

03

정보 보안과 디지털 윤리

- + 학습 목표**
 - 정보 보안의 필요성을 설명할 수 있다.
 - 정보 보안 기술을 활용하여 디지털 윤리를 실천할 수 있다.
- + 학습 요소**
 - 정보 보안, 정보 보안 기술, 디지털 윤리 실천 방안

생각 깨우기

다음 글과 그림을 보고 생각해 보자.

우리의 소중한 정보를 보호하기 위해서는 다양한 노력이 필요하다. 당장 실천할 수 있는 쉬운 노력은 내가 사용하는 비밀번호들을 자주 변경하는 것이다.



Q

정보 보안을 실천하기 위해 또 어떤 노력이 필요할까?

1 | 정보 보안의 이해

01 정보 보안의 개념

인터넷과 스마트폰, 컴퓨터 등의 발달은 정보의 빠른 유통과 함께 우리 사회에 많은 변화를 가져왔다. 스마트폰만 있으면 언제 어디서나 은행 거래가 가능해졌고, 버스나 지하철을 편하게 이용할 수 있다. 하지만 이런 편리함 속에는 해킹이나 피싱처럼 다양한 개인 정보가 유출될 위험이 존재하기 때문에 우리의 정보를 지키기 위한 노력이 필요하다.



정보 보안이란 외부의 불법적인 접근으로부터 정보를 보호하는 것으로, 정보의 수집, 가공, 전송 등의 동작이 이루어지는 도중에 훼손, 변조, 유출 등을 방지하는 기술이다. 정보 보안은 정보 보안의 3요소인 기밀성, 무결성, 가용성을 확보하는 데 목적이 있다.



▲ 정보 보안의 3요소 및 목적

해킹(Hacking)

다른 사람의 계정이나 컴퓨터 시스템에 무단으로 침입하여 데이터를 빼내거나 파괴하는 등의 행위를 말한다.

피싱(Phishing)

개인 정보(Private Data)와 낚는다(Fishing)의 합성어로 이메일이나 메신저 등을 이용하여 위조 사이트로 접속을 유도하여 개인 정보 탈취, 송금, 결제 등의 피해를 입히는 행위이다.

스미싱(Smishing)

문자(SMS)와 피싱(Phishing)의 합성어로, 문자 메시지를 이용한 피싱의 한 종류다.

피밍(Pharming)

피싱(Phishing)과 조작(Farming)의 합성어로 피싱의 진화된 형태로, 위조 사이트로 유도하는 피싱과 달리 위조 사이트로 강제 이동시키는 방법이다.

02 정보 보안의 실천 방안

디지털 기술이 발전하는 만큼 디지털 기술을 이용한 범죄 행위도 많이 발생하고 있다. 바이러스, 스팸 메일, 해킹, 랜섬웨어 등으로 인한 정보 유출은 사생활 침해뿐 아니라 막대한 재산상의 피해로 이어질 수도 있다. 이러한 피해를 방지하려면 정보를 안전하게 보호해야 하는데, 이를 위해서는 꼭 필요한 정보 보안 기술을 활용해야 한다.

정보 보안 실천은 공급자 측면과 사용자 측면에서 살펴볼 수 있다. 정보를 공급하는 입장에서는 내·외부 위협으로부터 네트워크와 시스템을 안전하게 보호해야 하고, 사용자 입장에서는 개인 정보의 유출이나 남용을 방지하기 위한 조치가 있어야 한다.

정보 공급자는 정보 생산자, 정보 제공자, 정보 관리자로 구분할 수 있다.

🔒 정보 보안 기술

암호화, 인증, 네트워크 보안 등이 있다.

⚙️ 정보 생산자

개발자, 인터넷 사업자 등

⚙️ 정보 제공자

포털 사업자, SNS 사업자 등

⚙️ 정보 관리자

호스팅 업체, 데이터 센터 등

정보 생산자

- 각종 콘텐츠의 개발과 생산, 가공을 통한 재생산을 통해 정보를 만들어낸다.
- 콘텐츠를 개발하고 생산하는 과정에서 사생활을 보호하고 저작권 침해가 발생하지 않도록 주의해야 한다.

정보 제공자

- 콘텐츠 배포 및 공급을 담당한다.
- 정보 생산자의 콘텐츠를 점검하고 악성 코드, 바이러스 등의 침입을 제한하여 안정성을 확보해야 한다.

정보 관리자

- 콘텐츠의 유통을 위한 서버 및 통신망을 관리하고 운영한다.
- 시스템을 해킹과 바이러스 등으로부터 안전하게 보호해야 하며, 개인 정보 침해가 발생하지 않도록 보호하고, 장애가 발생하였을 때 신속하게 복구해야 한다.

▶ 정보 보안 실천 방법

정보를 사용하는 사용자도 정보 보안을 위해 노력해야 한다. 컴퓨터의 비밀번호를 안전하게 설정하고 주기적으로 변경하며 백신과 보안 패치를 항상 업데이트한다. 또한 컴퓨터에 남아 있는 불필요한 개인 정보를 삭제하는 등 철저히 관리해야 한다.

🔒 보안 패치(Security Patch)

운영 체제나 응용 프로그램의 보안 취약점을 보완하는 소프트웨어로, 악성 코드 감염을 방지하고 컴퓨터 오류의 원인을 제거한다.

정보 공급자

내·외부 위협으로부터 네트워크와 시스템 보호, 사생활 및 저작권 침해 주의, 안정성 확보 등



정보 보안 실천

정보 사용자

개인 정보 유출, 남용 방지 조치(비밀번호, 백신 업데이트)



해 보기 1 나의 개인 정보 보호 점검하기

🗣️ 나의 정보 보안 실천을 위해 무엇을 해야 하는지 작성해 보자.

• 나의 정보 보안 실천 사항:

2 | 정보 보안 활용과 디지털 윤리의 실천

01 디지털 윤리

디지털 윤리란 디지털 기기를 활용하는 디지털 환경을 포함하여 디지털화된 사회를 살아가는 데 필요한 윤리적인 것과 비윤리적인 것을 바르게 판단하는 규범적 기준이다. 이는 인터넷, 가상 공간, 소셜 미디어 등 디지털 기술이 인간의 삶과 사회에 미치는 영향과 관련이 있으며, 디지털 윤리의 부재로 인해 개인 정보 유출, 사이버 사기, 해킹, 랜섬웨어 등의 범죄가 발생하기도 한다.

디지털 윤리를 실천하기 위해서는 온라인 환경에서 스스로를 보호하고, 다른 사람에게 피해를 끼치지 않도록 조심해야 한다. 기술이 발달하면서 사회적으로도 많은 발전을 이루었는데, 윤리 의식이 이를 따라가지 못하면 디지털 환경을 이용한 범죄도 증가하게 된다. 특히 디지털 기술을 기반으로 하는 범죄는 점점 치밀해지고 피해 규모도 커지고 있다.

트래픽

컴퓨터 네트워크에서 일정 시간 내에 흐르는 정보의 이동량을 말한다.

딥페이크(Deep Fake)

인공지능 기술을 활용해 특정 인물의 얼굴이나 특정 부위를 합성한 영상 편집물이다.

해킹(Hacking)



사용자 계정이나 컴퓨터 시스템에 무단으로 접근하여 장치와 네트워크를 손상하는 행위

[피해 사례]
미국의 거대 유통 기업이 1억 명이 넘는 고객의 금융 정보를 해킹당해 수천만 달러를 배상하였다.

디도스(DDos: Distributed Denial of Service)



'분산 서비스 거부 공격'이라고도 하며, 좀비 PC를 이용하여 대량의 트래픽을 유발해 시스템을 마비시키는 공격

[피해 사례]
국내 한 대학의 서버가 공격당해 2학기 수강 신청이 중지되는 피해가 발생하였다.


랜섬웨어(Ransomware)



컴퓨터를 감염시켜 접근을 제한한 뒤 정상 작동의 대가로 금품을 요구하는 유형의 악성 소프트웨어

[피해 사례]
해커가 한 대기업의 자료를 랜섬웨어로 감염시키고 요구한 금액이 지불되지 않자 모든 자료를 인터넷에 공개하였다.

피싱(Phishing)




이메일을 통해 가짜 금융 기관 웹사이트로 유도하여 개인 정보를 탈취하는 디지털 범죄(보이스 피싱, 메신저 피싱, 스미싱 등)

정상 문자 사례	피해 사례
<ul style="list-style-type: none"> [행정안전부] 신종 코로나바이러스 감염증 예방을 위해 손씻기, 기침예절, 마스크착용 등 수칙 준수와 발열 호흡기 증상 발생 시 1339 또는 보건소로 상담바랍니다. [서울시재난대책본부] 신종 코로나바이러스 대응 단계로 격상(1.27) 응급방문 후 발열, 호흡기 증상 발생시 1339 또는 보건소로 문의하시기 바랍니다. 	<ul style="list-style-type: none"> [Web발신] 국내 우형폐렴 급속도 확산 감염자및 접촉자 신분정보 확인하기 news.naver.com kr [Web발신] 코로나 전염병원자 유통소에서 수많은 사람과 접촉 http://.../pDX 접속 유통소 확인

디지털 성범죄

디지털 기기를 이용하여 상대방의 동의 없이 신체 일부나 성적인 장면을 불법 촬영하거나 합성, 유포, 협박, 저장, 전시, 유통, 소비하는 행위 및 사이버 공간에서 타인의 성적 자율권과 인격권을 침해하는 행위

[피해 사례]
딥페이크를 이용한 디지털 성범죄가 매년 증가하고 있으며, 연예인을 대상으로 하던 범죄가 일반인까지 그 범위가 넓어지고 있다. 한 남성이 딥페이크를 이용해 생성한 피해자 사진을 온라인에 게시하고 피해자를 협박한 사례가 있다.



▲ 디지털 범죄

02 디지털 윤리 실천하기

pass 앱

사실 전자 인증 서비스로 중요한 정보를 안전하게 관리할 수 있는 암호 관리 애플리케이션이다.

자기 학습형 사이버 면역 기술

시스템에 내재된 소프트웨어의 보안 취약점을 자동으로 탐색하고 원인을 분석하여 업데이트한다.

자기 변이 기술

상황에 따라 보호 대상이 스스로 서버 IP와 PORT 등을 랜덤하게 변화해 능동적인 사전 보안이 가능하게 한다.

디지털 윤리를 실천하기 위해 디지털 환경을 제공하는 생산자, 관리자, 소비자의 올바른 윤리 의식과 함께 적절한 보안 기술을 활용하는 것은 매우 중요하다.

디지털 환경을 제공하는 기관에서는 정보 보안 기술을 이용하여 정보를 보호하기 위해 노력해야 한다. 정보 보안을 위한 기술로는 암호화, 인증, 네트워크 보안이 있다.

구분	정보 보안 기술		
	암호화	인증	네트워크 보안
의미	정보를 읽기 어려운 값으로 변환하여 다른 사람이 볼 수 없도록 하는 기술	적법한 사용자, 올바른 출처를 확인하는 과정이나 행위	네트워크와 데이터의 무결성, 기밀성, 가용성에 대한 공격 및 장애로부터 컴퓨팅 시스템을 보호
종류	단방향 암호화, 비밀키 암호화, 공개키 암호화	pass 앱, 생체 인증, PIN 번호, 공동 인증서 등	악성 코드 차단 소프트웨어, 방화벽, 액세스 제어

▲ 다양한 정보 보안 기술



기술의 발전에 따라 새로운 보안 기술도 도입되고 있다. 생체 신호를 이용한 인증 기술, 사물 인터넷 위협에 대응하는 기술, 자기 학습형 사이버 면역 기술, 능동적 사이버 보안을 위한 자기 변이 기술 등 다양한 보안 기술이 개발되고 있다. 인공지능을 활용하여 악성 코드의 변종을 탐지하는 기술도 속 속 등장하고 있다.

개인도 정보 보호를 위해 노력해야 한다. 평소 컴퓨터나 스마트폰 등의 전자 기기를 사용할 때 정보 보안 설정 기술을 활용하거나 비밀번호를 주기적으로 바꾸는 등의 노력이 필요하다.

소단원 요약

- 1 정보 보안은 정보의 수집, 가공, 전송 등의 동작이 이루어지는 도중에 훼손, 변조, 유출 등을 방지하는 기술이다.
- 2 정보 보안은 공급자 측면과 사용자 측면에서 살펴볼 수 있다. 정보를 공급하는 입장에서는 내·외부 위협으로부터 네트워크와 시스템을 안전하게 보호해야 하고, 사용자 입장에서는 개인 정보의 유출이나 남용을 방지하기 위한 조치를 해야 한다.
- 3 디지털 윤리는 디지털 기기를 활용하는 디지털 환경을 포함하여 디지털 사회를 살아가는 데 필요한 윤리적인 것과 비윤리적인 것을 바르게 판단하는 규범적 기준이다.

소단원 자기 평가

평가 항목	평가 기준		
	잘함	보통	노력
1. [지식이해] 정보 보안의 필요성을 설명할 수 있다.			
2. [과정기능] 정보 보안 기술이 필요한 문제를 발견하고 해결 방법을 적용하여 디지털 윤리를 실천할 수 있다.			



스마트폰에 정보 보안 기술 적용하기

☺ 아침에 일어나서 잠들 때까지 항상 스마트폰과 함께한다고 해도 과언이 아닐 정도로 스마트폰은 우리의 생활 속에 깊숙이 들어와 있다. 전화, 문자는 물론 SNS, 알람, 은행 업무 등 다양하게 **스마트폰**을 활용하고 있는 만큼 개인 정보 보호를 위한 보안 설정이 올바르게 되어 있는지 확인해 보자.

1 스마트폰에 설치된 앱 중에서 자주 사용하는 앱 3가지를 적어 보자.

2 선택한 앱에서 사용되는 권한이 무엇인지 확인해 보자.

3 모둠을 구성하여 학생별로 선택한 앱과 사용되는 권한을 확인하고 불필요한 권한을 요구하는 앱이 무엇인지 작성하고, 왜 불필요한지 발표해 보자.

4 디지털 윤리 실천을 위해 정보 보안 기술을 어떻게 활용하고 있는지 적고 친구와 함께 디지털 윤리 실천 방법에 관해 토의해 보자.

내가 활용하는 정보 보안 기술	디지털 윤리 실천 방안
예 생체 정보를 이용한 스마트폰 잠금 설정	예 컴퓨터 이용 시 해킹 등으로 개인 정보가 유출되지 않도록 방화벽을 설정해야 한다.

탐구활동 자기평가	평가 항목	평가 기준		
		잘함	보통	노력
1.	정보 보안의 필요성을 이해하고, 정보 보안을 위해 스마트폰의 권한 설정을 할 수 있는가?			
2.	디지털 윤리 실천을 위해 정보 보안 기술을 활용할 수 있는가?			

• 잘함 (내용을 이해하고 설명함) • 보통 (내용을 이해함) • 노력 (내용을 부분적으로 이해함)