?6512345678

他们也可能冒充您的朋友、同事或家人，并在社交媒体账号上或通过WhatsApp与您联系。他们会谎称您已中奖，或者他们正在为您报名参加幸运抽奖，并要求您：

- 提供个人资料；或
- 将错误发给您的一次性密码转发给他们

2 电子商务骗局

网络犯罪分子会以诱人的优惠吸引受害人。他们会坚持您立即付款、在交货前通过银行转账或要求在付费平台之外进行交易。在收到您的钱后便失联。

不要成为网络犯罪的受害者，以下是如何防范：

- **不要**透露您的个人或财务资料以及密码或一次性密码
- 当被要求提供您的个人资料时，**不要**直接通过电子邮件或短信中提供的联系方式回复发件人，而是通过官方网站中列出的联系方式来回复
- 除非认识，否则**不要**相信那些自称来自政府但没有“**gov.sg**”的链接或电子邮件地址。可信赖的政府相关网站列表可到**www.gov.sg/trusted-sites**查询
- 当您收到不请自来的紧急广告或简讯，要您遵照某项指示的时候，**不要**惊慌，请打电话给家人或朋友咨询。如要寻求和诈骗相关的咨询，请上网**www.scamalert.sg**或拨打反诈骗热线**1800-722-6688**查询相关资料

什么是网络钓鱼？

网络犯罪分子经常使用一种名为“网络钓鱼“的方法，诱骗受害者提供他们的个人和财务资料，如银行户头号码、登录网站的资料，这包括密码和一次性密码（OTP）。

如何识别6个网络钓鱼的破绽

1

不协调和具误导性的信息

2

没有预料、突如其来的邮件

3

使用语调紧急或带威胁性的字眼

4

可疑的附件

5

承诺诱人奖品

6

索取机密资料

活动:

找找看，破绽在哪里？

您是否看出6个可疑的迹象？

- 语调紧急
- 承诺诱人奖品
- 错别字
- 不存在的新加坡政府部门
- 不协调和具误导性的信息
- 可疑的附件

Better cyber safe than sorry

欲知更多详情，请上网到新加坡网络安全局（CSA）或提防诈骗网页浏览。

www.csa.gov.sg **www.scamalert.sg**

安全贴士请扫描QR码:

更多有关诈骗的最新详情，请扫描QR码: