報告網路攻擊和事件，確保澳洲網路安全。

註冊

接受我們的免費警報服務：

cyber.gov.au

報告

向REPORTCYBER報告網路犯罪事件：

cyber.gov.au/report

聯繫方式

撥打1300 CYBER1或

訪問cyber.gov.au

此號碼僅適用於澳洲境內。

關注我們

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5.警惕網路詐騙

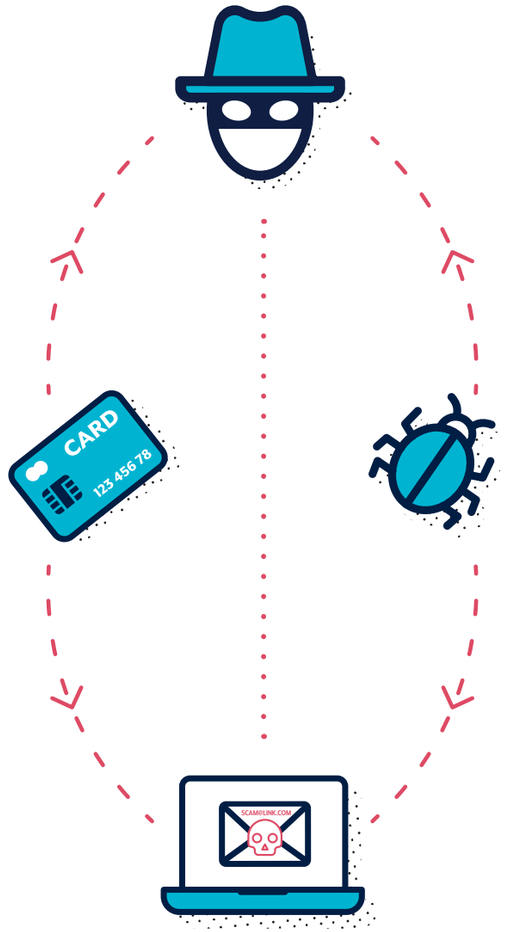
網路犯罪分子通常利用電子郵件、簡訊、電話和社交媒體，誘導您開啟附件、瀏覽網站、透露帳戶登入資訊、洩露敏感資訊或轉移資金或禮品卡。這些詐騙資訊看起來像是由您認為您認識的個人或組織或者您認為您可以信任的個人或組織發出的。

如欲識別詐騙資訊，請停止任何操作並思考以下幾個問題：

- **權威性：**該資訊是否是聲稱由某個官方機構發出？
- **緊迫性：**是否要求您在規定的時間內回覆？
- **情緒性：**該資訊是否讓您感到恐慌、害怕、充滿希望或好奇？
- **稀缺性：**該資訊是否提供了某種緊缺的東西？
- **實時事件性：**該資訊是否與實時的新聞報導、重大事件或一年中的特定事務處理時間（如報稅）有關？

如欲核查一條資訊是否合法，請按以下方法進行操作：

- 找到您可以信任的資訊來源。訪問官方網站，登入您的帳戶，或撥打他們公示的電話號碼。切勿使用簡訊或電話中獲取的連結或聯絡方式。
- 核查官方來源，看他們是否已經說過，某些絕不會問你的事。
  例如，您的開戶銀行可能已經告訴您，他們永遠不會要求您提供密碼。



關於識別詐騙訊息的更多資訊，請參閱澳洲網路安全中心（ACSC）出版的《察覺社會工程訊息》，並透過在**cyber.gov.au**上註冊ACSC的警報服務來瞭解最新情況。

透過簡單的幾個步驟便可有效保護您的設備和帳戶安全

透過以下步驟
減少被網路犯罪分子盯上的風險

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1.更新您的設備

網路犯罪分子常常利用系統或應用程式已知漏洞入侵設備。透過更新設備進行安全升級，修復此類漏洞。開啟自動更新功能，這樣無需您手動操作即可完成更新。

在您的所有設備上開啟自動更新功能：

- 行動電話
- 筆記型電腦
- 桌上型電腦

定期檢查以下程式或設備是否更新：

- 應用程式
- 程式
- 智慧設備

2.開啟多重要素驗證 (MFA)

MFA增加網路犯罪分子存取您檔案或帳戶的難度、提升您的網路安全。

啟動MFA，首先從您最
重要的帳戶開始：

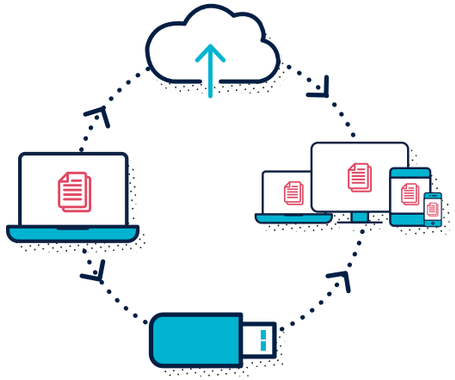
- 電子郵件帳戶
- 線上銀行和存有付款資訊的帳戶
- 社交媒體

3.對您的設備進行備份

備份是對存儲在您的設備上的資訊(如照片、文件、視訊和應用程式的資料)進行數字拷貝。可以將拷貝的資訊保存到外部存儲設備或雲端上。備份意味著您可以在設備丟失、被盜或損壞時恢復您的檔案。

定期對以下設備進行備份：

- 行動電話
- 筆記型電腦
- 桌上型電腦
- 平板電腦



4.設定安全口令

若無MFA，安全口令往往是保護您的資訊和帳戶免受網路犯罪分子侵害的唯一方法。

密碼片語用四個或以上的隨機詞作為密碼。變更您的密碼為密碼片語，密碼片語應該：

- 夠長：密碼片語愈長越好。 至少應由14個字元組成
- 難預測：使用隨機組合的無關詞
- 獨一無二：不要將同一個密碼片語用在多個帳戶