중소기업 침해사고 피해지원 서비스 동향 보고서(2025년 상반기)-기업 타깃형 스피어 피싱 사례 및 대응방안

등록일	@2025년 8월 20일 오후 2:24
최종수정일	@2025년 8월 20일 오후 4:20
저자&감수	KISA 중소기업 침해사고 피해지원 서비스
Proofreaders	

1. 개요

디지털 전환이 가속화되면서 중소기업의 업무 환경과 비즈니스 모델 역시 급격히 변화하고 있다. 이러한 변화에 따라 사이버 공격 역시 점점 더 지능적이고 정교한 방식으로 진화하고 있다.
특히, 불특정 다수를 대상으로 하는 피싱(Phishing) 공격과 특정 개인과 기업 임직원 등을 표적으로 삼는 스피어 피싱(Spear Phishing) 공격은 대표적인 디지털 침해사고 중 하나로 사용자 또는 기업의 정보를 탈취한 뒤, 금전적 이득을 취하는 행위이다. 이는 중소기업의 정보 자산과 재무적 안정성에 직접적인 위협을 가하고 있다.

또한, 최근 한국인터넷진흥원에 접수된 중소기업 침해사고 신고 사례를 분석한 결과, 공격자들은 기업의 규모, 업종, 조직 내 역할 등 공개된 기업 정보와 무차별 대입, 취약점 공격 등으로 탈취한 민감정보를 활용하여 정교한 설계, 맞춤형 공격을 시도하려는 경향을 보이고 있다.

이로 인해 피해 기업은 단기적인 경영 차질과 금전적 손실뿐 아니라, 대외 신뢰도 하락 등 장기적인 피해까지 입는 사례가 점차 증가하고 있다.

본 보고서에서는 피싱 및 스피어 피싱 침해사고의 실제 사례를 분석하여 피해 원인을 파악하고 그에 대한 효과적인 대응방안을 제시하고자 한다.

이를 통해 중소기업이 실제 현장에서 마주하는 디지털 위협을 보다 정확히 이해하고, 사전 예방 및 사고 대응 역량을 강화하는 데 실질적인 도움이 되기를 기대한다.

2025년 상반기 중소기업 침해사고 피해지원 서비스 통계

2025년 상반기에 접수된 주요 침해사고 사례를 유형별로 분석한 결과, 피싱 관련 침해사고는 1분기 대비 2분기에 24건 증가하였으며, 분기별 사고 유형 중 가장 증가된 빈도를 보였다.

실제 침해사고 사례를 분석한 결과, 악성 피싱 메일로 인한 악성코드 감염이나 계정 탈취 사례가 다수 확인되었다.
이러한 사례를 통해 주요 원인과 대응방안을 살펴보고자 한다.

25년 상반기 주요 침해사고 발생 유형

침해사고 유형	1분기 발생 비율(건수)	2분기 발생 비율(건수)	25년 상반기 발생 비율(건수)	분기별 증감

랜섬웨어	15.9%(27건)	9.5%(35건)	11.5%(62건)	8건 증가
피싱	**2.9%(5건)**	**7.9%(29건)**	**6.3%(34건)**	**24건 증가**
악성코드(파일) 유포지, 경유지	2.9%(5건)	6%(22건)	5%(27건)	17건 증가
악성코드 C2서버	5.3%(9건)	4.3%(16건)	4.5%(25건)	7건 증가

2. 사고 사례 분석

2-1. 피싱 침해사고의 변화

피싱 메일을 이용한 공격 시도는 공격자가 가장 흔히 사용하는 방식 중 하나로, 외부에 공개된 메일 주소를 수집한 뒤, 악성코드를 첨부하거나 악성 링크를 포함한 메일을 발송하여 수신자의 실행 · 클릭을 유도한다.

또한, 공격자는 메일 내용을 기업 또는 기관에서 보낸 정상적인 메일처럼 위장하여, 수신자가 이를 정상 업무 메일로 오인하도록 만든다.

최근 이러한 피싱 침해사고는 공격 방식이 더욱 지능적이고 정교하게 변화하고 있다.
전통적인 방식으로는 공격자가 자체 메일 서버를 구축하여 피싱 메일을 전송하거나, 관리자 권한을 탈취한 웹 서버에 메일 발송 기능이 포함된 악성 소스코드를 실행한 뒤 피싱 메일을 전송하였다.
그러나 최근에는 공격 대상 기업의 실제 메일 서버를 침투한 뒤, 기업 메일 주소를 이용해 피싱 공격을 수행하는 사례가 증가하고 있다.

또한, 기존에 주고받은 메일에 '답장 형식'으로 피싱 메일을 전송하는 방식으로 진화하고 있다. 이 경우 메일 본문 하단에는 기존의 정상 메일 내용이 함께 포함되기 때문에, 수신자는 이를 평소의 업무 메일로 인식하고 쉽게 속게 된다.
이처럼 기업 메일을 활용한 공격 시도는 점차 고도화되고 있으며, 그에 따른 피해 역시 확대되는 추세이다.

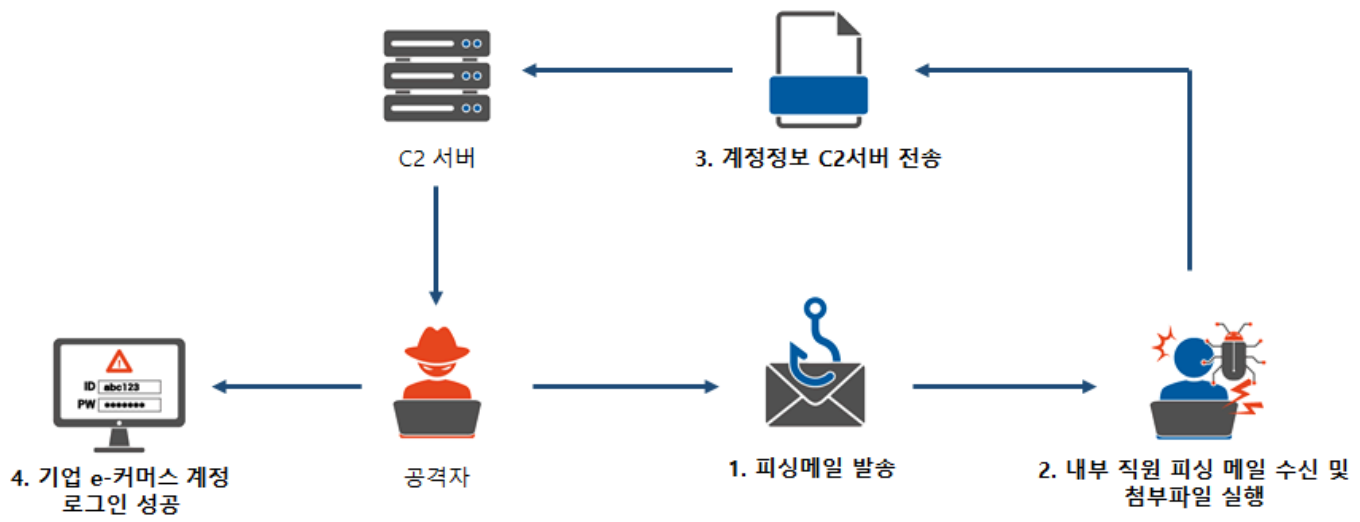
2-2. 유형별 피해 사례

1. 기업 e-커머스 계정 탈취를 통한 판매상품 변경

디지털 전환의 가속화는 기업의 업무 환경뿐만 아니라 소비 트렌드에도 큰 변화를 가져왔다.
e-커머스 플랫폼의 등장과 사용자 증가로 인해 소비자의 온라인 소비가 활발해 졌으며, 이에 따라 많은 기업들이 변화된 트렌드에 맞춰 e-커머스 플랫폼을 활용하여 상품을 판매하고 있다.

그러나 이러한 비즈니스 환경의 변화는 공격자에게 새로운 위협 수단으로 악용되기도 한다.
공격자는 기업을 대상으로 악성코드를 첨부한 피싱 메일을 발송하고, 이를 수신한 사용자가 악성코드를 실행하면, 기업이 보유한 e-커머스 계정이 탈취되는 피해가 발생할 수 있다.

다음은 실제 사례를 기반으로 “피싱 메일을 이용한 계정 탈취 과정”을 설명하고자 한다.



피싱 메일을 이용한 계정 탈취 과정

1) 피싱메일 발송

- 공격자는 정상적인 거래 메일을 위장한 피싱 메일을 기업 내부 직원에게 발송한다.
- 메일에는 악성 링크나 악성 첨부파일이 포함되어 있으며, 클릭 또는 실행 시 악성 코드가 작동하도록 설계되어 있다.

2) 내부 직원의 메일 수신 및 첨부파일 실행

- 수신자는 발신자가 신뢰할 수 있는 거래처 또는 내부 부서인 것으로 착각해 첨부파일을 열거나 링크를 클릭한다.
- 이 과정에서 계정 정보 탈취용 악성 코드가 실행된다.

3) 계정 정보 C2 서버 전송

- 악성 코드는 사용자의 로그인 ID, 비밀번호 등 계정 정보를 은밀하게 수집한다.
- 수집된 정보는 공격자의 C2(Command & Control) 서버로 전송된다.

4) 기업 e-커머스 계정 로그인 성공

- 공격자는 탈취한 계정으로 기업 e-커머스 시스템에 무단 접속한다.
- 이후 등록된 상품 정보를 위조하거나 가격을 변경하는 등 불법 행위를 수행한다.

<피해 영향>

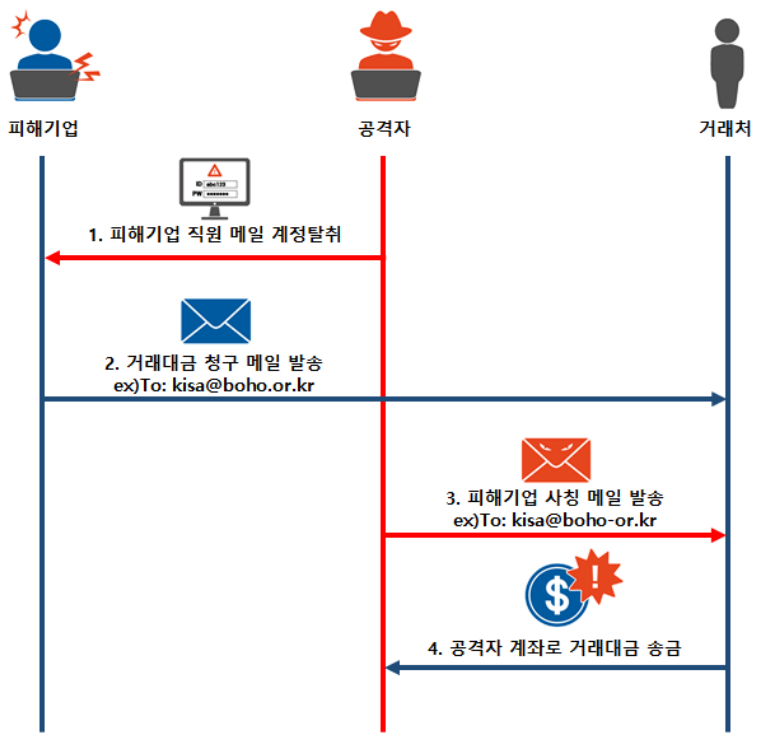
- 소비자 피해 : 소비자는 공격자가 변경한 상품을 실제로 구매하게 되며, 이 과정에서 다수의 반품 및 환불 요청이 발생한다.
- 기업 피해
  - 소비자 신뢰가 하락할 수 있다.
  - 금전적 손실이 발생할 수 있다.
  - 시스템 복구 및 보안 강화에 따른 추가 비용이 발생할 수 있다.
  - 브랜드 이미지 훼손 및 장기적으로 사업에 차질이 일어날 수 있다.

2. 기업 비즈니스 메일을 사칭한 거래대금 탈취

비즈니스 메일은 사업 제안, 업무 협의, 자료 전달 등 기업의 핵심적인 업무 소통 수단으로 활용된다. 특히 기업은 거래처에 거래대금을 청구할 때, 메일 본문에 수금용 계좌번호를 기재하는 경우가 많다.

이러한 특성을 악용한 공격자는 메일 계정을 탈취하거나 유사 도메인을 활용해 거래처를 속이고, 송금 계좌를 자신이 관리하는 계좌로 변경하여 금전을 편취한다.

다음은 실제 사례를 기반으로 “거래대금 탈취 개요도”를 설명하고자 한다.



거래대금 탈취 개요도

1) 계정 탈취

- 공격자는 피싱 메일, 악성코드, 취약점 공격 등을 통해 피해 기업 직원의 메일 계정을 먼저 탈취한다.
- 탈취 후, 해당 계정의 기존 메일 내용을 확인하여 거래처와의 최근 송 · 수신 메일을 파악한다.

2) 거래대금 청구 메일 발송

- 정상적인 거래 메일 형식을 그대로 모방하여, 거래처에 거래대금 청구 메일을 발송한다.
- 발신자 주소나 도메인을 피해 기업과 유사하게 위조해, 수신자가 의심하지 않도록 한다.

3) 사칭 메일을 통한 계좌 변경 안내

- 메일 본문에 공격자가 지정한 위조 계좌번호를 기재하고, “기존 계좌가 변경되었다”는 내용 등으로 자연스럽게 안내한다.

4) 거래대금 송금

- 거래처는 해당 메일을 정상 요청으로 착각해 공격자의 계좌로 거래대금을 송금하게 된다.

<피해 영향>

- 금전적 피해 : 송금액 전액 손실이 발생할 수 있다.
- 신뢰도 하락 : 거래처와의 관계 악화와 장기적 신뢰에 손상이 생길 수 있다.

- 법적 · 행정적 부담 : 피해 복구를 위한 법적 대응, 수사 협조, 추가 보안 강화 비용이 발생할 수 있다.

2-3. 사고 주요 원인

1. 무차별 대입 공격(Brute Force Attack)

무차별 대입 공격(Brute Force Attack)은 공격자가 로그인에 성공할 때까지 가능한 문자 조합을 무차별로 반복 입력하며 시도하는 방식이며, 사용자의 계정 정보가 예측하기 쉬운 조합일수록 이 공격에 더욱 취약하다.

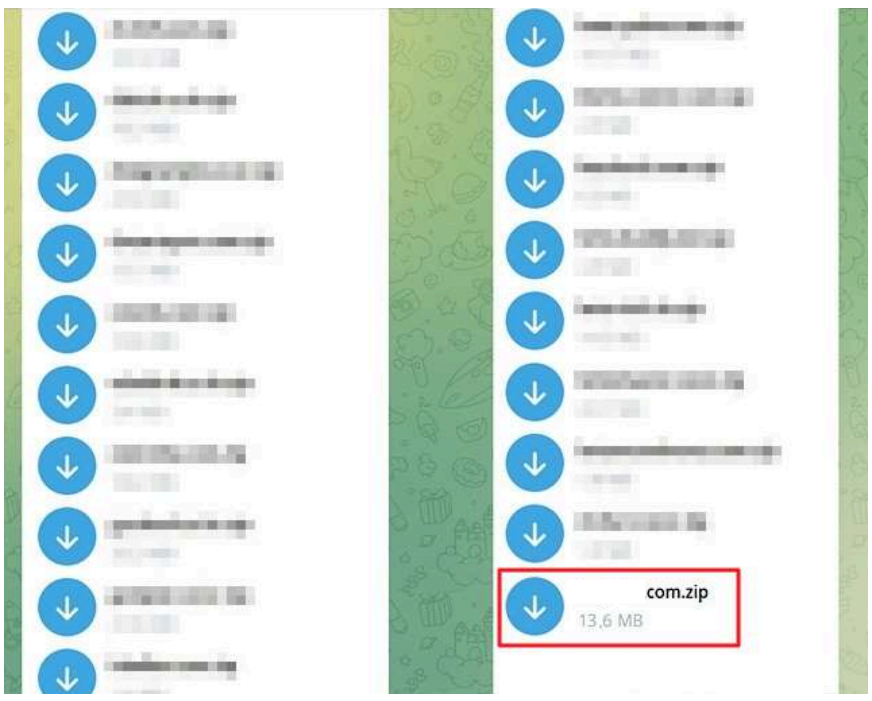
공격자는 외부에서 접근 가능한 기업용 메일 서비스를 대상으로 무차별 대입 공격을 수행해 로그인에 성공한 뒤, 내부 직원의 메일을 열람하거나 유출하고, 이를 악용해 거래처나 다른 직원에게 피싱 메일을 전송하는 등 2차 공격을 시도한다.

▼ 특정시각 [접속 시도 계정]을 사용하여 메일 서버에 로그인하려 했으나, 비밀번호가 잘못되어 인증에 실패한 로그

```
[08:08:38 3958.140411135846144] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
[08:08:41 3958.140411135846144] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
[08:08:44 3958.140411135846144] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
[08:08:50 3958.140411135846144] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
[08:08:56 3958.140411114833664] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
[08:09:02 3958.140411082397440] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
[08:09:04 3958.140411082397440] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
[08:09:07 3958.140411082397440] -INFO SIP:[메일서버 IP] AI:[접속 시도 계정] CMD:AUTH DS:invalid password
```

2. 크리덴셜 스터핑(Credential Stuffing)

크리덴셜 스터핑(Credential Stuffing)은 이미 유출된 아이디와 패스워드를 확보한 뒤, 이를 다양한 웹사이트나 서비스에 반복적으로 입력해 로그인을 시도하는 공격 기법이다. 이는 사용자가 동일한 계정 정보를 여러 서비스에 재사용하는 습관을 악용한 방식이다.



텔레그램(Telegram)에서 유통되는 기업의 계정정보(도메인명.zip) 관련 예시

텔레그램 등에서 유출 · 유통되는 압축 파일(도메인명.zip)에는 일반적으로 이메일 주소, 사용자명, 비밀번호, 그리고 경우에 따라 접속 IP와 브라우저 정보 등이 포함되어 있다.
공격자는 이 정보를 확보한 뒤 다음과 같은 절차로 크리덴셜 스터핑 공격을 수행한다.

1) 데이터 추출 및 정리

- 압축 파일을 해제해 CSV, TXT 등의 계정 목록을 확보한다.
- 불필요한 데이터(중복 계정, 형식 오류)를 제거하고, 이메일 · 비밀번호 쌍으로 정리한다.

2) 다중 사이트 로그인 시도

- 대상 웹서비스(쇼핑몰, 은행, 포털, 기업 내부 시스템)의 로그인 API나 웹페이지를 자동으로 호출하도록 설정한다.
- 동일한 계정 · 비밀번호 조합을 여러 사이트에 반복 입력하여 로그인을 시도한다.
- 이때, VPN · 프록시 · 봇넷을 사용해 IP를 계속 변경함으로써 방어 시스템의 차단을 회피한다.

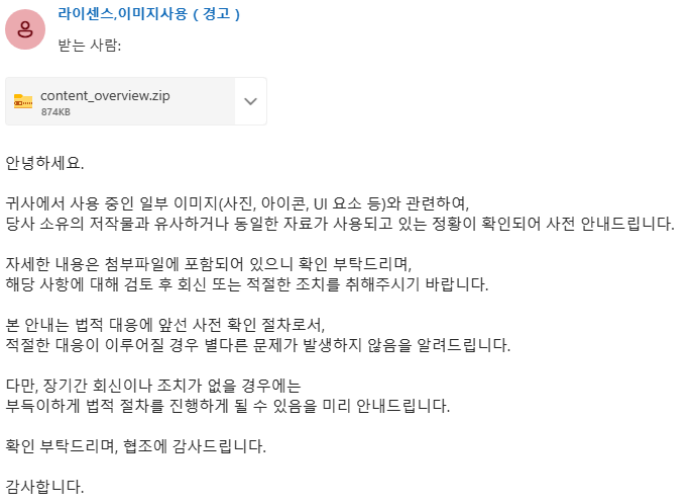
3) 성공 계정 활용

- 로그인에 성공한 계정은 추가 침해(내부 문서 탈취, 금전 결제, 악성 메일 발송)에 활용하거나, 다른 범죄자에게 재판매한다.
- 특히 내부 메일 계정 · 업무용 시스템 계정은 기업 침투의 발판이 된다.

이와 같이, 단순히 웹 서비스에 유출 계정을 무차별 대입(Brute Force)하는 것보다 실제 사용자의 유출 계정을 활용하는 크리덴셜 스터핑 공격은 성공 가능성이 높다. 또한 피해 기업이 비정상 로그인을 인지하기 어렵다는 특징을 갖고 있다.

3. 악성코드를 통한 정보탈취

공격자는 기업, 기관 또는 개인을 사칭해 업무와 관련된 내용처럼 위장한 메일을 발송하며, 메일 본문에 악성링크나 악성코드를 포함시켜 사용자의 실행을 유도한다. 이러한 메일을 신뢰한 사용자는 악성 사이트에 접속해 계정 정보를 입력하거나, 첨부된 악성 파일을 다운로드 및 실행함으로써 정보탈취 피해를 입게 된다.



악성코드 첨부 메일 예시

사용자에게 유포된 악성코드는 주로 정보탈취형 또는 원격제어형으로, 감염된 시스템에서 ▲운영체제 정보 ▲키보드 입력(키로깅) ▲브라우저에 저장된 계정 정보 ▲네트워크 설정 ▲프로세스 목록 등의 데이터를 수집한 뒤, 이를 C2 서버(Command and Control Server)로 전송한다.
이후 C2 서버로부터 추가 명령을 전달받아 원격 조작, 추가 악성코드 설치 등 2차 행위를 수행한다.

3. 대응방안

3-1. 일반 사용자를 위한 대응방안

의심스러운 메일 확인

- 출처가 불분명하거나, 제목이나 내용이 평소와 다르고, 파일 열람을 급히 요구하는 메일은 주의가 필요하다.
- 특히, 발신자 주소를 위조하는 경우가 많기 때문에, 보낸 사람의 메일 주소가 실제 도메인과 정확히 일치하는지 반드시 확인해야 한다.

예시)
@naver.com → @naver-com.**cc**
@google.com → @goog**l**e.com
@daum.net → @dau**u**m.net

첨부 파일 및 링크 주의

- 메일에 첨부된 스크립트 파일(JS, JAVA, VBS 등)이나 실행 파일(EXE, SCR 등)은 절대 실행하지 않도록 주의해야 한다.
- 파일명 뒤에 .pdf 등 허위 확장자를 붙이거나 공백을 삽입해 실제 확장자(EXE 등)가 보이지 않도록 위장하는 경우가 있으므로, 파일의 실제 확장자를 반드시 확인해야 한다.
- 의심스러운 첨부 파일은 즉시 실행하지 말고, 백신 프로그램으로 먼저 검사한다.
- 메일 본문에 포함된 URL 링크의 클릭을 유도하는 경우에도 주의가 필요하다. 링크를 클릭하기 전 마우스를 올려 실제 연결될 주소를 확인하고, 신뢰할 수 있는 도메인인지 확인해야 한다.

보안 프로그램 최신 상태 유지

- 운영체제, 백신, 기타 응용 프로그램의 보안 패치를 항상 최신 상태로 유지하고, 백신의 실시간 감시 기능을 반드시 활성화한다.

비정상 송금 요청 확인

- 평소와 다른 계좌로의 송금 요청이나 송금을 급히 요구하는 메일 · 메신저 등의 요청은 반드시 전화 등 다른 수단으로 추가 확인한다.
- 최근에는 거래처를 사칭한 공격자가 메신저의 음성 통화로 송금을 요청하는 사례가 확인되고 있으므로, 음성 통화 시에도 상대방의 신원을 반드시 확인하는 절차가 필요하다.

<비정상 송금 요청 확인 사례 예시>

예시1 : 거래처 사칭 메일
메일 제목 : [긴급] 송금 계좌 변경 안내
내용 : “귀사와의 거래 계좌가 변경되었음을 안내드립니다. 오늘 중으로 아래 새 계좌로 송금 부탁드립니다.”

예시2 : 상급자 사칭 메신저
메신저 내용 : “홍길동님, 지금 회의 중이라 통화가 어렵습니다. 급히 송금할 건이 있으니 아래 계좌로 300만 원만 이체해 주세요. 회의 끝나면 바로 설명드릴게요.”

예시3 : 음성 통화를 통한 계좌 변경 유도
(공격자가 거래처 담당자를 사칭해 실제 이름과 소속을 언급하며, 전화 시도)
전화 통화 : "회계팀에서 송금 계좌를 변경했습니다. 새로운 계좌번호를 알려드립니다."

메일 계정 보안 강화

- 패스워드는 주기적으로 변경하고, 영문 대 · 소문자, 숫자, 특수문자를 혼합하여 복잡하게 설정한다.
예시) '10H+20Min', 'I!Can&9it' 등
- 패스워드 선택 및 이용 안내서

KISA 암호이용활성화
한국인터넷진흥원(KISA)에서는 안전한 패스워드 설정 방법, 패스워드 보안 지침 등을 소개하는 '패스워드 선택 및 이용 안내서'를 배포하고 있습니다.제정 : 2008년 1월 개정 : 2019년 6월내용- 안전한 패스워드- 이러한 패스워드 사용하지 마세요- 안전한 패스워드 생성 Tip- 패스워드 보안 지침(이용자 측면)- 패스워드 보안 지침(관리자 측면)
https://seed.kisa.or.kr/kisa/Board/53/detailView.do

- 메일 서비스의 로그인 기록을 주기적으로 확인하고, 본인이 접속하지 않은 기록이 발견되면 즉시 비밀번호를 변경하고 보안 담당자에게 신고한다. 또한, “해외 로그인 차단” 기능을 적극 활용하는 것이 권장된다.
- 한국인터넷진흥원과 개인정보보호위원회가 공동 제공하는 "털린 내 정보 찾기 서비스”를 통해 계정 정보 유출 여부를 확인할 수 있다.

https://kidc.eprivacy.go.kr/
https://kidc.eprivacy.go.kr/

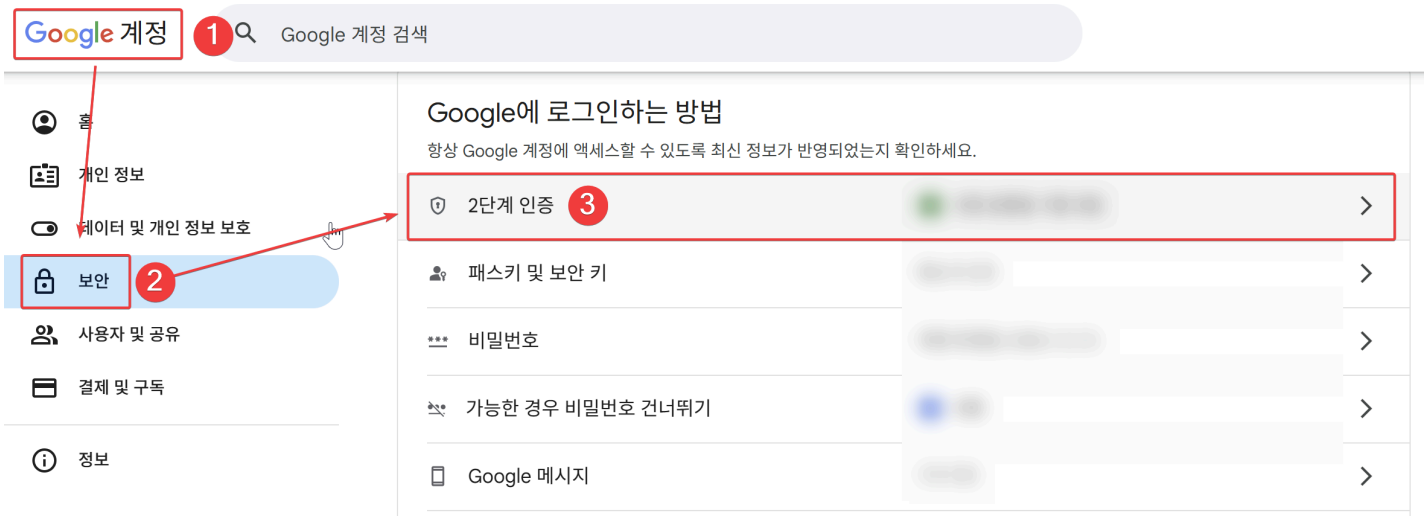
자세히 알아보기 > 사이버위협 : KISA 보호나라&KrCERT/CC
KISA https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000030&searchWrd=&menuNo=205027&pageIndex=3&categoryCode=&nttId=70087

3-2. 기업 및 기관을 위한 대응방안

메일 로그인 시 2단계 인증 도입(MFA, Multi-Factor Authentication)*

* MFA : 서로 다른 유형의 인증 수단을 두 가지 이상 결합하여 사용자의 신원을 확인하고 보안을 강화하는 방식

- 메일 계정이 유출되더라도 SMS, 구글 OTP 등 2단계 인증을 적용하면 피해를 크게 줄일 수 있으므로 필수적으로 도입해야 한다.



구글 계정 2단계 인증 설정 예시

- 2단계 인증(2FA, Two-Factor Authentication, 이중 인증)이란 무엇인지, 어떻게 안전하게 이용하는지에 대한 내용은 아래 카드 뉴스 페이지를 참고하면 쉽게 이해할 수 있다.

카드뉴스 > 사이버위협 : KISA 보호나라&KrCERT/CC

KISA https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0001030&searchWrd=&menuNo=205090&pageIndex=2&categoryCode=&nttId=71204

메일 보안 솔루션 도입 및 활용

- 도입 : 메일 서버 또는 게이트웨이에 DMARC(Domain-based Message Authentica tion, Reporting & Conformance)* 정책을 적용하고, 이를 지원하는 보안 솔루션을 구축한다.

  * DMARC : SPF와 DKIM을 통해 메일을 검증하고, 검증 결과에 따라 수신·격리·차단 여부를 자동 결정하는 프로토콜

- 활용

① SPF(Sender Policy Framework)*와 DKIM(DomainKeys Identified Mail)** 설정을 완료한 뒤, 주기적으로 정책 위반 로그와 리포트를 점검한다.

  * SPF : 메일 발신 서버 IP와 발신자 메일 도메인 주소 IP를 비교하여 동일 여부를 확인

  ** DKIM : 발신 메일에 전자서명을 추가하여 메일의 위변조 여부를 확인

② 의심 메일은 격리 폴더로 이동 후 관리자 검토 절차를 거친다.
③ 정책 위반이 반복되는 발신자 도메인은 블랙리스트에 등록하여 차단한다.

조직 내 보안 문화 정착

- 스피어 피싱 메일은 사람의 심리적 약점을 노리는 사회공학 기법을 활용하므로, 직원 교육이 예방의 핵심이다.
- 정기적인 메일 보안 교육을 실시하고, 최신 침해사고 사례와 대응 방법을 꾸준히 공유해야 한다.

해킹 메일 대응 모의 훈련 실시

- 해킹 메일 대응 모의훈련은 실제 피싱 공격 경험을 제공하여 임직원의 공격 인식과 경각심을 높이고, 조직의 대응 역량 강화에 효과적이다.
- '2025년 상반기 사이버 위기 대응 모의훈련' 결과, 재참여 기업의 피싱메일 열람률(16.2%)이 신규 참여 기업의 열람률(18.5%)보다 낮게 나타나, 반복적인 훈련이 보안 인식과 대응 능력 향상에 긍정적 영향을 미친다는 점이 확인되었다.

과학기술정보통신부

https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&pageIndex=9&bbsSeqNo=94&nttSeqNo=3185903&searchOpt=ALL&searchTxt=

- 한국인터넷진흥원은 민간 기업의 해킹 메일 대응 역량 강화를 위해 해킹 메일 대응 모의훈련 서비스를 제공하고 있다.

사이버 위기대응 모의훈련 > 기업 서비스 > 주요사업 소개 > 정보보호 서비스 : KISA 보호나라&KrCERT/CC

KISA https://www.boho.or.kr/kr/subPage.do?menuNo=205014

사이버 시큐리티 훈련 플랫폼 > 기업 서비스 > 주요사업 소개 > 정보보호 서비스 : KISA 보호나라&KrCERT/CC

KISA https://www.boho.or.kr/kr/subPage.do?menuNo=205015

3-3. 침해사고 발생 시 대응 조치 요령

초기 대응 조치

- 의심스러운 첨부파일 실행 또는 링크 클릭 시 즉시 인터넷 연결을 차단한다.
- 사고 조사를 위해 메일, 첨부파일 등 관련 증거는 삭제하지 말고 안전하게 보관한다.
- 신속하게 보안 담당자 및 관련 기관에 신고한다.
- 신고 연락처
  - 한국인터넷진흥원 (www.boho.or.kr/☎ 118)

사후 대응 조치

- 메일 계정 탈취가 의심될 경우, 즉시 비밀번호를 변경하고 계정 복구 절차를 진행한다.
- 백신 프로그램을 이용해 전체 시스템 검사를 실시한다.
- 유사 사고의 재발 방지를 위해 사고 내용을 조직 내에 신속히 공유하고 전파한다.

중소기업 침해사고 피해 지원 서비스

- 중소기업에서 침해사고가 발생할 경우, 한국인터넷진흥원에서 사고 원인 분석, 재발 방지 조치, 보안 컨설팅 및 교육 등 다양한 지원을 제공하므로 해당 서비스를 활용할 수 있다.

중소기업 피해지원 > 정보보호 서비스 : KISA 보호나라&KrCERT/CC

KISA https://www.boho.or.kr/kr/subPage.do?menuNo=205004

4. 결론

디지털 전환으로 시간과 공간에 구애 받지 않는 메일은 현대 사회에서 중요한 의사소통 수단을 넘어, 고객 응대, 고객 유치, 정보 공유 등 기업의 핵심 비즈니스 수단으로 자리매김하고 있다. 그러나 기업 메일 계정 탈취, 메일을 통한 악성코드 유포 등 사이버 위협이 빈번하게 발생하면서, 거래대금 탈취, 피싱 메일 열람에 의한 랜섬웨어 감염, e-커머스 영업 방해 등 다양한 피해가 발생하고 있다. 이는 기업 신뢰도 하락은 물론, 고객 확보의 어려움과 궁극적인 금전적 손실로 이어진다.

기업의 비즈니스 메일 침해사고를 예방하기 위해서는 메일 서버에 대한 기술적 조치가 필수적이다. 로그인 시 2단계 인증을 도입·적용하고, 사용자의 주기적인 패스워드 변경과 복잡한 패스워드 사용 정책을 설정해야 한다. 아울러 메일 보안 솔루션을 도입해 악성메일을 사전에 차단함으로써 피해 발생을 최소화해야 한다.

하지만, 기술적 대응보다 더 중요한 것은 사용자의 보안 인식 강화이다. 사이버 공격의 주요 대상은 사용자이며, 이들의 실수와 부주의를 노린 공격이 많다. 따라서 사용자는 발신자 주소의 정상 여부를 반드시 확인하고, 출처가 불분명한 메일은 즉시 삭제하거나 사내 정보보안팀에 신고해야 한다. 또한, 첨부파일은 백신 검사 후 안전성이 확인된 경우에만 실행해야 하며, 메일에 삽입된 URL 링크 또한 함부로 클릭하거나 접속하지 않아야 한다.

결국 디지털 전환은 우리에게 편리한 환경과 인프라를 제공하지만, 그 이면에는 여전히 보이지 않는 사이버 위협이 존재한다. 기업과 개인이 보안 수칙을 철저히 준수한다면 이러한 위협으로부터 안전하게 침해사고를 예방할 수 있을 것이다.