이름: _____ 날짜: _____ 점수: _____

공용 Wi-Fi 보안과 암호화

중간자 공격, 불법 액세스 포인트, 패킷 스니핑, VPN 터널, HTTPS 암호화.

공용 Wi-Fi 보안 학습 개요

보호됨
데이터 암호화
256비트 AES 표준

규정 준수
글로벌 표준
GDPR 및 CCPA 규정 체계

제로 트러스트
접근 정책
다중 요소 인증

환영합니다! 이 활동 자료집은 공공 Wi-Fi 보안을 안내합니다. 암호화되지 않은 네트워크, 중간자(MitM) 공격, 불량 액세스 포인트, 패킷 스니핑, VPN 터널, HTTPS 전송 보안을 살펴봅니다.

워크시트 체크포인트

- ☐ **파트 1-4: 사이버 보안과 위협 예방을 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 사이버 보안 가이드 열기

URL: https://www.vpn.com/cybersecurity/public-wifi-security/

나의 공용 Wi-Fi 보안 학습 로드맵

- 패킷 스니핑과 불법 액세스 포인트를 포함한 공용 Wi-Fi의 흔한 위험을 파악하세요.
- 전송 중인 데이터를 보호하도록 VPN 암호화 터널을 구축하세요.
- 원격 근무자를 위해 HTTPS와 안전한 웹 브라우저 설정을 적용하세요.

공용 Wi-Fi 보안 가이드 안내

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

공용 Wi-Fi 보안과 전송 구간 보호(소개)

암호화되지 않은 공용 Wi-Fi 핫스팟은 네트워크 트래픽을 패킷 스니핑과 Evil Twin 스푸핑에 노출시킵니다. 트래픽을 안전한 VPN 암호화 터널로 보내고 HTTPS 전용 HSTS 규칙을 적용하면 로컬 네트워크 가로채기로부터 세션을 보호할 수 있습니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 중간자(MitM) 공격이란 무엇입니까?

- A. 공유 네트워크에서 두 당사자 사이의 통신을 가로채 변조함
- B. 사용자 기록을 노리는 데이터베이스 추출 기법
- C. 웹 서버에 네트워크 트래픽 요청을 폭주시키기
- D. 로컬 하드 드라이브 저장 볼륨 지우기

2 2. 불량 액세스 포인트(이블 트윈)란 무엇입니까?

- A. 정상 네트워크와 같은 SSID로 구성된 악성 Wi-Fi 핫스팟
- B. 데이터베이스 백업을 모니터링하는 데 쓰는 관리 도구
- C. 보안 VPN 게이트웨이 구성
- D. 승인된 메일 서버를 매핑하는 DNS 레코드

3 3. VPN은 공용 Wi-Fi 트래픽을 어떻게 보호하나요?

- A. 모든 네트워크 패킷을 암호화 터널로 감싸 스니퍼가 읽을 수 없게 함
- B. 들어오는 모든 연결 요청을 자동으로 차단한다
- C. 물리적 네트워크 카드의 MAC 주소를 바꾼다
- D. 웹 브라우저의 캐시된 쿠키를 삭제한다

4 4. 패킷 스니핑이란 무엇입니까?

- A. 하드웨어나 소프트웨어 도구로 네트워크 패킷을 캡처하고 기록함
- B. 로컬 디렉터리에서 중복 파일 검사하기
- C. 사용자 역할에 따라 데이터베이스 읽기 권한 제한하기
- D. AES-256 키로 저장 드라이브 암호화하기

5 5. HTTPS의 역할은 무엇입니까?

- A. 브라우저와 웹 서버 사이의 세션 트래픽 암호화
- B. 게이트웨이에서 들어오는 이메일 메시지 필터링하기
- C. 페이지 로딩을 빠르게 하려고 이미지 압축하기
- D. 네트워크 연결 스토리지의 파일 구조 관리하기

체크포인트 2: 참/거짓 도전

6 질문 6

6. 연결된 사용자는 개방된 공용 Wi-Fi 네트워크에서 일반 텍스트 데이터를 쉽게 가로챌 수 있습니다.

○ 참 ○ 거짓

7 질문 7

7. 불법 액세스 포인트(Evil Twin)는 항상 네트워크 관리자의 승인을 받습니다.

○ 참 ○ 거짓

8 질문 8

8. VPN은 공용 네트워크의 패킷 스니핑으로부터 트래픽을 보호하는 데 효과가 없습니다.

○ 참 ○ 거짓

9 질문 9

9. HTTPS는 URL 경로만 암호화하고 패킷 페이로드는 평문으로 남깁니다.

○ 참 ○ 거짓

10 질문 10

10. WPA3 보안을 사용하는 Wi-Fi 핫스팟은 비밀번호가 없는 개방형 네트워크보다 더 강력한 보호를 제공합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 공용 Wi-Fi에서 개인 비밀번호를 빼내는 것은 통신 _____ 입니다.
2. 로컬 네트워크의 원시 패킷을 분석할 때는 패킷 _____ 을(를) 사용합니다.
3. 호텔 Wi-Fi를 흉내 내는 불법 핫스팟을 _____ (이)라고 합니다.
4. 웹 트래픽 전송을 보호하려면 _____ (으)로 암호화해야 합니다.
5. 모든 네트워크 출력을 암호화할 때는 클라이언트 _____ 을(를) 사용합니다.
6. 공용 네트워크를 거치는 암호화된 통신 경로를 _____ (이)라고 합니다.

어휘 단어 목록

가로채기 방화벽 스니핑 이블 트윈 터널 HTTPS VPN WPA3

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

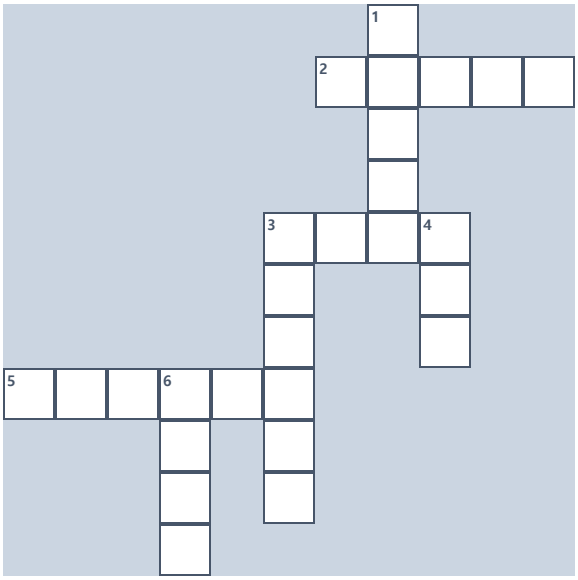
정의 연결하기

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

☐	**1. 가로채기**	**A**	최신 Wi-Fi 보안 표준.
☐	**2. 스니핑**	**B**	전송 중인 안전한 데이터 경로.
☐	**3. 이블 트윈**	**C**	들어오는 트래픽 필터링.
☐	**4. HTTPS**	**D**	Wi-Fi를 흉내 내는 불법 핫스팟.
☐	**5. VPN**	**E**	전송 중인 트래픽을 읽는 것.
☐	**6. 터널**	**F**	네트워크 데이터 패킷 캡처하기.
☐	**7. WPA3**	**G**	암호화된 가상 사설망.
☐	**8. 방화벽**	**H**	안전한 웹 전송.

체크포인트 5: 십자말풀이

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



가로

2. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5)

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

5. 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷 (6)

세로

1. 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5)

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

4. 네트워크를 지나는 데이터 패킷을 몰래 붙잡아 들여다보는 일 (3)

6. 정상 와이파이와 같은 이름으로 만들어 놓은 가짜 접속 지점 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

2 가로: 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5 글자):

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

5 가로: 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷 (6 글자):

세로

1 세로: 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5 글자):

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

4 세로: 네트워크를 지나는 데이터 패킷을 몰래 붙잡아 들여다보는 일 (3 글자):

6 세로: 정상 와이파이와 같은 이름으로 만들어 놓은 가짜 접속 지점 (4 글자):

체크포인트 6: 숨은 단어 찾기

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

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

어휘 단어 목록

와이어가드 | 오픈소스 | 스니핑 | 공용와이파이 트래픽 | 이블트윈 | 아이피주소 | 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. 와이어가드
B. 오픈소스
C. 스니핑
D. 공용와이파이
E. 이블트윈
F. 아이피주소
G. 오픈브이피엔
H. 트래픽

정의 및 연결 항목
1. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
2. 네트워크를 지나는 데이터 패킷을 몰래 붙잡아 들여다보는 일.
3. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
4. 인터넷에서 기기를 식별하는 고유한 숫자 주소.
5. 네트워크를 오가는 데이터의 흐름이나 양.
6. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜.
7. 정상 와이파이와 같은 이름으로 만들어 놓은 가짜 접속 지점.
8. 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 사이버 보안 개념과 용어를 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 가 어 와 드 이 _____
2. 핑 니 스 _____
3. 윈 이 트 블 _____
4. 엔 이 브 피 오 픈 _____
5. 스 오 소 픈 _____
6. 파 이 공 와 이 용 _____
7. 주 소 아 피 이 _____
8. 픽 래 트 _____

보너스 활동: 빠르게 생각하기

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

1	소프트웨어를 업데이트하는 이유			
2	Wi-Fi에 자동으로 연결되는 기기			
3	절대 공유하면 안 되는 정보			
4	오늘부터 시작할 수 있는 안전 습관			
5	카페에서 안전을 지키는 방법			
6	해킹당할 수 있는 기기			
7	해커가 개방형 Wi-Fi에서 볼 수 있는 것			
8	가짜 Wi-Fi 네트워크의 징후			
9	공용 Wi-Fi의 대안			
10	이메일의 경고 신호			
11	공용 Wi-Fi에서 하지 않는 일			
12	무료 Wi-Fi가 있는 장소			
13	계정을 보호하는 방법			
14	컴퓨터가 감염되었다는 신호			
15	수상해 보이는 Wi-Fi 이름			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 공용 Wi-Fi 패킷 스니핑 차단



상황: 공항 공용 Wi-Fi 네트워크에 연결한 한 원격 영업 임원이 여러 민감한 업무 이메일을 평문으로 보낸 직후 유출된 것을 알게 됩니다.

토론 질문: 공용 네트워크의 위험을 분석하고, 트래픽 암호화 해결책을 간략히 설명하세요.

사례 연구 2: 이블 트윈 가짜 핫스팟 방어



상황: 공격자들이 합법적인 카페 핫스팟을 흉내 낸 'CoffeeShop_Guest'라는 이름의 불법 무선 액세스 포인트를 설치하여, 아무것도 모르는 손님들의 네트워크 트래픽을 가로챕니다.

토론 질문: 불법 액세스 포인트를 탐지하고 차단하는 확인 단계를 자세히 설명하세요.

체크포인트 9: 암호 해독하기

사이버 보안 전문가는 온라인 위협 행위자로부터 네트워크 자산을 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 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

1	28	12	12	32	12		12	29	12	40	18	20	12	40
17	**38**	**6**	**21**	**18**	**40**	**1**		**12**	**20**	**7**	**19**	**28**	**19**	**29**

해독된 메시지:

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

체크포인트 10: 기초 사이버 보안 FAQ (파트 A)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q1: 공용 Wi-Fi는 왜 안전하지 않은가요?

공개 Wi-Fi는 무선 구간에서 트래픽을 암호화하지 않으므로, 주변 사람이 보호되지 않은 데이터를 가로챌 수 있습니다. [2]

Q2: 패킷 스니핑이란 무엇인가요?

패킷 스니퍼는 네트워크 인터페이스를 흐르는 원시 데이터를 캡처해 평문 비밀번호와 트래픽 세부 정보를 노출합니다.

Q3: 이블 트윈(Evil Twin)이란 무엇인가요?

신뢰할 수 있는 지역 Wi-Fi 핫스팟의 이름과 설정을 흉내 내 해커가 만든 불법 액세스 포인트.

Q4: VPN은 나를 어떻게 보호하나요?

트래픽을 암호화된 터널로 보내 로컬 네트워크 스니퍼가 내 탐색 활동을 볼 수 없게 합니다.

Q5: 공용 Wi-Fi에서 HTTPS가 나를 보호해 주나요?

예, 브라우저와 웹사이트 사이에 오가는 데이터를 암호화하며, VPN은 보호 계층을 하나 더 추가합니다.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: WPA3란 무엇인가요?

더 강력한 암호화와 오프라인 사전 공격 방어를 제공하는 최신 Wi-Fi Protected Access 표준입니다. [1]

Q7: 공용 Wi-Fi로 악성코드가 전달될 수 있나요?

예, 공격자는 트래픽을 가로채 브라우저 세션에 악성 다운로드 창(드라이브 바이 다운로드)을 삽입할 수 있습니다.

Q8: 파일 공유의 위험은 무엇인가요?

파일 공유가 켜져 있으면 공용 네트워크의 다른 사용자가 내 로컬 폴더 디렉터리를 읽거나 수정할 수 있습니다.

Q9: 캡티브 포털이란 무엇인가요?

호텔이나 카페 네트워크가 인터넷 접속을 허용할 때 쓰는 로그인 페이지로, 공격자가 위조하는 경우도 있습니다.

Q10: 사용하지 않을 때 Wi-Fi를 꺼야 하나요?

예, Wi-Fi를 끄면 기기가 신뢰할 수 없는 네트워크에 자동으로 연결되는 것을 막을 수 있습니다.

체크포인트 10: 심화 보안 FAQ (파트 C)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q1: 중간자 공격은 DNS를 어떻게 악용하나요?

불량 라우터에서 DNS 스푸핑을 사용해 대상 브라우저를 실제 도메인이 아닌 비슷하게 생긴 피싱 랜딩 페이지로 보냄으로써.

Q2: 세션 하이재킹이란 무엇인가요?

공격자가 공용 Wi-Fi에서 암호화되지 않은 세션 쿠키를 스니핑해 가져온 뒤 자격 증명 로그인을 우회합니다.

Q3: SSL 스트리핑이란 무엇인가요?

공격자가 사용자의 안전한 HTTPS 요청을 암호화되지 않은 HTTP로 낮춰 로그인 정보를 평문으로 가로채는 중간자 공격.

Q4: HSTS는 SSL 스트리핑을 어떻게 막나요?

HTTP Strict Transport Security는 브라우저가 HTTPS로만 연결하도록 강제하며, 암호화되지 않은 HTTP로의 대체 연결을 거부합니다. [3]

Q5: 스플릿 터널 VPN이란 무엇인가요?

회사 트래픽만 VPN으로 보내고 공용 인터넷 데이터는 직접 보내는 구성으로, 유출 경로가 노출될 위험이 있습니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q6: WPA2가 KRACK에 취약한 이유는 무엇인가요?

Key Reinstallation Attack은 WPA2 4-way 핸드셰이크를 악용하여 Wi-Fi 비밀번호 없이 패킷을 복호화합니다.

Q7: 클라이언트 격리란 무엇인가요?

연결된 Wi-Fi 기기끼리 직접 통신하지 못하게 해 로컬 스니핑을 막는 라우터 보안 설정.

Q8: 공격자는 가짜 DNS 서버를 어떻게 이용하나요?

가짜 DNS 서버를 클라이언트에 할당하는 악성 공유기를 설정하여 모든 웹 조회를 가로채고 변조합니다.

Q9: VPN이 내 로컬 MAC 주소를 숨길 수 있나요?

아니요. MAC 주소는 로컬 2계층 식별자이므로, 대신 기기에 내장된 MAC 무작위화(비공개 주소) 설정을 사용하세요.

Q10: 캡티브 포털 스푸핑 공격이란 무엇인가요?

무료 Wi-Fi 접속을 가장해 자격 증명을 훔치려고 불법 핫스팟에 가짜 인증 포털을 호스팅하는 공격자.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

보안 침해, 방어 메커니즘, 규정 준수 표준에 관한 실제 사실을 살펴보세요.

1. 보안 인사이트

원격 근무자는 카페, 호텔, 공항의 Wi-Fi를 자주 사용하는데, 이런 곳에서는 네트워크의 보안을 통제할 수 없습니다.

2. 보안 인사이트

이블 트윈 불법 핫스팟은 신뢰하는 네트워크의 이름과 MAC 주소를 똑같이 복사해 기기를 혼동시킬 수 있습니다.

3. 보안 인사이트

Wireshark 같은 패킷 스니핑 소프트웨어는 무료이며 암호화되지 않은 HTTP 비밀번호를 평문으로 보여줄 수 있습니다.

4. 보안 인사이트

WPA3 보안은 동등 인증 동시 협상(SAE)을 사용해 로컬 무차별 대입 공격으로부터 보호합니다.

5. 보안 인사이트

SSL 스트리핑 공격은 게이트웨이에서 최초의 HTTP 리디렉션을 가로채 기본적인 HTTPS 보호를 우회합니다.

6. 보안 인사이트

HTTP Strict Transport Security(HSTS) 응답 헤더는 브라우저가 암호화되지 않은 HTTP 연결로 되돌아가는 것을 막습니다. [3]

7. 보안 인사이트

'자동 연결'을 끄면 스마트폰이 공공장소의 비슷하게 위장한 악성 네트워크에 연결되는 것을 막을 수 있습니다.

8. 보안 인사이트

기업의 '상시 연결' VPN 구성은 모든 원격 근무자의 네트워크 트래픽이 기업 방화벽을 거치도록 강제합니다.

9. 보안 인사이트

불법 액세스 포인트는 위조된 DNS 응답을 돌려줘 대상 도메인을 피싱 서버로 보낼 수 있습니다.

10. 보안 인사이트

VPN이 없으면 공개 핫스팟의 다른 사용자가 여러분의 기기가 접속하는 사이트와 서버를 볼 수 있습니다.

기술 참고 자료 및 출처

이 학습 가이드와 인터랙티브 퍼즐은 전 세계 NIST, OWASP, 개인정보 보호 규정 준수 표준을 바탕으로 만들었습니다.

학술 및 업계 참고 자료

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

답안: 체크포인트 1 – 객관식

1 질문 1 정답: A

교사용 참고

중간자(MitM) 공격이란 무엇입니까? → 공유 네트워크에서 두 당사자 사이의 통신을 가로채 변조함

2 질문 2 정답: A

교사용 참고

불량 액세스 포인트(이블 트윈)란 무엇입니까? → 정상 네트워크와 같은 SSID로 구성된 악성 Wi-Fi 핫스팟

3 질문 3 정답: A

교사용 참고

VPN은 공용 Wi-Fi 트래픽을 어떻게 보호하나요? → 모든 네트워크 패킷을 암호화 터널로 감싸 스니퍼가 읽을 수 없게 함

4 질문 4 정답: A

교사용 참고

패킷 스니핑이란 무엇입니까? → 하드웨어나 소프트웨어 도구로 네트워크 패킷을 캡처하고 기록함

5 질문 5 정답: A

교사용 참고

HTTPS의 역할은 무엇입니까? → 브라우저와 웹 서버 사이의 세션 트래픽 암호화

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 — 정답: 참

교사용 참고

연결된 사용자는 개방된 공용 Wi-Fi 네트워크에서 일반 텍스트 데이터를 쉽게 가로챌 수 있습니다.

7 질문 7 — 정답: 거짓

교사용 참고

거짓: 이블 트윈은 공격자가 진짜 핫스팟을 흉내 내어 만든 허가되지 않은 핫스팟입니다.

8 질문 8 — 정답: 거짓

교사용 참고

거짓: VPN은 트래픽을 터널 안에서 암호화하므로 로컬 스니퍼가 이를 읽을 수 없습니다.

9 질문 9 — 정답: 거짓

교사용 참고

거짓: HTTPS는 URL 경로와 페이지 내용을 포함한 HTTP 교환 전체를 암호화합니다.

10 질문 10 — 정답: 참

교사용 참고

WPA3 보안을 사용하는 Wi-Fi 핫스팟은 비밀번호가 없는 개방형 네트워크보다 더 강력한 보호를 제공합니다.

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

E 1. 가로채기	F 2. 스니핑	D 3. 이블 트윈	H 4. HTTPS
G 5. VPN	B 6. 터널	A 7. WPA3	C 8. 방화벽

체크포인트 3: 답안 – 핵심 용어

1 가로채기	2 스니핑	3 이블 트윈	4 HTTPS
5 VPN	6 터널		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 G – 오픈브이피엔	2 C – 스니핑	3 B – 오픈소스	4 F – 아이피주소
5 H – 트래픽	6 A – 와이어가드	7 E – 이블트윈	8 D – 공용와이파이

교사를 위한 토론 참고

핵심 용어:
학생들이 가로채기, 스니핑, 이블 트윈을 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

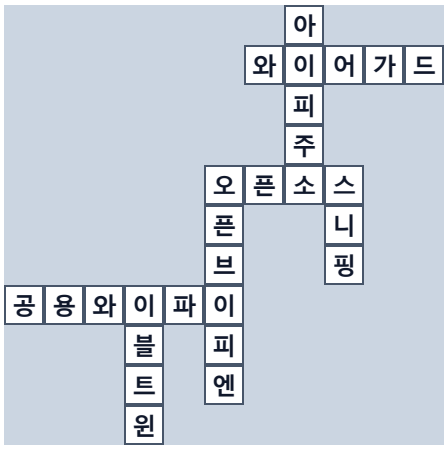
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

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

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 와이어가드 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5 글자)

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

5 가로: 공용와이파이 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷 (6 글자)

세로

1 세로: 아이피주소 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5 글자)

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

4 세로: 스니핑 네트워크를 지나는 데이터 패킷을 몰래 붙잡아 들여다보는 일 (3 글자)

6 세로: 이블트윈 정상 와이파이와 같은 이름으로 만들어 놓은 가짜 접속 지점 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 가어와드이 — **와이어가드**
2. 핑니스 — **스니핑**
3. 윈이트블 — **이블트윈**
4. 엔이브피오픈 — **오픈브이피엔**
5. 스오소픈 — **오픈소스**
6. 파이공와이용 — **공용와이파이**
7. 주소아피이 — **아이피주소**
8. 픽래트 — **트래픽**

비밀 암호 도전 정답

"공용 와이파이 트래픽 암호화"

사례 연구 답안

A 사례 연구 1: 공용 Wi-Fi 패킷 스니핑 차단

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 공항 공용 Wi-Fi 네트워크에 연결한 한 원격 영업 임원이 평문으로 보낸 민감한 업무 이메일 몇 통이 보낸 직후 유출된 것을 알아챕니다.
- 권장 전략 및 해결책: 모든 원격 근무 PC에서 기업용 VPN 클라이언트 사용을 의무화하세요. HTTPS 전용 브라우저 확장 프로그램을 적용하고, 클라이언트 방화벽에서 HTTP나 FTP 같은 암호화되지 않은 프로토콜을 차단합니다.

B 사례 연구 2: 이블 트윈 가짜 핫스팟 방어

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 공격자들이 정상적인 카페 핫스팟을 흉내 내 'CoffeeShop_Guest'라는 이름의 불법 무선 액세스 포인트를 설치하고, 아무것도 모르는 손님들의 네트워크 트래픽을 가로챕니다.
- 권장 전략 및 해결책: 액세스 포인트 BSSID MAC 주소를 점검해 네트워크의 진위를 확인합니다. 클라이언트 상태 검증을 적용해 개방형 네트워크 연결을 차단하고, 민감한 업무에는 휴대전화 핫스팟을 사용하도록 의무화합니다.