이름: _____ 날짜: _____ 점수: _____

온라인 사기와 사회공학 공격 보호 가이드

이메일 피싱, 위조 도메인, 보이스 피싱, 지원 사칭 사기, 별도 경로 검증, BEC

온라인 사기 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 온라인 사기 방어를 안내합니다. 가짜 피싱 웹사이트, 사회공학 기법, 지원 사기, 송금 사기 경로, 결제 확인 방법을 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/online-scams/

나의 온라인 사기 방지 학습 로드맵

- 지원 사기와 타이포스쿼팅 도메인의 흔한 징후를 파악하세요.
- 스푸핑에 대비해 이메일 검증 프로토콜(SPF, DKIM, DMARC)을 도입하세요.
- 기업 송금 사기를 막기 위해 별도 경로 거래 검증 절차를 수립하세요.

온라인 사기 가이드 안내

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

온라인 사기와 사회공학 공격 방어(소개)

온라인 사기는 피싱, 지원 팝업, 보이스피싱, 송금 사기를 통해 사람의 행동을 악용합니다. 대역 외 거래 확인과 SPF/DKIM/DMARC 도메인 규칙을 적용하면 사회공학 공격 경로를 게이트웨이에서 차단하는 데 도움이 됩니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 기술 지원 사기의 주된 징후는 무엇입니까?
   - A. 시스템이 감염되었다고 주장하며 전화를 걸라고 요구하는 팝업
   - B. 공식 레지스트리에서 내려받은 자동 보안 업데이트
   - C. 기업 도메인에서 자격 증명 자동 입력을 거부하는 비밀번호 관리자
   - D. 외부 드라이브 구성에서 실행되는 백그라운드 파일 백업

2. 2. 위조한 발신자 도메인으로 은행 정보를 훔치는 수법은 무엇입니까?
   - A. 이메일 피싱
   - B. 포트 스캔
   - C. 메모리 인젝션
   - D. 암호화 파기

3. 3. 전신 송금 사기를 나타내는 것은 무엇입니까?
   - A. 사회공학으로 피해자를 속여 가짜 기업 계좌로 송금하게 함
   - B. 랜섬웨어 페이로드로 시스템 데이터베이스 암호화하기
   - C. SQL 인젝션 명령으로 데이터베이스 조회하기
   - D. 시스템 파일을 오프라인 저장 디스크에 백업하기

4. 4. 사기범이 가짜 쇼핑 웹사이트를 만드는 이유는 무엇입니까?
   - A. 구매자의 신용카드 정보와 결제 자격 증명을 훔치기 위해
   - B. 샌드박스 악성코드 분석 데이터베이스 테이블을 호스팅하기 위해
   - C. 온라인 주문 배송 속도를 높이려고
   - D. 새 웹사이트 디자인을 무료로 테스트하려고

5. 5. 비싱(vishing)은 무엇을 의미합니까?
   - A. 자격 증명을 훔치려고 전화망으로 하는 음성 피싱 사기
   - B. 로컬 네트워크에서 보안되지 않은 시스템 기기 검사하기
   - C. 무단 침해 후 시스템 데이터베이스 복원하기
   - D. 안전한 가상 컨테이너 안에서 신뢰할 수 없는 코드 실행하기

체크포인트 2: 참/거짓 도전

6 질문 6

6. 피싱 사기는 일반 사용자만 노리고 임원을 노리는 웨일링 대상은 절대 노리지 않습니다.

○ 참 ○ 거짓

7 질문 7

7. 위조 도메인은 amaz0n.com처럼 약간의 오타를 써서 신뢰받는 브랜드를 흉내 내는 경우가 많습니다.

○ 참 ○ 거짓

8 질문 8

8. 지원 사기는 전화를 건 사람에게 원격 접속 권한을 주면 해결할 수 있습니다.

○ 참 ○ 거짓

9 질문 9

9. 사회공학은 두려움과 긴급함 같은 인간 심리를 이용해 보안 규칙을 우회합니다.

○ 참 ○ 거짓

10 질문 10

10. 송금 요청은 항상 별도의 소통 채널로 확인해야 합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 사용자를 속이는 사기성 이메일을 _____ (이)라고 합니다.
2. 신뢰하는 브랜드를 흉내 낸 웹 주소는 _____ 된 주소입니다.
3. 은행 정보를 노리는 음성 사기를 _____ (이)라고 합니다.
4. 바이러스 제거를 대가로 돈을 요구하는 팝업은 기술 지원 _____ 입니다.
5. 결제 요청이 진짜인지 알아보려면 별도의 연락 수단으로 하는 _____ 이(가) 필요합니다.
6. 사업 거래 대금을 사기범의 계좌로 빼돌리는 수법은 _____ 입니다.

어휘 단어 목록

보이스피싱 | 비밀번호 | 사기 | 송금 사기 | 신용 정보 | 위조 | 피싱 | 확인

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

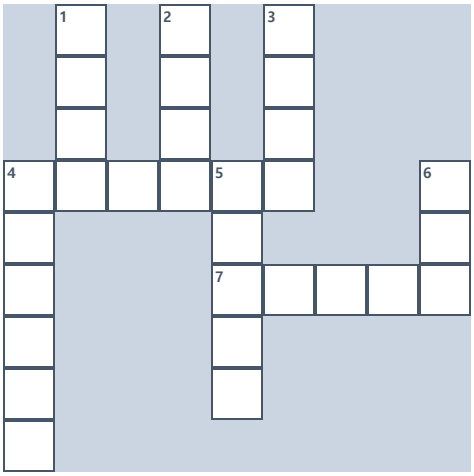
정의 연결하기

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

☐	**1. 피싱**	**A**	은행 거래를 범죄자의 계좌로 사기성으로 돌리는 것.
☐	**2. 위조됨**	**B**	피해자에게서 돈이나 접속 정보를 빼앗으려는 사기 수법.
☐	**3. 비싱**	**C**	모바일 계정 로그인 정보를 훔치려고 사기 문자 메시지를 보내는 행위.
☐	**4. 사기**	**D**	인증 정보와 계정 정보를 훔치기 위한 사기성 음성 통화.
☐	**5. 검증**	**E**	C레벨 임원의 로그인 정보를 훔치려는 표적형 피싱 공격.
☐	**6. 전신 송금**	**F**	정상처럼 보이도록 꾸며낸 이메일 발신자 또는 웹사이트 주소.
☐	**7. 웨일링**	**G**	로그인 정보와 비밀번호를 훔치기 위한 사기성 이메일 캠페인.
☐	**8. 스미싱**	**H**	신뢰할 수 있는 다른 연락 수단으로 결제 정보를 확인하기.

체크포인트 5: 십자말풀이

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



가로

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

7. 특정한 사람이나 조직을 겨냥해 맞춤형으로 보내는 피싱 (5)

세로

1. 믿을 수 있는 다른 연락 수단으로 결제 정보를 확인하는 일 (4)

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

3. 계정 주인을 확인하려고 입력하는 문자열 (4)

4. 개인 데이터가 허가 없이 외부로 새어 나가는 일 (6)

5. 인증 정보와 계좌 정보를 빼내려는 사기성 음성 통화 (5)

6. 문자 메시지에 가짜 링크를 넣어 정보를 빼내는 사기 수법 (3)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

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

7 가로: 특정한 사람이나 조직을 겨냥해 맞춤형으로 보내는 피싱 (5 글자):

세로

1 세로: 믿을 수 있는 다른 연락 수단으로 결제 정보를 확인하는 일 (4 글자):

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

3 세로: 계정 주인을 확인하려고 입력하는 문자열 (4 글자):

4 세로: 개인 데이터가 허가 없이 외부로 새어 나가는 일 (6 글자):

5 세로: 인증 정보와 계좌 정보를 빼내려는 사기성 음성 통화 (5 글자):

6 세로: 문자 메시지에 가짜 링크를 넣어 정보를 빼내는 사기 수법 (3 글자):

체크포인트 6: 숨은 단어 찾기

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

다	안	검	하	워	색	도	신	스	타	비	접	결	방	네
개	싱	암	라	메	카	다	리	비	넷	접	워	확	카	파
다	피	이	워	호	템	데	보	송	밀	보	개	터	타	바
리	스	추	나	트	인	소	술	호	추	번	송	시	답	다
격	이	터	파	터	개	출	밀	피	개	미	호	서	속	암
자	보	관	기	버	인	이	스	험	밀	개	스	미	싱	출
공	송	아	주	시	정	템	하	피	벽	용	바	가	마	사
결	싱	화	터	싱	보	방	출	메	어	넷	타	위	밀	인
보	카	기	이	데	유	방	공	속	트	피	번	번	격	험
정	시	메	도	네	출	사	스	공	송	정	싱	리	바	답
용	개	인	정	보	보	호	카	스	어	요	아	추	답	추
신	서	넷	워	확	차	데	타	위	유	속	사	소	가	마
가	확	전	카	방	나	타	송	타	안	워	기	확	차	험
격	밀	하	기	리	추	스	안	위	응	보	인	나	다	위
결	이	속	메	미	공	터	관	주	리	자	데	피	마	서

어휘 단어 목록

개인정보유출 스미싱 신용정보 스피어피싱 보이스피싱 개인정보보호 비밀번호 추가확인

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. 개인정보유출**
- **B. 스미싱**
- **C. 신용정보**
- **D. 스피어피싱**
- **E. 보이스피싱**
- **F. 개인정보보호**
- **G. 비밀번호**
- **H. 추가확인**

정의 및 연결 항목

1. 문자 메시지에 가짜 링크를 넣어 정보를 빼내는 사기 수법.
2. 인증 정보와 계좌 정보를 빼내려는 사기성 음성 통화.
3. 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일.
4. 믿을 수 있는 다른 연락 수단으로 결제 정보를 확인하는 일.
5. 계정 주인을 확인하려고 입력하는 문자열.
6. 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보.
7. 개인 데이터가 허가 없이 외부로 새어 나가는 일.
8. 특정한 사람이나 조직을 겨냥해 맞춤형으로 보내는 피싱.

체크포인트 7: 뒤섞인 단어 도전

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

1. 정 개 보 유 출 인 _____

2. 신 정 보 용 _____

3. 스 보 싱 피 이 _____

4. 호 번 비 밀 _____

5. 싱 미 스 _____

6. 피 스 어 싱 피 _____

7. 보 개 보 호 정 인 _____

8. 추 인 확 가 _____

보너스 활동: 빠르게 생각하기

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

1	해킹당할 수 있는 기기			
2	사기범이 자주 쓰는 표현			
3	사기범이 요구하는 결제 수단			
4	온라인 사기의 종류			
5	너무 좋아서 믿기 어려운 제안			
6	사기를 신고할 수 있는 곳			
7	사이버 보안과 관련된 단어			
8	사기에 대해 알려 줄 수 있는 사람			
9	백업하는 것			
10	이메일의 경고 신호			
11	컴퓨터가 감염되었다는 신호			
12	온라인 쇼핑몰을 확인하는 방법			
13	계정을 보호하는 방법			
14	사기를 당했을 때 할 일			
15	데이터가 유출된 후에 할 일			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 기업 송금 사기 예방



상황: 한 재무 부서가 위조된 거래처 주소에서 온 긴급 이메일을 받는데, 앞으로의 청구서 송금을 새로운 라우팅 번호로 보내 달라는 내용입니다.

토론 질문: 송금 사기 확인 정책을 간략히 설명하고, 이메일 인증 차단 장치를 명시하세요.

사례 연구 2: 경영진 대상 웨일링 피싱 사고



상황: 한 임원이 보안 이사회 회의 문서가 있다고 주장하는 피싱 링크를 클릭하여, 위조된 포털에 주요 회사 자격 증명을 입력했습니다.

토론 질문: 사고 대응 단계를 자세히 설명하고, 임원의 로그인 기록을 감사하는 방법을 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

19	29	1	12	40	3		13	24	6	15	20	6	28

18	40	10	40	12	12	38	6		17	20	7	13	40	19	20	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 사이버 보안 FAQ (파트 A)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q1: 온라인 사기란 무엇인가요?

디지털 채널을 이용해 피해자를 속여 돈을 보내게 하거나 개인 자격 증명을 넘기게 하는 사기 수법.

Q2: 이메일 피싱의 주요 징후는 무엇인가요?

계정 정지처럼 긴급함을 내세우며 공식 도메인과 일치하지 않는 링크로 유도하는 메시지.

Q3: 타이포스쿼팅이란 무엇인가요?

가짜 피싱 사이트를 운영하려고 유명 브랜드의 흔한 오타(예: amaz0n.com)가 들어간 도메인을 등록하는 것.

Q4: 지원 사기란 무엇인가요?

PC가 감염되었다고 주장하며 전화번호로 연락해 가짜 정리 소프트웨어나 원격 접속 서비스에 돈을 내게 하는 팝업. [1]

Q5: 비싱(vishing)이란 무엇인가요?

음성 전화를 이용해 피해자가 은행 계좌나 로그인 정보를 알려 주도록 속이는 피싱 공격.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 전신 사기(wire fraud)란 무슨 뜻인가요?

판매업체나 임원을 사칭해 결제 거래를 사기 계좌로 돌리는 행위.

Q7: 웨일링(whaling)이란 무엇인가요?

C레벨 기업 임원 같은 가치가 높은 대상을 직접 노리는 매우 표적화된 스피어 피싱.

Q8: 스미싱이란 무엇인가요?

모바일 기기로 보내지는 사기 문자 메시지로, 가짜 포털이나 배송 추적 업데이트로 가는 링크 안내가 들어 있습니다.

Q9: 대역 외 검증이 중요한 이유는 무엇인가요?

별도의 통신 채널(예: 전화 통화)로 거래 세부 정보를 확인하여 침해된 이메일 스레드를 피합니다.

Q10: 가짜 에스크로 계정 사기는 어떻게 이루어지나요?

사기범이 대금을 안전하게 보관한다고 주장하는 위조 에스크로 사이트를 만든 뒤 구매자의 송금 예치금을 가로챕니다.

체크포인트 10: 심화 보안 FAQ (파트 C)

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

Q1: 사기범은 BEC(비즈니스 이메일 사기)를 어떻게 이용해 송금 사기를 저지르나요?

정상 직원의 이메일 계정을 탈취하고 청구서 대화를 감시하다가 사기 은행 계좌가 적힌 수정된 청구 정보를 보냅니다.

Q2: 온라인 사기에서 IDN 호모그래프 공격의 위험은 무엇인가요?

일반 글자와 똑같이 보이는 비ASCII 문자(예: 키릴 문자 'a')를 사용해 실제 브랜드를 흉내 낸 가짜 도메인을 등록하는 것입니다.

Q3: 사기 탐지에서 이메일 헤더 검사가 중요한 이유는 무엇인가요?

실제 출발지 서버 IP와 SPF/DKIM 검증 상태를 보여 주어 발신 도메인이 위조되었는지 알려 줍니다.

Q4: 지원 사기범은 원격 데스크톱 소프트웨어를 어떻게 악용하나요?

AnyDesk나 TeamViewer 같은 유틸리티로 피해자의 기기에 접속해 악성코드를 심고 저장된 비밀번호를 훔칩니다.

Q5: 선불 수수료 사기의 목적은 무엇인가요?

존재하지 않는 큰 금전적 보상을 대가로 처리 수수료를 먼저 내도록 피해자를 속이는 것입니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

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

Q6: 사기범은 표적 피싱에 소셜 미디어 프로파일링을 어떻게 활용하나요?

기업 조직도와 직원 이름을 수집하여 그럴듯한 스피어 피싱 이메일을 작성합니다.

Q7: 가짜 쇼핑몰이 큰 폭의 할인을 내거는 이유는 무엇인가요?

구매자가 신용카드 정보를 입력하도록 유인하여 자격 증명을 카딩 포럼에서 재사용하거나 되팔기 위해 가로채려는 것입니다.

Q8: DMARC 레코드는 피싱 사기를 어떻게 막나요?

DMARC를 사용하면 도메인 소유자가 수신 측에 정렬된 SPF 및 DKIM 검사를 통과하지 못한 메일을 격리하거나 거부하도록 요청하여 직접적인 위조를 차단할 수 있습니다. [5]

Q9: 자격 증명 탈취 포털의 위협은 무엇인가요?

Microsoft 365나 Google 워크스페이스와 똑같아 보이도록 만든 위조 랜딩 페이지로, 로그인 정보가 입력되는 즉시 훔칩니다.

Q10: 보안팀은 사기 도메인을 어떻게 신고하고 비활성화하나요?

등록 대행사의 악용 신고 이메일, 호스팅 제공업체, Google Safe Browsing 등록부에 사기 증거를 제출함으로써.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

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

1. 보안 인사이트

2025년 FBI IC3에 가장 많이 신고된 범죄 유형은 피싱과 스푸핑으로, 191,561건이 접수되었습니다. [2]

2. 보안 인사이트

비즈니스 이메일 침해(BEC)는 2025년 FBI의 IC3에 보고된 피해액만 30억 달러가 넘었습니다. [2]

3. 보안 인사이트

오타를 노린 도메인은 실제 브랜드 이름과 한두 글자만 달라서 얼핏 보면 놓칠 수 있습니다.

4. 보안 인사이트

기술 지원 사기로 인해 2025년에 FBI IC3에 보고된 피해액이 21억 달러를 넘었습니다. [2]

5. 보안 인사이트

브라우저가 punycode 형태로 표시하지 않으면 동형 문자 공격은 주소 표시줄에서 똑같아 보입니다.

6. 보안 인사이트

SMS 문자 사기(스미싱)는 링크가 담긴 짧고 다급한 메시지를 사용하므로 피해자가 사기를 알아챌 만한 맥락이 거의 없습니다.

7. 보안 인사이트

고래 사냥형 공격(웨일링)은 대규모 송금 결제를 승인할 권한을 가진 임원의 이메일을 노립니다.

8. 보안 인사이트

알고 있는 저장된 전화번호로 전화를 걸어 결제 변경을 확인하는 것은 BEC 송금 사기에 대한 핵심 방어책입니다.

9. 보안 인사이트

가짜 에스크로 계정 웹사이트는 온라인 마켓에서 흔한 사기입니다. 안전한 결제 서비스처럼 보이지만 구매자의 송금액을 가로챕니다.

10. 보안 인사이트

Google Safe Browsing은 피싱이나 악성코드로 표시한 사이트를 열기 전에 사용자에게 경고합니다.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] 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

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

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

[5] 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

기술 지원 사기의 주된 징후는 무엇입니까? → 시스템이 감염되었다고 주장하며 전화를 걸라고 요구하는 팝업

2 질문 2 정답: A

교사용 참고

위조한 발신자 도메인으로 은행 정보를 훔치는 수법은 무엇입니까? → 이메일 피싱

3 질문 3 정답: A

교사용 참고

전신 송금 사기를 나타내는 것은 무엇입니까? → 사회공학으로 피해자를 속여 가짜 기업 계좌로 송금하게 함

4 질문 4 정답: A

교사용 참고

사기범이 가짜 쇼핑 웹사이트를 만드는 이유는 무엇입니까? → 구매자의 신용카드 정보와 결제 자격 증명을 훔치기 위해

5 질문 5 정답: A

교사용 참고

비싱(vishing)은 무엇을 의미합니까? → 자격 증명을 훔치려고 전화망으로 하는 음성 피싱 사기

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 정답: 거짓

교사용 참고

거짓: 피싱은 임원도 표적으로 삼으며, 웨일링은 고위 경영진을 겨냥한 피싱입니다.

7 질문 7 정답: 참

교사용 참고

위조 도메인은 amaz0n.com처럼 약간의 오타를 써서 신뢰받는 브랜드를 흉내 내는 경우가 많습니다.

8 질문 8 정답: 거짓

교사용 참고

거짓: 지원 사기범에게 원격 접근 권한을 주면 악성코드를 심고 데이터를 훔칠 수 있습니다.

9 질문 9 정답: 참

교사용 참고

사회공학은 두려움과 긴급함 같은 인간 심리를 이용해 보안 규칙을 우회합니다.

10 질문 10 정답: 참

교사용 참고

송금 요청은 항상 별도의 소통 채널로 확인해야 합니다.

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

G 1. 피싱	F 2. 위조됨	D 3. 비싱	B 4. 사기
H 5. 검증	A 6. 전신 송금	E 7. 웨일링	C 8. 스미싱

체크포인트 3: 답안 – 핵심 용어

1 피싱	2 위조	3 보이스피싱	4 사기
5 확인	6 송금 사기		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 B – 스미싱	2 E – 보이스피싱	3 F – 개인정보보호	4 H – 추가확인
5 G – 비밀번호	6 C – 신용정보	7 A – 개인정보유출	8 D – 스피어피싱

교사를 위한 토론 참고

핵심 용어:
학생들이 피싱, 위조됨, 비싱을 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	검	하	워	색	도	신	스	타	비	접	결	방	네
개	싱	암	라	메	카	다	리	비	넷	접	워	확	카	파
다	피	이	워	호	템	데	보	송	밀	보	개	터	타	바
리	스	추	나	트	인	소	술	호	추	번	송	시	답	다
격	이	터	파	터	개	출	밀	피	개	미	호	서	속	암
자	보	관	기	버	인	이	스	험	밀	개	스	미	싱	출
공	송	아	주	시	정	템	하	피	벽	용	바	가	마	사
결	싱	화	터	싱	보	방	출	메	어	넷	타	위	밀	인
보	카	기	이	데	유	방	공	속	트	피	번	번	격	험
정	시	메	도	네	출	사	스	공	송	정	싱	리	바	답
용	개	인	정	보	보	호	카	스	어	요	아	추	답	추
신	서	넷	워	확	차	데	타	위	유	속	사	소	가	마
가	확	전	카	방	나	타	송	타	안	워	기	확	차	험
격	밀	하	기	리	추	스	안	위	응	보	인	나	다	위
결	이	속	메	미	공	터	관	주	리	자	데	피	마	서

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

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

7 가로: 스피어피싱 특정한 사람이나 조직을 겨냥해 맞춤형으로 보내는 피싱 (5 글자)

세로

1 세로: 추가확인 믿을 수 있는 다른 연락 수단으로 결제 정보를 확인하는 일 (4 글자)

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

3 세로: 비밀번호 계정 주인을 확인하려고 입력하는 문자열 (4 글자)

4 세로: 개인정보유출 개인 데이터가 허가 없이 외부로 새어 나가는 일 (6 글자)

5 세로: 보이스피싱 인증 정보와 계좌 정보를 빼내려는 사기성 음성 통화 (5 글자)

6 세로: 스미싱 문자 메시지에 가짜 링크를 넣어 정보를 빼내는 사기 수법 (3 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 정개보유출인 — **개인정보유출**
2. 신정보용 — **신용정보**
3. 스보싱피이 — **보이스피싱**
4. 호번비밀 — **비밀번호**
5. 싱미스 — **스미싱**
6. 피스어싱피 — **스피어피싱**
7. 보개보호정인 — **개인정보보호**
8. 추인확가 — **추가확인**

비밀 암호 도전 정답

"확인 절차로 피싱을 탐지하세요"

사례 연구 답안

A 사례 연구 1: 기업 송금 사기 예방

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 재무 부서가 위조된 판매업체 주소에서 온 긴급 이메일을 받습니다. 앞으로의 청구서 송금을 새 라우팅 번호로 보내 달라는 요청입니다.
- 권장 전략 및 해결책: 모든 결제에 이중 승인 정책을 시행하세요. 미리 저장해 둔 전화번호로 별도 경로 확인을 하고, 게이트웨이에서 위조된 도메인의 이메일을 차단합니다.

B 사례 연구 2: 경영진 대상 웨일링 피싱 사고

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 임원이 보안 이사회 회의 문서가 있다고 주장하는 피싱 링크를 클릭해, 위조된 포털에 기본 회사 계정 정보를 입력했습니다.
- 권장 전략 및 해결책: 임원의 기기를 격리하세요. 모든 회사 세션 토큰과 자격 증명을 재설정하고, 데이터 유출 여부를 접근 로그에서 검토하며, 모든 로그인에 하드웨어 MFA를 도입하세요.