호주를 안전하게 보호할 수 있도록 사이버 공격과 사건을 신고하십시오

등록하십시오

무료 경계 서비스:
cyber.gov.au

신고하십시오

사이버 범죄 신고용 REPORTCYBER:
cyber.gov.au/report

연락처

전화 1300 CYBER1 번 또는 웹사이트
visit cyber.gov.au
이 번호는 호주 내에서만 사용되는 번호입니다.

팔로우하십시오

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. 스캠을 조심하십시오

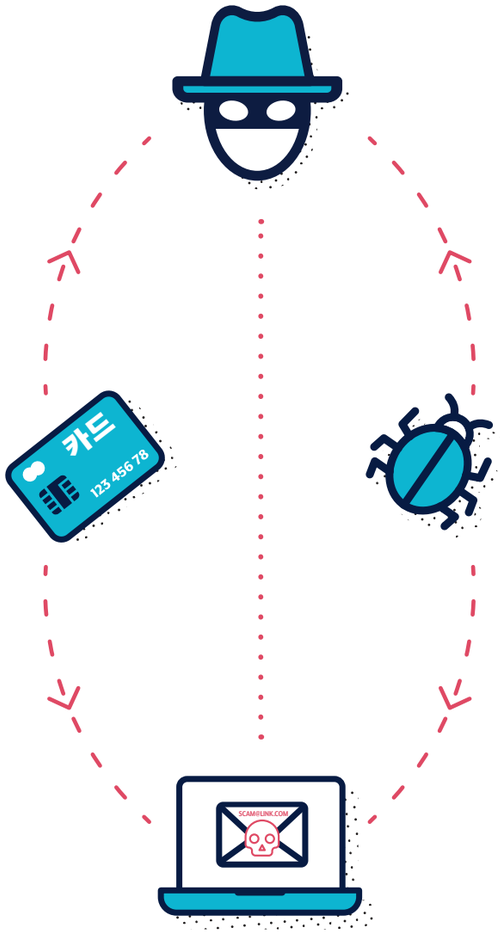
사이버 범죄자들을 이메일, SMS, 전화, 소셜 미디어 등을 이용하여 첨부 파일을 열게 하거나, 웹사이트를 방문하게 하거나, 계정 로그인 정보나 민감한 정보를 공개하게 하거나, 현금 또는 기프트 카드를 이체하도록 속입니다. 이러한 메시지들은 여러분이 잘 알거나 신뢰할 수 있다고 생각하는 개인, 또는 기관에서 발송한 것처럼 보이게 만들어져 있습니다.

스캠 메시지에 속지 않으려면, 잠시 멈추고 다음을 생각하십시오:

- **공신력:** 공적인 위치에 있는 사람이 해당 메시지를 보내는 것이라고 주장하고 있습니까?
- **시급성:** 메시지에 대응할 시간이 제한되어 있다고 말합니까?
- **감정:** 메시지가 공포, 두려움, 희망, 또는 호기심을 자극합니까?
- **희귀성:** 메시지가 뭔가 공급이 부족한 것을 제공하겠다고 제안합니까?
- **시사:** 메시지가 최신 뉴스, 중요 이벤트, 또는 연중 특정 시기(예: 세금 신고 기간)와 관련이 있나요?

메시지의 합법성을 확인하려면:

- 신뢰할 수 있는 곳에서 확인하십시오. 공식 웹사이트를 방문하거나 계정에 로그인하거나 광고에 게재된 전화 번호로 전화해 보십시오. 수신 메시지나 전화 상으로 받은 링크나 연락처를 이용하지 마십시오.
- 공식적인 기관에서는 결코 요구하지 않는 사항들을 물어보는지 확인하십시오. 예를 들면, 거래 은행에서는 고객의 비밀번호를 결코 물어보지 않는다고 고지했을 수 있습니다.



스캠 메시지 색출 관련 상세 정보가 필요한 경우, 호주 사이버 보안 센터(ACSC)의 SNS 조작 유포 감지법을 참고하시고, ACSC 웹사이트 경계 서비스에 등록하시기 바랍니다: **cyber.gov.au.**

기기와 계정 보호를 위한 간편 조치

다음 조치를 통해 사이버 범죄 대상 위험을 줄이십시오

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. 기기를 업데이트한다

사이버 범죄자들은 시스템이나 앱 상의 알려진 취약점들을 이용, 해킹을 시도합니다. 기기 업데이트에는 이러한 약점들을 해결하는 보안 업그레이드가 포함되어 있습니다. 자동 업데이트 기능을 켜 두면 자동으로 업데이트가 실행됩니다.

본인이 사용하는 모든 기기에 자동 업데이트 기능을 켜 두십시오:

- 휴대전화
- 랩탑
- 데스크탑

다음에 대한 업데이트 기능을 주기적으로 확인하십시오:

- 앱
- 프로그램
- 스마트 기기

2. 다중인증(MFA)을 활성화하세요

MFA는 사이버 범죄자들이 파일이나 계정에 접근하는 것을 어렵게 만들어 보안성을 개선합니다.

가장 중요한 계정부터 MFA를 활성화시키십시오:

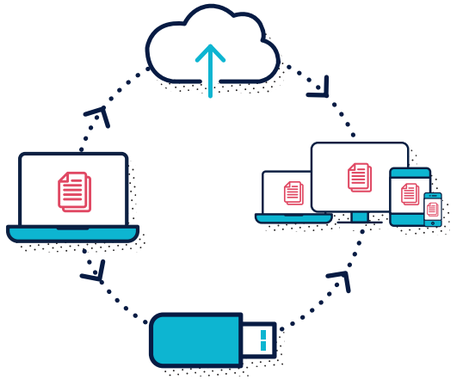
- 이메일 계정
- 지급 상세 정보가 저장된 온라인 은행 거래 및 계좌
- 소셜 미디어

3. 기기 백업을 해 둔다

백업이란 사진, 문서, 비디오, 앱 데이터와 같이 기기에 저장된 정보를 디지털 형식으로 복사해 두는 것을 말합니다. 외부 저장 기기나 클라우드에 저장할 수도 있습니다. 백업을 해 두면 기기를 분실하거나 도난, 손실을 입은 경우에도 파일들을 재생할 수 있습니다.

기기를 주기적으로 백업하십시오:

- 휴대전화
- 랩탑
- 데스크탑
- 태블릿



4. 구절형 암호를 설정한다

MFA를 이용할 수 없는 경우, 안전한 구절형 암호가 범죄자들로부터 정보와 계정을 보호할 수 있는 유일한 도구가 되는 경우가 종종 있습니다.

구절형 암호는 4개 이상의 단어를 무작위로 선택하여 비밀번호로 쓰는 것입니다. 비밀번호를 구절형 암호로 바꿀 때 다음에 유의하십시오:

- 길게 만든다: 문구가 길면 길수록 더 좋습니다. 적어도 14자 이상 되도록 하십시오.
- 예측 불가능하게 한다: 관련성이 없는 단어들을 무작위로 이용하십시오.
- 중복 사용하지 않는다: 구절형 암호를 복수의 계정에 반복적으로 사용하지 마십시오.