이름: _____ 날짜: _____ 점수: _____

# 피싱 공격과 사회공학

스피어 피싱, 고래 사냥 사기, SPF/DKIM/DMARC 프로토콜, 발신자 스푸핑, 직원 보안 교육.

## 피싱 공격 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 피싱 공격과 사회공학을 안내합니다. 스피어 피싱, 웨일링, 도메인 사칭, SPF/DKIM/DMARC 프로토콜, 링크 안전, 직원 인식 교육을 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/phishing-attacks/

# 나의 피싱 대응 학습 로드맵

- 흔한 피싱, 보이스 피싱, 지원 팝업 사기를 파악하세요.
- 대역 외 거래 검증 절차를 도입하세요.
- SPF, DKIM, DMARC 규칙을 구성해 위조된 도메인을 차단하세요.

### 피싱 공격 가이드 안내

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

### 피싱 공격과 사회공학(소개)

피싱 공격은 표적형 메시지, 웨일링 사기, 도메인 스푸핑으로 사용자 로그인 자격 증명을 수집합니다. 기업 시스템을 보호하려면 게이트웨이에 SPF, DKIM, DMARC 규칙을 적용하고 대역 외 승인 단계를 함께 두어야 합니다.

**각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.**

## 체크포인트 1: 객관식 도전

**1** 1. 스피어 피싱이란 무엇입니까?

- A. 특정 개인이나 조직에 맞춰 만든 표적형 피싱 이메일
- B. 무작위 주소 수백만 개로 보내는 대량 이메일
- C. 트래픽으로 웹 서버를 마비시키는 네트워크 공격
- D. 사용자 레코드를 노리는 데이터베이스 추출 기법

**2** 2. 스푸핑에 대응하기 위해 도메인이 DNS에 허가된 발신 IP 주소를 나열할 수 있게 해 주는 프로토콜은 무엇입니까?

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

**3** 3. 웨일링 공격이란 무엇입니까?

- A. 유명 기업 임원을 특정해 노리는 피싱 캠페인
- B. 데이터베이스 백업을 노린 SQL 인젝션 공격
- C. 근거리 통신망(LAN) 라우터 장비의 물리적 도난
- D. 자동화된 자격 증명 스터핑 무차별 대입 검사

**4** 4. DKIM은 무엇을 합니까?

- A. 이메일에 암호 서명을 추가해 발신자의 진위를 검증함
- B. 방화벽에서 들어오는 네트워크 패킷 트래픽을 차단한다
- C. 저장 중인 데이터베이스 스토리지 볼륨을 암호화한다
- D. 이메일 첨부 파일에서 시그니처 기반 악성코드를 검사한다

**5** 5. DMARC의 역할은 무엇입니까?

- A. SPF/DKIM 검사에 실패한 메일을 수신 메일 서버가 어떻게 처리할지 지시함
- B. 미리 계산된 레인보우 테이블로 시스템 비밀번호 해독하기
- C. 전송 전에 이메일 첨부 파일 압축하기
- D. 네트워크 라우팅 접근 권한 구성하기

## 체크포인트 2: 참/거짓 도전

**6 질문 6**

6. 스피어 피싱은 임의의 주소 수백만 개에 보내는 일반적인 대량 이메일에 의존합니다.

○ 참 ○ 거짓

**7 질문 7**

7. DMARC 정책은 메일 서버에 허가되지 않은 위조 메시지를 거부하도록 지시할 수 있습니다.

○ 참 ○ 거짓

**8 질문 8**

8. SPF 검증은 이메일 본문의 암호화 서명을 확인하는 방식으로 동작합니다.

○ 참 ○ 거짓

**9 질문 9**

9. 고래 사냥형 공격(웨일링)은 데이터베이스 파일에 접근하기 위해 하위직 기업 관리자를 노립니다.

○ 참 ○ 거짓

**10 질문 10**

10. 결제 요청을 대역 외로 확인하면 금융 송금 사기를 막는 데 도움이 됩니다.

○ 참 ○ 거짓

## 체크포인트 3: 핵심 용어 채우기

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

1. 특정 직원의 개인 정보를 이용해 겨냥하는 방식은 _____ 피싱입니다.
2. 메일 헤더를 속여 메시지가 정상처럼 보이게 하는 것을 발신자 _____ (이)라고 합니다.
3. 승인된 메일 서버 IP를 나열한 DNS 레코드 목록은 _____ 입니다.
4. 발신자 검증을 제공하는 이메일 서명 표준은 _____ 입니다.
5. SPF와 DKIM 검사에 실패한 메일을 거부하는 정책을 세울 때는 _____ 을(를) 사용합니다.
6. C레벨 임원을 노린 피싱 캠페인을 _____ (이)라고 합니다.

**어휘 단어 목록**

스피어 | 알림 서비스 | 웨일링 | 위조 | 피해자 | DKIM | DMARC | SPF

**여기에 답을 쓰세요:**

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

# 체크포인트 4: 보안 개념 연결

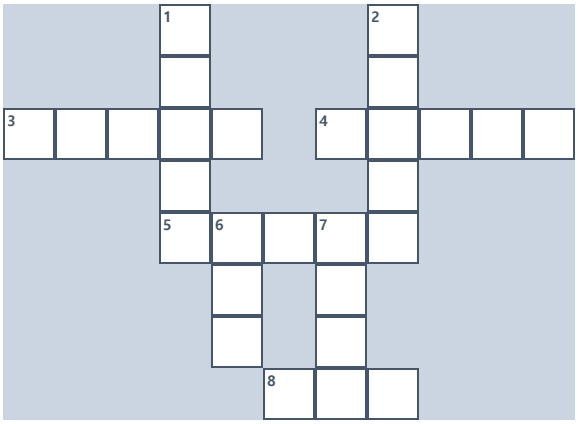
**정의 연결하기**

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

| | | | |
|---|---|---|---|
| ☐ | **1. 스피어** | **A** | 음성 기반 사기 전화. |
| ☐ | **2. 스푸핑** | **B** | C레벨 임원을 노립니다. |
| ☐ | **3. SPF** | **C** | 정책 거부 지침. |
| ☐ | **4. DKIM** | **D** | DNS에서 허가된 발신자 IP. |
| ☐ | **5. DMARC** | **E** | 사회공학 이메일. |
| ☐ | **6. 웨일링** | **F** | 개인 맞춤형 표적 이메일. |
| ☐ | **7. 피싱** | **G** | 발신자 이메일 주소 위조. |
| ☐ | **8. 비싱** | **H** | 이메일의 암호화 서명. |

## 체크포인트 5: 십자말풀이

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




### 가로

**3. 이메일에 포함되는 암호학적 서명 (5)**

**4. DNS에 등록해 메일을 보낼 수 있는 서버를 정해 두는 이메일 인증 방식 (5)**

**5. 특정인을 겨냥해 개인 정보를 이용한 맞춤형으로 보내는 피싱 (5)**

**8. 경영진 등 고위 인사를 노린 표적 피싱 (3)**

### 세로

**1. 계정에 이상이 생기면 바로 알려 주는 기능 (5)**

**2. 전화 통화로 속여 돈이나 정보를 빼내는 사기 (5)**

**6. 범죄나 사고로 손해를 입은 사람 (3)**

**7. 사람을 속이려고 보내는 가짜 이메일 (4)**

# 체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

## 가로

**3 가로: 이메일에 포함되는 암호학적 서명 (5 글자):**

**4 가로: DNS에 등록해 메일을 보낼 수 있는 서버를 정해 두는 이메일 인증 방식 (5 글자):**

**5 가로: 특정인을 겨냥해 개인 정보를 이용한 맞춤형으로 보내는 피싱 (5 글자):**

**8 가로: 경영진 등 고위 인사를 노린 표적 피싱 (3 글자):**

## 세로

**1 세로: 계정에 이상이 생기면 바로 알려 주는 기능 (5 글자):**

**2 세로: 전화 통화로 속여 돈이나 정보를 빼내는 사기 (5 글자):**

**6 세로: 범죄나 사고로 손해를 입은 사람 (3 글자):**

**7 세로: 사람을 속이려고 보내는 가짜 이메일 (4 글자):**

## 체크포인트 6: 숨은 단어 찾기

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

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 다 | 버 | 해 | 보 | 정 | 웨 | 청 | 명 | 소 | 파 | 번 | 격 | 개 | 암 | 워 |
| 험 | 싱 | 번 | 라 | 청 | 카 | 다 | 도 | 피 | 벽 | 공 | 정 | 림 | 타 | 하 |
| 라 | 피 | 연 | 정 | 술 | 소 | 송 | 서 | 접 | 싱 | 안 | 험 | 방 | 타 | 바 |
| 도 | 스 | 알 | 다 | 워 | 넷 | 검 | 인 | 술 | 알 | 메 | 속 | 메 | 프 | 다 |
| 리 | 이 | 방 | 하 | 방 | 에 | 링 | 이 | 싱 | 험 | 디 | 일 | 네 | 위 | 번 |
| 자 | 보 | 템 | 용 | 네 | 스 | 연 | 스 | 스 | 이 | 위 | 웨 | 일 | 링 | 디 |
| 관 | 속 | 아 | 답 | 주 | 피 | 소 | 보 | 피 | 비 | 터 | 바 | 가 | 마 | 아 |
| 스 | 공 | 지 | 비 | 방 | 에 | 털 | 암 | 디 | 어 | 청 | 벽 | 파 | 시 | 이 |
| 비 | 넷 | 타 | 용 | 연 | 프 | 송 | 벽 | 관 | 격 | 피 | 워 | 전 | 전 | 리 |
| 서 | 스 | 메 | 응 | 청 | 워 | 사 | 주 | 험 | 속 | 기 | 싱 | 도 | 바 | 프 |
| 림 | 디 | 지 | 털 | 서 | 명 | 타 | 소 | 어 | 색 | 아 | 알 | 프 | 네 | 피 |
| 알 | 벽 | 정 | 림 | 카 | 송 | 파 | 시 | 링 | 격 | 사 | 검 | 마 | 해 | 가 |
| 림 | 결 | 타 | 암 | 나 | 파 | 속 | 파 | 서 | 크 | 용 | 카 | 자 | 스 | 리 |
| 이 | 보 | 용 | 도 | 알 | 주 | 서 | 시 | 피 | 안 | 나 | 다 | 시 | 공 | 연 |
| 위 | 응 | 디 | 관 | 방 | 템 | 응 | 도 | 차 | 송 | 명 | 바 | 네 | 도 | 링 |

**어휘 단어 목록**

에스피에프 · 피해자 · 웨일링 · 디지털서명 · 피싱메일 · 스피어피싱 · 보이스피싱 · 알림서비스

# 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. 에스피에프 |
| B. 피해자 |
| C. 웨일링 |
| D. 디지털서명 |
| E. 피싱메일 |
| F. 스피어피싱 |
| G. 보이스피싱 |
| H. 알림서비스 |

| 정의 및 연결 항목 |
| --- |
| 1. 범죄나 사고로 손해를 입은 사람. |
| 2. DNS에 등록해 메일을 보낼 수 있는 서버를 정해 두는 이메일 인증 방식. |
| 3. 계정에 이상이 생기면 바로 알려 주는 기능. |
| 4. 경영진 등 고위 인사를 노린 표적 피싱. |
| 5. 전화 통화로 속여 돈이나 정보를 빼내는 사기. |
| 6. 사람을 속이려고 보내는 가짜 이메일. |
| 7. 이메일에 포함되는 암호학적 서명. |
| 8. 특정인을 겨냥해 개인 정보를 이용한 맞춤형으로 보내는 피싱. |

## 체크포인트 7: 뒤섞인 단어 도전

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

1. 에 피 에 프 스
2. 링 일 웨
3. 일 피 메 싱
4. 스 싱 피 보 이
5. 자 해 피
6. 서 디 털 명 지
7. 피 싱 스 어 피
8. 스 알 서 비 림

# 보너스 활동: 빠르게 생각하기

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

| | | | | |
|---|---|---|---|---|
| 1 | 해킹당할 수 있는 기기 | | | |
| 2 | 피싱 이메일의 징후 | | | |
| 3 | 컴퓨터가 감염되었다는 신호 | | | |
| 4 | 가짜 긴급함을 만드는 단어 | | | |
| 5 | 발신자를 확인하는 방법 | | | |
| 6 | IT 도움을 요청할 수 있는 사람 | | | |
| 7 | 백업하는 것 | | | |
| 8 | 알고 있는 물고기나 바다 생물 | | | |
| 9 | 사기범이 사칭하는 회사 | | | |
| 10 | 오늘부터 시작할 수 있는 안전 습관 | | | |
| 11 | 가짜 링크를 클릭한 후에 할 일 | | | |
| 12 | 데이터가 유출된 후에 할 일 | | | |
| 13 | 피싱이 일어나는 경로 | | | |
| 14 | 이메일로 절대 보내지 않는 것 | | | |
| 15 | 계정을 보호하는 방법 | | | |

# 체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

### 사례 연구 1: 최고경영진 대상 웨일링 공격 대응

👷

**상황:** 한 최고재무책임자(CFO)가 기밀 도메인 구매를 마무리하기 위해 50,000달러를 신속히 송금해 달라는, CEO를 사칭한 매우 개인화된 이메일을 받습니다.

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

### 사례 연구 2: SPF/DKIM/DMARC 게이트웨이 정책 적용하기

👷

**상황:** 한 기업이 발신 마케팅 이메일이 자주 스팸으로 분류되고 해커들이 회사의 브랜드 도메인을 적극적으로 스푸핑하고 있어 보안 감사를 통과하지 못하고 있습니다.

**토론 질문:** 이메일의 진위를 확인하는 기술적, 관리적 제어를 수립하세요.

# 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

| 7 | 25 | 12 | 40 | 6 | | 13 | 24 | 7 | 1 | 24 | 7 | 12 | 38 | 6 | 28 | | 10 | 20 | 1 | 40 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | |

| 17 | 20 | 7 | 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: 피싱이란 무엇인가요?**

피싱은 범죄자가 사기 메시지를 보내 사용자가 민감한 데이터를 공유하도록 속이는 사회공학 공격입니다.

**Q2: 피싱과 스피어 피싱의 차이는 무엇인가요?**

피싱은 일반적인 내용으로 넓은 집단을 노리고, 스피어 피싱은 맞춤형 세부 정보를 이용해 특정 피해자를 노립니다.

**Q3: 웨일링(whaling)이란 무엇인가요?**

웨일링은 관리 권한을 가진 고위 임원을 겨냥한 고도로 표적화된 피싱 공격입니다.

**Q4: 이메일 스푸핑이란 무엇인가요?**

이메일 스푸핑은 수신자가 출처를 믿도록 속이기 위해 발신자 주소를 위조한 이메일 메시지를 만드는 것입니다.

**Q5: SPF는 스푸핑을 어떻게 막나요?**

허가된 발신 IP 주소 목록을 DNS에 게시하여 수신 서버가 메일의 출처를 확인할 수 있게 합니다. [1]

# 체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

### Q6: DKIM이란 무엇인가요?

DomainKeys Identified Mail은 이메일 헤더에 암호화 서명을 추가하여 도메인이 책임을 졌으며 메시지가 변경되지 않았음을 증명합니다.

### Q7: DMARC는 무엇의 약자인가요?

Domain-based Message Authentication, Reporting, and Conformance. [2]

### Q8: DMARC 정책이란 무엇인가요?

SPF/DKIM 검사에 실패한 메시지를 메일 서버가 어떻게 처리할지 알려 주는 정책(none, quarantine, reject). [2]

### Q9: 비싱(vishing)이란 무엇인가요?

공격자가 사기 전화를 이용해 관리 정보나 금융 정보를 빼내는 보이스 피싱.

### Q10: 링크 스캐너는 어떻게 도움이 되나요?

수신한 이메일 링크를 검사하고 다시 써서 클릭하는 시점에 이동할 웹 페이지가 안전한지 확인합니다.

# 체크포인트 10: 심화 보안 FAQ (파트 C)

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

**Q1: 동형이의어(호모그래프) 공격은 어떻게 작동하나요?**

공격자는 비ASCII 유니코드 문자 중 모양이 비슷한 문자로 도메인 이름을 등록해 정상 도메인 이름처럼 보이게 합니다.

**Q2: 퓨니코드 표현이란 무엇인가요?**

DNS가 처리할 수 있도록 유니코드 도메인 이름을 'xn--'로 시작하는 ASCII 호환 문자열로 변환하는 인코딩.

**Q3: 'p=reject'가 가장 안전한 DMARC 상태인 이유는 무엇인가요?**

수신 서버가 SMTP 세션 중에 DMARC(정렬된 SPF/DKIM)를 통과하지 못한 메일을 거부하도록 요청하여 직접적인 스푸핑을 차단합니다. [2]

**Q4: 공격자는 SPF 규칙을 어떻게 우회하나요?**

비슷하게 생긴 도메인(타이포스쿼팅)을 악용하거나 정상적인 제3자 메일 서비스의 탈취된 계정을 이용함으로써.

**Q5: 비즈니스 이메일 침해(BEC)란 무엇인가요?**

공격자가 기업 이메일 계정을 탈취하거나 사칭해 사기성 결제를 승인하게 만드는 기업 대상 사기.

# 체크포인트 10: 심화 보안 FAQ (파트 D)

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

### Q6: 다중 인증은 피싱을 어떻게 막나요?

비슷하게 꾸민 랜딩 페이지만으로는 훔칠 수 없는 보조 토큰(하드웨어 키 등)을 요구합니다.

### Q7: 자격 증명 탈취용 랜딩 페이지란 무엇인가요?

입력된 사용자 이름, 비밀번호, MFA 토큰을 실시간으로 가로채도록 만든 위장 로그인 포털.

### Q8: 서브도메인 하이재킹이란 무엇인가요?

공격자가 사용되지 않는 DNS 서브도메인 포인터를 장악해 신뢰받는 상위 도메인 아래에 악성 피싱 랜딩 페이지를 호스팅합니다.

### Q9: DKIM 정렬(alignment) 검사는 어떻게 작동하나요?

'From' 헤더의 도메인이 DKIM 헤더에서 메시지에 암호학적으로 서명한 도메인과 일치하는지 확인합니다.

### Q10: 이메일 게이트웨이의 역할은 무엇인가요?

수신 이메일 필터링, 링크 감사, 첨부 파일 샌드박싱, SPF/DKIM/DMARC 준수 검증.

# 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. [4]

**2. 보안 인사이트**

비즈니스 이메일 침해(BEC)는 2025년 FBI의 IC3에 보고된 피해액만 30억 달러가 넘었습니다. [4]

**3. 보안 인사이트**

동형 문자 공격은 키릴 문자 유사 글자를 사용하여 브라우저에서 정확히 일치하는 브랜드 도메인을 눈으로는 똑같이 보이게 만듭니다.

**4. 보안 인사이트**

'p=reject'를 사용하면 도메인은 수신자에게 인증에 실패한 메일을 스팸으로 분류하지 말고 전달 단계에서 거부하라고 요청합니다. [2]

**5. 보안 인사이트**

CEO를 노리는 웨일링 공격은 흔히 기밀 합병이나 도메인 구매를 이유로 긴급 결제를 요구합니다.

**6. 보안 인사이트**

자격 증명 탈취 포털은 실제 로그인 페이지를 복제해 피해자가 공격자의 양식에 곧바로 비밀번호를 입력하게 만듭니다.

**7. 보안 인사이트**

CISA의 공동 피싱 지침은 DMARC, SPF, DKIM, 피싱에 강한 MFA와 함께 사용자 교육을 권장합니다. [3]

**8. 보안 인사이트**

SPF 평가는 DNS를 조회하는 항목 10개로 제한되며, 이 한도를 넘으면 'permerror' 결과가 반환됩니다. [1]

**9. 보안 인사이트**

FIDO2 하드웨어 보안 키는 원격 인증 정보 탈취에 대해 암호학적으로 뒷받침되는 보호를 제공합니다.

**10. 보안 인사이트**

피싱은 공격자가 조직에 처음 침투하는 가장 흔한 방법 중 하나이며, 그래서 정기적인 보안 인식 교육이 효과적인 방어책입니다.

# 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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

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

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

[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

스피어 피싱이란 무엇입니까? → 특정 개인이나 조직에 맞춰 만든 표적형 피싱 이메일

**2 질문 2** 정답: A

### 교사용 참고

SPF는 도메인의 허가된 발신 호스트를 DNS에 게시하여 수신자가 봉투 발신자를 확인할 수 있게 합니다.

**3 질문 3** 정답: A

### 교사용 참고

웨일링 공격이란 무엇입니까? → 유명 기업 임원을 특정해 노리는 피싱 캠페인

**4 질문 4** 정답: A

### 교사용 참고

DKIM은 무엇을 합니까? → 이메일에 암호 서명을 추가해 발신자의 진위를 검증함

**5 질문 5** 정답: A

### 교사용 참고

DMARC의 역할은 무엇입니까? → SPF/DKIM 검사에 실패한 메일을 수신 메일 서버가 어떻게 처리할지 지시함

## 답안: 체크포인트 2 – 참 또는 거짓

**6 질문 6** — 정답: 거짓

### 교사용 참고

거짓: 스피어 피싱은 일반적인 대량 피싱과 달리 특정 사람을 겨냥해 맞춤 제작됩니다.

**7 질문 7** — 정답: 참

### 교사용 참고

DMARC 정책은 메일 서버에 허가되지 않은 위조 메시지를 거부하도록 지시할 수 있습니다.

**8 질문 8** — 정답: 거짓

### 교사용 참고

거짓: SPF는 발신 IP를 DNS와 대조하여 확인하며, 암호화 서명을 검증하는 것은 DKIM입니다.

**9 질문 9** — 정답: 거짓

### 교사용 참고

거짓: 웨일링은 결제를 승인하고 민감한 데이터에 접근할 수 있는 고위 임원을 표적으로 삼습니다.

**10 질문 10** — 정답: 참

### 교사용 참고

참: 별도의 알려진 채널로 결제 요청을 확인하면 송금 사기를 막는 데 도움이 됩니다.

# 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. 스피어 | G 2. 스푸핑 | D 3. SPF | H 4. DKIM |
| C 5. DMARC | B 6. 웨일링 | E 7. 피싱 | A 8. 비싱 |

## 체크포인트 3: 답안 – 핵심 용어

| | | | |
|---|---|---|---|
| 1 스피어 | 2 위조 | 3 SPF | 4 DKIM |
| 5 DMARC | 6 웨일링 | | |

## 체크포인트 6 대체 활동: 답안 – 단어 연결

| | | | |
|---|---|---|---|
| 1 B – 피해자 | 2 A – 에스피에프 | 3 H – 알림서비스 | 4 C – 웨일링 |
| 5 G – 보이스피싱 | 6 E – 피싱메일 | 7 D – 디지털서명 | 8 F – 스피어피싱 |

### 교사를 위한 토론 참고

**핵심 용어:**
학생들이 스피어, 스푸핑, SPF을(를) 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

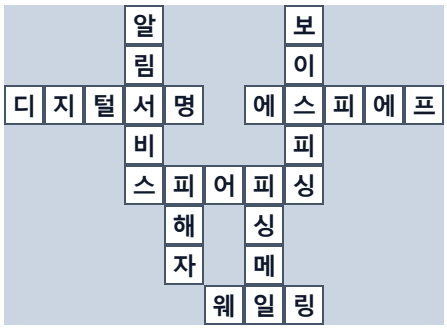
**출처 평가:**
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

# 퍼즐 답안과 교사용 참고

## 단어 찾기 정답

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 다 | 버 | 해 | 보 | 정 | 웨 | 청 | 명 | 소 | 파 | 번 | 격 | 개 | 암 | 워 |
| 험 | 싱 | 번 | 라 | 청 | 카 | 다 | 도 | 피 | 벽 | 공 | 정 | 림 | 타 | 하 |
| 라 | 피 | 연 | 정 | 술 | 소 | 송 | 서 | 접 | 싱 | 안 | 험 | 방 | 타 | 바 |
| 도 | 스 | 알 | 다 | 워 | 넷 | 검 | 인 | 술 | 알 | 메 | 속 | 메 | 프 | 다 |
| 리 | 이 | 방 | 하 | 방 | 에 | 링 | 이 | 싱 | 험 | 디 | 일 | 네 | 위 | 번 |
| 자 | 보 | 템 | 용 | 네 | 스 | 연 | 스 | 스 | 이 | 위 | 웨 | 일 | 링 | 디 |
| 관 | 속 | 아 | 답 | 주 | 피 | 소 | 보 | 피 | 비 | 터 | 바 | 가 | 마 | 아 |
| 스 | 공 | 지 | 비 | 방 | 에 | 털 | 암 | 디 | 어 | 청 | 벽 | 파 | 시 | 이 |
| 비 | 넷 | 타 | 용 | 연 | 프 | 송 | 벽 | 관 | 격 | 피 | 워 | 전 | 전 | 리 |
| 서 | 스 | 메 | 응 | 청 | 워 | 사 | 주 | 험 | 속 | 기 | 싱 | 도 | 바 | 프 |
| 림 | 디 | 지 | 털 | 서 | 명 | 타 | 소 | 어 | 색 | 아 | 알 | 프 | 네 | 피 |
| 알 | 벽 | 정 | 림 | 카 | 송 | 파 | 시 | 링 | 격 | 사 | 검 | 마 | 해 | 가 |
| 림 | 결 | 타 | 암 | 나 | 파 | 속 | 파 | 서 | 크 | 용 | 카 | 자 | 스 | 리 |
| 이 | 보 | 용 | 도 | 알 | 주 | 서 | 시 | 피 | 안 | 나 | 다 | 시 | 공 | 연 |
| 위 | 응 | 디 | 관 | 방 | 템 | 응 | 도 | 차 | 송 | 명 | 바 | 네 | 도 | 링 |

## 십자말풀이 정답




## 십자말풀이 정답 교사용 안내

### 가로

**3 가로: 디지털서명** 이메일에 포함되는 암호학적 서명 (5 글자)

**4 가로: 에스피에프** DNS에 등록해 메일을 보낼 수 있는 서버를 정해 두는 이메일 인증 방식 (5 글자)

**5 가로: 스피어피싱** 특정인을 겨냥해 개인 정보를 이용한 맞춤형으로 보내는 피싱 (5 글자)

**8 가로: 웨일링** 경영진 등 고위 인사를 노린 표적 피싱 (3 글자)

### 세로

**1 세로: 알림서비스** 계정에 이상이 생기면 바로 알려 주는 기능 (5 글자)

**2 세로: 보이스피싱** 전화 통화로 속여 돈이나 정보를 빼내는 사기 (5 글자)

**6 세로: 피해자** 범죄나 사고로 손해를 입은 사람 (3 글자)

**7 세로: 피싱메일** 사람을 속이려고 보내는 가짜 이메일 (4 글자)

# 뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

### 단어 맞추기 정답

1. 에피에프스 — **에스피에프**
2. 링일웨 — **웨일링**
3. 일피메싱 — **피싱메일**
4. 스싱피보이 — **보이스피싱**
5. 자해피 — **피해자**
6. 서디털명지 — **디지털서명**
7. 피싱스어피 — **스피어피싱**
8. 스알서비림 — **알림서비스**

### 비밀 암호 도전 정답

**"메일 점검으로 사기 탐지"**

# 사례 연구 답안

## A 사례 연구 1: 최고경영진 대상 웨일링 공격 대응

교사용 풀이

### 채점 기준

**학생 답안에는 다음 사항이 포함되어야 합니다.**

- 상황 분석: 최고재무책임자(CFO)가 CEO를 사칭한 매우 개인화된 이메일을 받습니다. 기밀 도메인 구매를 마무리하기 위해 50,000달러를 급히 송금하라는 요청입니다.
- 권장 전략 및 해결책: 위조된 발신 도메인을 차단하도록 'p=reject' 정책으로 DMARC를 구성합니다. 게이트웨이에서 외부 발신자 경고 배너를 추가하고, 모든 금융 거래에는 별도 경로(대역 외)의 구두 확인을 요구합니다.

## B 사례 연구 2: SPF/DKIM/DMARC 게이트웨이 정책 적용하기

교사용 풀이

### 채점 기준

**학생 답안에는 다음 사항이 포함되어야 합니다.**

- 시나리오 분석: 한 기업이 발송 마케팅 이메일이 자주 스팸으로 분류되고 해커들이 회사의 브랜드 도메인을 적극적으로 사칭하고 있어 보안 감사를 통과하지 못하고 있습니다.
- 권장 전략 및 해결책: 허용된 발신자 IP를 명시한 SPF용 TXT 레코드를 게시하세요. 발신 메일 서버에 DKIM 서명 키를 설정하고, 수신되는 DMARC XML 피드백 보고서를 분석해 악용 사례를 찾아냅니다.