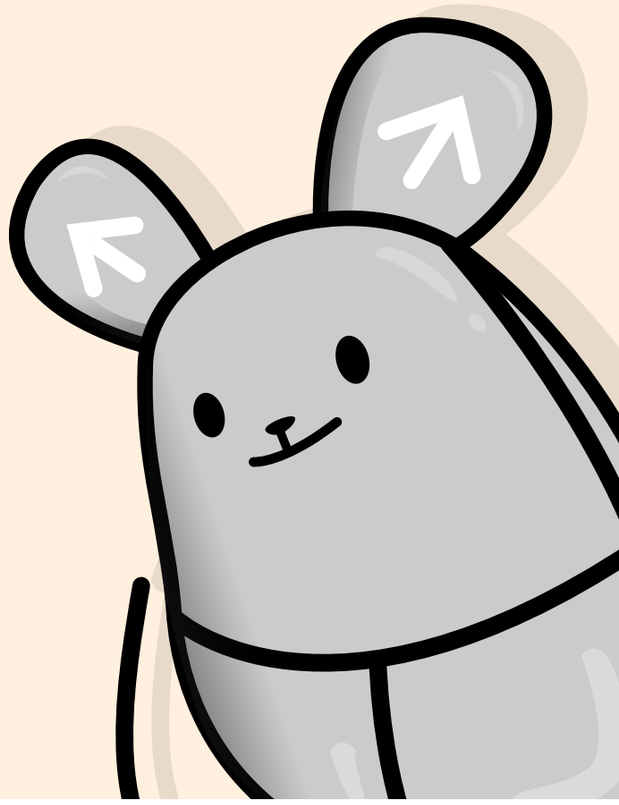
安全上网

保护您的个人资料



个人资料是能够识别个人身份的信息。它包含以下信息：

- 姓名
- 出生日期
- 身份证号码
- 护照号
- 地址
- 电话号码
- 定位数据
- 银行账号和信用卡号码
- 帐户用户名和密码

这些信息会如何被滥用?

网络罪犯可以窃取并利用这些信息犯案，例如：

入侵您的账户

冒名购物

盗用您的身份、
跟踪您或向您勒索

为什么我需要知道这些?

- 在2020年1月至4月间，跟技术支援有关的骗局造成770万元的损失，网络罪犯以解决网络连接问题或调查黑客事件为借口，诱骗受害者安装“软件应用程序”。
- 随后，骗子通过该恶意软件盗取并滥用受害者的个人资料。
- 在其他案例中，受害者被诱导点击包含数码蠕虫或木马的可疑链接，这些蠕虫或木马可以复制、删除或篡改个人资料。

1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

#安全上网

点击之前先检查

支持单位：
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
CSA SINGAPORE

支持：
SG:D | GET READY!

骗子可能会通过哪些途径盗取我的个人资料?

您可以留意以下迹象!

网络钓鱼

- 网络钓鱼是骗子常用的一种诈骗手段，可以诱使您提供个人资料或财务信息，例如登录账号信息、银行户头以及信用卡密码。
- 其形式包括虚假电邮、手机简讯或模仿正规公司的虚假网站。

恶意软件

- 恶意软件是一种可能会破坏您的设备或窃取您的资料的软件。
- 骗子可能会诱使您点击电子邮件或信息中含有恶意软件的的可疑链接或附件。

入侵

- 骗子可能会入侵未加密的无线网络。这样他们就能够查看您的文件或追踪您的线上活动。

1CLICK AWAY
Be Safe · Be Smart · Be Kind

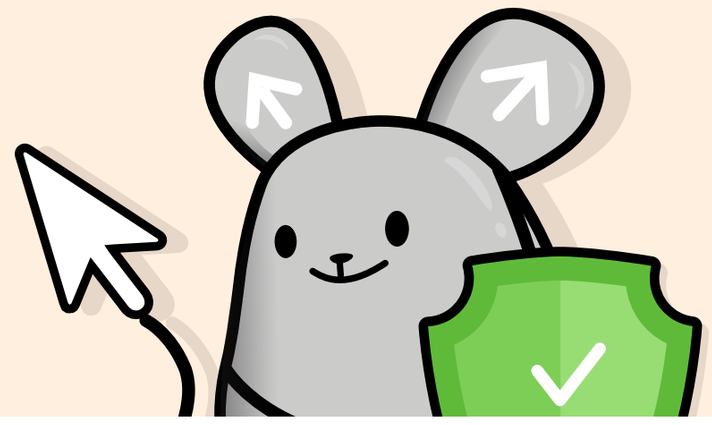
MEDIA LITERACY COUNCIL

点击之前先检查

支持单位:
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
CSA SINGAPORE

支持:
SG:D | GET READY!

我要如何保护我的个人资料?



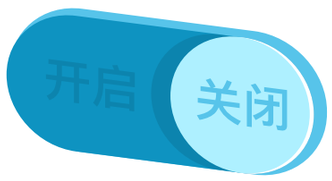
您可以采取以下措施保护自己的个人资料!

- 避免发布联系信息，例如您的家庭住址或电话号码。
- 不要在设备上保存您的银行账户和个人信息。记得在每次完成交易后退出登录。

- 留意陌生人发送的电子邮件或简讯，尤其要注意那些要求您提供个人资料、点击链接或者下载附件的电邮和简讯。
- 骗子经常冒充政府官员或知名企业（例如银行和电信公司）的代表，以取得您的信任。如果您无法确认发送人的真实身份，请不要回复或点击任何链接。

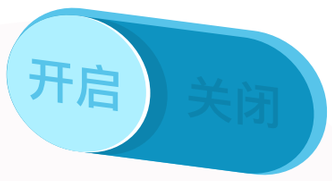
- 在不使用时请关闭设备上的蓝牙，因为黑客可以通过蓝牙找出您设备上的安全漏洞。
- 使用高强度密码，并尽可能开启双重身份验证，以提供额外保护。
- 请勿使用未加密的无线网络进行涉及个人资料或机密资料的交易。
- 及时更新设备上安装的所有软件和应用程序。这样能够修复安全漏洞并安装安全补丁，以防范新的病毒和恶意软件。

蓝牙



加密无线网络

更新软件



1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

点击之前先检查

支持单位：
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
CSA SINGAPORE

支持：
SG:D | GET READY!