이름: _____ 날짜: _____ 점수: _____

신원 도용 예방과 자산 보안 가이드

자격 증명 유출, MFA, 다크 웹 모니터링, 신용 동결 알림, 사회공학

신원 도용 예방 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 신원 도용 예방 및 피해 완화를 안내합니다. 자격 증명 유출, 다중 인증, 다크웹 모니터링, 신용 동결 알림, 사회공학 방어를 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/identity-theft/

나의 신원 보호 학습 로드맵

- 다크 웹 포럼에서 자격 증명이 노출될 위험을 이해합니다.
- 다중 인증(MFA)과 신용 동결 알림을 도입하세요.
- 표적형 사회공학 사기에 대비한 기업 보안 방어 체계를 설계하세요.

신원 도용 가이드 안내

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

신원 도용 예방과 자산 보안 (소개)

신원 도용은 유출된 인증 정보와 취약한 로그인을 악용하여 개인 및 기업 계정을 탈취합니다. MFA, 신용 동결, 다크 웹 스캐너, SPF/DKIM/DMARC 프레임워크를 도입하면 디지털 사칭에 대한 핵심적인 방어가 됩니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 신원 도용범이 로그인 자격 증명을 훔치는 데 사용하는 주된 방법은 무엇입니까?
   - A. 가짜 이메일 알림으로 사용자를 속여 위조된 포털에 비밀번호를 입력하게 함
   - B. 사용자 회사 사무실 근처에서 라디오 방송 청취하기
   - C. 사용자의 로컬 서버 저장 드라이브 조각 모음하기
   - D. 외부 네트워크 백업 구성 연결 끊기

2. 2. 자격 증명 유출에 대해 가장 강력한 방어를 제공하는 보안 통제는 무엇입니까?
   - A. 하드웨어 키를 사용하는 다중 인증
   - B. 브라우저 기본 형식으로 긴 비밀번호 만들기
   - C. 이메일 사용자 이름을 6개월마다 바꾸기
   - D. 저장된 쿠키 추적 브라우저 기록 삭제하기

3. 3. 신용 동결을 나타내는 것은 무엇입니까?
   - A. 도둑이 무단 대출을 받지 못하도록 신용 보고서를 잠금
   - B. 데이터베이스에서 은행 계좌 거래 내역 삭제하기
   - C. 스캐너의 신용카드 마그네틱 판독기 비활성화하기
   - D. 로컬 데이터베이스 하드 드라이브의 저장 데이터 암호화하기

4. 4. 다크 웹 모니터링이 유용한 이유는 무엇입니까?
   - A. 유출된 자격 증명이 불법 데이터베이스에 나타나면 사용자에게 알려 줌
   - B. 활성 악성코드가 가상 샌드박스에서 실행되는 것을 막는다
   - C. 가상 네트워크에서 브라우저 라우팅 속도를 높인다
   - D. 백엔드 데이터베이스 SQL 인젝션 접근 시도를 차단한다

5. 5. 사회공학이란 무엇을 의미합니까?
   - A. 사람들을 조종해 기밀 자격 증명을 스스로 알려 주게 함
   - B. 활성 보안 취약점이 있는지 기업 서버 포트 스캔하기
   - C. 시스템 데이터베이스 파일을 오프라인 하드 드라이브에 백업하기
   - D. 암호화된 어니언 노드 세 개를 거쳐 네트워크 패킷 라우팅하기

체크포인트 2: 참/거짓 도전

6 질문 6

6. 신원 도용은 온라인 디지털 계정에만 영향을 미치며 실물 우편에는 영향을 미치지 않습니다.

○ 참 ○ 거짓

7 질문 7

7. 모든 개인 계정에 MFA를 적용하면 대부분의 크리덴셜 스터핑 봇 공격을 막을 수 있습니다.

○ 참 ○ 거짓

8 질문 8

8. 신용 동결은 신용 조회를 막지만 본인의 은행 계좌에 접근하지 못하게 합니다.

○ 참 ○ 거짓

9 질문 9

9. 비밀번호 관리자는 위조된 도메인에서 비밀번호 자동 입력을 거부해 사용자를 피싱으로부터 보호합니다.

○ 참 ○ 거짓

10 질문 10

10. 피싱 이메일은 흔히 긴급한 표현을 써서 감정적이고 성급한 반응을 유도합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 신원 도용범은 개인 비밀번호와 사용자 _____ 을(를) 노립니다.
2. 데이터베이스 침해를 사용자에게 알리면 비공개 계정 _____ 을(를) 파악할 수 있습니다.
3. 로그인할 때 임시 코드를 요구하는 방식을 _____ (이)라고 합니다.
4. 해커 포럼에서 도난당한 데이터를 찾아보는 일은 다크웹 _____ 입니다.
5. 승인되지 않은 신용 조회를 차단하려면 신용 _____ 이(가) 필요합니다.
6. 직원들에게 피싱 인식 교육을 하면 적극적인 보안 _____ 을(를) 구축하는 데 도움이 됩니다.

어휘 단어 목록

다단계 인증 | 동결 | 모니터링 | 방어 | 스푸핑 | 신고 | 유출 | 인증 정보

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

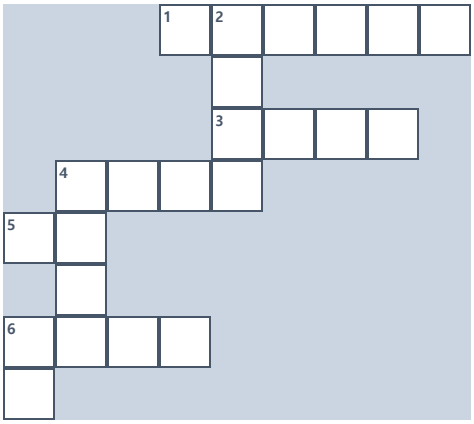
정의 연결하기

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

☐	**1. 자격 증명**	**A**	계정 로그인을 보호하는 보조 인증 단계(예: 하드웨어 키).
☐	**2. 누출**	**B**	합법적인 조직을 흉내 내는 가짜 웹사이트나 이메일 만들기.
☐	**3. MFA**	**C**	사기성 대출 신청을 막기 위해 신용 파일에 대한 접근을 제한하는 것.
☐	**4. 모니터링**	**D**	개인 사용자 기록이 담긴 비공개 데이터베이스의 무단 노출.
☐	**5. 동결**	**E**	신원 도용으로부터 보호하는 데 사용되는 교육과 기술적 통제입니다.
☐	**6. 방어**	**F**	사용자를 속여 로그인 정보를 넘기게 하려고 사기 메시지를 보내는 행위.
☐	**7. 스푸핑**	**G**	도난당한 회사 데이터를 찾기 위해 온라인 포럼과 해커 채널을 살피는 것.
☐	**8. 피싱**	**H**	디지털 신원을 인증하는 데 사용하는 사용자 이름, 비밀번호, 비공개 토큰입니다.

체크포인트 5: 십자말풀이

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



가로

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

3. 개인 정보가 허가 없이 외부로 새어 나가는 일 (4)

4. 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보 (4)

5. 백업해 둔 자료로 원래 상태를 되돌리는 일 (2)

6. 사기성 대출을 막기 위해 내 신용 정보 조회를 막아 두는 조치 (4)

세로

2. 로그인에 쓰는 사용자 이름, 비밀번호, 보안 토큰 같은 정보 (4)

4. 남의 개인 정보를 이용해 그 사람인 척 행세하는 범죄 (4)

6. 범죄나 피해 사실을 관계 기관에 알리는 일 (2)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

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

3 가로: 개인 정보가 허가 없이 외부로 새어 나가는 일 (4 글자):

4 가로: 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보 (4 글자):

5 가로: 백업해 둔 자료로 원래 상태를 되돌리는 일 (2 글자):

6 가로: 사기성 대출을 막기 위해 내 신용 정보 조회를 막아 두는 조치 (4 글자):

세로

2 세로: 로그인에 쓰는 사용자 이름, 비밀번호, 보안 토큰 같은 정보 (4 글자):

4 세로: 남의 개인 정보를 이용해 그 사람인 척 행세하는 범죄 (4 글자):

6 세로: 범죄나 피해 사실을 관계 기관에 알리는 일 (2 글자):

체크포인트 6: 숨은 단어 찾기

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

소	스	출	라	용	메	다	안	답	파	워	검	템	원	시
타	암	접	연	방	네	개	암	신	라	도	카	다	관	넷
결	보	워	동	카	파	다	데	워	고	호	스	데	보	전
보	정	개	터	카	마	관	증	나	네	용	소	기	호	증
송	증	리	응	다	개	격	인	타	터	신	밀	출	속	고
서	인	속	암	아	인	험	신	호	버	이	위	비	복	원
속	신	개	송	아	정	메	시	원	스	하	화	용	바	가
마	사	결	복	화	보	터	복	방	도	고	도	넷	카	격
결	밀	인	카	호	보	데	번	방	공	용	접	트	번	번
동	공	험	리	메	호	템	네	사	시	개	송	정	관	바
용	신	용	정	보	응	카	스	출	소	사	증	응	서	넷
신	워	동	차	정	번	타	격	신	접	사	주	마	가	동
전	카	방	나	보	타	송	타	보	트	기	차	험	공	밀
파	호	관	증	유	시	안	격	청	보	나	나	격	결	데
접	도	고	공	출	터	험	메	리	자	데	유	마	서	관

어휘 단어 목록

신고 · 신용정보 · 개인정보보호 · 복원 · 정보유출 · 신원도용 · 인증정보 · 신용동결

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. 신고
B. 신용정보
C. 개인정보보호
D. 복원
E. 정보유출
F. 신원도용
G. 인증정보
H. 신용동결

정의 및 연결 항목
1. 사기성 대출을 막기 위해 내 신용 정보 조회를 막아 두는 조치.
2. 범죄나 피해 사실을 관계 기관에 알리는 일.
3. 로그인에 쓰는 사용자 이름, 비밀번호, 보안 토큰 같은 정보.
4. 남의 개인 정보를 이용해 그 사람인 척 행세하는 범죄.
5. 백업해 둔 자료로 원래 상태를 되돌리는 일.
6. 개인 정보가 허가 없이 외부로 새어 나가는 일.
7. 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보.
8. 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일.

체크포인트 7: 뒤섞인 단어 도전

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

1. 고 신 _____

2. 호 개 정 보 보 인 _____

3. 출 정 유 보 _____

4. 보 정 인 증 _____

5. 보 신 정 용 _____

6. 원 복 _____

7. 도 신 용 원 _____

8. 신 결 동 용 _____

보너스 활동: 빠르게 생각하기

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

1	신원을 도용당했을 때 할 일			
2	소셜 미디어에 공유하면 안 되는 것			
3	백업하는 것			
4	지갑에 들어 있는 카드나 신분증			
5	보호해야 하는 문서			
6	데이터가 유출된 후에 할 일			
7	소프트웨어를 업데이트하는 이유			
8	신원 도용범이 원하는 정보			
9	해킹당할 수 있는 기기			
10	데이터가 유출될 수 있는 곳			
11	오늘부터 시작할 수 있는 안전 습관			
12	컴퓨터가 감염되었다는 신호			
13	본인임을 증명하는 방법			
14	신원 도용의 징후			
15	이메일의 경고 신호			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 경영진 신원 도용 방어



상황: 한 유명 C레벨 임원이 고객을 속이기 위해 자신의 개인 이메일을 흉내 낸 오타 도메인 이름의 표적이 되었습니다. 브랜드 보호 계획을 설계하세요.

토론 질문: 브랜드 스푸핑 위험을 분석하고, SPF/DKIM/DMARC 및 인증 제어를 자세히 설명하세요.

사례 연구 2: 기업 자격 증명의 다크 웹 노출



상황: 다크 웹 데이터베이스 유출본에 한 기업의 시스템 관리자들이 가진 수백 개의 기업 자격 증명이 들어 있습니다. 완화 전략을 설계하세요.

토론 질문: 자격 증명 정리 절차를 간략히 설명하고, 비밀번호 관리자 도입 계획을 세우세요.

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

4	20	4	20	3	1	27		12	40	3	13	38	12	12	38	6	28

4	40	13	40	17	24	6		10	40	3	12	34	3		8	28	19	28

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: 신원 도용이란 무엇인가요?

공격자가 비밀번호나 SSN 같은 개인 기록을 훔쳐 다른 사람을 사칭하고 금전적 이득을 얻는 범죄.

Q2: 신원 도용의 가장 흔한 원인은 무엇인가요?

피싱은 도둑이 비밀번호를 얻는 주요 수법으로, 사용자를 가짜 위조 웹사이트로 유인합니다.

Q3: 다중 인증(MFA)은 신원을 어떻게 보호하나요?

MFA는 로그인할 때 하드웨어 키 같은 두 번째 증명을 요구하므로, 비밀번호를 도난당해도 공격자를 막을 수 있습니다.

Q4: 신용 동결이란 무엇인가요?

신용평가 기관이 내 신용 파일을 공유하지 못하게 막아, 도둑이 내 명의로 새 대출을 받지 못하게 하는 무료 서비스. [2]

Q5: 다크 웹 모니터링이란 무엇인가요?

해커 포럼에서 유출된 이메일, 비밀번호, 개인 기록을 확인하고 데이터가 노출되면 알려 주는 소프트웨어.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 크리덴셜 스터핑이란 무슨 뜻인가요?

유출된 비밀번호 목록을 수백 개의 웹사이트에 대입해 활성 계정을 탈취하는 자동화된 봇입니다.

Q7: 이메일 스푸핑이 위험한 이유는 무엇인가요?

공격자가 이메일의 발신자 이름을 위조할 수 있게 하여, 피싱 메시지가 믿을 만한 동료에게서 온 것처럼 보이게 합니다.

Q8: 비밀번호 관리자는 신원 도용을 어떻게 막나요?

모든 계정에 복잡하고 고유한 비밀번호를 저장하고, 가짜 피싱 도메인에서는 자격 증명 자동 입력을 거부합니다.

Q9: 스피어 피싱이란 무엇인가요?

속을 가능성을 높이려고 피해자의 이름과 세부 정보에 맞춰 만든 매우 표적화된 피싱 공격.

Q10: 신용 알림은 신용 동결과 어떻게 다른가요?

알림은 대출 기관이 계좌를 개설하기 전에 신원을 확인하게 하고, 동결은 신용 파일 접근을 완전히 차단합니다. [2]

체크포인트 10: 심화 보안 FAQ (파트 C)

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

Q1: SIM 스와핑은 어떻게 신원 도용으로 이어지나요?

공격자는 통신사 직원을 속여 피해자의 전화번호를 새 SIM 카드로 옮기게 하고, SMS 기반 2FA 코드를 가로챕니다.

Q2: 신원 도용 방지에서 DMARC의 역할은 무엇인가요?

DMARC를 사용하면 도메인 소유자가 위조된 이메일이 받은편지함에 도달하는 것을 차단하여, 기업 도메인을 흉내 내는 가짜 이메일을 막을 수 있습니다.

Q3: 합성 신원 도용이 탐지하기 어려운 이유는 무엇인가요?

도둑들은 실제 사회보장번호(SSN)에 가짜 이름과 생년월일을 결합해 완전히 새로운 신용 프로필을 만들어 기본적인 사기 경보를 피합니다.

Q4: 데이터 브로커는 개인 신원 정보를 어떻게 악용하나요?

중개업체(데이터 브로커)는 공공 기록, 웹 행동, 구매 이력을 수집해 프로필 자료를 만드는데, 이 자료는 유출되거나 판매될 수 있습니다.

Q5: SMS 기반 MFA가 취약하다고 여겨지는 이유는 무엇인가요?

SMS 트래픽은 가로채기, 피싱, 통신사 수준의 SIM 스와핑 공격에 취약합니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

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

Q6: 신용 파일 잠금이란 무엇인가요?

동결과 비슷한 상용 서비스로, 모바일 앱으로 신용 파일을 즉시 잠그거나 해제할 수 있습니다.

Q7: 기업 데이터 유출은 신원 도용을 어떻게 부추기나요?

유출된 데이터베이스는 수백만 건의 평문 인증 정보를 노출하여, 도둑이 표적형 신원 사기를 저지르는 데 필요한 원시 데이터를 제공합니다.

Q8: 소셜 미디어에 지나치게 많은 정보를 공유하면 어떤 위험이 있나요?

반려동물 이름, 출생지, 어머니의 결혼 전 성을 공개적으로 공유하면 도둑에게 흔한 계정 복구 질문의 답을 알려 주게 됩니다.

Q9: 생체 인식 로그인은 신원 프로필을 어떻게 보호하나요?

생체 인식은 지문이나 얼굴 같은 특징에 로그인을 연결합니다. 기기 안에 보관하면 훔치기 어렵지만, 저장된 생체 데이터는 유출될 수 있습니다.

Q10: Red Flags Rule은 신원 도용에 어떻게 대응하나요?

금융 기관이 신원 도용의 경고 신호를 탐지하고 대응하는 서면 프로그램을 마련하도록 요구하는 연방 규정.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

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

1. 보안 인사이트

FTC가 운영하는 IdentityTheft.gov에서는 미국 피해자가 신원 도용을 신고하고 개인별 복구 계획을 받을 수 있습니다. [1]

2. 보안 인사이트

하드웨어 보안 키는 피싱에 강한 MFA이며, CISA가 권장하는 가장 강력한 종류의 MFA입니다. [4]

3. 보안 인사이트

유출된 비밀번호는 데이터 침해의 흔한 진입점이며, 이후 신원 도용 사기로 이어집니다.

4. 보안 인사이트

신용 동결은 연방법에 따라 무료이며, 해제될 때까지 대출 기관이 신용 파일을 조회하지 못하게 합니다. [2]

5. 보안 인사이트

DMARC를 사용하면 도메인 소유자가 메일 서버에 검사를 통과하지 못한 위조 이메일을 거부하거나 격리하도록 지시할 수 있습니다. [7]

6. 보안 인사이트

SIM 스와핑을 이용하면 해커가 뱅킹 포털의 SMS 기반 2단계 인증을 우회할 수 있습니다.

7. 보안 인사이트

합성 신원 사기는 실제 정보와 가짜 정보를 섞어 대출 기관이 탐지하기 어렵게 만듭니다.

8. 보안 인사이트

많은 사람이 여러 온라인 계정에 같은 비밀번호를 재사용하므로, 한 번의 유출로 여러 계정이 노출될 수 있습니다.

9. 보안 인사이트

데이터 브로커는 많은 소비자에 대한 상세한 정보 파일을 모으기 때문에 개인정보 위험이 한곳에 집중됩니다.

10. 보안 인사이트

신원 도용에서 회복하려면 청구 이의 제기나 신용 보고서 수정 같은 작업에 몇 달이 걸릴 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] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).
https://www.rfc-editor.org/rfc/rfc7489.html

답안: 체크포인트 1 – 객관식

1 질문 1 정답: A

교사용 참고

신원 도용범이 로그인 자격 증명을 훔치는 데 사용하는 주된 방법은 무엇입니까? → 가짜 이메일 알림으로 사용자를 속여 위조된 포털에 비밀번호를 입력하게 함

2 질문 2 정답: A

교사용 참고

자격 증명 유출에 대해 가장 강력한 방어를 제공하는 보안 통제는 무엇입니까? → 하드웨어 키를 사용하는 다중 인증

3 질문 3 정답: A

교사용 참고

신용 동결을 나타내는 것은 무엇입니까? → 도둑이 무단 대출을 받지 못하도록 신용 보고서를 잠금

4 질문 4 정답: A

교사용 참고

다크 웹 모니터링이 유용한 이유는 무엇입니까? → 유출된 자격 증명이 불법 데이터베이스에 나타나면 사용자에게 알려 줌

5 질문 5 정답: A

교사용 참고

사회공학이란 무엇을 의미합니까? → 사람들을 조종해 기밀 자격 증명을 스스로 알려 주게 함

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 — 정답: 거짓

교사용 참고

신원 도용은 도난당한 우편물이나 문서처럼 오프라인에서도 시작될 수 있습니다.

7 질문 7 — 정답: 참

교사용 참고

모든 개인 계정에 MFA를 적용하면 대부분의 크리덴셜 스터핑 봇 공격을 막을 수 있습니다.

8 질문 8 — 정답: 거짓

교사용 참고

신용 동결은 새로운 신용 조회를 막지만 기존 계정에는 영향을 주지 않습니다.

9 질문 9 — 정답: 참

교사용 참고

비밀번호 관리자는 위조된 도메인에서 비밀번호 자동 입력을 거부해 사용자를 피싱으로부터 보호합니다.

10 질문 10 — 정답: 참

교사용 참고

피싱 이메일은 흔히 긴급한 표현을 써서 감정적이고 성급한 반응을 유도합니다.

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. 자격 증명	D 2. 누출	A 3. MFA	G 4. 모니터링
C 5. 동결	E 6. 방어	B 7. 스푸핑	F 8. 피싱

체크포인트 3: 답안 – 핵심 용어

1 인증 정보	2 유출	3 다단계 인증	4 모니터링
5 동결	6 방어		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 H – 신용동결	2 A – 신고	3 G – 인증정보	4 F – 신원도용
5 D – 복원	6 E – 정보유출	7 B – 신용정보	8 C – 개인정보보호

교사를 위한 토론 참고

핵심 용어:
학생들이 자격 증명, 누출, MFA을(를) 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

소	스	출	라	용	메	다	안	답	파	워	검	템	원	시
타	암	접	연	방	네	개	암	신	라	도	카	다	관	넷
결	보	워	동	카	파	다	데	워	고	호	스	데	보	전
보	정	개	터	카	마	관	증	나	네	용	소	기	호	증
송	증	리	응	다	개	격	인	타	터	신	밀	출	속	고
서	인	속	암	아	인	험	신	호	버	이	위	비	복	원
속	신	개	송	아	정	메	시	원	스	하	화	용	바	가
마	사	결	복	화	보	터	복	방	도	고	도	넷	카	격
결	밀	인	카	호	보	데	번	방	공	용	접	트	번	번
동	공	험	리	메	호	템	네	사	시	개	송	정	관	바
용	신	용	정	보	응	카	스	출	소	사	증	응	서	넷
신	워	동	차	정	번	타	격	신	접	사	주	마	가	동
전	카	방	나	보	타	송	타	보	트	기	차	험	공	밀
파	호	관	증	유	시	안	격	청	보	나	나	격	결	데
접	도	고	공	출	터	험	메	리	자	데	유	마	서	관

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

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

3 가로: 정보유출 개인 정보가 허가 없이 외부로 새어 나가는 일 (4 글자)

4 가로: 신용정보 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보 (4 글자)

5 가로: 복원 백업해 둔 자료로 원래 상태를 되돌리는 일 (2 글자)

6 가로: 신용동결 사기성 대출을 막기 위해 내 신용 정보 조회를 막아 두는 조치 (4 글자)

세로

2 세로: 인증정보 로그인에 쓰는 사용자 이름, 비밀번호, 보안 토큰 같은 정보 (4 글자)

4 세로: 신원도용 남의 개인 정보를 이용해 그 사람인 척 행세하는 범죄 (4 글자)

6 세로: 신고 범죄나 피해 사실을 관계 기관에 알리는 일 (2 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 고신 — **신고**
2. 호개정보보인 — **개인정보보호**
3. 출정유보 — **정보유출**
4. 보정인증 — **인증정보**
5. 보신정용 — **신용정보**
6. 원복 — **복원**
7. 도신용원 — **신원도용**
8. 신결동용 — **신용동결**

비밀 암호 도전 정답

"다단계 인증으로 디지털 신원 보호"

사례 연구 답안

A 사례 연구 1: 경영진 신원 도용 방어

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 유명 최고 경영진이 고객을 속이기 위해 개인 이메일을 흉내 낸 오타 도메인 이름의 표적이 되었습니다. 브랜드 보호 계획을 설계하세요.
- 권장 전략 및 해결책: 임원 이름의 흔한 철자 변형을 모두 등록하세요. 도메인 위조를 막기 위해 이메일 인증 프로토콜(DMARC, DKIM, SPF)을 적용하고, 모든 최고 경영진의 회사 계정 로그인에 하드웨어 MFA를 적용하세요.

B 사례 연구 2: 기업 자격 증명의 다크 웹 노출

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 다크 웹 데이터베이스 덤프에 한 기업의 시스템 관리자들에게 속한 수백 개의 회사 자격 증명이 들어 있습니다. 대응 전략을 설계하세요.
- 권장 전략 및 해결책: 전사 비밀번호 재설정을 실시합니다. 기업용 비밀번호 관리자 사용을 의무화합니다. 모든 시스템 포털에 MFA를 적용하고 지속적인 자동 다크 웹 모니터링 알림을 설정합니다.