이름: _____ 날짜: _____ 점수: _____

내 IP 주소를 숨기는 방법 워크시트

IP 주소 숨기기, 위치 마스킹, 프록시, Tor, DNS/WebRTC 누출 방지

VPN 학습 개요

학습자
학생 신분
네트워크 수비 트랙

보안
연결 상태
데이터 패킷 보호하기

켜짐
유출 방지
DNS 및 IPv6 유출 방지

환영합니다! 이 활동 자료집은 가상 사설망(VPN)의 기본 원리를 안내합니다. 암호화된 터널이 데이터를 보호하는 방식, 네트워크 프로토콜이 작동하는 방식, 개인정보 누출을 찾아내고 줄이는 방법을 살펴봅니다.

워크시트 체크포인트

- ☐ **파트 1-4: VPN 개념과 프로토콜을 익힙니다.**
- ☐ **파트 5-7: 십자말풀이와 단어 찾기 퍼즐을 풉니다.**
- ☐ **파트 8-9: 사례 연구와 암호 도전 과제를 풉니다.**
- ☐ **파트 10: 기초 및 심화 FAQ 페이지를 살펴봅니다.**
- ☐ **파트 11: 흥미로운 실제 사실 10가지를 살펴봅니다.**
- ☐ **보너스: 빠르게 생각하기 도전**

VPN.com VPN 가이드 열기

URL: https://www.vpn.com/vpn/

나의 VPN 학습 로드맵

- IP 주소가 어떻게 작동하며 어떻게 위치를 유출하는지 설명하세요.
- 네트워크 주소를 숨기는 데 쓰이는 프록시, Tor, VPN을 비교하세요.
- DNS 및 WebRTC 누출을 탐지하고 예방하는 방법을 파악하세요.
- 웹사이트가 공용 IP로 사용자를 어떻게 추적하는지 이해합니다.
- IP 보호를 위한 멀티홉 라우팅과 암호화 터널을 평가하세요.

IP 보호 워크시트 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. IP 주소 숨기기와 누출 방지에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

내 IP 숨기기 (소개)

IP 주소는 실제 위치와 네트워크 사용 습관을 드러내는 디지털 우편 주소입니다. IP를 숨기는 것은 온라인 추적, 표적 프로파일링, 위치 기반 차단에 맞서는 첫 번째 방어선입니다. 주소를 안전하게 가리는 방법을 이해하면 온라인에서 개인정보를 보호하는 데 도움이 됩니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 기기의 공인 IP 주소는 내가 방문하는 웹사이트에 무엇을 알려 줍니까?

- A. 사용자의 신용카드 번호
- B. 대략적인 위치와 인터넷 서비스 제공업체 이름
- C. 전체 로컬 파일 디렉터리
- D. 키보드 언어 설정

2 2. IP를 숨기고 시스템 전체의 모든 트래픽을 암호화하는 방법은 무엇입니까?

- A. 표준 웹 프록시
- B. 브라우저 쿠키 삭제하기
- C. 가상 사설망(VPN)
- D. 기본 방화벽 비활성화하기

3 3. 무료 웹 프록시를 사용할 때의 주요 개인정보 보호상 한계는 무엇입니까?

- A. 공용 네트워크에서 데이터 트래픽을 암호화하지 않음
- B. 외부 운영 체제를 설치해야 한다
- C. 미국에서는 완전히 불법이다
- D. 전용 전화선 연결이 필요하다

4 4. Tor 네트워크는 어떻게 사용자에게 높은 익명성을 제공합니까?

- A. 연결 속도를 높여서
- B. 자원봉사자가 운영하는 세 개의 릴레이를 거쳐 트래픽을 보내서
- C. 이름을 전 세계 데이터베이스에 등록해서
- D. 정부 기관만 접속하도록 제한해서

5 5. DNS 유출이란 무엇입니까?

- A. 이메일을 잘못된 주소로 보내는 오류
- B. DNS 쿼리가 VPN 터널을 우회해 ISP로 갈 때
- C. 로컬 라우터 전원 공급 장치의 하드웨어 고장
- D. 로컬 네트워크 어댑터 드라이버 업데이트

체크포인트 2: 참/거짓 도전

6 질문 6

6. 프록시 서버는 VPN처럼 백그라운드 OS 트래픽을 암호화합니다.

○ 참 ○ 거짓

7 질문 7

7. Tor 라우팅은 보안성이 매우 높지만 네트워크 탐색 속도가 느려집니다.

○ 참 ○ 거짓

8 질문 8

8. WebRTC 유출은 VPN 세션이 활성화된 동안에도 실제 IP를 노출할 수 있습니다.

○ 참 ○ 거짓

9 질문 9

9. VPN을 켜고 누출이 없다면 인터넷 서비스 제공업체는 내가 방문하는 웹사이트를 볼 수 없습니다.

○ 참 ○ 거짓

10 질문 10

10. IP 주소를 숨기면 브라우저 핑거프린팅을 통한 추적이 차단됩니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

아래 각 문장을 읽고 단어 목록에서 알맞은 용어를 골라 빈칸을 채우세요.

1. 보안 터널을 우회하여 도메인 조회 정보를 노출하는 현상을 _____ (이)라고 합니다.
2. 브라우저 기반 _____ 통신 API는 실수로 고유 IP 주소를 유출할 수 있습니다.
3. 웹 _____ 은(는) 브라우저 트래픽을 우회시키지만 패킷 페이로드는 암호화하지 않습니다.
4. _____ 네트워크의 다중 계층 암호화는 높은 수준의 익명성을 제공합니다.
5. 공인 _____ 은(는) 통신사가 할당하며 사용자의 지역을 드러냅니다.
6. 지역 미디어 차단을 우회하는 것은 _____ 마스킹을 통해 이루어집니다.

어휘 단어 목록

분할 터널링 | 위치 | 프록시 | DNS 유출 | IP 주소 | ISP 추적 | Tor | WebRTC

여기에 답을 쓰세요:

1.
2.
3.
4.
5.
6.

체크포인트 4: 네트워크 개념 연결

정의 연결하기

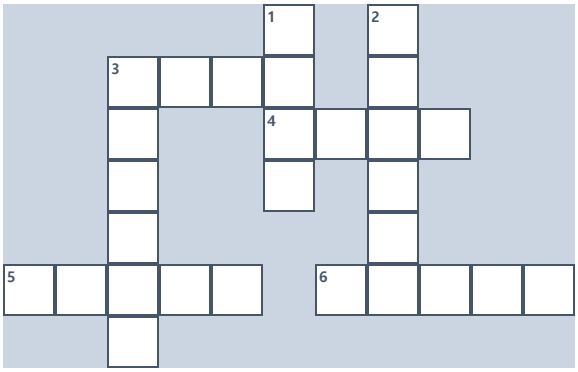
왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. IP 주소**	**A**	기기의 모든 트래픽을 암호화하여 VPN 서버를 거쳐 보냅니다.
☐	**2. VPN 터널**	**B**	자원봉사자가 운영하는 서버 세 개를 거쳐 데이터를 라우팅하며 단계마다 계층을 암호화합니다.
☐	**3. Tor 네트워크**	**C**	지역 차단을 우회하기 위해 다른 나라의 서버를 거쳐 연결을 라우팅하는 것.
☐	**4. 웹 프록시**	**D**	인터넷에서 기기 인터페이스를 식별하는 고유한 숫자 라벨입니다.
☐	**5. DNS 유출**	**E**	시스템 암호화 없이 애플리케이션 계층에서 브라우저 트래픽을 우회시킵니다.
☐	**6. WebRTC API**	**F**	통신사가 암호화되지 않은 인터넷 트래픽의 목적지를 기록하는 것입니다.
☐	**7. 위치 가리기**	**G**	VPN 터널 밖에서 처리되어 방문한 도메인이 ISP에 노출되는 쿼리입니다.
☐	**8. ISP 추적**	**H**	터널을 우회해 실제 IP 주소를 노출할 수 있는 음성/영상용 브라우저 기능입니다.

© VPN.com | VPN 워크시트

체크포인트 5: 십자말풀이

활성화된 흰색 칸에 글자를 입력해 십자말풀이를 푸세요. 숫자는 아래 열쇠에 해당합니다.



가로

3. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4)

4. 기기가 현재 어느 곳에 있는지를 나타내는 지리적 정보 (4)

5. 인터넷에서 기기 인터페이스를 식별하는 고유한 숫자 표시 (5)

6. 기기의 모든 트래픽을 암호화해 VPN 서버를 거쳐 보내는 연결 (5)

세로

1. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4)

2. 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일 (6)

3. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜 (6)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

화면 낭독기와 키보드 사용자는 아래 입력란에 십자말풀이 정답을 직접 입력할 수 있습니다.

가로

3 가로: 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4 글자):

4 가로: 기기가 현재 어느 곳에 있는지를 나타내는 지리적 정보 (4 글자):

5 가로: 인터넷에서 기기 인터페이스를 식별하는 고유한 숫자 표시 (5 글자):

6 가로: 기기의 모든 트래픽을 암호화해 VPN 서버를 거쳐 보내는 연결 (5 글자):

세로

1 세로: VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4 글자):

2 세로: 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일 (6 글자):

3 세로: 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜 (6 글자):

체크포인트 6: 숨은 단어 찾기

아래 격자에 숨어 있는 핵심 어휘 8개를 찾으세요. 단어는 가로, 세로, 대각선으로 배치될 수 있습니다.

다	서	피	하	크	오	주	엔	도	타	밀	개	접	화	트
공	널	비	라	주	카	다	시	오	방	속	크	킬	카	파
라	터	전	크	기	도	이	안	연	픈	보	격	넷	타	바
스	화	링	다	트	인	청	술	기	링	소	연	스	색	다
험	호	넷	파	넷	개	널	번	분	공	치	스	버	공	비
자	암	리	기	버	인	전	아	관	번	공	킬	스	위	치
널	격	결	아	소	정	템	도	이	하	벽	인	바	가	마
링	사	속	치	벽	보	넷	브	화	피	널	주	방	타	험
널	번	터	카	기	보	전	이	화	위	주	개	트	데	데
터	위	리	스	소	호	주	트	사	템	격	소	연	호	시
할	오	픈	브	이	피	엔	바	색	카	도	할	응	아	위
분	링	색	버	방	크	킬	카	이	타	험	픈	개	치	사
요	마	가	킬	송	카	화	나	타	결	타	안	정	워	술
카	리	위	번	하	기	시	링	템	안	험	보	답	보	나
다	험	접	전	개	소	치	격	넷	리	소	스	차	이	엔

어휘 단어 목록

아이피주소 오픈소스 개인정보보호 암호화터널 위치정보 오픈브이피엔 분할터널링 킬스위치

체크포인트 6 대체 활동: 접근성을 고려한 어휘 연결

단어 찾기의 8개 어휘를 각각 알맞은 설명과 연결하고, 빈칸에 글자(A-H)를 쓰세요.

어휘 용어
A. 아이피주소
B. 오픈소스
C. 개인정보보호
D. 암호화터널
E. 위치정보
F. 오픈브이피엔
G. 분할터널링
H. 킬스위치

정의 및 연결 항목
1. 기기의 모든 트래픽을 암호화해 VPN 서버를 거쳐 보내는 연결.
2. 선택한 앱만 VPN을 거치지 않고 직접 연결하게 하는 기능.
3. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
4. 인터넷에서 기기 인터페이스를 식별하는 고유한 숫자 표시.
5. 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일.
6. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능.
7. 기기가 현재 어느 곳에 있는지를 나타내는 지리적 정보.
8. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.

© VPN.com | VPN 워크시트

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 VPN 개념과 용어를 알아내세요. 정답을 입력란에 쓰세요.

1. 주 피 아 소 이 _____

2. 호 개 정 보 보 인 _____

3. 보 위 정 치 _____

4. 터 링 널 분 할 _____

5. 스 오 소 픈 _____

6. 터 암 화 널 호 _____

7. 피 오 이 엔 브 픈 _____

8. 킬 치 위 스 _____

보너스 활동: 빠르게 생각하기

각 범주마다 답을 3개씩 쓰세요. 목록을 가장 먼저 채운 사람이 이깁니다.

1	여행 중에 VPN을 사용하는 이유			
2	알고 있는 브라우저			
3	VPN이 숨길 수 있는 것			
4	개인정보 보호와 관련된 단어			
5	이 워크시트에서 기억하고 싶은 단어			
6	웹사이트가 IP로 추측할 수 있는 것			
7	IP 주소에 들어 있는 숫자나 기호			
8	VPN에 대한 오해			
9	알고 있는 VPN 서비스			
10	인터넷 서비스 제공업체가 볼 수 있는 것			
11	좋은 VPN 제공업체가 하는 약속			
12	실제 IP를 노출시킬 수 있는 것			
13	위치를 숨기는 이유			
14	IP 주소를 숨기는 방법			
15	VPN을 사용할 수 있는 기기			

© VPN.com | VPN 워크시트

체크포인트 8: VPN 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사라(카페에 있는 학생)

👩‍💻 "안녕하세요! 저는 Coffee & Bytes에 앉아 있어요. 'Free_Wi-Fi_No_Password'라는 보안이 없는 공용 네트워크가 있어요. 학교 이메일에 로그인하고 과제를 올리고 싶은데 해커가 걱정돼요. VPN 없이 이 네트워크를 쓰면 어떤 위험이 있고, VPN은 제 데이터를 어떻게 보호하나요?"

Alex(여행하는 학생)

👨‍💻 "큰일 났어요! 프로젝트 때문에 해외에 와 있는데 우리나라 서버에서 호스팅되는 생물 다큐멘터리를 보려고 해요. 그런데 사이트에 '현재 위치에서는 이 동영상을 볼 수 없습니다.'라고 떠요. 왜 차단되는 걸까요, VPN은 어떻게 도움이 될까요?"

체크포인트 9: 암호 해독하기

IP 숨기기 학습을 마치려면 디지털 흔적을 숨기는 것에 관한 이 비밀 메시지를 해독하세요.

자모-숫자 암호화 키

ㄱ=1 ㄲ=2 ㄴ=3 ㄷ=4 ㄸ=5 ㄹ=6 ㅁ=7 ㅂ=8 ㅃ=9 ㅅ=10
ㅆ=11 ㅇ=12 ㅈ=13 ㅉ=14 ㅊ=15 ㅋ=16 ㅌ=17 ㅍ=18 ㅎ=19 ㅏ=20
ㅐ=21 ㅑ=22 ㅒ=23 ㅓ=24 ㅔ=25 ㅕ=26 ㅖ=27 ㅗ=28 ㅘ=29 ㅙ=30
ㅚ=31 ㅛ=32 ㅜ=33 ㅝ=34 ㅞ=35 ㅟ=36 ㅠ=37 ㅡ=38 ㅢ=39 ㅣ=40

8	28	12	20	3		17	24	3	24	6	6	28		13	33	10	28	6	38	6

1	20	7	15	33	10	25	12	32

해독된 메시지:

팁: 각 숫자는 아래 키의 한글 자모 하나를 나타냅니다. 자모를 차례로 모아 글자를 만드세요(예: ㅂ+ㅗ = 보).

체크포인트 10: 기초 VPN FAQ (파트 A)

가상 사설망(VPN) 사용에 대해 잠재 고객이 가장 자주 묻는 질문과 답을 살펴보세요.

Q1: VPN이란 무엇이며 어떻게 작동하나요?

가상 사설망(VPN)은 인터넷 연결을 암호화하고 트래픽을 안전한 원격 서버를 거쳐 보냅니다. 이렇게 하면 공인 IP 주소가 가려지고, VPN 터널로 전달된 트래픽에 대해 로컬 네트워크 관찰자와 ISP가 볼 수 있는 정보가 제한됩니다.

Q2: 왜 VPN을 사용해야 하나요?

VPN은 디지털 개인정보를 보호하고, 공용 Wi-Fi 네트워크(카페나 공항 등)에서 연결을 안전하게 하며, ISP가 암호화된 트래픽의 종류를 식별하지 못할 때 활동 기반 속도 제한을 줄일 수 있고, 지역 제한을 우회해 해외 콘텐츠에 접근하게 하며, 원격 근무 자원을 보호하는 데 도움이 됩니다.

Q3: VPN을 쓰면 온라인에서 완전히 익명이 되나요?

아니요. VPN은 IP 주소를 숨기고 트래픽을 암호화하지만, 브라우저 쿠키, 로그인된 계정(Google이나 Facebook 등), 브라우저 핑거프린팅을 통해, 또는 VPN 제공업체가 데이터를 기록하는 경우에는 여전히 추적될 수 있습니다.

Q4: 웹 프록시는 내 IP 주소를 숨겨 주나요?

예, 하지만 프록시를 거쳐 보낸 트래픽, 보통은 브라우저 트래픽에만 해당합니다. 대부분의 웹 프록시는 데이터를 암호화하지 않으므로 ISP나 네트워크 운영자가 여러분이 주고받는 내용을 여전히 볼 수 있습니다.

Q5: IP를 숨기는 것은 합법인가요?

많은 나라에서는 합법이지만, 일부 나라는 VPN과 IP 주소를 숨기는 다른 도구를 제한하거나 금지합니다. IP를 숨긴다고 해서 불법 행위가 합법이 되지는 않으므로, 사용하기 전에 현지 법을 확인하세요.

체크포인트 10: 기초 VPN FAQ (파트 B)

가상 사설망(VPN) 사용에 대해 잠재 고객이 가장 자주 묻는 질문과 답을 살펴보세요.

Q6: Tor는 내 IP를 숨겨 주나요?

예. Tor는 트래픽을 자원봉사자가 운영하는 릴레이 세 곳(가드, 중간, 출구)을 거쳐 보내므로 웹사이트에는 출구 릴레이의 주소가 보이고, 어느 릴레이도 사용자가 누구이며 어디에 접속하는지 모두 알지 못합니다. [1]

Q7: 내 IP는 무엇을 드러내나요?

공용 IP는 보통 ISP와 국가나 도시 같은 대략적인 위치를 드러냅니다. 사이트는 이를 이용해 방문 기록을 서로 연결하거나 지역 차단을 적용할 수도 있습니다.

Q8: 숨겨졌는지 어떻게 확인하나요?

VPN에 연결한 다음 IP 확인 사이트에 접속해 DNS 및 WebRTC 누출 테스트를 실행하세요. 표시되는 IP와 DNS 서버는 ISP가 아닌 VPN의 것이어야 합니다. 실제 IP가 나타나면 누출 방지를 켜세요.

Q9: 휴대폰과 스마트 TV에서 VPN을 사용할 수 있나요?

예. 최신 VPN 제공업체는 iOS, Android, macOS, Windows, Linux, 스마트 TV용 전용 앱과 가정 네트워크의 모든 기기를 보호하는 공유기 설정을 제공합니다.

Q10: 킬 스위치란 무엇인가요?

킬 스위치는 VPN 연결이 끊기면 기기를 인터넷에서 자동으로 분리하는 보안 기능입니다. 이렇게 하면 암호화되지 않은 데이터나 실제 IP 주소가 유출되는 것을 막습니다.

체크포인트 10: 심화 VPN FAQ (파트 C)

가상 사설망과 보안 터널링 프로토콜의 기술적, 구조적 측면을 탐구합니다.

Q1: IP 주소를 숨겨도 웹사이트가 나를 추적할 수 있는 이유는 무엇인가요?

IP를 숨겨도 브라우저 핑거프린팅은 막지 못합니다. 추적기는 화면 해상도, 설치된 글꼴, 브라우저 설정 같은 세부 정보를 조합해 식별자를 만들 수 있고, 쿠키나 로그인한 계정으로도 신원이 식별될 수 있으므로 개인정보 보호에 중점을 둔 브라우저도 함께 사용하세요. [3]

Q2: 이중 VPN 또는 멀티홉 라우팅이란 무엇인가요?

멀티홉은 트래픽을 두 개 이상의 VPN 서버를 차례로 거쳐 라우팅합니다. 이렇게 하면 두 번째 암호화 계층이 추가되고, 한 서버가 침해되더라도 두 번째 홉에서는 사용자의 실제 IP 주소가 숨겨지도록 도와줍니다.

Q3: WebRTC 누출이란 무엇이며 VPN은 이를 어떻게 방지하나요?

WebRTC는 VPN이 켜져 있어도 실제 로컬 IP 주소와 공인 IP 주소를 드러낼 수 있는 브라우저 프로토콜입니다. 프리미엄 VPN은 데스크톱/모바일 앱과 브라우저 확장 프로그램에서 WebRTC 요청을 차단하거나 위장합니다.

Q4: IPv6 트래픽이 내 실제 IP 주소를 유출할 수 있나요?

예, VPN이 IPv4만 터널링하는 경우입니다. 그러면 기기가 IPv6 트래픽을 터널 밖으로 보내 ISP가 할당한 주소가 노출될 수 있습니다. IPv6를 터널링하거나 차단하는 VPN을 쓰고, IPv6 누출 테스트로 확인하세요.

Q5: 난독화는 VPN 차단을 어떻게 우회하나요?

난독화(또는 "스텔스 VPN")는 VPN 트래픽 패킷을 일반 HTTPS 웹 트래픽(포트 443)처럼 보이게 위장합니다. 정부나 학교/사무실 네트워크가 VPN을 차단하려고 사용하는 심층 패킷 검사(DPI)를 통과하는 데 도움이 됩니다.

체크포인트 10: 심화 VPN FAQ (파트 D)

가상 사설망과 보안 터널링 프로토콜의 기술적, 구조적 측면을 탐구합니다.

Q6: 스플릿 터널링을 쓰면 내 실제 IP 주소가 노출되나요?

예, 제외한 앱에는 해당됩니다. 터널 밖으로 보낸 트래픽은 실제 IP를 사용하며, RFC 8828에 따르면 브라우저가 제한하지 않는 한 WebRTC는 분할 터널 VPN 아래에 있는 ISP 주소를 드러낼 수 있습니다. [2]

Q7: 공유 IP 주소란 무엇이며 개인정보 보호에 어떻게 도움이 되나요?

공유 IP에서는 여러 VPN 사용자가 같은 시간에 같은 주소로 온라인에 접속한 것처럼 보입니다. 그래서 웹사이트가 한 번의 방문을 여러분 한 사람과 연결하기가, 여러분만 쓰는 전용 IP보다 훨씬 어렵습니다.

Q8: IP를 숨기려고 VPN을 쓴다는 사실을 내 ISP가 볼 수 있나요?

대체로 그렇습니다. ISP는 사용자가 VPN 서버의 IP 주소에 연결한다는 사실, 연결 시점, 보낸 데이터의 양은 볼 수 있지만, 방문한 웹사이트나 암호화된 터널 안의 내용은 볼 수 없습니다.

Q9: DNS 누출 방지란 무엇인가요?

DNS 유출 방지는 기기가 웹사이트 조회 쿼리(DNS 쿼리)를 ISP의 서버 대신 VPN의 비공개 암호화 DNS 서버를 통해 보내도록 합니다. 이렇게 하면 ISP가 사용자가 방문하는 사이트를 추적하는 것을 막을 수 있습니다.

Q10: IP를 숨기는 데는 프록시와 VPN 중 어느 쪽이 더 나은가요?

대개 VPN이 더 낫습니다. VPN은 기기의 모든 앱에서 IP를 숨기고 트래픽을 암호화하는 반면, 웹 프록시는 보통 브라우저만 다루고 암호화를 더하지 않는 경우가 많습니다.

파트 11: 흥미로운 VPN 사실 10가지와 실제 사례

VPN의 역사, 시장, 기술에 관한 매우 유용한 실제 사실과 통찰을 살펴보세요.

1. 최초의 VPN 프로토콜

PPTP(Point-to-Point Tunneling Protocol)는 1990년대 Microsoft 주도 그룹이 만든 초기 VPN 프로토콜로, 지금은 안전하지 않다고 여겨지므로 최신 VPN은 WireGuard나 OpenVPN을 사용합니다.

2. 핑거프린팅

IP를 숨겨도 브라우저 핑거프린팅은 막지 못하며, 화면 해상도와 설치된 글꼴 같은 세부 정보로 신원이 식별될 수 있습니다. [3]

3. WireGuard 혁명

WireGuard는 효율을 위해 설계된 매우 간결한 코드베이스를 갖추고 있어, 기존 프로토콜보다 보안 취약점을 감사하기 쉽습니다.

4. WEBRTC 주소 노출

RFC 8828은 브라우저가 제한하지 않는 한 WebRTC가 VPN의 공인 주소와 VPN이 사용하는 ISP 주소를 모두 알아낼 수 있다고 경고합니다. [2]

5. 5 EYES 동맹의 기원

미국, 영국, 캐나다, 호주, 뉴질랜드의 파이브 아이즈 정보 파트너십은 연합국 간의 제2차 세계대전 시기 신호정보 협력에서 비롯되었습니다.

6. 심층 패킷 검사

고급 방화벽은 심층 패킷 검사(DPI)를 사용해 네트워크 패킷 메타데이터를 분석하고 표준 VPN 연결 특성을 차단합니다.

7. TOR 회선 재사용

Tor는 같은 회로를 약 10분간 재사용한 뒤 새 회로를 만들기 때문에 탐색 활동을 서로 연결하기 어렵습니다. [1]

8. 탈중앙화 VPN

탈중앙화 VPN(dVPN)은 사용자들이 운영하는 노드 네트워크에 트래픽을 분산하여 단일 중앙 제공업체에 대한 의존도를 줄입니다.

9. TOR와 VPN 익명성 비교

VPN은 하나의 제공업체를 거쳐 트래픽을 터널링하지만, Tor(The Onion Router)는 개인정보 보호를 극대화하기 위해 자원봉사자가 운영하는 세 개의 릴레이(가드, 중간, 출구)를 거쳐 트래픽을 보냅니다. [1]

10. 프록시 대 VPN 터널

웹 프록시는 사이트에 보이는 브라우저 트래픽의 IP 주소를 바꾸지만, VPN과 달리 보통 그 트래픽을 암호화하지 않고 기기의 다른 앱도 다루지 않습니다. [5]

기술 참고 자료 및 출처

이 워크시트 전반에서 사용한 인용 문헌, 암호화 규격, 공식 문서 표준.

학술 및 업계 참고 자료

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

답안: IP 주소 숨기기, 위치 가리기, 프록시, Tor, DNS/WebRTC 누출 방지

1 질문 1

정답: B

교사용 참고

기기의 공인 IP 주소는 내가 방문하는 웹사이트에 무엇을 알려 줍니까? → 대략적인 위치와 인터넷 서비스 제공업체 이름

2 VPN 시스템 암호화

지연 시간

정답: C

교사용 참고

브라우저 트래픽만 우회시키는 프록시와 달리 VPN은 시스템 전체에 암호화된 터널을 만들어 백그라운드 애플리케이션, 게임, OS 쿼리까지 보호합니다. 출처: Tor Project Relays, W3C WebRTC API.

3 프록시 암호화 부재

Wi-Fi 보안

정답: A

교사용 참고

웹 프록시는 패킷 페이로드를 암호화하지 않고 브라우저 트래픽만 전달하므로, 네트워크 운영자나 ISP가 여러분의 콘텐츠 트래픽을 여전히 추적할 수 있습니다. 인용: IETF Proxy Vulnerabilities.

4 질문 4

정답: B

교사용 참고

Tor 네트워크는 어떻게 사용자에게 높은 익명성을 제공합니까? → 자원봉사자가 운영하는 세 개의 릴레이를 거쳐 트래픽을 보내서

5 DNS 터널 유출

개인정보 보호

정답: B

교사용 참고

DNS 유출은 도메인 이름 확인 요청이 VPN 터널을 우회해 ISP의 리졸버로 곧바로 전달되어 방문한 도메인 기록이 노출되는 현상입니다. 출처: DNSSEC Tunnel Testing, EFF Tracking Evasion.

답안: 체크포인트 2 – 참 또는 거짓

6 **프록시 한계 상세** IP 마스킹 정답: 거짓

교사용 참고

프록시는 애플리케이션 계층에서 작동하며 VPN 터널처럼 시스템 전체 네트워크 드라이버와 통합되지 않습니다. 인용: IETF Proxy Vulnerabilities.

7 **질문 7** 정답: 참

교사용 참고

계층형 암호화를 적용하여 자원봉사자 릴레이 세 곳을 거쳐 트래픽을 보내면 지연 시간이 늘어나므로, Tor는 보통 직접 연결보다 느립니다.

8 **질문 8** 정답: 참

교사용 참고

WebRTC는 로컬 주소를 드러낼 수 있으며, 일부 VPN 설정에서는 터널 아래에 있는 인터넷 서비스 제공업체가 할당한 공인 IP까지 드러낼 수 있습니다(RFC 8828).

9 **질문 9** 정답: 참

교사용 참고

DNS나 WebRTC 누출이 없으면 인터넷 서비스 제공업체는 내가 방문한 사이트가 아니라 VPN 서버로 가는 암호화된 트래픽만 볼 수 있습니다.

10 **핑거프린팅의 한계** 로그 미보관 정답: 거짓

교사용 참고

핑거프린팅은 IP가 숨겨져도 계속 보이는 기기 설정 지표(화면 해상도, 글꼴, 플러그인)를 대상으로 합니다. 출처: EFF Tracking Evasion.

어휘 정답 및 채점 기준표

교사용 채점 기준: 정확하게 연결한 항목마다 1점(총 8점), 문맥 용어마다 1점(총 6점)을 줍니다.

체크포인트 4: 답안 – 개념 연결

D 1. IP 주소	A 2. VPN 터널	B 3. Tor 네트워크	E 4. 웹 프록시
G 5. DNS 유출	H 6. WebRTC API	C 7. 위치 가리기	F 8. ISP 추적

체크포인트 3: 답안 – 핵심 용어

1 DNS 유출	2 WebRTC	3 프록시	4 Tor
5 IP 주소	6 위치		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 D – 암호화터널	2 G – 분할터널링	3 F – 오픈브이피엔	4 A – 아이피주소
5 C – 개인정보보호	6 H – 킬스위치	7 E – 위치정보	8 B – 오픈소스

교사를 위한 토론 참고

핵심 용어:
학생들이 IP 주소, VPN 터널, Tor 네트워크를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

사례 연구:
학생들이 의견이 아니라 워크시트의 사실을 근거로 권고안을 제시하게 하세요.

출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

다	서	피	하	크	오	주	엔	도	타	밀	개	접	화	트
공	널	비	라	주	카	다	시	오	방	속	크	킬	카	파
라	터	전	크	기	도	이	안	연	픈	보	격	넷	타	바
스	화	링	다	트	인	청	술	기	링	소	연	스	색	다
험	호	넷	파	넷	개	널	번	분	공	치	스	버	공	비
자	암	리	기	버	인	전	아	관	번	공	킬	스	위	치
널	격	결	아	소	정	템	도	이	하	벽	인	바	가	마
링	사	속	치	벽	보	넷	브	화	피	널	주	방	타	험
널	번	터	카	기	보	전	이	화	위	주	개	트	데	데
터	위	리	스	소	호	주	트	사	템	격	소	연	호	시
할	오	픈	브	이	피	엔	바	색	카	도	할	응	아	위
분	링	색	버	방	크	킬	카	이	타	험	픈	개	치	사
요	마	가	킬	송	카	화	나	타	결	타	안	정	워	술
카	리	위	번	하	기	시	링	템	안	험	보	답	보	나
다	험	접	전	개	소	치	격	넷	리	소	스	차	이	엔

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

3 가로: 오픈소스 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4 글자)

4 가로: 위치정보 기기가 현재 어느 곳에 있는지를 나타내는 지리적 정보 (4 글자)

5 가로: 아이피주소 인터넷에서 기기 인터페이스를 식별하는 고유한 숫자 표시 (5 글자)

6 가로: 암호화터널 기기의 모든 트래픽을 암호화해 VPN 서버를 거쳐 보내는 연결 (5 글자)

세로

1 세로: 킬스위치 VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4 글자)

2 세로: 개인정보보호 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일 (6 글자)

3 세로: 오픈브이피엔 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜 (6 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 주피아소이 — **아이피주소**
2. 호개정보보인 — **개인정보보호**
3. 보위정치 — **위치정보**
4. 터링널분할 — **분할터널링**
5. 스오소픈 — **오픈소스**
6. 터암화널호 — **암호화터널**
7. 피오이엔브픈 — **오픈브이피엔**
8. 킬치위스 — **킬스위치**

비밀 암호 도전 정답

"보안 터널로 주소를 감추세요"

사례 연구 답안

A 상황 A: 공용 네트워크 보안

스니핑과 암호화 사라의 딜레마

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 위험: 패킷 스니핑, 데이터 가로채기, 중간자 공격. 같은 카페 네트워크에 있는 누군가가 그녀의 로그인 정보나 숙제 파일을 가로챌 수 있습니다.
- VPN 보호: VPN이 올바르게 설정되어 있으면 네트워크 패킷 페이로드를 암호화하여, 가로챈 터널 트래픽을 수동적으로 엿보는 로컬 네트워크 감시자가 읽을 수 없게 합니다.

B 시나리오 B: 차단된 리소스에 접근하기

지역 차단과 IP Alex의 딜레마

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 차단된 이유: 스트리밍 호스트가 지역 차단을 사용해, 여행 중인 그의 로컬 IP 주소를 실제 국가에 대응시키고 지역별 라이선스에 따라 차단하기 때문입니다.
- VPN이 도움이 되는 이유: 자기 나라에 있는 서버를 거쳐 트래픽을 보내 실제 위치를 가립니다. 사이트에는 자국 IP로 보이므로 접속할 수 있습니다.