

비밀을 지켜주세요

실제 상황에서 개인 정보 보호 및 보안 이해하기

차시 개요

1차시 그건 제가 한 게 아닌데요!	2~6학년
2차시 효과적인 비밀번호를 만드는 방법	2~6학년
3차시 혼자만 알기	2~6학년
4차시 Interland: 보물의 탐	2~6학년

학습 주제

게임이나 휴대전화, 디지털 어시스턴트, 컴퓨터 등 인터넷에 연결하는 기기를 사용하는 사람은 누구나 온라인 개인 정보 보호와 보안에 관한 기본사항을 알아야 합니다. 사용하는 기기와 기기에 저장된 개인 정보, 즉 나와 내 가족, 친구에 관한 모든 정보를 보호하기 위해서는 어떤 정보가 들어오고 나가는지, 효과적인 비밀번호는 어떻게 설정해야 하는지 생각해 봐야 합니다.

학습 목표

- ✓ **학습:** 개인 정보 보호와 보안이 중요한 이유와 이들이 서로 어떤 관계로 연결되어 있는지 알아봅니다.
- ✓ **연습:** 안전한 비밀번호를 만들고 본인과 본인의 보호자만 알고 있도록 하는 방법을 연습합니다.
- ✓ **검토:** 사기, 해커 및 기타 위협으로부터 보호하는 도구와 설정을 검토합니다.

교육과정 요소

ISTE Standards for Educators: 1a, 2c, 3b, 3c, 3d, 4b, 6a, 6d, 7a
ISTE Standards for Students 2016: 1c, 1d, 2b, 2d, 3d, 6a
AASL Learning Standards: I.b.2, I.c.1, I.c.3, II.c.1, III.a.2, III.b.1, III.c.1, III.d.1, III.d.2, IV.b.3, V.d.3, VI.a.1, VI.d.1

비밀을 지켜 주세요

어휘 설명

1~4 차시

개인 정보 보호: 사람들의 데이터와 개인 정보(민감한 정보라고도 함)를 보호하는 행동

보안: 사람들의 기기와 기기의 소프트웨어를 보호하는 행동

1차시

디지털 발자국: 디지털 발자국은 온라인에 남아 있는 나에 관한 모든 정보입니다. 사진이나 오디오, 동영상, 텍스트에서부터 '좋아요'와 내가 친구의 프로필에 남긴 댓글까지 모든 흔적이 디지털 발자국에 포함됩니다. 걸을 때 땅에 발자국이 남듯이 내가 온라인에서 게시하는 콘텐츠도 흔적을 남깁니다.

평판: 다른 사람이 나에 대해 갖는 생각이나 의견, 인상, 신념입니다. 다른 사람이 나를 어떻게 생각하는지 확실히 알 수는 없지만 긍정적이거나 좋게 생각하기를 바라는 경우가 많습니다.

2차시

해커: 컴퓨터를 사용해서 다른 사람이나 조직의 기기와 데이터에 허가받지 않고 접근하는 사람입니다.

비밀번호 또는 암호: 무언가에 접근하기 위해 사용하는 보안을 위한 코드 조합입니다. 형태는 다양할 수 있습니다. 예를 들어 휴대전화를 잠그는 데는 숫자만으로 된 코드를, 이메일이나 다른 계정에는 훨씬 더 복잡한 비밀번호를 사용할 수도 있습니다. 일반적으로 비밀번호는 최대한 길고 복잡하면서 기억하기 쉽게 만들어야 합니다.

3차시

설정: 디지털 제품이나 앱, 웹사이트 등에서 내가 공유하는 정보와 내 계정의 취급 방식을 관리, 즉 '설정'하는 영역입니다. 개인 정보 보호 설정도 여기에서 이루어집니다.

2단계 인증(2단계 확인이라고도 함): 서비스에 로그인하기 위해 비밀번호와 일회성 코드처럼 별도의 2가지 단계, 즉 2개의 '요소'가 필요한 보안 프로세스입니다. 예를 들어 비밀번호를 입력한 후 휴대전화 문자로 받은 코드나 앱에서 생성된 코드를 입력해야 할 수 있습니다.

비밀을 지켜 주세요: 1차시

그건 제가 한 게 아닌데요!

비밀번호 공유의 결과와 그 행동이 가져올 수 있는 영향을 알아봅니다.

학습 목표



- ✓ **학습:** 비밀번호를 공유하면 다른 사람이 내 디지털 발자국을 제어하게 된다는 점을 이해합니다.
- ✓ **생각:** 누군가가 내 계정에 로그인하면 어떤 일이 벌어질지 생각해 봅니다.
- ✓ **이해:** 다른 사람의 행동이 나의 디지털 발자국과 **나 자신**에게 어떤 영향을 미치는지 이해합니다.

토론 주제



비밀번호를 공유하면 어떤 일이 벌어질까요?

사용 중인 앱이나 기기에 설정한 비밀번호를 생각해 보세요. 휴대전화를 잠금 해제하기 위한 비밀번호나 좋아하는 게임 또는 동영상 앱에 로그인하기 위한 비밀번호도 좋습니다. 그 비밀번호를 다른 사람과 공유한 적이 있나요? 솔직히 말해도 괜찮습니다. 많은 사람이 비밀번호를 공유하니깐요. 하지만 비밀번호를 공유해서는 안 되는 아주 중요한 이유가 있습니다.

여러분은 디지털 발자국을 남기게 됩니다. 디지털 발자국은 온라인에서 여러분을 나타냅니다. 디지털 발자국이란 좋아요, 댓글, 대화명, 사진, 메시지, 녹음 등 여러분이 온라인에서 남기는 모든 흔적이며, 이 모든 정보가 합쳐져서 다른 사람들이 생각하는 내 모습이 만들어집니다. 그래서 디지털 발자국은 여러분의 평판, 즉 여러분에 대한 다른 사람의 생각에 영향을 미칩니다. 사람들은 여러분이 남기는 발자국을 바탕으로 여러분에 관해 추측하고 가정합니다. 온라인에서 활동할 때는 이 점을 꼭 명심하세요.

또 한 가지 명심해야 할 점은 비밀번호를 공유하면 그 사람에게 여러분의 디지털 발자국에 대한 제어 권한을 주는 셈이라는 것입니다. 그 사람이 여러분의 디지털 발자국을 만들어 다른 사람들의 눈에 비치는 여러분의 모습을 바꾸어 놓을 수 있습니다. 그 생각은 못 했죠? 그 사람이 여러분의 계정으로 남긴 발자국이므로 다른 사람들은 모두 여러분이 저지른 짓이라고 생각하게 됩니다. 다시 말해 여러분의 비밀번호를 아는 누군가가 여러분이 원하지 않는 일을 한다면 사람들은 여러분이 했다고 생각할 거예요. 그래서 비밀번호를 공유하지 않는 것이 정말 중요합니다.

예: 친구에게 소셜 미디어 계정의 비밀번호를 공유한다고 가정합니다. 그 친구가 여러분의 계정으로 로그인하여 같은 반에 있는 누군가에게 '숙제 답 좀 보내줄래?'하고 메시지를 보냅니다. 메시지를 받은 학생은 다음날 학교에서 여러분이 숙제의 답을 보여달라고 했다고 선생님께 말합니다. 그러면서 여러분이 비밀번호를 공유한 친구가 여러분의 계정으로 보낸 메시지를 선생님께 보여줍니다. 선생님은 누구 말을 믿을까요? 이 일이 여러분의 평판에 어떤 영향을 미칠까요? 또 어떤 일이 일어날 수 있을까요?

반 친구들과 함께 어떤 일이 일어날지 생각해 보세요. 예: 선생님이 집으로 전화를 할 수 있습니다. 숙제 점수가 깎일지도 모릅니다. 내 디지털 발자국이 내가 학교에서 부정행위를 하려고 한 것처럼 보이게 만듭니다. 그 메시지를 보낸 친구와 싸우게 됩니다.

여러분의 디지털 발자국은 온라인에서 여러분을 나타낸다는 점을 기억하세요. 누군가와 비밀번호를 공유하면 내 디지털 발자국의 제어 권한을 주는 것이며, 이로 인해 인터넷을 비롯한 어느 곳에서나 사람들이 생각하는 내 모습에 영향을 미칠 수 있습니다. 함께 더 깊이 생각해 봅시다.

다음 페이지에 계속 →

학습 활동



필요한 자료:

- 워크시트: "그건 제가 한 게 아닌데요!" (학생 2인 1조마다 하나씩)

1. 학생들이 짝을 짓도록 합니다.

2. 계정을 선택합니다.

학생이 어떤 계정(소셜 미디어 계정, 게임 계정, 휴대전화, 태블릿/컴퓨터, 스트리밍 서비스 등)의 비밀번호를 공유할지 선택하고 워크시트 상단에 적습니다.

3. 행동을 선택합니다.

파트너가 아래 선택지에서 선택한 행동 또는 직접 생각한 행동을 첫 번째 상자에 적습니다. 이 행동은 계정의 비밀번호를 받은 사람이 하는 행동입니다. 생각한 행동을 그리거나 적거나 다음 행동 중 하나를 선택합니다.

- 좋아하는 사람이 최근에 남긴 게시물에 모두 '좋아요'를 누른다.
- 10만원 어치 옷을 산다.
- '가연이 너무 짜증 나지 않아?'와 같은 메시지를 보낸다.
- 내가 좋아하는 게임을 플레이하면서 점수를 잃는다.
- 새로운 앱을 다운로드한다.
- 내 소셜 미디어 페이지에 부끄러운 사진을 공유한다.
- 내 문자 메시지를 모두 읽고 다른 사람에게 공유한다.
- 부적절한 TV 프로그램을 시청한다.

4. 결과를 만듭니다.

학생이 자신이 선택하거나 생각한 행동의 결과로 일어날 수 있는 일을 두 번째 상자에 적습니다.

5. 토론

전체 학생 중 몇 명에게 자신이 선택한 행동과 그로 인한 결과를 발표시킵니다.

발표가 끝나면 파트너에게 다음과 같이 질문할 수 있습니다.

- 왜 그 행동을 선택(생각)했나요?
- 그 결과를 어떻게 생각했나요?
- 이런 결과가 나타날 줄 알았다면 다른 행동을 했을 것 같나요?

6. 디지털 발자국

학생이 마지막 상자에 이 행동과 그 결과가 자신의 감정, 삶, 디지털 발자국 중 하나 또는 전부에 미치는 영향을 한 문장으로 적습니다. 이 일이 내 평판, 즉 나에 관한 다른 사람의 생각에 어떤 영향을 미치는지 생각해 보도록 학생을 지도합니다. 학생이 그린 그림이나 적은 내용과 자신이 만든 이야기에 관해 어떻게 생각하는지 자원해서 발표하도록 하거나 한 조를 골라 발표하게 합니다.

비밀번호를 공유할 때는 다른 사람에게 내 디지털 발자국의 제어 권한을 주는 것입니다. 그러나 그 사람이 내 디지털 발자국으로 하는 일에 대한 책임은 나에게 있습니다. 사람들이 온라인에서 나를 어떻게 생각하는지 내가 직접 제어하고 싶다면 부모님이나 완전히 신뢰하는 다른 어른을 제외하고는 아무에게도 비밀번호를 공유하지 마세요.

정리

워크시트: 1차시

그건 제가 한 게 아닌데요!

비밀번호를 공유한 계정:

☐ 소셜 미디어 계정

☐ 게임 계정

☐ 휴대전화

☐ 태블릿/컴퓨터

☐ 스트리밍 서비스

☐ _____

행동

결과

디지털 발자국의 영향

효과적인 비밀번호를 만드는 방법

안전한 비밀번호를 만들고 비밀번호를 만든 후 안전하게 지키는 방법을 알아봅니다.

학습 목표



- ✓ **인식:** 부모님이나 보호자를 제외하고는 누구와도 비밀번호를 공유하지 않는 것의 중요성을 인식합니다.
- ✓ **이해:** 기기를 보호하는 화면 잠금의 중요성을 이해합니다.
- ✓ **인지:** 추측하기는 어렵지만 기억하기는 쉬운 비밀번호를 만드는 방법을 인지합니다.
- ✓ **선택:** 2단계 인증 등 로그인 설정에 적절한 보안 방법을 선택합니다.

토론 주제



소 잃고 외양간 고치기 전에 조치를 취해야 합니다.

디지털 기술 덕분에 친구, 학급의 학생들, 선생님, 친척과 소통하기가 쉬워졌습니다. 이들과 휴대전화와 태블릿, 노트북, 디지털 어시스턴트에서 말, 사진, 동영상을 사용하여 문자 메시지나 게임, 게시물, 메시지를 통해 다양한 방식으로 연결할 수 있습니다. (여러분은 **친구**와 어떻게 소통하나요?)

하지만 정보를 쉽게 공유할 수 있게 해주는 이런 도구가 해커와 사기범이 정보를 훔쳐 우리의 기기를 손상시키고 우리의 신원을 도용하거나 관계와 평판을 해치는 데도 사용될 수 있습니다.

우리 자신과 우리의 정보, 그리고 기기를 보호하려면 간단하게는 휴대전화에 화면 잠금을 설정하고, 잠겨 있지 않거나 학교에서처럼 많은 사람이 사용하는 기기에는 개인 정보를 저장하지 않도록 주의해야 하며, 무엇보다도 안전한 비밀번호를 만들어 **누구에게도 공유하지 말아야 합니다.**

- 사람들이 가장 많이 사용하는 비밀번호 두 가지가 뭘까요? (답: “1 2 3 4 5 6”과 “password”)
- 이렇게 안전하지 않은 비밀번호로는 무엇이 있고, 그런 비밀번호가 왜 안전하지 않은지 생각해 봅시다. (예: 내 성과 이름, 전화번호, '초콜릿', 반려견의 이름, 주소 등)

이 비밀번호가 안전하다고 생각하는 사람이 있나요? ;)

학습 활동



필요한 자료:

- 학생 또는 여러 명의 학생이 함께 사용할 인터넷에 연결된 기기
- 화이트보드 또는 프로젝트 화면
- 활동지: '안전한 비밀번호 만들기 가이드라인'

매우 안전한 비밀번호를 만드는 방법입니다.

- 여러분이 기억할 수 있는 재미있는 문구를 생각해 봅시다. 좋아하는 노래 가사나 책 제목, 영화 대사가 될 수도 있습니다.
- 그 문구에 있는 각 단어의 첫 번째 글자나 몇 글자를 선택합니다.
- 글자 몇 개를 기호나 숫자로 바꿉니다.
- 일부는 대문자로, 일부는 소문자로 만듭니다.

비밀번호 게임을 하면서 새로 배운 방법을 연습해 봅시다.

1. 비밀번호 만들기

두 명씩 팀을 나눕니다. 팀마다 60초 동안 비밀번호를 만듭니다.

난이도 옵션: 비밀번호를 정확히 추측하는 데 필요한 맥락이 어느 정도 필요한지 확인하기 위해 학생이 먼저 반 전체에 힌트를 공유합니다.

2. 비밀번호 비교

한 번에 두 팀이 보드에 비밀번호를 적습니다.

3. 투표

비밀번호 쌍에 모두 투표를 해서 어떤 비밀번호가 더 안전한지 논의합니다.

정리

안전한 비밀번호를 만드는 것은 중요하고도 재미있는 일입니다.

활동지: 2차시

안전한 비밀번호 만들기 가이드라인

정보를 안전하게 보호하기 위해 비밀번호를 만드는 팁입니다.

안전한 비밀번호는 여러분은 기억하기 쉽지만 다른 사람은 추측하기 어려운 설명적인 문구나 문장을 기반으로 해야 합니다. 예를 들면 여러분이 가장 좋아하는 게임 타이틀이나 노래에 나오는 여러 단어나 여러분이 했던 일을 나타내는 문장에 나오는 단어의 첫 글자를 기반으로 글자와 숫자, 기호를 조합하면 됩니다. 예를 들어, '나는 3학년 때 서부 초등학교에 다녔다(I went to Western Elementary School for grade 3)'라는 문장으로 lw2We\$t4g3과 같은 비밀번호를 만들 수 있습니다.

보통 수준의 비밀번호는 악성 소프트웨어가 추측하기는 어렵고 안전하지만, 여러분을 아는 사람이라면 추측할 수 있는 비밀번호입니다(예: 'IwenttoWestern').

취약한 비밀번호는 일반적으로 반려견의 이름과 같은 개인 정보를 사용하며 알아내기가 쉽고 여러분을 아는 사람이 추측할 수 있는 비밀번호입니다(예: 'IloveBuddy' 또는 'Ilikechocolate').

권장사항

- 중요한 계정마다 각기 다른 비밀번호를 사용하세요.
- 8자 이상으로 설정하세요. 기억할 수만 있다면 길수록 더 좋습니다.
- 문자(대소문자)와 숫자, 기호를 조합해서 사용하세요.
- 비밀번호를 적어두면 위험하므로 적어둘 필요 없이 기억하기 쉬운 비밀번호를 만드세요.
- 부모님이나 보호자 외에 누군가가 비밀번호를 안다고 생각되면 즉시 비밀번호를 변경하세요.
- 비밀번호를 주기적으로 변경하세요.
- 기기에 강력한 화면 잠금을 사용하세요. 기기가 다른 사람의 손에 들어갈 경우에 대비해 자동으로 잠기도록 설정하세요.
- 브라우저에 내장된 비밀번호 관리자 등을 사용하여 비밀번호를 관리하는 것도 좋습니다. 그러면 계정마다 각기 다른 비밀번호를 사용하면서 전부 기억할 필요가 없습니다.

주의사항

- 이름, 주소, 이메일, 전화번호, 주민등록번호, 엄마의 성, 생일, 반려견의 이름 등 개인 정보를 비밀번호로 사용하지 마세요.
- 별명이나 초콜릿, 학교 이름, 좋아하는 스포츠팀, 연속되는 숫자(123456) 등 추측하기 쉬운 비밀번호를 사용하지 마세요. 'password'를 비밀번호로 사용해서도 안 됩니다.
- 부모님이나 보호자 외에는 누구에게도 비밀번호를 공유하지 마세요.
- 다른 사람이 찾을 수 있는 곳에 비밀번호를 적어두지 마세요.

비밀을 지켜 주세요: 3차시

혼자만 알기

교사는 학교 기기를 사용하여 개인 정보 보호 설정을 변경할 때 어디에서 무엇을 확인해야 하는지 보여줍니다.

학습 목표



- ✓ **맞춤설정:** 사용하는 온라인 서비스의 개인 정보 보호 설정을 맞춤설정합니다.
- ✓ **결정:** 사용하는 사이트와 서비스에서 공유할 정보를 결정합니다.
- ✓ **이해:** 2단계 인증(2단계 확인)이 무엇이고 언제 사용하는지 이해합니다.

토론 주제



개인 정보 보호 및 보안

온라인 개인 정보 보호와 온라인 보안은 긴밀하게 연결되어 있습니다. 대부분의 앱과 소프트웨어에서는 우리가 공유하는 정보의 종류와 방식을 제어하는 방법을 제공합니다.

- 앱이나 웹사이트를 사용할 때 '내 계정'이나 '설정'과 같은 옵션을 찾아보세요. 거기에서 개인 정보 보호 및 보안 설정을 찾아 다음과 같은 사항을 결정할 수 있습니다.
- 내 페이지 또는 프로필에 표시되는 정보
 - 내 게시물, 사진, 동영상 또는 내가 공유하는 콘텐츠를 볼 수 있는 사람

개인 정보를 보호하기 위해 이런 설정을 사용하는 방법을 배우고 이 설정을 잊지 않고 최신 상태로 유지한다면 개인 정보와 보안, 안전을 관리하는 데 도움이 될 것입니다.

설정도 중요하지만 누가 여러분과 친구를 맺거나 여러분을 팔로우할 수 있는지도 생각해 봐야 합니다. 이 옵션은 설정에 없을 수도 있습니다. 오프라인 친구와 가족만 나를 팔로우하게 하거나 내 친구 목록에 추가하는 것이 가장 안전한 방법입니다. 다른 사람을 허용한다면 여러분이 한 번도 만난 적 없는 사람이 여러분이 공유하는 콘텐츠를 볼 수도 있다는 사실을 잊어서는 안 됩니다. 이로 인해 조금 무서운 일이 일어날 수도 있고 때로는 모르는 사람의 팔로우를 부모님이 전혀 허용하지 않는 경우도 있습니다. 여러분이 신뢰하는 어른과 상의하면서 여러분에게 가장 좋은 방법, 즉 여러분의 안전을 지키면서 여러분이 가장 안심할 수 있는 방법이 무엇인지 알아보세요.

이런 결정은 **언제나** 부모님이나 보호자와 함께 내려야 합니다. 부모님이나 보호자와 개인 정보 보호 설정을 함께 살펴보는 일은 재미있을 수도 있습니다. 여러분이 얼마나 똑똑한지 부모님이나 보호자에게 보여줄 수 있으니까요.

학습 활동



필요한 자료:

- 수업 중 시연에 적절한 예시 계정(예: 임시 이메일이나 학급 계정)을 보여줄 수 있는 학교 기기를 프로젝터에 연결

검토 항목

학교 기기를 프로젝터 화면에 연결했습니다. 함께 이 앱의 설정 페이지로 가서 어떤 옵션이 있는지 확인해 봅시다. 여러분의 도움이 필요합니다. [학생들이 다음과 같은 설정을 도울 수 있도록 지도]

- 비밀번호 변경하기
- 페이지 또는 사진과 동영상을 포함하는 온라인 프로필을 공개 또는 비공개(내가 선택한 가족과 친구만 볼 수 있음)로 설정하기
- 위치와 기타 설정 확인하기: 여러분에게 가장 좋은 선택지는 무엇인가요?
- 누군가가 알 수 없는 기기에서 내 계정에 로그인하려고 할 때 알림 받기

비밀을 지켜 주세요: 4차시

Interland: 보물의 탑

지원 요청! 보물의 탑이 잠금 해제되어 Internaut의 연락처 정보와 개인 메시지 등 소중한 정보가 큰 위험에 노출되었습니다. 해커보다 먼저 안전한 비밀번호로 요새를 쌓아서 비밀을 영구적으로 안전하게 보호하세요.

데스크톱이나 태블릿 같은 모바일 기기에서 웹 브라우저를 열고 g.co/TowerOfTreasure로 이동합니다.

토론 주제



학생들이 보물의 탑을 플레이하도록 하고 아래 질문을 사용하여 게임에서 얻은 교훈에 관한 심층 토의를 진행합니다. 혼자 플레이해도 좋지만 짝을 지어도 됩니다. 어린 학생들에게 특히 좋은 방법입니다.

- 안전한 비밀번호는 무엇으로 구성되나요?
- 실제 생활에서 안전한 비밀번호를 만들어야 하는 경우는 언제인가요? 안전한 비밀번호를 만드는 방법에 관해 어떤 팁을 얻었나요?
- 해커란 무엇인가요? 이 캐릭터의 행동을 설명하고 게임에 어떤 영향을 미쳤는지 설명해 주세요.
- 보물의 탑으로 인해 앞으로 정보를 어떻게 보호할지 여러분의 계획이 바뀌었나요?
- 이 강의를 듣고 게임을 플레이한 후 행동의 변화가 생길 것 같은 점 하나를 이야기해 주세요.
- '안전한 비밀번호' 테스트를 통과할 수 있는 비밀번호 3개를 연습 삼아 만들어 보세요.
- 보호해야 하는 민감한 정보에는 어떤 것이 있나요?

정리

- 누군가가 나를 태그할 때 알림 받기
- **2단계 인증(2단계 확인) 사용하기**
- **계정에 로그인할 수 없는 경우를 대비해 복구 정보 설정하기**
- **문제 신고하기**

어떤 개인 정보 보호와 보안 설정이 여러분에게 적합한지를 부모님이나 보호자와 논의해야 합니다. 하지만 가장 중요한 보안 설정은 여러분의 머릿속에 있다는 점을 기억하세요. 여러분이 성장할수록 어떤 개인 정보를 공유할지, 언제 공유할지, 누구와 공유할지를 스스로 더 많이 결정하게 될 거예요. 지금부터 그런 결정을 내리는 방법을 익혀야 합니다.

중요한 계정마다 각기 다른 안전한 비밀번호를 선택하는 것이 중요한 첫 단계입니다. 이제 비밀번호를 기억하고 안전하게 보호해야 합니다.