이름: _____ 날짜: _____ 점수: _____

VPN 고르는 방법 워크시트

VPN 제공업체, 보안 표준, 감사, 로깅 정책 평가

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

- 개인정보 보호를 위해 제공업체의 관할권과 무로그 정책을 평가하세요.
- WireGuard와 OpenVPN 같은 터널링 프로토콜의 속도를 비교하세요.
- 킬 스위치와 RAM 전용 서버 노드 같은 보안 기능을 분석하세요.
- 선택할 때 독립적인 보안 감사와 요금제를 확인하세요.
- 속도와 지역 제한 해제 필요에 따라 서버 위치를 선택하세요.

선택 워크시트 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 안전한 VPN 인프라 선택에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

VPN 고르기(소개)

알맞은 VPN을 고르려면 마케팅 과장 너머를 봐야 합니다. 믿을 만한 제공업체라면 입증된 무로그 정책, 안전한 암호화 프로토콜, 오픈 소스 클라이언트를 갖추고 있어야 합니다. 보안 기능, 관할권, 속도 성능을 평가하면 디지털 보호 요구에 맞는 VPN을 고를 수 있습니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 안전한 VPN 제공업체를 고를 때 핵심 요소는 무엇입니까?
   - A. 서버 국가 수
   - B. 독립적으로 감사를 받은 무로그 정책
   - C. 가장 낮은 월 요금제
   - D. 화려한 광고 후원

2. 2. 속도와 감사 가능성의 균형이 가장 좋은 VPN 프로토콜은 무엇입니까?
   - A. PPTP(레거시)
   - B. L2TP/IPSec
   - C. OpenVPN over TCP만
   - D. WireGuard

3. 3. 민감한 활동에는 무료 VPN을 피해야 하는 이유는 무엇입니까?
   - A. 미국에서 금지되어 있음
   - B. 이들은 종종 사용자의 웹 탐색 기록을 판매한다
   - C. 기본적인 웹 브라우징을 지원하지 않는다
   - D. 연결하려면 특수한 하드웨어가 필요하다

4. 4. 제공업체의 본국 법적 관할권은 무엇을 결정합니까?
   - A. 서버 연결 속도
   - B. 지원되는 기기 종류
   - C. 데이터 보관과 수색 영장을 규정하는 현지 법률
   - D. 클라이언트 애플리케이션의 시각적 테마

5. 5. VPN 클라이언트의 '킬 스위치' 기능의 주된 목적은 무엇입니까?
   - A. VPN 연결이 끊기면 인터넷 접속을 차단하기 위해
   - B. 기기에 설치된 모든 애플리케이션을 삭제하기 위해
   - C. 서버 연결 속도를 두 배로 높이려고
   - D. 유휴 상태일 때 운영 체제를 다시 시작하려고

체크포인트 2: 참/거짓 도전

6 질문 6

6. VPN은 기기를 악성코드 다운로드와 바이러스 파일로부터 보호합니다.

○ 참 ○ 거짓

7 질문 7

7. Deloitte 같은 회사의 독립 감사는 무로그 주장을 검증합니다.

○ 참 ○ 거짓

8 질문 8

8. 제공업체 본국의 법은 사용자 데이터 개인정보 보호에 영향을 주지 않습니다.

○ 참 ○ 거짓

9 질문 9

9. WireGuard의 간결한 코드베이스는 OpenVPN보다 감사하기 쉽습니다.

○ 참 ○ 거짓

10 질문 10

10. 무료 VPN은 서버 비용을 충당하기 위해 광고를 팔거나 사용자를 추적하는 경우가 많습니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 독립적으로 검증된 _____ 정책은 VPN 제공업체가 온라인 기록을 저장하지 않겠다고 약속하는 것입니다.

2. 높은 속도를 제공하면서 코드베이스가 매우 작은 최신 프로토콜은 _____ 입니다.

3. VPN 연결이 갑자기 끊기면 모든 트래픽을 멈추는 안전 기능을 _____ (이)라고 합니다.

4. 제공업체의 법적 _____ 을(를) 평가하면 감시 조약의 적용을 받는지 알 수 있습니다.

5. 서버에 _____ 디스크를 사용하면 재부팅 후 사용자 데이터가 남지 않도록 하는 데 도움이 됩니다.

6. 무지식 주장 정책을 확인하려면 신뢰할 수 있는 업체의 제3자 보안 _____ 이(가) 필요합니다.

어휘 단어 목록

감사 관할권 무로그 무료 VPN 킬 스위치 OPENVPN RAM 전용 WireGuard

여기에 답을 쓰세요:

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

체크포인트 4: 네트워크 개념 연결

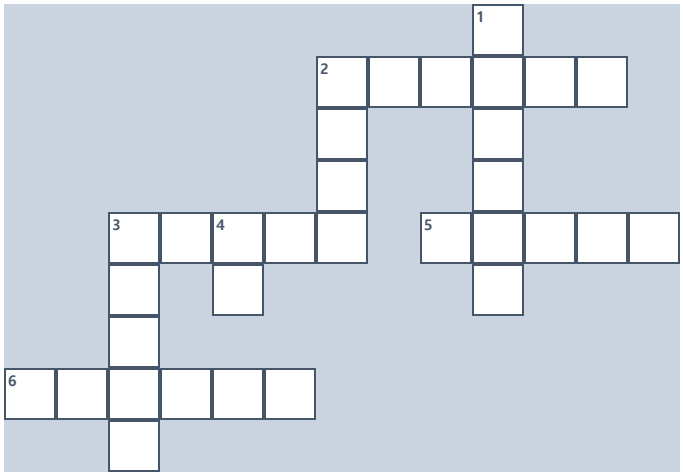
정의 연결하기

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

☐	**1. WireGuard**	**A**	브라우저 데이터를 기록하고 판매하여 수익을 내는 경우가 많은 고위험 연결 서비스.
☐	**2. 감사받은 로그**	**B**	보안 터널 연결이 끊기면 인터넷 라우팅을 차단하는 안전 장치.
☐	**3. 관할권**	**C**	미국, 영국, 캐나다, 호주, 뉴질랜드 간의 국제 정보 공유 동맹.
☐	**4. 킬 스위치**	**D**	휘발성 메모리에서 실행되어 데이터가 디스크에 저장되지 않는 하드웨어 인프라.
☐	**5. Five Eyes**	**E**	VPN 제공업체의 법적 의무를 규율하는 지리적 지역입니다.
☐	**6. 무료 VPN**	**F**	감사하기 쉬운 약 4,000줄의 코드를 사용하는 최신 고속 프로토콜.
☐	**7. RAM 전용 서버**	**G**	WireGuard보다 코드 규모가 훨씬 크지만 폭넓게 감사받은 성숙한 오픈 소스 프로토콜.
☐	**8. OpenVPN**	**H**	독립적인 제3자 사이버 보안 업체가 검증한 개인정보 보호 주장.

체크포인트 5: 십자말풀이

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



가로

2. 코드가 크고 오랫동안 널리 감사받은, 소스가 공개된 성숙한 프로토콜 (6)

3. 로그를 기록하고 브라우저 데이터를 팔아 수익을 내는 경우가 많은 고위험 연결 서비스 (5)

5. 코드가 약 4,000줄로 작아 감사하기 쉬운 최신 고속 프로토콜 (5)

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

세로

1. 미국, 영국, 캐나다, 호주, 뉴질랜드 다섯 나라의 정보 공유 동맹 (6)

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

3. 사용자의 활동 기록을 남기지 않겠다는 방침 (5)

4. 요청을 받아 데이터나 서비스를 제공하는 컴퓨터 (2)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

2 가로: 코드가 크고 오랫동안 널리 감사받은, 소스가 공개된 성숙한 프로토콜 (6 글자):

3 가로: 로그를 기록하고 브라우저 데이터를 팔아 수익을 내는 경우가 많은 고위험 연결 서비스 (5 글자):

5 가로: 코드가 약 4,000줄로 작아 감사하기 쉬운 최신 고속 프로토콜 (5 글자):

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

세로

1 세로: 미국, 영국, 캐나다, 호주, 뉴질랜드 다섯 나라의 정보 공유 동맹 (6 글자):

2 세로: 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4 글자):

3 세로: 사용자의 활동 기록을 남기지 않겠다는 방침 (5 글자):

4 세로: 요청을 받아 데이터나 서비스를 제공하는 컴퓨터 (2 글자):

체크포인트 6: 숨은 단어 찾기

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

하	정	책	요	와	주	파	번	공	개	벽	워	위	밀	라
요	책	카	다	템	화	공	정	와	엔	타	파	라	송	크
술	정	주	송	안	결	안	위	방	이	타	바	도	피	다
워	그	넷	답	인	술	피	접	도	로	어	다	서	버	리
방	로	파	방	즈	개	이	어	위	픈	네	가	격	밀	자
스	무	술	네	연	인	시	오	데	위	오	험	드	접	아
응	메	소	보	비	정	터	바	픈	가	마	아	개	픈	비
스	방	료	암	오	보	청	화	타	브	리	이	넷	타	술
비	송	전	벽	험	보	격	워	전	전	이	관	스	메	청
서	요	트	사	메	호	험	접	기	템	바	피	로	카	주
료	파	이	브	아	이	즈	드	검	아	피	그	엔	버	오
무	벽	정	엔	카	송	타	리	즈	격	사	답	마	픈	가
엔	결	타	벽	나	파	접	파	서	크	용	카	소	스	관
이	보	술	템	피	메	서	리	무	안	나	스	다	리	개
송	격	청	픈	험	방	스	청	도	차	송	와	마	버	템

어휘 단어 목록

개인정보보호 무로그정책 파이브아이즈 오픈소스 무료서비스 서버 와이어가드 오픈브이피엔

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. 개인정보보호**
- **B. 무로그정책**
- **C. 파이브아이즈**
- **D. 오픈소스**
- **E. 무료서비스**
- **F. 서버**
- **G. 와이어가드**
- **H. 오픈브이피엔**

정의 및 연결 항목

1. 로그를 기록하고 브라우저 데이터를 팔아 수익을 내는 경우가 많은 고위험 연결 서비스.
2. 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일.
3. 코드가 크고 오랫동안 널리 감사받은, 소스가 공개된 성숙한 프로토콜.
4. 요청을 받아 데이터나 서비스를 제공하는 컴퓨터.
5. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
6. 코드가 약 4,000줄로 작아 감사하기 쉬운 최신 고속 프로토콜.
7. 미국, 영국, 캐나다, 호주, 뉴질랜드 다섯 나라의 정보 공유 동맹.
8. 사용자의 활동 기록을 남기지 않겠다는 방침.

체크포인트 7: 뒤섞인 단어 도전

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

1. 정 개 보 보 호 인 _____

2. 즈 파 브 이 아 이 _____

3. 서 무 스 비 료 _____

4. 어 드 가 와 이 _____

5. 그 책 무 정 로 _____

6. 소 스 오 픈 _____

7. 버 서 _____

8. 브 엔 오 피 이 픈 _____

보너스 활동: 빠르게 생각하기

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

1	VPN이 숨길 수 있는 것			
2	가격보다 더 중요한 것			
3	VPN 후기를 읽을 수 있는 곳			
4	VPN이 막아 주지 못하는 위협			
5	VPN 영업팀에 할 질문			
6	인터넷 서비스 제공업체가 볼 수 있는 것			
7	VPN을 고를 때 체크리스트에 넣을 항목			
8	VPN을 사용할 장소			
9	VPN 제공업체의 경고 신호			
10	개인정보 보호와 관련된 단어			
11	가장 먼저 테스트할 것			
12	좋은 VPN 제공업체가 하는 약속			
13	여행 중에 VPN을 사용하는 이유			
14	VPN을 사용할 수 있는 기기			
15	VPN에 대한 오해			

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

선택 가이드 학습을 마치려면 안전한 인프라 선택에 관한 이 숨겨진 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	1	28	10	24	6	38	6		8	40	1	32	19	21

12	20	3	13	24	3		10	40	10	38	17	25	7

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: VPN을 쓰면 인터넷 속도가 느려지나요?

예, 약간 그렇습니다. 암호화 과정과 VPN 서버까지의 물리적 거리가 지연 시간과 오버헤드를 더합니다. 영향은 제공업체, 프로토콜, 서버 거리, 기기, 네트워크 상태에 따라 다릅니다.

Q5: 어떻게 수익을 내나요?

비즈니스 모델을 확인하세요. 구독, 프리미엄 요금제, 데이터 판매는 모두 VPN을 얼마나 신뢰할 수 있는지에 영향을 주며, 데이터를 전혀 수집하지 않는 서비스는 그 데이터를 팔 수 없습니다. 먼저 개인정보 처리방침을 읽어 보세요. [1]

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: 무료 VPN을 사용해도 되나요?

무료 VPN은 광고, 제한된 기능, 사용 분석, 데이터 한도 또는 기타 수익 모델에 의존할 수 있습니다. 사용하기 전에 제공업체의 개인정보 처리방침, 소유 구조, 감사, 비즈니스 모델을 확인해야 합니다.

Q7: '노로그(no-logs)' 정책이란 무엇인가요?

무로그 정책은 제공업체가 보관하지 않는다고 밝힌 활동 및 연결 데이터를 설명합니다. 정확한 범위는 다양하므로 정책과 독립 감사 결과를 검토해야 합니다.

Q8: 가장 좋은 VPN을 어떻게 고르나요?

감사를 받은 로그 미보관 정책, 강력한 프로토콜(WireGuard, OpenVPN), 안전한 서버 위치, 빠른 속도, RAM 전용 서버, 킬 스위치 기능, 그리고 정보 공유 동맹(5/9/14 Eyes 등) 밖의 관할권을 확인하세요.

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: WireGuard, OpenVPN, IKEv2의 차이는 무엇인가요?

WireGuard는 약 4,000줄의 코드로 이루어진 최신 경량 프로토콜로, 빠른 속도와 짧은 연결 시간을 제공합니다. OpenVPN은 보안성이 매우 높고 오랜 검증을 거친 오픈 소스 프로토콜입니다. IKEv2는 네트워크를 전환할 때 빠르게 재연결할 수 있어 모바일 기기에 탁월합니다.

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: RAM 전용 서버란 무엇이며 왜 중요한가요?

기존 서버는 압수되거나 침해될 수 있는 하드 드라이브에 데이터를 씁니다. RAM 전용(디스크 없는) 서버는 전적으로 휘발성 메모리(RAM)에서 실행됩니다. 서버를 재부팅하거나 전원을 끄면 메모리에 있는 데이터는 지워집니다.

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 터널링이란 무엇이며 언제 사용해야 하나요?

스플릿 터널링을 사용하면 어떤 앱을 암호화된 VPN 터널로 라우팅하고 어떤 앱을 인터넷에 직접 연결할지 고를 수 있습니다. 민감한 은행 앱은 VPN을 거치게 하고 로컬 게임은 직접 연결해, VPN으로 인한 지연을 피하는 데 사용하세요.

Q7: 전방 비밀성(Perfect Forward Secrecy)은 어떻게 작동하나요?

PFS는 세션마다 고유한 임시 암호화 키를 생성하도록 보장합니다. 나중에 개인 키가 유출되더라도 각 세션이 독립된 키를 사용했기 때문에 과거나 미래의 세션을 복호화하는 데 쓸 수 없습니다.

Q8: 5/9/14 Eyes 동맹이란 무엇이며 왜 신경 써야 하나요?

관할권은 제공업체가 마주할 수 있는 법적 절차에 영향을 줄 수 있지만, 실제 개인정보 보호 위험은 제공업체가 보관하는 데이터, 기술 구조, 소유 구조, 투명성 보고, 감사 이력에도 좌우됩니다.

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: VPN을 누가 운영하고 보증하는지 왜 확인해야 하나요?

평판이 중요합니다. 회사의 소유주와 경영진을 조사하고, 공개된 제3자 감사 결과를 찾아보며, 신뢰하기 전에 독립 보안 전문가와 언론이 뭐라고 말하는지 확인하세요. [1]

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. [1]

2. 시장 가치 평가

전 세계 VPN 시장은 원격 근무 수요와 기업 보안 요구가 늘면서 빠르게 성장했습니다.

3. WireGuard 혁명

WireGuard는 효율을 위해 설계된 매우 간결한 코드베이스를 갖추고 있어, 기존 프로토콜보다 보안 취약점을 감사하기 쉽습니다. [3]

4. 엄격한 감사 기준

상위 VPN 제공업체는 Deloitte, KPMG, PwC 같은 회사에 무로그 주장 확인을 맡기고, Cure53 같은 보안 회사에 앱과 서버 테스트를 맡깁니다. [4]

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. 기업 사용

많은 조직이 원격 근무 직원에게 데이터베이스 같은 내부 시스템에 접속할 수 있도록 VPN을 제공하므로, VPN은 직장에서 흔히 쓰이는 보안 도구입니다.

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. [5]

10. 데이터 유출 비용

VPN을 모든 사용자와 기기를 확인하는 제로 트러스트 접근 모델과 함께 쓰면 조직이 데이터를 보호하고 데이터 유출의 피해를 줄이는 데 도움이 됩니다.

기술 참고 자료 및 출처

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

학술 및 업계 참고 자료

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

[2] 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

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

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

답안: VPN 제공업체, 보안 표준, 감사, 로그 정책 평가하기

1 감사를 거친 로그 정책 프로토콜

정답: B

교사용 참고

독립적으로 감사받은 무로그 정책은 제공업체의 제로 날리지 개인정보 보호 주장을 확인하는 가장 실용적인 방법입니다. 화려한 마케팅이나 자체 주장만으로는 충분하지 않습니다. 출처: Deloitte Advisory, Cure53 Audit.

2 WireGuard의 우수성 지연 시간

정답: D

교사용 참고

WireGuard는 간결한 코드베이스(~4,000줄)와 함께 커널 공간에서 빠르고 현대적인 연결 라우팅을 제공해 감사가 매우 효율적입니다. 인용: IETF Protocol RFC, WireGuard Project.

3 질문 3

정답: B

교사용 참고

무료 VPN도 서버 비용을 부담해야 하며, FTC는 일부 VPN 앱이 광고 제공 등을 위해 사용자 데이터를 제3자와 공유한다고 경고합니다.

4 법적 관할권 라우팅 제어

정답: C

교사용 참고

관할권은 VPN이 감시법, 현지 데이터 보존 의무, 비공개 정부 소환 영장의 적용을 받는지를 결정합니다. 출처: Privacy Rights Clearinghouse.

5 킬 스위치 보호 개인정보 보호

정답: A

교사용 참고

킬 스위치는 터널이 끊어지면 시스템 네트워크 어댑터의 라우팅을 즉시 차단하여 실제 IP와 DNS 노출 유출을 막습니다. 출처: IETF Tunnel RFC.

답안: 체크포인트 2 – 참 또는 거짓

6 **악성코드의 한계** IP 마스킹 정답: 거짓

교사용 참고

VPN은 안전한 암호화 통로를 제공하지만 페이로드나 파일을 검사하지는 않습니다. 악성코드를 차단하려면 백신 소프트웨어가 필요합니다. 출처: Deloitte Advisory.

7 **독립 감사** 속도 정답: 참

교사용 참고

감사 보고서는 서버 소프트웨어 구성, RAM 전용 구성 준수 여부, 로깅 데이터베이스 부재를 검증합니다. 출처: Deloitte Advisory, Cure53 Audit.

8 **질문 8** 정답: 거짓

교사용 참고

제공업체는 본국의 법을 따라야 하며, 여기에는 데이터 보관 규정과 보유한 데이터를 넘겨 달라는 명령이 포함될 수 있습니다.

9 **프로토콜 코드베이스 크기** 방화벽 정답: 참

교사용 참고

코드베이스가 작을수록 잠재적 공격 표면이 줄고 보안팀이 프로토콜 무결성을 검증하기 쉬워집니다. 출처: WireGuard Project.

10 **광고 수익화** 로그 미보관 정답: 참

교사용 참고

구독료가 없는 무료 VPN은 수익을 내기 위해 데이터 마이닝, 트래픽 프로파일링, 브라우저 광고 삽입에 의존합니다. 인용: EDRi Retention Guidelines.

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

F 1. WireGuard	H 2. 감사받은 로그	E 3. 관할권	B 4. 킬 스위치
C 5. Five Eyes	A 6. 무료 VPN	D 7. RAM 전용 서버	G 8. OpenVPN

체크포인트 3: 답안 – 핵심 용어

1 무로그	2 WireGuard	3 킬 스위치	4 관할권
5 RAM 전용	6 감사		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 E – 무료서비스	2 A – 개인정보보호	3 H – 오픈브이피엔	4 F – 서버
5 D – 오픈소스	6 G – 와이어가드	7 C – 파이브아이즈	8 B – 무로그정책

교사를 위한 토론 참고

핵심 용어:
학생들이 WireGuard, 감사받은 로그, 관할권을 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

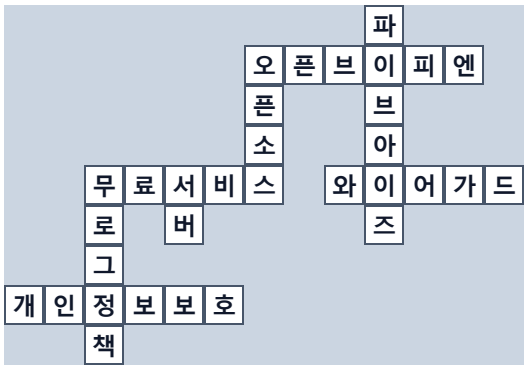
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

하	정	책	요	와	주	파	번	공	개	벽	워	위	밀	라
요	책	카	다	템	화	공	정	와	엔	타	파	라	송	크
술	정	주	송	안	결	안	위	방	이	타	바	도	피	다
워	그	넷	답	인	술	피	접	도	로	어	다	서	버	리
방	로	파	방	즈	개	이	어	위	픈	네	가	격	밀	자
스	무	술	네	연	인	시	오	데	위	오	험	드	접	아
응	메	소	보	비	정	터	바	픈	가	마	아	개	픈	비
스	방	료	암	오	보	청	화	타	브	리	이	넷	타	술
비	송	전	벽	험	보	격	워	전	전	이	관	스	메	청
서	요	트	사	메	호	험	접	기	템	바	피	로	카	주
료	파	이	브	아	이	즈	드	검	아	피	그	엔	버	오
무	벽	정	엔	카	송	타	리	즈	격	사	답	마	픈	가
엔	결	타	벽	나	파	접	파	서	크	용	카	소	스	관
이	보	술	템	피	메	서	리	무	안	나	스	다	리	개
송	격	청	픈	험	방	스	청	도	차	송	와	마	버	템

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 오픈브이피엔 코드가 크고 오랫동안 널리 감사받은, 소스가 공개된 성숙한 프로토콜 (6 글자)

3 가로: 무료서비스 로그를 기록하고 브라우저 데이터를 팔아 수익을 내는 경우가 많은 고위험 연결 서비스 (5 글자)

5 가로: 와이어가드 코드가 약 4,000줄로 작아 감사하기 쉬운 최신 고속 프로토콜 (5 글자)

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

세로

1 세로: 파이브아이즈 미국, 영국, 캐나다, 호주, 뉴질랜드 다섯 나라의 정보 공유 동맹 (6 글자)

2 세로: 오픈소스 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4 글자)

3 세로: 무로그정책 사용자의 활동 기록을 남기지 않겠다는 방침 (5 글자)

4 세로: 서버 요청을 받아 데이터나 서비스를 제공하는 컴퓨터 (2 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 정개보보호인 — **개인정보보호**
2. 즈파브이아이 — **파이브아이즈**
3. 서무스비료 — **무료서비스**
4. 어드가와이 — **와이어가드**
5. 그책무정로 — **무로그정책**
6. 소스오픈 — **오픈소스**
7. 버서 — **서버**
8. 브엔오피이픈 — **오픈브이피엔**

비밀 암호 도전 정답

"보고서를 비교해 안전 시스템"

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.