



Australian Government



즉각적인 조치로
보안을 유지하세요.

온라인에서 안전을 유지하는 방법

쉬운 읽기 버전



안내서 사용법



호주 정부에서 알려드립니다.

이 안내서는 호주 정부에서 작성했습니다.



일부 단어는 **굵은 글씨**로 표시했습니다.

이 경우 단어들의 뜻을 설명했습니다.

28 페이지에 이러한 단어 목록이 있습니다.



믿고 의지할 수 있는 사람에게 다음과 같은 도움을
요청하셔도 좋습니다.

- 이 안내서 읽기
- 추가 정보 찾기.



이 문서는 다른 안내서를 요약한 읽기 쉬운 버전입니다.

이 안내서에는 가장 중요한 정보만 포함되어 있습니다.



다른 안내서는 우리 웹사이트에서 확인할 수 있습니다.

www.actnowstaysecure.gov.au

이 안내서의 내용

안내서 소개	4
계정을 안전하게 유지하기	6
설정을 확인하여 정보 보호하기	10
기기 보호하기	16
사기	20
알리기	25
단어 목록	28
문의하기	30

안내서 소개



우리 모두는 온라인에서 안전을 지키는 방법에 대해
생각해야 합니다.

이것을 **사이버** 안전이라고 부릅니다.



사이버는 인터넷과 관련된 것을 말합니다.



이 안내서는 온라인에서 자신을 지키기 위해 할 수 있는 몇
가지 방법을 설명합니다.

예를 들어, **사이버 범죄**로부터 자신을 지키는 방법입니다.

사이버 범죄란 범죄자가 인터넷을 이용해 범죄를 저지르는
것을 말합니다.



예를 들어, 인터넷을 사용하여

- 개인 정보를 훔치고
- 온라인 계정이나 프로필을 탈취할 수 있습니다.

사이버 범죄는 어떤 기기에서도 발생할 수 있습니다.



여기에는 다음이 포함됩니다.

- 컴퓨터
- 스마트폰
- 스마트워치.



사이버 범죄로부터 자신의 안전을 지키는 방법이 있습니다.



다음 페이지에서 그 방법을 설명합니다.

계정을 안전하게 유지하기



온라인 계정을 안전하게 지키는 방법에 대해 생각해야 합니다.

강력하고 서로 다른 암호문을 사용하세요



암호문은 더 강력한 형태의 비밀번호입니다.

다른 사람이 추측하기 매우 어렵습니다.



강력하고 서로 다른 암호문을 사용하는 것은 계정을 보호하는 가장 좋은 방법 중 하나입니다.



각 온라인 계정마다 다른 암호문을 사용해야 합니다.



강력한 암호문에는

- 서로 관련 없는 4 개 이상의 단어와
- 15 개 이상의 글자와 숫자가 들어갑니다.



대문자를 포함해도 됩니다.



다음과 같은 기호도 사용할 수 있습니다.

- 짧은 선
- 달러 기호
- 이메일 @ 기호.



암호문에는 개인정보를 사용하지 않아야 합니다.



예를 들어

- 자신의 생일
- 가족이나 반려동물의 이름은 안 됩니다.

계정에 로그인할 때 추가 단계를 설정하세요



다중 인증(MFA)을 사용하여 온라인 계정을 보호할 수 있습니다.

MFA 는 로그인할 때마다 2 가지 이상의 서로 다른 방법을 사용하는 것을 말합니다.



예를 들어, 먼저 암호문을 입력합니다.

그 다음 휴대전화로 받은 코드를 입력합니다.

다음과 같은 방법을 선택할 수 있습니다.



- 코드를 제공하는 앱을 휴대전화에 설치하기



- 이메일로 코드 받기



- 문자 메시지로 코드 받기.



MFA 는 다른 사람이 온라인 계정에 접근하기 더 어렵게 만듭니다.

암호문을 알게 되더라도 말입니다.

설정을 확인하여 정보 보호하기



온라인에서 정보가 보호되도록 설정되어 있는지 확인할 수 있습니다.

여기에는 다음과 같은 설정이 포함됩니다.



- 온라인 계정
- 기기
- 앱.

설정으로 가서



- 설정을 변경하고
- 어떤 앱이 개인정보를 사용할 수 있는지 선택할 수 있습니다.

자신의 기기에서 설정을 찾으려면



- 톱니바퀴 모양 아이콘을 찾거나
- 또는
- 기기의 검색창에 '설정'을 입력하세요.



앱이나 온라인 계정에서는 메뉴를 열어 설정을 찾을 수 있습니다.

메뉴는 보통 가로선 3 개 모양입니다.

이러한 설정 중 일부는 다음과 같은 정보를 공유할 수 있습니다.



- 본인이 누구인지
- 현재 위치
- 거주지 등입니다.



이러한 정보를 온라인에서 공유하면 사이버 범죄의 위험에 노출될 수 있습니다.



사이버 범죄자는 당신의 정보를 이용해 당신인 척할 수 있습니다.

예를 들어, 사이버 범죄자는 다음과 같은 정보를 사용할 수 있습니다.



- 당신의 거주지



- 가족의 이름



- 반려동물의 이름.



아는 사람만 소셜 미디어 프로필을 볼 수 있도록 계정을 설정할 수 있습니다.

예를 들어, 페이스북 프로필을 설정할 수 있습니다.



이러한 설정을 보통 개인정보 보호 설정이라고 부릅니다.



위치 설정도 통제할 수 있습니다.

위치 설정은 기기의 위치를 보여줍니다.



위치 설정은 켜거나 끌 수 있습니다.

또한 어떤 앱이 위치 설정을 사용할 수 있는지 선택할 수 있습니다.



다음 항목에 대해 이를 설정할 수 있습니다.

- 온라인 계정
- 기기
- 앱.

일부 앱은 다음과 같은 권한을 요청할 수 있습니다.



- 카메라 사용



- 사진 보기.



익숙한 앱에만 카메라와 사진 사용을 허용해야 합니다.

기기 보호하기



온라인에서 안전을 유지하기 위해 기기를 보호할 수 있는 방법에 대해 생각해 보세요.

예를 들어, 휴대폰이나 스마트워치 같은 기기입니다.



이는 인터넷에 연결되는 기기일수록 특히 중요합니다.

기기 업데이트하기



기기를 업데이트하여 온라인에서 기기 안전을 지킬 수 있습니다.

예를 들어 휴대폰과 노트북을 업데이트할 수 있습니다.



기기에 따라 '소프트웨어 업데이트'라고 표시될 수 있습니다.



업데이트는 기기를 사이버 범죄로부터 보호할 수 있도록
해 줍니다.



기기가 자동으로 업데이트되도록 설정할 수 있습니다.



기기 업데이트 방법에 대한 자세한 내용은 아래
웹사이트에서 확인할 수 있습니다.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

공공 와이파이



공공 와이파이를 사용할 때는 주의해야 합니다.



공공 와이파이는 공공장소에서 무료로 사용할 수 있는
무선 인터넷입니다.

예를 들어, 다음과 같은 곳에서 사용할 수 있습니다.



- 카페
- 공항
- 호텔.



공공 와이파이를 사용할 때는 웹사이트에 입력하는 정보에 주의해야 합니다.

예를 들어, 다음과 같은 정보입니다.



- 은행 정보
- 이메일 계정
- 소셜 미디어 계정.



일부 사이버 범죄자는 공공 와이파이를 사용해

- 당신이 온라인에서 무엇을 하는지 보거나
- 당신의 정보를 훔칠 수 있습니다.

왜냐하면



- 공공 와이파이에는 누구나 사용할 수 있고



- 기기를 보호하는 것이 더 어렵기 때문입니다.



공공 와이파이를 안전하게 사용하는 방법은 아래
웹사이트에서 확인할 수 있습니다.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

사기



사기라고 부르는 경우는 누군가가

- 당신을 속하려고 할 때
- 당신의 돈을 뺏으려고 할 때입니다



사기범은 사기를 저지르는 사람을 말합니다.

사기범은 당신을 속하려고 다음과 같은 수단을 사용할 수 있습니다,



- 문자 메시지나 전화
- 이메일
- 소셜미디어
- 웹사이트.



사기범은 친절해 보일 수 있습니다.

하지만 당신을 속여서 당신의 정보를 넘기도록 하려는 속셈일 수 있습니다.

그 정보를 이용해 사기범은



- 당신의 온라인 계정에 들어가고



- 당신인 척 가장하고



- 당신의 돈을 훔칠 수 있습니다.

사기범은 또한



- 당신을 속이기 위해 가짜 계정을 만들고



- 클릭을 유도하는 링크나 광고를 공유할 수도 있습니다.

사기를 식별하는 방법

다음과 같은 경우 사기일 가능성이 있습니다.



- 무언가를 빨리 하라고 재촉할 때



- 많은 돈을 준다고 제안할 때



- 돈을 요구할 때



- 링크를 클릭하도록 요청할 때.



사기범은 당신이 알고 있고 신뢰하는 기관인 것처럼
가장할 수도 있습니다.

예를 들어, 은행인 것처럼 가장합니다.



사기범이 이렇게 가장하는 이유는 당신으로부터
개인정보를 제공받기 위해서입니다.



상대방이 사기범이라고 생각되면 대화를 중단해야 합니다.



상대방이 스스로 주장하는 사람이 맞는지 확인해야 합니다.

해당 사람이나 기관이 맞는지 자신이 직접 확인한 신뢰할 수
있는 연락처로 연락해보십시오.



무언가 이상하다고 느껴지면 자신을 보호하기 위해 빠르게
대응해야 합니다.

사기 신고하기



Scamwatch 는 호주인들이

- 사기를 이해하고
- 사기를 신고하도록 도와드립니다.



Scamwatch 는 사기를 겪은 사람들도 도와드립니다.



Scamwatch 웹사이트에서 사기를 신고할 수 있습니다.

www.scamwatch.gov.au/report-a-scam

알리기



다른 사람들이 온라인에서 스스로를 보호할 수 있는 방법에 대해 알려야 합니다.

다음과 같이 하면 됩니다.



- 사이버 범죄 신고하기



- 알고 있는 내용을 가족과 친구에게 공유하기.



다음 페이지에서 알리는 방법을 설명하겠습니다.

사이버 범죄 신고하기

사이버 범죄 신고는 정부가 다음과 같은 대응을 하는 데 도움이 됩니다.



- 사이버 범죄자가 사람들을 어떤 방식으로 공격하는지 파악



- 더 많은 사람들 보호.



사이버 범죄는 ReportCyber 웹사이트에서 신고할 수 있습니다.

www.cyber.gov.au/report

온라인에서 안전하게 지내는 방법을 가족과 친구에게 이야기하기



온라인에서 안전하게 지내는 방법을 가족과 친구에게 이야기하는 것이 좋습니다.

또한 그들로부터 배울 수도 있습니다.



온라인 안전에 대해 알고 있는 내용을 나누면 자신과 주변 사람들을 보호할 수 있습니다.



기기를 다른 사람과 함께 사용하는 경우에는 특히 중요합니다.

단어 목록

이 목록은 이 안내서에서 굵게 표시된 단어들의 뜻을 설명합니다.



사이버

사이버는 인터넷과 관련된 것을 말합니다.

사이버 범죄

사이버 범죄란 범죄자가 인터넷을 이용해 범죄를 저지르는 것을 말합니다.



예를 들어, 이들은 인터넷을 이용해

- 개인 정보를 훔치고
- 온라인 계정이나 프로필을 탈취할 수 있습니다.



위치 설정

위치 설정은 기기의 위치를 보여줍니다.



다중 인증 (MFA)

MFA 는 로그인할 때마다 2 가지 이상의 서로 다른 방법을 사용하는 것을 말합니다.



암호문

암호문은 더 강력한 형태의 비밀번호입니다.

다른 사람이 추측하기가 매우 어렵습니다.



공공 와이파이

공공 와이파이는 공공장소에서 무료로 사용할 수 있는 무선 인터넷입니다.



사기

사기라고 부르는 경우는 누군가가

- 당신을 속하려고 할 때
- 당신의 돈을 뺏으려고 할 때입니다.



사기범

사기범은 사기를 저지르는 사람을 말합니다.

문의하기



호주 사이버 보안 핫라인(Australian Cyber Security Hotline)으로 전화할 수 있습니다.

1300 292 371 번



웹사이트를 방문할 수 있습니다.

www.actnowstaysecure.gov.au



사이버 범죄는 ReportCyber 웹사이트에서 신고할 수 있습니다.

www.cyber.gov.au/report



Information Access Group 은 스톡 사진과 맞춤형 이미지를 사용하여 이 쉬운 읽기 자료를 제작했습니다. 이미지는 허가 없이 재사용할 수 없습니다. 이미지에 대한 문의는 www.informationaccessgroup.com 를 방문해 주세요. 문의 시 작업 번호 6342 를 알려 주시기 바랍니다.