이름: _____ 날짜: _____ 점수: _____

다크웹 대 딥웹: 보안 및 차이점

검색 엔진 색인, 딥 웹 데이터베이스, Tor 어니언 라우팅, 네트워크 익명성과 위험

다크 웹과 딥 웹 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 딥웹과 다크웹의 차이를 안내합니다. 색인되지 않은 데이터베이스, Tor 브라우저 어니언 라우팅, .onion 암호화 도메인, 익명성 보안 위험을 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/dark-web-vs-deep-web/

나의 딥웹 및 다크웹 전략 학습 로드맵

- 딥 웹(색인되지 않은 데이터베이스)과 다크 웹(어니언 서비스)을 비교하세요.
- 어니언 라우팅이 네트워크 트래픽을 어떻게 암호화하고 중계하는지 이해합니다.
- 검증되지 않은 Tor 네트워크 사이트에 접속할 때의 보안 위험을 평가하세요.
- 위협 인텔리전스 크롤링을 위한 보안 게이트웨이와 샌드박스 정책을 배포하세요.
- 어니언 서비스 도메인의 암호화 주소 형식을 분석하세요.

딥웹 및 다크웹 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 딥 웹과 다크 웹의 개인정보 보호에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

딥웹 데이터베이스 대 다크웹 어니언 라우팅 (소개)

딥 웹은 개인 이메일이나 기업 은행 포털처럼 비밀번호와 로그인 뒤에 있는 색인되지 않은 페이지로 이루어져 있습니다. 다크 웹은 딥 웹의 부분집합으로 의도적으로 숨겨져 있으며, 익명으로 접속하려면 (Tor 같은) 특수 브라우저와 어니언 네트워크가 필요합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 딥 웹과 서피스 웹의 차이는 무엇입니까?

- A. 딥 웹 페이지는 공개 검색 엔진에 색인되지 않음
- B. 딥 웹 트래픽은 불법이며 수사기관이 감시한다
- C. 딥 웹 사이트는 접근하려면 Tor 같은 특수 브라우저가 필요하다
- D. 딥 웹 페이지는 항상 표면 웹 페이지보다 빨리 로드된다

2 2. 다크 웹에는 어떻게 접속하나요?

- A. 어니언 라우팅 네트워크를 이용하는 전용 브라우저를 통해
- B. 일반 라우터에 사용자 지정 DNS 설정을 구성하여
- C. 초대받은 사람만 쓸 수 있는 비공개 표면 웹 검색 콘솔을 통해
- D. 표준 광고 차단 브라우저 확장 프로그램을 설치해서

3 3. 딥 웹에서 가장 큰 비중을 차지하는 구조는 무엇입니까?

- A. 비밀번호로 보호된 사용자 데이터베이스와 비공개 계정
- B. 불법 물품을 거래하는 불법 암시장 포럼
- C. 암호화되지 않은 피어 투 피어 파일 공유 프로토콜
- D. 공개 검색 엔진 캐시 데이터베이스

4 4. 어니언 라우팅은 네트워크 트래픽에 어떤 작용을 합니까?

- A. 패킷을 암호화해 여러 릴레이를 거쳐 보냄
- B. ISP 노드를 우회하여 다운로드 속도를 높인다
- C. 장치 하드웨어 일련번호를 IP 기록에 연결한다
- D. 클릭할 때마다 웹 브라우저 쿠키를 삭제한다

5 5. Tor 네트워크에서만 사용되는 도메인 접미사는 무엇입니까?

- A. 암호화된 .onion 최상위 확장자
- B. 표준적인 기존 .com 상업용 확장자
- C. Web3 분산형 .eth 블록체인 확장자
- D. 국가 코드 .ai 기술 확장자

체크포인트 2: 참/거짓 도전

6 질문 tf 6

6. 딥 웹과 다크 웹은 같은 네트워크 영역을 가리킵니다.

○ 참 ○ 거짓

7 질문 tf 7

7. 기업 인트라넷 포털은 딥 웹에 속합니다.

○ 참 ○ 거짓

8 질문 tf 8

8. 어니언 라우팅은 모든 전송 노드에서 데이터 패킷을 완전히 복호화합니다.

○ 참 ○ 거짓

9 질문 tf 9

9. 다크 웹에 접속하면 기기가 높은 악성코드 위험에 노출됩니다.

○ 참 ○ 거짓

10 질문 tf 10

10. 일반 웹 검색 엔진은 onion 사이트를 크롤링하고 색인합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 비공개 은행 포털은 색인되지 않은 _____ 영역에 있습니다.
2. 특수 토르 노드가 숨겨진 _____ 서비스를 호스팅합니다.
3. 토르 웹사이트는 암호화 방식의 _____ 최상위 확장자를 씁니다.
4. 암호화된 다중 계층 트래픽 경로를 _____ (이)라고 합니다.
5. 일반 검색 엔진은 공개적으로 _____ 된 페이지를 수집합니다.
6. 어니언 네트워크는 클라이언트 IP를 암호화해 사용자 _____ 을(를) 지킵니다.

어휘 단어 목록

다크웹 | 딥웹 | 라우팅 | 색인 | 암호 키 | 어니언 | 익명성 | 인터넷 주소

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

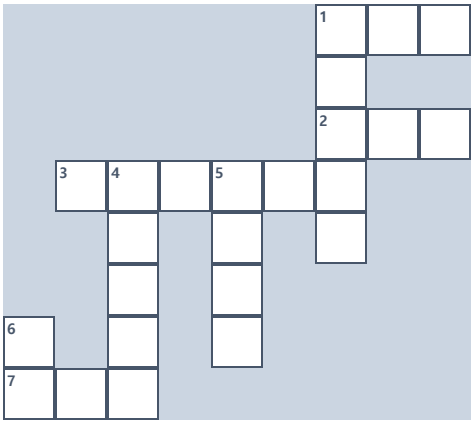
정의 연결하기

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

1. 딥 웹 영역	A	특수한 브라우저로만 접근할 수 있는 암호화된 네트워크 구간.
2. 다크 웹 포털	B	데이터를 여러 겹으로 암호화하여 세 개의 노드를 거쳐 중계하는 것.
3. 어니언 확장자	C	색인되지 않은 시스템 기록을 보관하는 안전한 백엔드 저장소.
4. Tor 라우팅	D	Tor 네트워크에서 쓰는 암호화 최상위 도메인 접미사.
5. 색인된 페이지	E	Tor 네트워크에 접속하는 데 사용하는 진입점 노드입니다.
6. 사용자 익명성	F	Google에서 수집되어 검색 가능한 표면 웹 콘텐츠.
7. 비공개 데이터베이스	G	클라이언트의 공인 IP 주소를 서버로부터 숨기는 것.
8. 진입 게이트웨이	H	비공개 로그인, 이메일, 데이터베이스 기록 같은 색인되지 않은 웹 콘텐츠입니다.

체크포인트 5: 십자말풀이

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



가로

1. 특수한 소프트웨어로만 접속하는 숨겨진 웹 (3)

2. 데이터를 잠그고 푸는 열쇠 역할의 값 (3)

3. 개인정보를 안전하게 지키는 일 (6)

7. 웹사이트를 찾아가는 데 쓰는 문자열 (3)

세로

1. 데이터를 겹겹이 암호화해 노드 세 곳을 거쳐 전달하는 방식 (5)

4. 인터넷에서 사이트를 찾아가는 주소 (5)

5. 정보와 시스템을 위험에 빠뜨리는 요소 (4)

6. 검색 엔진에 잡히지 않는 웹 영역 (2)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

1 가로: 특수한 소프트웨어로만 접속하는 숨겨진 웹 (3 글자):

2 가로: 데이터를 잠그고 푸는 열쇠 역할의 값 (3 글자):

3 가로: 개인정보를 안전하게 지키는 일 (6 글자):

7 가로: 웹사이트를 찾아가는 데 쓰는 문자열 (3 글자):

세로

1 세로: 데이터를 겹겹이 암호화해 노드 세 곳을 거쳐 전달하는 방식 (5 글자):

4 세로: 인터넷에서 사이트를 찾아가는 주소 (5 글자):

5 세로: 정보와 시스템을 위험에 빠뜨리는 요소 (4 글자):

6 세로: 검색 엔진에 잡히지 않는 웹 영역 (2 글자):

체크포인트 6: 숨은 단어 찾기

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

다 안 청 파 트 청 시 협 관 카 벽 연 전 터 버
접 화 라 스 차 다 위 터 다 송 트 키 카 타 다
번 협 트 정 리 밀 보 데 하 크 접 용 카 마 위
웹 위 나 버 술 도 호 정 웹 이 웹 험 요 다 개
용 안 타 인 답 개 암 딥 접 검 안 결 화 아 격
정 보 서 번 공 인 암 다 결 검 접 딥 웹 이 사
템 험 리 파 방 정 술 마 중 가 마 사 송 색 방
용 색 넷 검 스 보 터 카 개 암 비 용 카 정 번
밀 터 속 연 네 보 비 비 속 격 호 험 스 시 버
소 바 관 접 이 호 크 위 바 요 차 화 관 딥 메
주 인 터 넷 주 소 사 웹 요 안 터 트 키 차 암
웹 밀 카 개 답 연 사 도 마 가 키 데 차 호 넷
나 카 이 카 보 트 호 차 격 속 암 파 키 정 위
웹 관 보 개 주 하 나 나 개 송 밀 결 스 검 속
용 격 스 위 자 밀 중 마 안 위 답 응 술 나 격

어휘 단어 목록

인터넷주소 보안위협 개인정보보호 다중암호화 딥웹 웹주소 다크웹 암호키

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. 인터넷주소
B. 보안위협
C. 개인정보보호
D. 다중암호화
E. 딥웹
F. 웹주소
G. 다크웹
H. 암호키

정의 및 연결 항목
____ 1. 웹사이트를 찾아가는 데 쓰는 문자열.
____ 2. 특수한 소프트웨어로만 접속하는 숨겨진 웹.
____ 3. 데이터를 겹겹이 암호화해 노드 세 곳을 거쳐 전달하는 방식.
____ 4. 인터넷에서 사이트를 찾아가는 주소.
____ 5. 정보와 시스템을 위험에 빠뜨리는 요소.
____ 6. 개인정보를 안전하게 지키는 일.
____ 7. 데이터를 잠그고 푸는 열쇠 역할의 값.
____ 8. 검색 엔진에 잡히지 않는 웹 영역.

체크포인트 7: 뒤섞인 단어 도전

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

1. 주 넷 인 소 터 _____

2. 호 개 정 보 보 인 _____

3. 웹 딥 _____

4. 크 웹 다 _____

5. 협 보 위 안 _____

6. 호 다 암 화 중 _____

7. 소 주 웹 _____

8. 키 호 암 _____

보너스 활동: 빠르게 생각하기

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

1	다크 웹을 멀리해야 하는 이유			
2	검색 엔진이 찾을 수 없는 것			
3	해킹당할 수 있는 기기			
4	Tor를 사용하는 합법적인 이유			
5	소프트웨어를 업데이트하는 이유			
6	이메일의 경고 신호			
7	다크 웹에서 불법으로 판매되는 것			
8	IT 도움을 요청할 수 있는 사람			
9	오늘부터 시작할 수 있는 안전 습관			
10	데이터가 유출된 후에 할 일			
11	딥 웹에 속하는 것			
12	로그인해서 사용하는 사이트			
13	익명성과 관련된 단어			
14	절대 공유하면 안 되는 정보			
15	'수면 아래'에 있는 것			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 데이터 유출 식별



상황: 기업 보안 감사에서 민감한 고객 데이터베이스 기록이 어니언 마켓에서 거래되고 있음이 밝혀집니다. 이 데이터는 Google에 색인되어 있지 않습니다.

토론 질문: 어떤 웹 영역이 관련되어 있으며 이 유출이 어떻게 일어났는지 설명하세요.

사례 연구 2: 익명성과 악성코드 위험 비교



상황: 한 분석가가 Tor 웹사이트에서 위협 인텔리전스 피드를 확인하려고 합니다. 이 분석가는 Tor 브라우저를 다운로드하고 해당 사이트에 접속합니다.

토론 질문: 익명성의 이점을 평가하고 악성코드 완화 단계를 간략히 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

12	24	3	40	12	24	3		6	20	12	33	17	40	12	12	38	6	28

12	40	1	7	26	12	10	24	12		12	37	13	40

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: 딥 웹이란 무엇인가요?

딥 웹은 온라인 뱅킹, 이메일 데이터베이스, 유료 구독 저널 등 검색 엔진이 색인할 수 없는 모든 웹 페이지로 이루어져 있습니다.

Q2: 다크 웹이란 무엇인가요?

다크 웹은 딥 웹의 작은 부분집합으로, 의도적으로 숨겨져 있으며 어니언 네트워크를 사용하는 특수 브라우저로만 접속할 수 있습니다.

Q3: 검색 엔진은 페이지를 어떻게 색인하나요?

검색 엔진은 자동화된 프로그램(스파이더)을 실행해 공개 링크를 따라가며, 로봇 지시문으로 크롤링을 막지 않은 페이지를 색인합니다.

Q4: 온라인 뱅킹이 딥 웹에 속하는 이유는 무엇인가요?

은행 포털은 로그인과 비밀번호 뒤에 있으므로 공개 검색 엔진이 계좌 명세서 페이지를 색인하지 못하게 막습니다.

Q5: Tor 브라우저의 어니언 라우팅이란 무엇인가요?

어니언 라우팅은 트래픽을 계층별로 암호화해 여러 릴레이로 전달하여 사용자 IP 주소를 가리는 전송 방식입니다.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 다크 웹에 접속하는 것은 불법인가요?

아니요. 다크 웹 접속은 대부분의 국가에서 합법이지만, 불법 시장이나 사이버 범죄 활동에 참여하는 것은 금지되어 있습니다.

Q7: 다크 웹 사이트는 왜 로딩이 느린가요?

트래픽은 최소 세 개의 글로벌 릴레이(진입, 중간, 출구)를 거쳐 라우팅되고 복호화되므로 전송 지연이 늘어납니다.

Q8: .onion 도메인 접미사는 무슨 뜻인가요?

Tor 네트워크에서 쓰이는 특수한 최상위 도메인 접미사로, 표준 DNS 서버가 아니라 암호학적으로 생성된 주소를 가리킵니다.

Q9: 다크 웹 링크에는 어떤 위험이 있나요?

이 사이트들은 보안 검사가 없어 사용자가 악성코드 감염, 피싱 스크립트, 거래 사기에 높은 비율로 노출됩니다.

Q10: Tor 네트워크 라우팅 프로토콜은 누가 만들었나요?

이 기술은 정부 통신을 보호하기 위해 1990년대에 미국 해군 연구소(U.S. Naval Research Laboratory)가 처음 개발했습니다.

체크포인트 10: 심화 보안 FAQ (파트 C)

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

Q1: 중간 노드는 Tor의 익명성을 어떻게 보호하나요?

각 노드는 라우팅 데이터의 한 겹만 복호화하므로 이전 홉과 다음 홉만 알 뿐, 출발지와 목적지를 모두 알지는 못합니다.

Q2: 출구 노드의 역할은 무엇인가요?

출구 노드는 마지막 암호화 계층을 복호화하여 트래픽을 공개 목적지 서버나 어니언 서버로 내보냅니다.

Q3: Tor 브리지 게이트웨이란 무엇인가요?

브리지는 Tor 브라우저 접속을 제한하는 지역에서 ISP 차단과 검열을 우회하는 데 쓰는, 공개 목록에 없는 Tor 진입 릴레이입니다.

Q4: 다크 웹 행위자는 암호화폐를 어떻게 악용하나요?

행위자들은 익명 암호화폐를 사용해 다크 마켓에서 금융 거래를 하며 일반 은행 거래 점검을 피합니다.

Q5: 일반 검색 엔진이 딥 데이터베이스를 크롤링하지 못하는 이유는 무엇인가요?

크롤러는 로그인 자격 증명을 입력하거나, 보안 CAPTCHA를 풀거나, 딥 데이터베이스에 접근하는 데 필요한 백엔드 SQL 쿼리 스크립트를 실행할 수 없습니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

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

Q6: Tor 네트워크의 디렉터리 서버란 무엇인가요?

클라이언트가 라우팅 경로를 구성할 때 사용하는 활성 진입, 중간, 출구 릴레이 목록을 관리하는 신뢰할 수 있는 서버입니다.

Q7: 악의적인 행위자는 출구 노드 스니핑을 어떻게 수행하나요?

악의적인 출구 노드 운영자는 암호화되지 않은 HTTP 트래픽이 Tor 네트워크를 떠날 때 가로채 사용자 이름과 쿠키를 훔칠 수 있습니다.

Q8: Tor와 I2P는 어떻게 다른가요?

Tor는 중앙집중식 릴레이 디렉터리와 공개 웹 접속용 출구 노드를 사용하고, I2P는 내부 호스팅에 분산형 P2P 구조를 사용합니다.

Q9: 법 집행 기관은 다크 웹 시장을 어떻게 추적하나요?

수사 기관은 블록체인 분석을 사용하고, 물리 서버 호스팅 환경을 추적하고, 위장 작전을 벌여 운영자를 식별합니다.

Q10: DNS 유출은 어떻게 클라이언트의 익명성을 해치나요?

DNS 유출은 브라우저의 DNS 쿼리가 암호화된 Tor 네트워크를 거치지 않고 현지 ISP를 통해 직접 전송될 때 발생합니다.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

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

1. 보안 인사이트

대부분의 콘텐츠가 로그인과 데이터베이스 뒤에 있으므로 딥 웹은 검색 가능한 표면 웹보다 훨씬 큽니다.

2. 보안 인사이트

다크 웹은 딥 웹 중 의도적으로 숨겨진 작은 부분으로, Tor 같은 도구로 접속합니다.

3. 보안 인사이트

Tor 라우팅은 데이터 패킷을 세 번 암호화하며, 각 릴레이 노드에서 양파처럼 암호화 계층을 한 겹씩 벗깁니다.

4. 보안 인사이트

Tor는 미국 해군 연구소가 진행한 어니언 라우팅 프로젝트에서 시작되었고, 코드는 무료 소프트웨어로 공개되었습니다. [1]

5. 보안 인사이트

어니언 주소는 공개 키 쌍에서 암호학적으로 생성된 56자 영숫자 문자열입니다.

6. 보안 인사이트

출구 노드는 평문 트래픽을 읽을 수 있으므로, Tor에서도 안전한 세션 데이터를 위해 TLS/HTTPS가 여전히 필요합니다.

7. 보안 인사이트

인트라넷 사이트, 클라우드 드라이브, 비공개 데이터베이스는 딥 웹에서 가장 큰 데이터 저장 영역입니다.

8. 보안 인사이트

DuckDuckGo 같은 전문 검색 엔진은 어니언 포털을 운영하여 Tor 네트워크에서 익명 검색을 가능하게 합니다.

9. 보안 인사이트

매일 200만 명이 넘는 사용자가 검열을 우회하고 통신 사생활을 지키기 위해 Tor 네트워크에 접속합니다.

10. 보안 인사이트

Operation Bayonet 같은 국제 법 집행 작전은 호스팅 하드웨어를 압수하여 주요 다크 마켓플레이스를 폐쇄했습니다.

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] Tor Project. (n.d.). Why is it called Tor?

https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?

https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.

https://metrics.torproject.org/userstats-relay-country.html

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

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

[5] 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

답안: 체크포인트 1 – 객관식

1 검색 색인 딥웹 정답: A

교사용 참고

딥웹 페이지는 로그인 장벽과 데이터베이스 뒤에 있어 검색 스파이더가 크롤링하지 못합니다. 출처: IETF RFC 3986.

2 Tor 접속 다크 웹 정답: A

교사용 참고

다크 웹은 Tor 같은 브라우저로만 접속할 수 있는 숨겨진 어니언 서비스로 이루어져 있습니다. 출처: IETF RFC 3986.

3 딥 데이터베이스 데이터베이스 정답: A

교사용 참고

비밀번호로 보호되는 계정과 기업 기록이 딥 웹의 가장 큰 부분을 차지합니다. 인용: NIST Digital Identity.

4 어니언 라우팅 Tor 네트워크 정답: A

교사용 참고

어니언 라우팅은 데이터 패킷을 계층별로 암호화해 여러 노드를 거쳐 전달함으로써 익명성을 높입니다. 인용: IETF RFC 3986.

5 어니언 도메인 접미사 정답: A

교사용 참고

암호화 방식의.onion 도메인 접미사는 공용 DNS 없이 Tor 내부에서 트래픽을 라우팅합니다. 출처: IETF RFC 3986.

답안: 체크포인트 2 – 참 또는 거짓

6 **웹 구간** 구조 정답: 거짓

교사용 참고

딥 웹은 색인되지 않은 모든 페이지를 포함하는 반면, 다크 웹은 암호화된 어니언 네트워크의 작은 일부입니다. 출처: IETF RFC 3986.

7 **기업 인트라넷** 딥웹 정답: 참

교사용 참고

인트라넷 사이트는 비밀번호 포털 뒤에 있고 색인되지 않으므로 딥 웹에 속합니다. 출처: NIST Digital Identity.

8 **계층 암호화** 릴레이 정답: 거짓

교사용 참고

어니언 릴레이는 사용자의 익명성을 지키기 위해 라우팅 계층을 하나만 복호화하며 패킷 전체를 복호화하지 않습니다. 인용: IETF RFC 3986.

9 **악성코드 노출** 위협 정답: 참

교사용 참고

다크웹 마켓은 보안 필터링이 없어 악성코드 감염 위험이 매우 큽니다. 출처: Center for Internet Security (CIS).

10 **질문 10** 정답: 거짓

교사용 참고

일반 검색 엔진 크롤러는 Tor를 사용하지 않으므로 .onion 사이트에 접근하거나 색인할 수 없습니다.

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

H 1. 딥 웹 영역	A 2. 다크 웹 포털	D 3. 어니언 확장자	B 4. Tor 라우팅
F 5. 색인된 페이지	G 6. 사용자 익명성	C 7. 비공개 데이터베이스	E 8. 진입 게이트웨이

체크포인트 3: 답안 – 핵심 용어

1 딥웹	2 다크웹	3 어니언	4 라우팅
5 색인	6 익명성		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 F – 웹주소	2 G – 다크웹	3 D – 다중암호화	4 A – 인터넷주소
5 B – 보안위협	6 C – 개인정보보호	7 H – 암호키	8 E – 딥웹

교사를 위한 토론 참고

핵심 용어:
학생들이 딥 웹 영역, 다크 웹 포털, 어니언 확장자를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

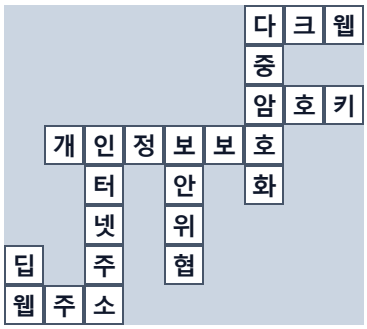
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

다	안	청	파	트	청	시	협	관	카	벽	연	전	터	버
접	화	라	스	차	다	위	터	다	송	트	키	카	타	다
번	협	트	정	리	밀	보	데	하	크	접	용	카	마	위
웹	위	나	버	술	도	호	정	웹	이	웹	험	요	다	개
용	안	타	인	답	개	암	딥	접	검	안	결	화	아	격
정	보	서	번	공	인	암	다	결	검	접	딥	웹	이	사
템	험	리	파	방	정	술	마	중	가	마	사	송	색	방
용	색	넷	검	스	보	터	카	개	암	비	용	카	정	번
밀	터	속	연	네	보	비	비	속	격	호	험	스	시	버
소	바	관	접	이	호	크	위	바	요	차	화	관	딥	메
주	인	터	넷	주	소	사	웹	요	안	터	트	키	차	암
웹	밀	카	개	답	연	사	도	마	가	키	데	차	호	넷
나	카	이	카	보	트	호	차	격	속	암	파	키	정	위
웹	관	보	개	주	하	나	나	개	송	밀	결	스	검	속
용	격	스	위	자	밀	중	마	안	위	답	응	술	나	격

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

1 가로: 다크웹 특수한 소프트웨어로만 접속하는 숨겨진 웹 (3 글자)

2 가로: 암호키 데이터를 잠그고 푸는 열쇠 역할의 값 (3 글자)

3 가로: 개인정보보호 개인정보를 안전하게 지키는 일 (6 글자)

7 가로: 웹주소 웹사이트를 찾아가는 데 쓰는 문자열 (3 글자)

세로

1 세로: 다중암호화 데이터를 겹겹이 암호화해 노드 세 곳을 거쳐 전달하는 방식 (5 글자)

4 세로: 인터넷주소 인터넷에서 사이트를 찾아가는 주소 (5 글자)

5 세로: 보안위협 정보와 시스템을 위험에 빠뜨리는 요소 (4 글자)

6 세로: 딥웹 검색 엔진에 잡히지 않는 웹 영역 (2 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 주넷인소터 — **인터넷주소**
2. 호개정보보인 — **개인정보보호**
3. 웹딥 — **딥웹**
4. 크웹다 — **다크웹**
5. 협보위안 — **보안위협**
6. 호다암화중 — **다중암호화**
7. 소주웹 — **웹주소**
8. 키호암 — **암호키**

비밀 암호 도전 정답

"어니언 라우팅으로 익명성 유지"

사례 연구 답안

A 사례 연구 1: 데이터 유출 식별

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 기업 보안 감사에서 민감한 고객 데이터베이스 기록이 어니언 마켓플레이스에서 거래되고 있음이 드러납니다. 이 데이터는 Google에 색인되어 있지 않습니다.
- 권장 전략 및 해결책: 관련 영역: 비공개 데이터베이스는 딥 웹(색인되지 않았지만 안전한 영역)에 속합니다. 도난당한 데이터를 거래하는 마켓플레이스는 다크 웹(어니언 네트워크)에 있습니다. 발생 경위: 해커가 서버 방어를 뚫고 딥 웹에서 데이터베이스를 훔친 뒤, 법 집행 기관의 추적을 피하려고 다크 웹에 익명으로 올렸습니다.

B 사례 연구 2: 익명성과 악성코드 위험 비교

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 분석가가 Tor 웹사이트에서 위협 인텔리전스 피드를 확인하려 합니다. Tor 브라우저를 내려받아 사이트에 접속합니다.
- 권장 전략 및 해결책: 이점: Tor는 트래픽을 세 개의 노드를 거쳐 보내 분석가의 회사 IP를 가립니다. 위험 및 완화책: 다크 웹 링크에는 평판 검증이 없습니다. 분석가는 Tor를 격리된 가상 머신(VM) 안에서 실행하고, Tor 설정에서 JavaScript를 끄며, 회사 네트워크를 보호하기 위해 어떤 파일도 내려받지 않아야 합니다.