Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

개인 사이버 보안 첫 단계

cyber.gov.au

개인 사이버 보안 시리즈

개인 사이버 보안 시리즈

'The Personal Cyber Security: First Steps (개인 사이버 보안: 첫 단계)' 지침은 일반 호주인들이 사이버 보안의 기본 사항을 이해하는 데 도움이 되도록 고안된 세 가지 지침 시리즈 중 첫 번째입니다. 흔히 일어나는 사이버 위협으로부터 여러분이 스스로를 보호하기 위해 취할 수 있는 조치에 관해 알아보세요.

첫 단계

다음 단계

발전된 단계

목차

서론 1

자동 업데이트 활성화하기 2

다중인증(MFA) 활성화하기 4

주기적으로 기기 백업하기 5

중요 계정은 암호문구(passphrase)로 보호하기 6

휴대기기 보호하기 7

나의 사이버 보안 사고방식을 발전시키기 8

개요 체크리스트 11

용어 사전 12

서론

개인 사이버 보안이 무엇인가요?

점점 더 기술 중심이 되는 세상에서 우리는 매일 사이버 위협에 취약한 기기와 계정을 사용합니다:

- 여러분의 기기에는 컴퓨터, 휴대전화, 태블릿, 그리고 기타 인터넷에 연결된 기기 등이 포함될 수 있습니다.
- 또한 여러분은 이메일, 은행 업무, 쇼핑, 소셜미디어, 게임 등을 위해 온라인 계정을 사용하실 수 있습니다.

개인 사이버 보안은 여러분이 여러분의 계정 및 기기를 사이버 위협으로부터 보호하기 위해 취할 수 있는 지속적인 조치입니다.

사이버 위협은 무엇인가요?

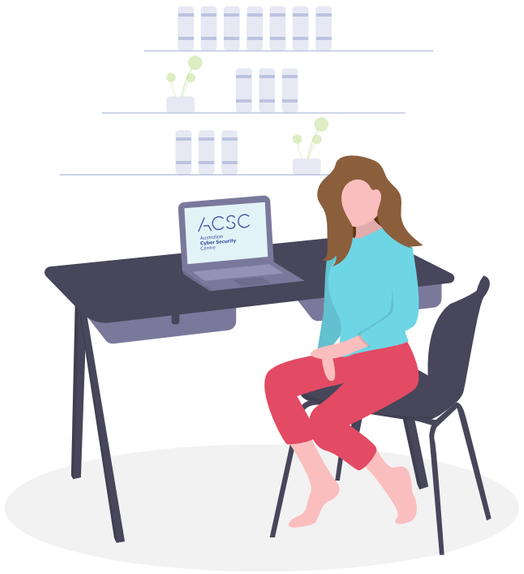
일상적으로 호주인에게 영향을 미치는 주요 사이버 위협은 **사기 및 악성코드입니다**.

- 악성코드는 해를 입히도록 설계된 **악성 소프트웨어를 설명하는 데 사용되는 포괄적인 용어입니다**. 여기에는 바이러스, 웜, 스파이웨어, 트로이 목마 및 랜섬웨어가 포함될 수 있습니다. 사이버 범죄자들은 여러분의 정보 및 금전을 훔치고 여러분의 기기 및 계정을 통제하기 위해 악성코드를 사용합니다.
- **사기는 사이버 범죄자들이 보내는 메시지로**, 여러분이 민감 정보를 제공하게 하거나 여러분의 기기에 악성코드를 활성화하도록 설계되었습니다.

이러한 공격은 피해자들에게 중대한 개인적 및 금전적 영향을 미칠 수 있습니다. 또한 정교함과 빈도가 증가하고 있습니다.

이 지침은 저를 사이버 위협으로부터 어떻게 보호하나요?

사이버 보안에 관해 처음 배우고 있거나 최신 정보를 알아보고 계시다면, 이 지침이 좋은 출발점이 될 것입니다. 'The Personal Cyber Security: First Steps (개인 사이버 보안: 첫 단계)' 지침은 사이버 보안의 기본 사항을 이해하는 데 도움이 되도록 마련된 세 가지 가이드 시리즈 중 첫 번째입니다.



자동 업데이트 활성화하기

업데이트란 무엇인가요?

업데이트는 여러분이 컴퓨터 및 휴대기기에 설치한 소프트웨어(프로그램, 앱 및 운영 시스템)의 개선된 버전입니다.

- 소프트웨어 업데이트는 소프트웨어 '버그(코딩 에러 또는 취약점)'를 고침으로써 **여러분의 기기를 보호하는 데 도움이 됩니다**. 사이버 범죄자 및 악성코드는 이러한 '버그'를 이용해 여러분의 기기에 접근하고 여러분의 개인 정보, 계정, 금융 정보 및 신분을 도용할 수 있습니다.
- **새로운 소프트웨어 '버그'는 계속해서 발견되고 있으며** 사이버 범죄자들에 의해 남용되고 있습니다. 여러분 기기의 소프트웨어 업데이트는 여러분을 사이버 공격으로부터 보호하는 데 도움이 됩니다.

자동 업데이트는 어떻게 설정하나요?

자동 업데이트는 새 업데이트가 제공되는 즉시 설치하는 기본 또는 '설정 후 내버려두기' 설정입니다.

- 모든 소프트웨어 및 기기의 **자동 업데이트를 켠 후 컨펌하세요**.
- 소프트웨어와 기기에 따라 **자동 업데이트 활성화 방법이 다를 수 있습니다**.
- 수면 시간 또는 일반적으로 기기를 사용하지 않는 시간과 같은 가능한 한 **편리한 시간대에 자동 업데이트가 되도록 설정하세요**.

기기는 켜 있는 상태로 전원이 연결되어 있어야 하며, 사용 가능한 저장 공간이 있어야 합니다.

팁: 기기의 소프트웨어를 업데이트하라는 메시지가 뜨면, 가능한 한 빨리 진행해야 합니다.

자동 업데이트 활성화 방법에 관한 더 자세한 정보를 원하시면 cyber.gov.au에서 'Updates'를 검색하세요.

자동 업데이트 설정이 없다면 어떻게 해야 하나요?

자동 업데이트 설정이 없는 경우, 소프트웨어 또는 기기의 설정 메뉴를 통해 정기적으로 새 업데이트를 확인하고 설치해야 합니다.

오래된 기기 및 소프트웨어가 업데이트를 받지 않으면 어떻게 하나요?

기기, 운영 시스템 또는 소프트웨어가 너무 오래된 경우, 제조업자 또는 개발자의 지원을 더 이상 받지 못할 수도 있습니다.

어떠한 상품이 '지원 종료(End of Support)' 상태에 도달하면, 해당 상품은 더 이상 업데이트를 받지 못합니다. 이러한 경우 여러분은 사이버 공격에 노출될 수 있습니다. 지원이 종료된 상품의 예시로는 윈도우 7 운영 시스템과 아이폰 7이 있습니다.

기기, 운영 시스템 또는 소프트웨어가 지원 종료된 경우, ACSC는 보안을 유지하기 위해 가능한 한 빨리 업그레이드할 것을 권장합니다.

더 자세한 정보를 원하시면, cyber.gov.au에서 'End of support'를 검색하세요

개인 사이버 보안: 첫 단계

다중인증(MFA) 활성화 시키기

다중인증(MFA)은 무엇인가요?

여러분의 가장 중요한 계정의 보안을 개선하기 위해 다중인증(MFA)을 사용할 수 있습니다. MFA는 계정에 대한 접근 권한을 부여하기 전에 두개 이상의 인증 유형 조합을 생성하도록 요구합니다.

- **여러분이 아는 것** (예: PIN 번호, 비밀번호 또는 암호문구)
- **여러분이 소지하는 것** (예: 스마트카드, 물리적 토큰, 인증 앱, SMS 또는 이메일)
- **여러분의 신체와 관련된 것** (예: 지문, 얼굴 인식 또는 홍채 스캔)

MFA는 사이버 범죄자가 여러분의 계정에 대한 초기 접근을 어렵도록 만듭니다. 더 많은 인증 단계를 추가함으로써 계정에 접근하기 위해 더 많은 시간, 노력 및 자료를 소비하도록 만듭니다.

저의 가장 중요한 계정을 보호하기 위해 다중인증(MFA)을 어떻게 활성화 시키나요?

계정, 기기 또는 소프트웨어 어플리케이션에 따라 MFA 활성화 단계가 다릅니다. 중요한 계정부터 지금 MFA를 활성화 해야 합니다.

- 모든 온라인 뱅킹 및 금융 계정 (예: 여러분의 은행계좌, PayPal 계정)
- 모든 이메일 계정 (예: Gmail, Outlook, Hotmail, Yahoo!)

많은 이메일 계정을 보유하고 있는 경우, 온라인 뱅킹 또는 기타 주요 서비스와 연동된 이메일들을 우선시 하세요.

다중인증(MFA) 활성화 방법에 관한 더 자세한 정보를 원하시면 cyber.gov.au에서 'Multi-factor authentication' 또는 'MFA'를 검색하세요.

주기적으로 기기 백업하기

백업이란 무엇인가요?

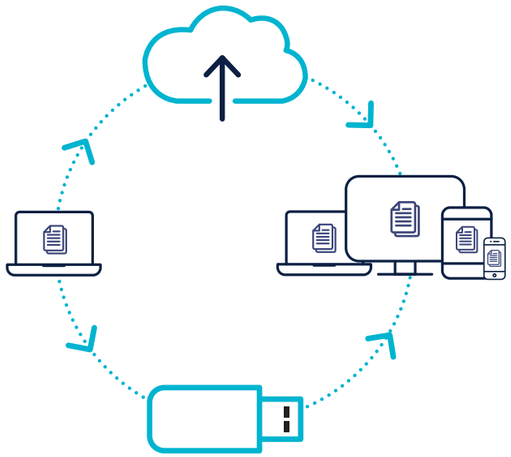
백업은 여러분 정보의 디지털 복사본입니다. 여기에는 여러분이 외부 저장 장치 또는 클라우드에 저장한 사진, 금융 정보 또는 기록이 포함될 수 있습니다.

정보 백업은 하나의 예방 조치로, 정보가 분실, 도난 또는 파손된 경우 복구할 수 있도록 합니다.

저의 기기와 파일을 어떻게 백업하나요?

파일 및 기기는 주기적으로 백업해야 합니다. 백업 주기가 일간, 주간, 월간일지는 여러분이 정하면 됩니다. 백업 주기를 결정하는 데 다음 요소가 고려될 수 있습니다:

- 기기에 저장된 새로운 파일 수
- 파일에 대한 변경 수



팁: 백업을 주기적으로 확인하여 복구 절차를 익히세요. 여러분의 백업이 제대로 실행되는지 늘 확인하세요.

정보 백업 방법에 관한 더 자세한 정보를 원하시면 cyber.gov.au에서 'Backups'를 검색하세요.

중요 계정은 암호문구(passphrase)로 보호하세요.

다중인증(MFA)은 여러분의 계정을 사이버 범죄자들로부터 보호할 수 있는 가장 효과적인 방법 중 하나입니다. **MFA 사용이 불가능하다면**, 독특하고 강력한 암호문구(passphrase)가 단순한 비밀번호보다 여러분의 계정을 더욱 잘 보호할 수 있습니다.

암호문구(passphrase)란 무엇인가요?

암호문구(passphrase)는 연관성이 없는 4개 이상의 단어를 비밀번호로 사용합니다.

예: 'crystal onion clay pretzel'

- **암호문구는** 단순한 비밀번호보다 **더 안전합니다**.
- 암호문구는 **사이버 범죄자가 알아내기 어렵지만 여러분이 기억하기에는 쉽습니다.**

암호문구(passphrase)는 어떻게 만드나요?

다음과 같은 암호문구를 만드세요:

- **긴:** 최소 14자, 연관성이 없는 4개 이상의 단어를 조합하세요. 암호문구가 길수록 더 안전합니다.
- **예상 불가능한**: 연관성이 없는 4개 이상의 단어를 무작위로 고르세요. 유명한 문구, 명언 또는 가사는 사용하지 않습니다.
- **독특한**: 여러 계정에 걸쳐 같은 문구를 사용하지 않습니다.

특정 웹사이트나 서비스는 기호, 대문자 또는 숫자를 포함하는 복잡한 비밀번호를 요구하며, 이를 암호문구에 포함해도 됩니다. 최고의 보안을 위해 여러분의 암호문구는 여전히 길고 예상 불가능하며, 독특해야 합니다.

어떤 계정들을 암호문구(passphrase)로 보호해야 하나요?

여러분의 가장 중요한 계정들이 다중인증(MFA)으로 보호되지 않았다면, 비밀번호를 독특하고 강력한 암호문구로 바꾸세요. 다음의 계정부터 시작하세요:

- 온라인 뱅킹 및 금융 계정
- 이메일 계정

많은 이메일 계정을 보유하고 있는 경우, 온라인 뱅킹 또는 기타 주요 서비스와 연동된 이메일들을 우선시 하세요.

일반적으로 계정 설정 메뉴를 통해 비밀번호를 독특하고 강력한 암호문구로 변경할 수 있습니다.

팁: 여러 개의 암호문구를 외우는 데 어려움이 있는 경우 비밀번호 매니저 이용을 고려해 보세요. 비밀번호 매니저를 이용할 경우 여러분은 하나의 비밀번호만 기억해도 되며, 나머지는 비밀번호 매니저가 알아서 기억해 줄 것입니다. 더 자세한 정보를 원하시면 cyber.gov.au에서 'password manager'를 검색하세요.

안전한 암호문구 생성 방법에 관한 더 자세한 정보를 원하시면 cyber.gov.au에서 'Passphrases'를 검색하세요

휴대기기 보호하기

오늘 날 스마트폰과 태블릿은 우리의 일상생활에서 사용됩니다. 우리는 그러한 것들을 사용해 연결하고, 쇼핑하고, 일하고, 은행 업무를 보고, 피트니스 상태를 추적하고, 언제 어디서나 수백 가지 작업을 완료합니다.

휴대기기가 손상, 분실 또는 도난 당하면 어떤 일들이 생길 수 있나요?

- 사이버 범죄자들이 여러분의 금전이나 신분을 도용하는 데 사용될 수 있습니다. 그들은 소셜미디어와 이메일 계정들을 포함해 여러분의 기기에 저장된 정보를 이용해 범죄를 저지릅니다.
- (백업되지 않은 경우) 사진, 메모 또는 메시지와 같이 대체할 수 없는 데이터를 잃을 수 있습니다.
- 사이버 범죄자가 여러분의 전화번호를 사용해 다른 사람들에게 사기를 칠 수 있습니다.

저의 휴대기기를 어떻게 보호하나요?

기기 보안:

- 암호문구, 비밀번호, PIN 번호 또는 비밀코드로 기기를 **잠그세요**. 유추하기 어렵도록 만드세요 - 여러분의 생일과 잠금 패턴은 사이버 범죄자들이 유추하기 쉽습니다. 최선의 보호를 위해 암호문구를 사용하세요(6페이지 참조). 또한 기기 잠금 해제를 위한 얼굴 인식 또는 지문 인식 사용을 고려해 볼 수 있습니다.
- 짧은 시간 동안 사용하지 않으면 기기가 자동으로 잠기도록 설정되어 있는지 **확인하세요**.
- 공공 충전소에서 기기를 충전하지 말고 제3자의 충전기 사용을 **피하세요.**
- 휴대전화를 지갑처럼 **취급하세요**. 항상 안전하게 보관하세요.

소프트웨어 및 앱 보안:

- 기기의 자동 업데이트 기능을 **사용해** 새로운 애플리케이션 및 운영 시스템 업데이트가 제공되는 즉시 설치하세요.
- 앱을 다운로드 하기 전 암호문구나 비밀번호가 요구되도록 기기를 **설정하세요**. 자녀 보호 기능 또한 이 목적으로 사용될 수 있습니다.
- 새로운 앱(특히 무료 앱)을 설치하기 전 개인 정보 보안 권한을 **확인하세요**. 신뢰 가능한 판매업체의 앱만 설치하세요.

데이터 보안:

- 원격 잠금 및 삭제 기능이 여러분의 기기에서 지원된다면 **활성화 시키세요.**
- 기기를 판매하거나 처분하기 전 개인 정보를 꼼꼼히 삭제했는지 **확인하세요.**

연결 보안:

- 사용하지 않을 때는 블루투스와 와이파이를 **끄세요.**
- 여러분의 기기가 자동으로 새로운 와이파이 네트워크에 연결되지 않도록 설정을 **확인하세요.**

휴대전화 보호 방법에 관한 더 자세한 정보를 원하시면 cyber.gov.au에서 'Secure your mobile phone'을 검색하세요.

사이버 보안 사고방식을 발전시키기

개인 사이버 보안은 단순히 설정 변경에 대한 것이 아니라 여러분의 사고방식과 행동을 바꾸는 것에 대한 것이기도 합니다.

사이버 사기에 주의하세요

사이버 범죄자들은 이메일, 메시지, 소셜미디어 또는 전화를 이용해 호주인을 대상으로 사기를 시도하는 것으로 알려져 있습니다. 그들은 여러분이 알고 있다고 생각하거나 신뢰해야 한다고 생각하는 개인이나 조직인 것처럼 가장할 수 있습니다.

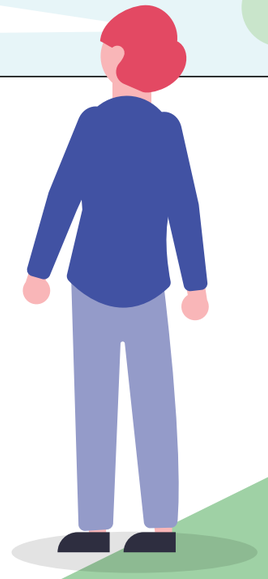
그들은 메시지나 전화를 통해 여러분이 다음과 같은 특정 행동을 취하도록 여러분을 속이려고 할 것입니다:

- 은행 계좌 정보, 비밀번호 및 신용카드 번호 공개
- 여러분의 컴퓨터에 대한 원격 접근권 부여
- 악성코드가 포함될 수 있는 첨부파일 열람
- 자금 이체 또는 기프트 카드 발송

사기 문자를 어떻게 구별하나요?

사기 문자를 구별하기 어려울 수도 있습니다. 사이버 범죄자들은 종종 특정 방법을 이용해 여러분을 속입니다. 문자는 다음 특징을 포함할 수 있습니다:

- **권위:** 여러분의 거래 은행과 같은 곳에서 누군가가 자신이 직원이라고 주장하는 문자인가요?
- **긴급성:** 문제가 있다거나, 답변 또는 지불을 하기까지 시간이 촉박하다는 내용의 문자인가요?
- **감정:** 여러분에게 패닉, 희망 또는 호기심을 유발하는 문자인가요?
- **희소성:** 재고가 부족한 것을 제공하거나 좋은 거래를 약속하는 문자인가요?
- **시사:** 현재의 뉴스나 큰 사건에 대한 문자인가요?



피싱 또는 사기 문자 구별 방법에 관한 더 자세한 정보를 원하시면 cyber.gov.au에서 'Learn the basics'를 검색하세요

사기 문자를 받으면 무엇을 해야 하나요?

사기 문자나 전화를 받게 되면, 이를 무시, 삭제 또는 scamwatch.gov.au를 통해 ACCC 의 Scamwatch에 신고해야 합니다.

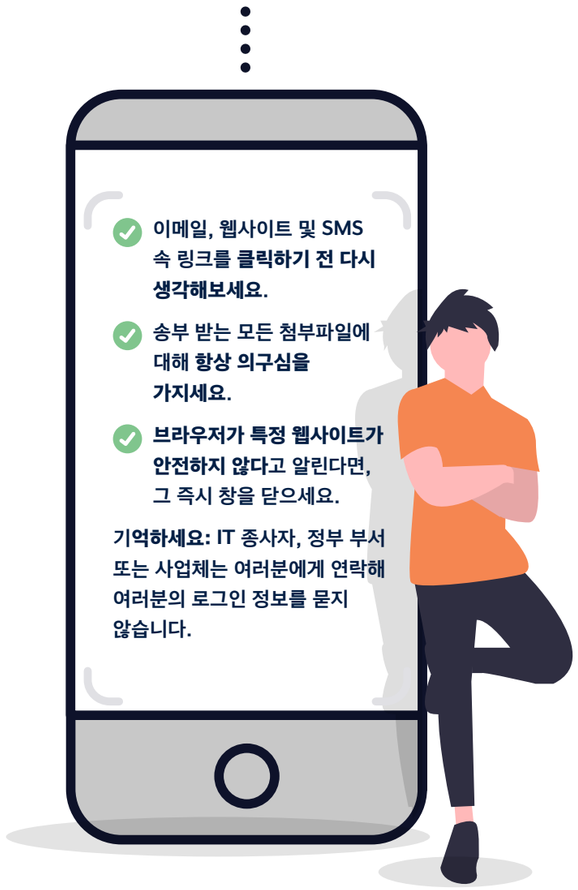
여러분의 사이버 보안에 대한 우려가 있을 경우 ACSC의 사이버 보안 핫라인 **1300 CYBER1**(1300 292 371)번으로도 전화하실 수 있습니다.

사기에 휘말렸고 여러분의 은행 계좌, 신용 또는 현금 카드가 위험에 노출되었다고 판단되는 경우 그 즉시 여러분의 금융기관에 연락하세요. 그들이 여러분의 계정을 닫거나 거래를 막을 수 있을 수도 있습니다.

어떠한 문자가 사기인지 아닌지 확실하지 않을 때는 어떻게 해야 하나요?

특정 문자나 전화가 정말 여러분이 신뢰하는 기관(여러분의 거래 은행 등)으로부터 온 것이라고 생각되면 여러분이 신뢰할 수 있는 연락 방법을 모색하세요. 공식 웹사이트를 검색하거나, 광고된 공식 전화번호로 연락하거나, 오프라인 상점 또는 지점을 방문하세요. 문자 또는 전화로 받은 링크 또는 연락처는 사기 목적을 위한 것일 수도 있기 때문에 사용하지 마세요.

팁:
클릭하기 전 다시 생각해보세요.



- **이메일, 웹사이트 및 SMS 속 링크를 클릭하기 전 다시 생각해보세요.**
- **송부 받는 모든 첨부파일에 대해 항상 의구심을 가지세요.**
- **브라우저가 특정 웹사이트가 안전하지 않다고 알린다면, 그 즉시 창을 닫으세요.**

기억하세요: IT 종사자, 정부 부서 또는 사업체는 여러분에게 연락해 여러분의 로그인 정보를 묻지 않습니다.

여러분이 사이버 범죄의 피해자라고 생각되는 경우 cyber.gov.au/report를 통해 ACSC의 ReportCyber에 신고하거나ACSC의 사이버 보안 핫라인 1300 Cyber(1300 292 371)번으로 전화하세요.

또한 ACSC의 무료 알림 서비스에 가입해 최근 위협에 대한 최신 정보를 얻을 수 있습니다. cyber.gov.au에서 'Subscribe to the ACSC alert service'를 검색하세요. 새로운 사이버 위협이 파악되면 저희가 여러분에게 알림을 보낼 것입니다.

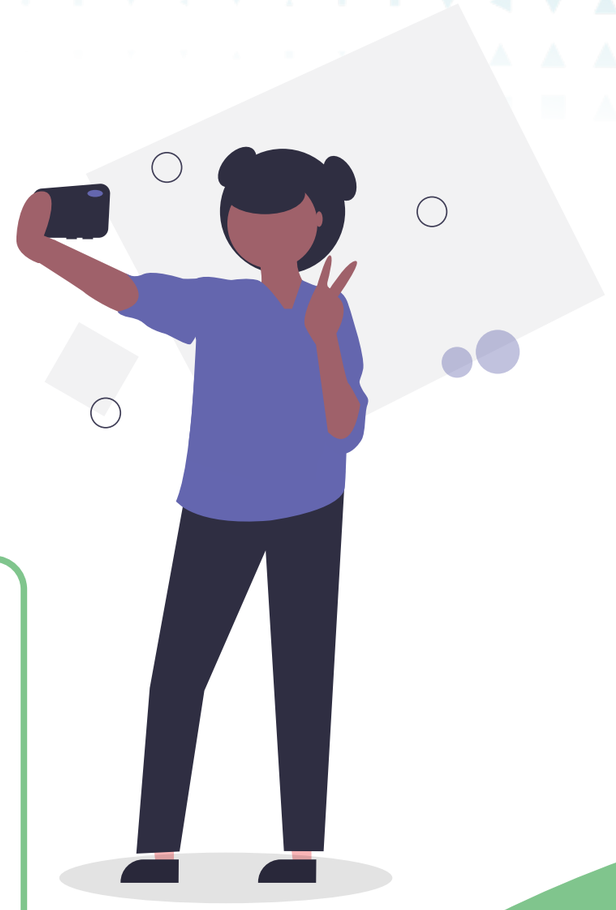
소셜미디어에 무언가를 공유하기 전 잠시 멈춰서 생각해 보세요

사이버 범죄자들은 여러분이 소셜미디어 계정에 공개적으로 올린 정보를 자신들의 사기 및 사이버공격에 이용할 수 있습니다.

인터넷상의 정보는 영구적이며 한번 게시된 정보는 완전히 삭제될 수 없다는 점을 기억하세요.

게시물을 올리기 전 '잠시 멈춰서 생각하기'를 어떻게 실천하나요?

- **생각하세요:** 사이버 범죄자는 이 정보를 어떻게 사용해 나 또는 내 계정을 표적으로 삼을 수 있을까?
- **생각하세요:** 나는 오프라인에서 완전히 낯선 사람에게 이 정보나 이미지를 보여줘도 괜찮을까?



어떤 종류의 정보를 공유하지 않아야 하나요?

사이버 범죄자가 여러분을 식별하거나 사기를 통해 여러분을 조정하거나 여러분의 계정 복구 질문을 추측하는 데 사용할 수 있는 온라인 정보(사진 포함)를 공유하지 마세요. 이는 다음 정보를 포함할 수 있습니다:

- 출생지 및 출생일
- 주소 및 전화번호
- 고용주 및 고용 이력
- 재학한 학교
- 여러분을 표적으로 만들 수 있는 모든 기타 개인 정보

개요 체크리스트

본 지침에 따라 모든 단계를 완료하셨나요?

편리한 이 체크리스트를 이용해 여러분의 진행 상태를 확인하세요:

- **나는 나의 모든 기기에 자동 업데이트를 활성화 시켰다:**
  - 컴퓨터(데스크톱 및 노트북)
  - 휴대전화
  - 태블릿
- **나는 나의 가장 중요한 계정에 다중인증을 사용하고 있다:**
  - 나의 모든 은행 뱅킹 및 금융 계좌(예: 거래 은행, PayPal 계정)
  - 나의 모든 이메일 계정 (예: Gmail, Outlook, Hotmail, Yahoo!)
- **나는 나의 기기들을 주기적으로 백업하고 있다:**
  - 컴퓨터(데스크톱 및 노트북)
  - 휴대전화
  - 태블릿
- **나는 다중인증(MFA)으로 보호되지 않은 가장 중요한 계정의 경우 독특하고 강력한 암호문구(passphrase)를 사용하고 있다:**
  - 온라인 뱅킹 및 금융 계좌
  - 이메일 계정
- **나는 나의 휴대 기기를 보호하고 있다:**
  - 노트북
  - 휴대전화
  - 태블릿
- **나는 나의 일상생활에 사이버 보안 사고방식을 실천하고 있다:**
  - 나는 사기 문자를 구별할 수 있다.
  - 나는 사기 문자를 받으면 무엇을 해야 하는지 알고 있다.
  - 나는 확실하지 않은 경우 특정 문자가 사기인지 아닌지 확인하는 방법을 알고 있다.
  - 나는 링크 및 첨부파일을 클릭하기 전 생각한다.
  - 나는 소셜미디어에 무언가를 공유하기 전 생각한다.
- **나는 내가 만약 사이버 범죄 또는 사기의 피해자가 된다면 어디서 도움을 청해야 할지 알고 있다.**

용어 사전

계정 복구
일련의 질문 또는 기타 확인 방법을 사용해 계정에 대한 접근 권한을 복구 또는 다시 얻거나 계정 암호를 변경하는 프로세스

악성코드
사용자 컴퓨터에 대한 무단 접근 및 제어 권한을 얻고, 정보를 도용하고, 네트워크를 방해하거나 비활성화하는 데 사용되는 악성 소프트웨어

앱
이는 모바일 앱이라고도 불리며 스마트폰 또는 태블릿에 흔히 사용되는 소프트웨어를 일컫는 단어

첨부 파일
이메일 메시지와 함께 전송되는 파일

운영 시스템
컴퓨터 하드웨어가 컴퓨터 프로그램과 통신하고 이를 운영할 수 있도록 컴퓨터 하드 드라이브에 설치되는 소프트웨어(예: Microsoft Windows, Apple macOS, iOS, Android)

물리적 토큰
일반적으로 키링에 맞고 다중인증(MFA)을 사용해 컴퓨터 사용자의 신원을 확인하는 데 사용되며 보안 코드를 생성하는 물리적 장치

인증 앱
다중인증(MFA)을 통한 접근을 허용하기 위해 컴퓨터 사용자의 신원을 확인하는 데 사용되는 앱

클라우드
방대하고 분산된 저장 및 처리 능력을 제공하는 원격 서버 네트워크

원격 접근
오프사이트 위치에서 장치 및 네트워크에 대한 접근 및 제어 권한

사이버 범죄자
정보를 손상시키거나 훔치기 위해 불법적으로 컴퓨터 시스템이나 계정에 접속하는 개인

기기
컴퓨터 사용 또는 통신 장치(예: 컴퓨터, 노트북, 휴대전화 또는 태블릿)

소프트웨어
일반적으로 프로그램이라고 하는, 사용자가 컴퓨터나 컴퓨터의 하드웨어와 상호 작용하거나 작업을 수행할 수 있도록 하는 일련의 지시

지원 종료
회사가 제품 또는 서비스에 대한 지원을 중단하는 상황으로, 일반적으로 회사가 새 버전을 출시하고 이전 버전에 대한 지원을 종료하면서 특정 하드웨어 및 소프트웨어 제품에 적용한다

면책 조항

본 지침의 자료는 일반적인 성격을 지니며 법률 자문으로 간주되거나 특정 상황이나 긴급 상황에서 도움을 받기 위해 의존되어서는 안 됩니다. 모든 중요한 문제에 대해서는 자신의 상황과 관련해 적절하고 독립적인 전문가의 조언을 구해야 합니다.

연방정부는 본 지침에 포함된 정보에 의존한 결과로 발생한 어떠한 손상, 손실 또는 비용에 대해서도 책임을 지지 않습니다.

더 자세한 정보를 원하거나, 사이버 보안 사고를 신고하려면 저희에게 연락하세요:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

이 번호는 호주 내에서만 사용되는 번호입니다.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre