2022년 10월

건강 및 안전 소식지 - 사이버 범죄 예방

캘리포니아 발달장애서비스국

이 소식지가 유용했나요?

여기를 클릭하세요.

사이버 범죄 예방

인터넷은 세상과 연결되는 훌륭한 수단이지만, 위험할 수도 있습니다. 외출할 때 문단속을 하듯이, 인터넷을 사용할 때도 나와 내 정보를 안전하게 지키고 사이버 범죄 피해를 막기 위한 예방 조치가 필요합니다.

인터넷 안전하게 사용하는 방법

사이버 범죄란?

사이버 범죄란 인터넷을 통해 사람들에게 발생하는 범죄를 말합니다. 주로 다른 사람의 개인 정보나 돈을 훔치는 형태로 발생합니다. 많은 사람들이 사이버 범죄 피해를 당하고도 알아차리지 못하는 경우가 있습니다. 따라서 범죄를 예방하고 도움을 받아 재발을 막으려면, 사이버 범죄를 인식하는 방법을 알아두는 것이 중요합니다.

인터넷은 공공장소입니다

- 여러분이 어떤 웹사이트에 접속하는지, 때로는 어떤 정보를 입력하는지 다른 사람들이 볼 수 있습니다.
- 인터넷에 올린 정보는 누구든지 볼 수 있다는 점을 명심하세요.
- 은행 업무와 같이 꼭 필요한 경우가 아니라면, 인터넷상에서 개인 정보(사회보장번호, 은행 계좌, 의료 기록 등)를 공유할 때 매우 신중해야 합니다.
- 상점이나 식당에서 제공하는 무료 공용 와이파이는 항상 주의해서 사용해야 합니다.
- 공용 와이파이는 편리하지만 보안에 취약한 경우가 많습니다. 즉, 아이디나 비밀번호 같은 개인 정보가 다른 사람에게 노출되거나 도난당할 수 있습니다.

개인 정보 설정을 정기적으로 확인하세요

- 개인 정보 설정을 통해 공유할 정보의 범위와 내 정보를 볼 수 있는 사람을 선택할 수 있습니다.
  - 페이스북이나 인스타그램 같은 소셜 미디어에서도 개인 정보 설정을 통해 정보 공유 범위를 제어할 수 있습니다.
- 휴대전화 앱별로 개인 정보 설정을 변경하여 앱이 접근할 수 있는 정보(위치 정보, 데이터 권한 등)를 제한하세요.
- 온라인 계정에 접속할 때 반드시 비밀번호를 입력하도록 개인 정보 설정을 확인하세요.
  - 2단계 인증이란 은행이나 카드사 등 온라인 계정에 로그인할 때마다 문자, 전화, 이메일로 전송된 인증 코드를 한 번 더 입력하는 방식입니다. 이를 통해 본인이 직접 로그인하는 것인지 확실하게 확인할 수 있습니다.
  - 모든 온라인 계정에 2단계 인증을 설정하는 것이 좋습니다.

웰니스 및 안전 소식지는 우리 지역사회에서 발생할 수 있는 각종 위험 요소를 당사자와 가족, 관계자분들께 미리 알려 드리고자 발달장애서비스국에서 제작합니다. 이 소식지에 대한 의견과 개선할 점을 이 설문조사를 통해 제공해 주세요. 소식지 설문조사

온라인 계정에 강력한 비밀번호 사용하세요

- 비밀번호를 복잡하게 만들고 정기적으로 변경하는 습관을 들이세요. 온라인 계정을 보호하는 가장 좋은 방법입니다.
- 강력한 비밀번호는 최소 8자 이상이며, 영문 대소문자, 숫자, 특수기호를 섞어 구성합니다. 비밀번호는 길수록 더 안전합니다.
    - **취약한 비밀번호 예시**: password, 본인이름, 12345
    - **안전한 비밀번호 예시**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs
- 생일이나 이름처럼 남들이 쉽게 추측할 수 있는 비밀번호는 피하세요.
- 계정마다 서로 다른 비밀번호를 설정해야 합니다.
- 비밀번호를 종이에 적어 두고 아무 데나 두지 마세요. 특히 컴퓨터 근처는 피하세요.
- 비밀번호는 믿을 수 있는 사람하고만 공유하고, 안전한 곳에 보관해야 합니다.

바이러스와 악성 코드를 조심하세요

- 멀웨어(Malware, 악성 코드)란 컴퓨터에 해를 끼치는 소프트웨어를 말합니다. 바이러스도 멀웨어의 일종입니다.
    - 바이러스와 멀웨어는 사용자의 허락 없이 컴퓨터 시스템에 침입하여 '감염'을 일으킵니다.
    - 바이러스와 멀웨어는 몰래 컴퓨터에 침투해 정보를 훔치거나, 속도를 늦추고 시스템을 마비시키며, 심지어 컴퓨터를 완전히 장악할 수도 있습니다.

- 주로 감염된 이메일을 열거나 감염된 링크를 클릭할 때 컴퓨터로 침투합니다.
    - 경품이나 무료 선물을 준다는 링크는 클릭하기 전에 각별히 주의하세요.
    - 게임, 화면 보호기, 다운로드 파일처럼 보이지만 실제로는 멀웨어나 바이러스일 수 있습니다.

클릭하기 전에 한 번 더 생각하세요

- 온라인으로 받은 이메일이나 메시지의 발신자를 꼼꼼히 확인하세요.
    - 발신자의 이메일 주소가 내가 알고 있는 주소와 일치하는지 확인해야 합니다.

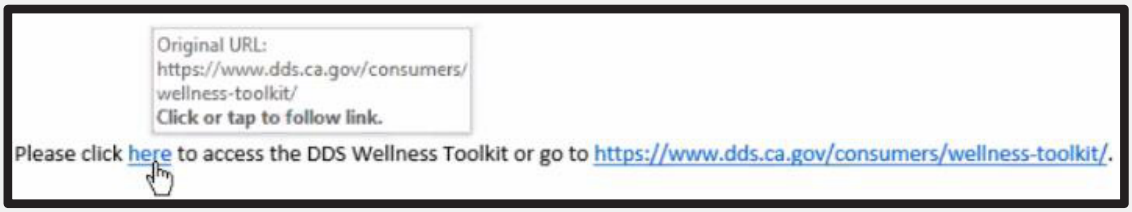
- 당장 답장을 보내라며 재촉하거나, 은행 계좌에 문제가 생겼다며 위기감을 조성한다면 특히 조심해야 합니다. 이런 메시지는 사기일 가능성이 매우 높습니다.
- 피싱은 진짜처럼 보이는 가짜 메시지로 사람들을 속여 개인 정보를 빼내는 인터넷 사기 수법입니다.

    - 답장하기 전에 낯선 발신자, 맞춤법 오류, 내용과 다른 링크, 뜬금없는 첨부 파일, 빨리 처리하라는 재촉 등이 없는지 확인하세요.
- 모르는 첨부 파일은 열지 말고, 수상한 링크는 클릭하지 마세요. 가짜 파일이나 링크를 통해 바이러스가 설치되면 컴퓨터나 휴대폰이 망가지고 더 많은 정보가 유출될 수 있습니다.
    - 링크나 첨부 파일이 있는 예상 밖의 이메일을 받았다면, 반드시 보낸 사람에게 전화나 문자로 확인하세요.
- 미국 국세청(IRS)은 우편으로만 통지서를 발송합니다. IRS를 사칭하는 전화, 이메일, 문자 메시지에는 절대 응답하지 마세요.

웰니스 및 안전 소식지는 우리 지역사회에서 발생할 수 있는 각종 위험 요소를 당사자와 가족, 관계자분들께 미리 알려 드리고자 발달장애서비스국에서 제작합니다. 이 소식지에 대한 의견과 개선할 점을 이 설문조사를 통해 제공해 주세요. 소식지 설문조사

이메일·문자를 보내기 전에 상대방을 확인하세요

- 온라인상의 상대방은 실제로는 자신이 말하는 사람과 다를 수 있습니다.
- 낯선 사람이나 한 번도 직접 만난 적 없는 사람에게는 절대 개인 정보나 본인 사진을 보내지 마세요.
- 알게 된 지 얼마 안 됐거나 직접 만난 적 없는 사람에게는 절대 돈을 보내지 마세요.
- 온라인 양식이나 웹사이트에 사회보장번호나 계좌 번호를 입력하기 전에, 정보를 요청한 곳이 믿을 수 있는 곳인지 반드시 확인하세요.
    - 보낸 사람 이름이나 링크 위에 마우스 커서를 올려 이메일 주소가 해당 기업이나 기관의 공식 주소가 맞는지 확인하세요.



- 로고를 복사해 진짜처럼 보이게 만든 이메일일 수 있습니다. 오타, 이상한 내용, 흐릿한 이미지가 있는지 꼼꼼히 확인하세요.
- 발신자가 의심스럽다면 해당 기업이나 기관의 공식 연락처로 직접 문의하세요.

사이버 범죄 피해를 입은 경우

- 즉시 신뢰할 수 있는 사람에게 알리세요.
- 개인 계좌가 도용되었다면 즉시 은행이나 카드사에 전화하여 알리세요. 도용된 계좌와 연결된 체크카드나 신용카드는 사용을 중지하세요.
- 해킹당한 계정이나 로그인 정보의 비밀번호를 즉시 변경하세요.
- 계좌에 의심스러운 거래 내역이 없는지 지속적으로 확인하세요.

웰니스 및 안전 소식지는 우리 지역사회에서 발생할 수 있는 각종 위험 요소를 당사자와 가족, 관계자분들께 미리 알려 드리고자 발달장애서비스국에서 제작합니다. 이 소식지에 대한 의견과 개선할 점을 이 설문조사를 통해 제공해 주세요. 소식지 설문조사