报告网络攻击和事件，确保澳大利亚网络安全。

注册

接受我们的免费警报服务：

cyber.gov.au/acsc/register

报告

向REPORTCYBER报告网络犯罪事件：

cyber.gov.au/report

联系方式

拨打1300 CYBER1或

访问cyber.gov.au

关注我们

ACSC Australian Cyber Security Centre

5.警惕网络诈骗

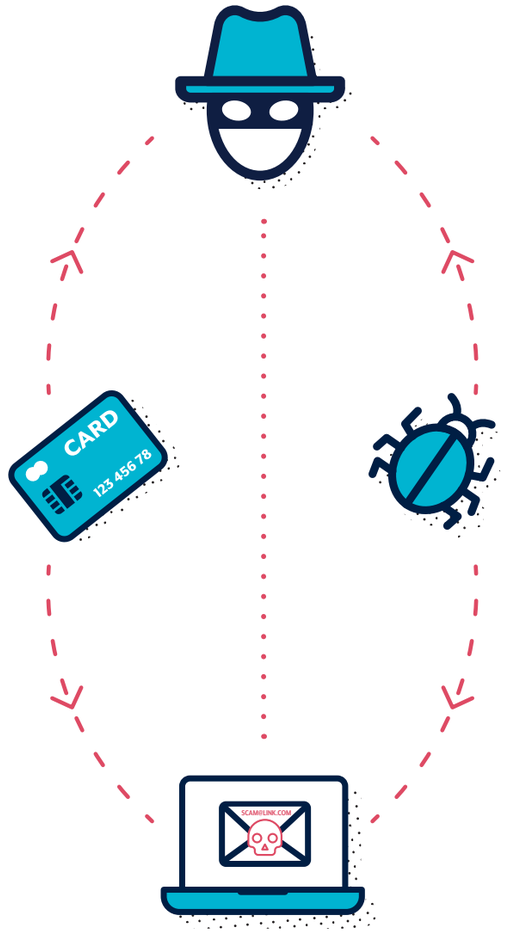
网络犯罪分子通常利用电子邮件、短信、电话和社交媒体，诱导您打开附件、访问网站、透露账户登录信息、泄露敏感信息或转移资金或礼品卡。这些信息伪装成是由您认为您认识或者可以信赖的个人或机构发出的。

如欲识别诈骗信息，请停下来先想一想以下几个问题：

- **权威性：**该信息是否声称由某个官方机构发出？
- **紧迫性：**是否要求您在规定的时间内回复？
- **情绪性：**该信息是否让您感到恐慌、害怕、充满希望或好奇？
- **稀缺性：**该信息是否提供了某种紧缺物品？
- **时事性：**该信息是否与时事新闻报道、重大事件或一年中的某些特定时间（如报税）有关？

如欲核查信息是否来自合法渠道：

- 找到您可以信任的信息来源。访问官方网站，登录您的账户，或拨打他们公示的电话号码。切勿使用您收到的信息或通过电话获得的信息中的任何链接或联系方式。
- 核查官方信息来源是否已经告诉您他们永远不会要求您做的事情。例如，您的开户银行可能已经告诉您，他们永远不会要求您提供密码。



关于识别诈骗信息的更多信息，请参阅澳大利亚网络安全中心（ACSC）出版的《检测社会工程信息》，并通过在**cyber.gov.au**上注册ACSC的警报服务来了解最新情况。

通过简单的几个步骤

便可有效保护您的设备和账户安全

通过以下步骤
减少被网络犯罪分子盯上的风险

ACSC Australian Cyber Security Centre

cyber.gov.au

1.更新您的设备软件

网络犯罪分子常常利用系统或应用程序存在的漏洞入侵设备。更新后的版本均设有安全升级，可以修复这些漏洞。打开自动更新功能，这样无需您手动操作即可完成更新。

在您的所有设备上打开自动更新功能：

- 移动电话
- 笔记本电脑
- 台式电脑

定期检查以下程序或设备是否更新：

- 应用程序
- 程序
- 智能设备

2.激活多重身份验证（MFA）

MFA通过增加网络犯罪分子访问您的文件或账户的难度来提升您的网络安全。

激活MFA，首先从您最重要的帐户开始：

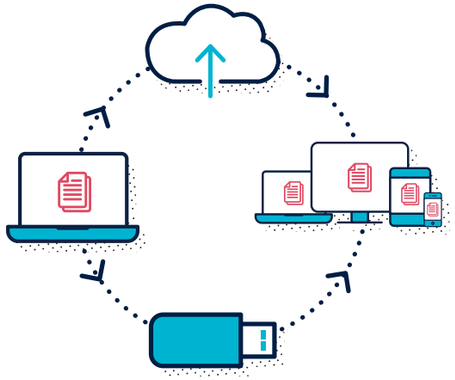
- 电子邮件帐户
- 网上银行和存储有支付信息的账户
- 社交媒体

3.对您的设备进行备份

备份是对存储在您的设备上的信息（如照片、文档、视频和应用程序的数据）进行数字拷贝。可以将拷贝的信息保存到外部存储设备或云端上。备份意味着您可以在设备丢失、被盗或损坏时恢复您的文件。

定期对以下设备进行备份：

- 移动电话
- 笔记本电脑
- 台式电脑
- 平板电脑



4.设置安全性高的强密码

在无法激活MFA的情况下，安全口令往往是保护您的信息和账户免受网络犯罪分子侵害的唯一方法。

密码短语使用四个或以上的随机词作为密码。将您的密码更改为密码短语，确保密码短语：

- 足够长：密码短语越长越好。确保其至少包含14个字符
- 不可预测：使用随机组合的不相关词
- 独特：不要在多个账户中重复使用密码短语