Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

인터넷을 안전하게 사용하는 방법

시니어들을 위한 안내

cyber.gov.au

서론

온라인 서비스를 이용함으로써 친구 및 가족과 계속해서 연락하고, 특정 주제에 대해 배울 수 있으며, 게임도 즐길 수 있습니다.

운전하기 전 벨트를 매는 것처럼 인터넷을 사용하기 전에도 더욱 안전하기 위해 몇 가지 단계를 따라야 합니다.

호주 사이버보안센터(ACSC)는 모든 사람이 온라인 상태일 때 보안을 유지할 수 있도록 하고 있습니다. 본 문서는 여러분이 인터넷을 사용할 때 스스로를 보호하기 위해 실천할 수 있는 몇 가지 기본적인 사이버 보안 습관들을 소개합니다.

호주 사이버보안센터(ACSC)는 호주 신호정보국(ASD)의 소속으로, 호주에 대한 사이버 위협을 예방, 발견 및 해결하기 위한 조언, 지원 및 조치를 제공합니다. ACSC는 호주를 온라인 사용하기에 가장 안전한 국가를 만드는 데 일조하고 있습니다.

사이버 보안에 관한 정보, 지침 및 조언을 원하시면 cyber.gov.au를 방문하세요.

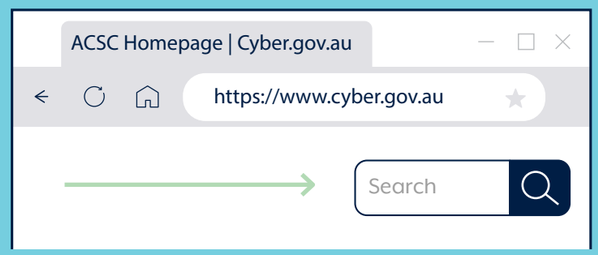
시니어들을 위한 사이버 보안

팁 1: 기기를 업데이트하세요

소프트웨어 업데이트는 자동차 정비와 비슷합니다. 업데이트는 기기 성능을 향상시키고 기기가 더욱 안전하도록 합니다.

사이버 범죄자들은 기기 해킹을 위한 새로운 방법을 늘 모색하고 있습니다. 기기의 업데이트 자동 설치를 활성화시킴으로써 소프트웨어의 취약점을 고치고 해커들의 활동을 막을 수 있습니다.

더 자세한 정보를 원하시면 cyber.gov.au에서 'Updates'를 검색하세요.



알고 계셨나요:

또한 업데이트를 하게 되면 여러분 기기에 새로운 기능이 추가되고 운영 속도가 빨라질 수 있습니다.

팁 2: 다중인증(multi-factor authentication, MFA)을 활성화하세요

**계정의 다중인증(MFA)은 집 인터컴 화면과 같습니다.
이는 여러분을 무단 침입하려는 범죄자로부터 보호합니다.**

다중인증(MFA)이 활성화되면 계정 로그인 시 여러 가지 정보를 제공해야 합니다. 예를 들어, 여러분의 소셜미디어 계정에 로그인하려면 비밀번호와 문자 인증 코드를 입력해야 할 수도 있습니다.

여러 단계의 다중인증은 사이버 범죄자의 해킹을 더욱 어렵게 만듭니다. 이는 그들이 비밀번호 등 한 부분을 추리해 낼 수 있지만 여러분의 계정에 접근하기 위해 퍼즐 조각과 같은 다른 정보까지 알아야 하기 때문입니다.

더 자세한 정보를 원하시면 cyber.gov.au에서 'Multi-factor authentication' 또는 'MFA'를 검색하세요.

기억하세요:

다중인증(MFA) 활성화에 도움이 필요한 경우, 친구 또는 가족에게 도움을 청하세요.

팁 3: 기기를 백업하세요

'백업'은 중요한 파일들을 복사해 안전한 곳에 보관하는 작업입니다. 이는 원본을 분실할 경우를 대비해 소중한 사진을 복사해 별도로 안전하게 보관하는 것과 같습니다.

컴퓨터, 휴대전화 또는 태블릿을 백업하면 파일의 복사본이 온라인이나 별도의 기기에 저장됩니다. 중요한 파일과 소중한 사진의 백업을 갖고 있으면 안심이 될 것입니다.

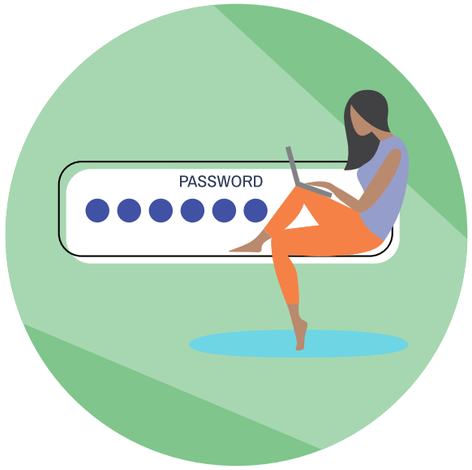
기기에 문제가 생기거나 사이버 범죄자가 기기를 해킹한 경우 백업으로부터 여러분의 파일들을 쉽게 복원할 수 있습니다.

더 자세한 정보를 원하시면 cyber.gov.au에서 'Backups'를 검색하세요.

알고 계셨나요:

기기를 정기적으로 백업하면 항상 가장 최신의 파일들을 열람할 수 있습니다.

팁 4: 암호문구(passphrase)를 사용하세요

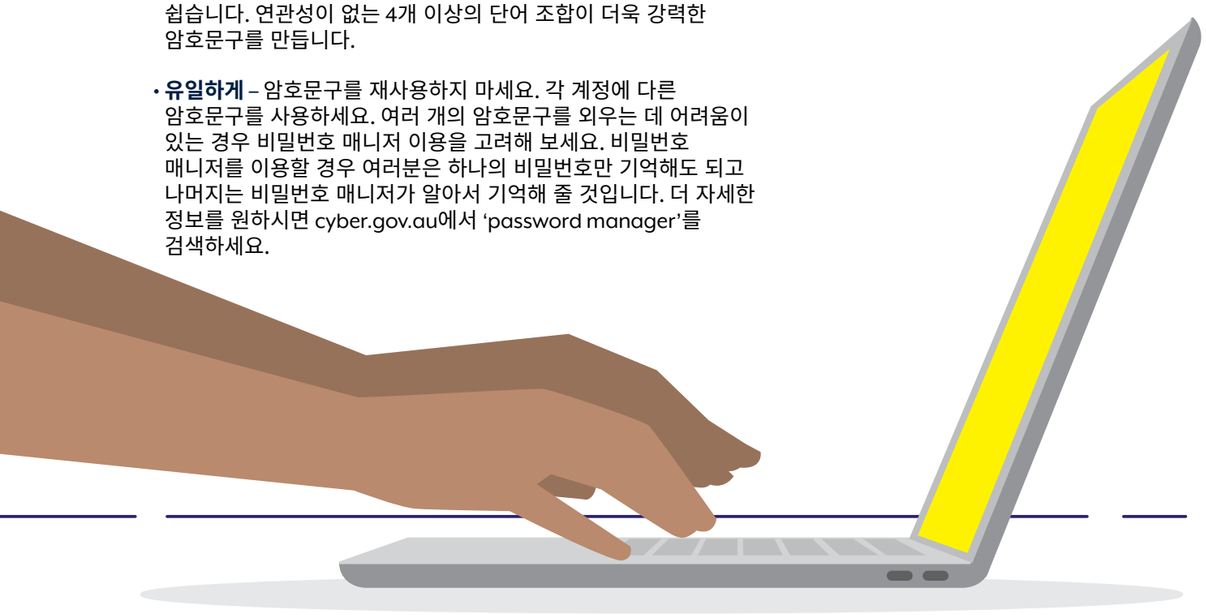


비밀번호가 계정에 자물쇠를 거는 것이라고 한다면, 암호문구(passphrase)는 계정에 자체 보안 시스템을 설치하는 것과 같습니다! 암호문구는 비밀번호의 더욱 강력하고 안전한 버전입니다.

다중인증(MFA)을 활성화할 수 없다면, 계정을 보호하기 위해 암호문구(passphrase)를 사용하세요. 암호문구는 연관성이 없는 4개 이상의 단어를 조합한 비밀번호이기 때문에 사이버 범죄자가 추측하기 어렵지만 여러분이 기억하기에는 쉽습니다.

다음의 특징을 고려해 암호문구를 만드세요:

- **길게** – 길수록 좋습니다. 최소 14개 이상의 문자를 목표로 하세요. 여러분이 기억할 수 있고 연관성이 없는 4개 이상의 단어 조합이 가장 좋습니다.
  예시: 'purple duck potato boat'.
- **예상 불가능하게** – 예상할 수 없는 암호문구일수록 좋습니다. 문장은 좋은 암호문구가 될 수 있지만 상대적으로 맞추기가 더 쉽습니다. 연관성이 없는 4개 이상의 단어 조합이 더욱 강력한 암호문구를 만듭니다.
- **유일하게** – 암호문구를 재사용하지 마세요. 각 계정에 다른 암호문구를 사용하세요. 여러 개의 암호문구를 외우는 데 어려움이 있는 경우 비밀번호 매니저 이용을 고려해 보세요. 비밀번호 매니저를 이용할 경우 여러분은 하나의 비밀번호만 기억해도 되고 나머지는 비밀번호 매니저가 알아서 기억해 줄 것입니다. 더 자세한 정보를 원하시면 cyber.gov.au에서 'password manager'를 검색하세요.



안전한 암호문구 생성에 관해 더 자세한 정보를 원하시면 cyber.gov.au에서 'Passphrases'를 검색하세요.

알고 계셨나요:

사이버 범죄자들은 교활하기 때문에 익숙한 이름과 이메일 주소를 사용할 수도 있습니다.

다음의 경우 주의를 기울이세요:

- 청구서를 긴급히 지불하라고 하는 경우
- 개인 정보나 비밀번호를 변경하라고 하는 경우
- 링크를 클릭하거나 첨부파일을 열람하라고 하는 경우

팁 5: 사기를 인식하고 신고하세요

사기를 더 빨리 신고할수록 저희가 더 빠른 조처를 할 수 있습니다.

누군가가 인터넷을 사용해 여러분에게 사기를 친다고 생각되는 경우, 위험을 감수하기 보다 능동적이고 신중하게 알아보는 것이 더 좋습니다.

그들이 제시하는 조건이 비이상적으로 너무 좋다면, 아마 여러분의 의심이 맞을 겁니다. 메시지가 여러분이 경품에 당첨되었거나 여러분의 컴퓨터에 바이러스가 생겼다고 하더라도 해당 메시지는 여러분에게만 발송된 것이 아닙니다.

이는 사기꾼으로부터 온 메시지일 수 있으며 그들은 여러분을 이용하고자 하는 것입니다.

사기꾼들은 종종 여러분이 신뢰하는 사람 또는 기관인 척 연기할 것임을 기억하세요. 여러분이 신뢰하는 사람이 보낸 듯한 메시지가 새로운 전화번호나 이메일 주소, 또는 소셜미디어 계정으로부터 온다면 의구심을 가지세요. 답장을 하기 전, 신뢰할 수 있는 별도의 연락 방식을 통해 그들이 실제로 여러분이 신뢰하는 사람 또는 기관이 맞는지 여부를 먼저 확인하세요. 예를 들어, 여러분의 자녀가 보낸 듯한 메시지가 새로운 번호로부터 온다면 일단 답장하지 마세요. 소셜미디어를 통해 자녀가 진짜로 전화번호를 변경했는지 여부를 먼저 확인하세요.

결론

인터넷을 안전하게 사용하는 방법에 대해 배우셨기 때문에 이제는 자신있게 웹 검색을 하고 온라인상에서의 시간을 계속해서 즐기시면 됩니다.

사이버 범죄자들은 개인들을 목표 삼을 수 있는 새로운 방법을 늘 모색하고 있음을 기억하세요.

가끔 사이버 보안 노하우를 연마하고 보안을 유지하는 새로운 방법을 배우는 것이 좋습니다.

보너스 팁

온라인상의 안전을 유지하는 더 많은 방법이 궁금하신가요? 다음 팁을 고려해 보세요.

여러분이 무엇을 게시하는지 생각해보세요.

여러분이 온라인으로 공유하는 정보와 해당 정보를 누가 열람할 수 있는지를 신중히 고려해 보세요. 실제로 아는 사람들의 친구 추가 요청만 수락하세요.

신규 위협에 대한 알림을 받으세요.

무료 알림 서비스에 가입하세요. 해당 서비스는 새로운 사이버 위협이 발견될 때마다 여러분에게 이를 알려줄 것입니다.

또한 이 서비스는 사이버 공격 발생 시 여러분이 무엇을 해야 하는지에 대해서도 알려줄 것입니다.

가족 및 친구들과 사이버 보안에 관해 이야기 나누세요.

여러분의 사이버 보안 스킬이 향상되었으니, 이제 배운 내용을 가족과 친구들과 공유하세요. 차후 그들이 복잡한 상황에 당면하게 된다면 여러분의 지식이 도움이 될 수도 있습니다.

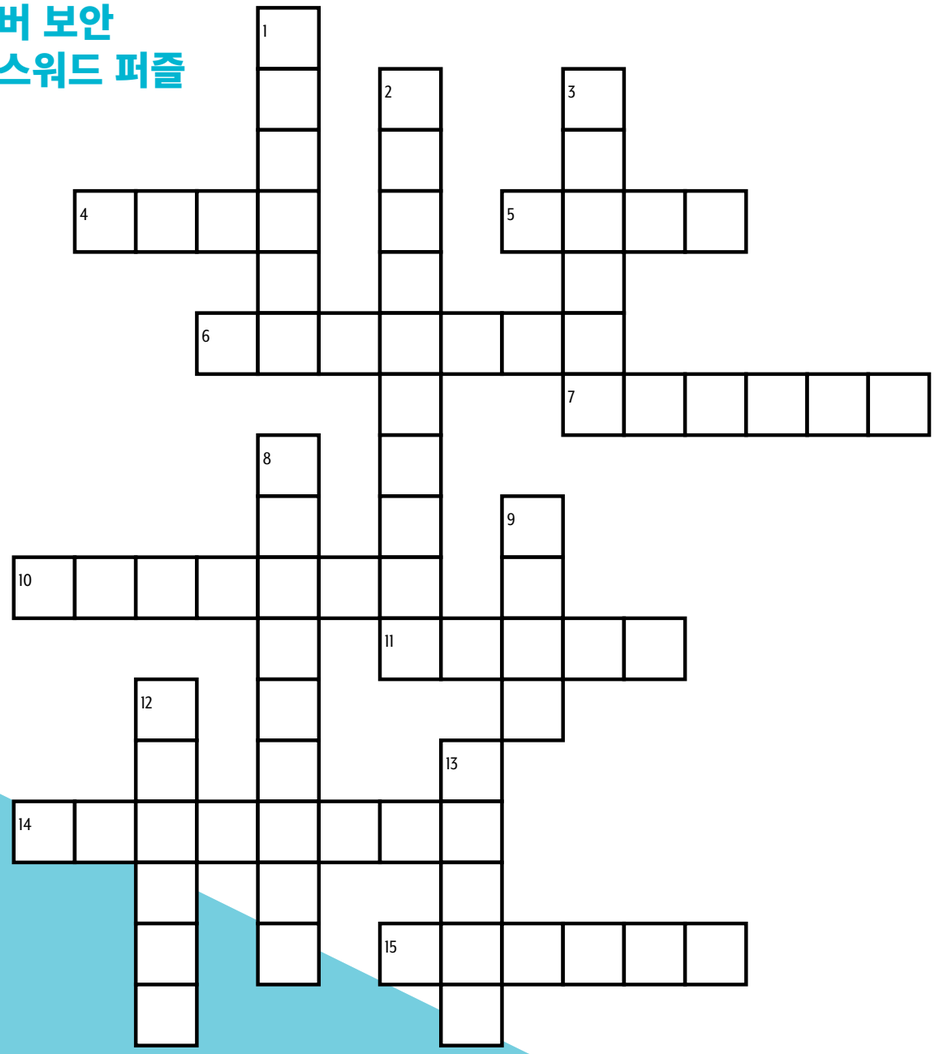
온라인으로 은행 업무를 보거나 쇼핑할 때는 공용 와이파이 사용을 피하세요.

공용 와이파이는 비디오 시청 또는 웹사이트 열람에는 좋으나 돈과 관련된 모든 온라인 활동은 가정 인터넷 연결만 사용하도록 하세요. 공용 와이파이는 위험할 수 있습니다.

호주의 안전을 유지하기 위해 사이버 보안 및 사고를 신고하세요.

본인이 사이버 범죄의 피해자라고 생각되는 경우, 빠르게 조치를 취하세요. cyber.gov.au에서 더 많은 조언을 구하세요.

사이버 보안 크로스워드 퍼즐



세로

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

가로

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

보조 안내 자료

더 자세한 정보를 원하시면 저희의 개인 사이버 보안 시리즈를 열람해 보세요: 3개의 지침으로 구성된 이 시리즈는 일반적인 호주인들이 사이버 보안의 기본과 흔한 사이버 위협으로부터 자신을 보호하기 위해 취할 수 있는 조치를 이해하도록 돕기 위해 고안되었습니다.

cyber.gov.au에서 3개의 지침 모두 열람하실 수 있습니다.

크로스워드 퍼즐 답:

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

노트

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 원하시거나 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