기업의 안전한 메일 사용을 위한

악성메일 모의훈련 안내서

KIWONTECH

| 01 | 훈련 개요

KIWONTECH

▪ 추진 배경

① 'FBI'에 따르면 2020 사이버 주요 범죄 유형은 랜섬웨어와 ***피싱 스캠**이며, 피해 규모가 가장 큰 것은 기업 대상 ***지능형 사기 메일(BEC)**임.

② 'FireEye'에 따르면 사용자의 스팸 메일 열람률이 3%인 것에 비해 **스피어피싱 시도 이메일 열람률은 70%**에 달한다고 함.

③ 'FireEye'에 따르면 사용자의 스팸 메일 링크 클릭률이 5%인 것에 비해 **스피어피싱 시도 이메일의 링크 클릭률은 50%**에 달한다고 함.

* 피싱 스캠(Phishing Scams) : 공공기관, 은행과 같은 신뢰할 수 있는 단체로 사칭하여 개인 정보를 탈취하는 지능형 공격(APT) 수법이다.

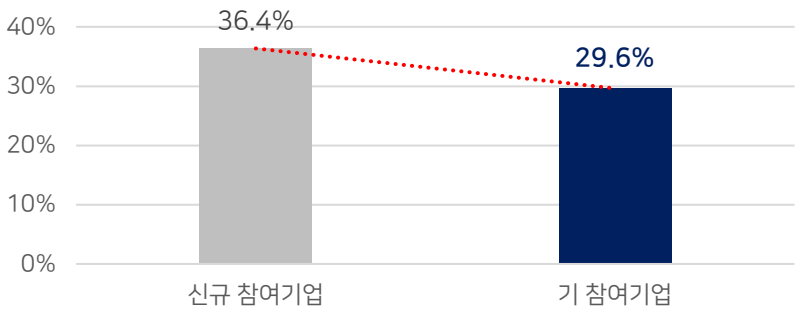
* BEC(Business Email Compromise) : 기업을 대상으로 한 이메일 침해 공격을 뜻하며 송금과 관련된 직원이나 경영진, 회사의 공식 메일 계정으로 사기 거래 피싱 공격을 가하기 때문에 금전 피해가 크다.

▪ 추진 목표

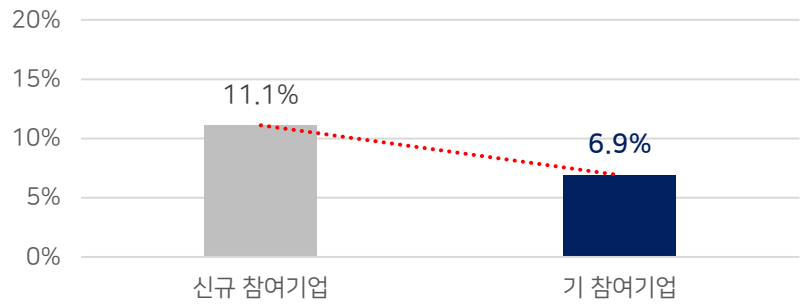
① 고도화된 지능형 사기 메일에 대한 훈련 대상자의 대처 능력 파악, 훈련 결과를 토대로 보완점 도출

② 훈련 대상자가 사기 메일의 수법을 직접 확인하고, 경각심을 고취시켜 임직원의 이메일 보안 의식 제고 및 악성 메일에 의한 피해 방지

[참고] 과학기술정보통신부와 한국인터넷진흥원 주최 '21년 상반기 사이버위기대응 모의훈련' 결과, 기 참여기업의 메일 열람률과 첨부파일 클릭률이 신규 참여기업에 비해 낮게 나타남.



[차트] 메일 열람률



[차트] 첨부파일 클릭률

| 01 | 훈련 개요

KIWONTECH

▪ 훈련 절차

[1단계] 훈련 대상사에서 요청한 시나리오를 토대로 악성메일 제작
[2단계] 훈련 일시에 훈련 대상자에게 제작한 악성메일 발송
[3단계] 악성메일 발송 시점부터 훈련 종료일까지 평가 항목에 대한 데이터 수집
[4단계] 수집한 데이터를 토대로 결과 보고서 도출
[5단계] 결과 보고서를 토대로 임직원들의 악성메일에 대한 대처 능력 파악 및 대응책 수립

▪ 훈련 시나리오

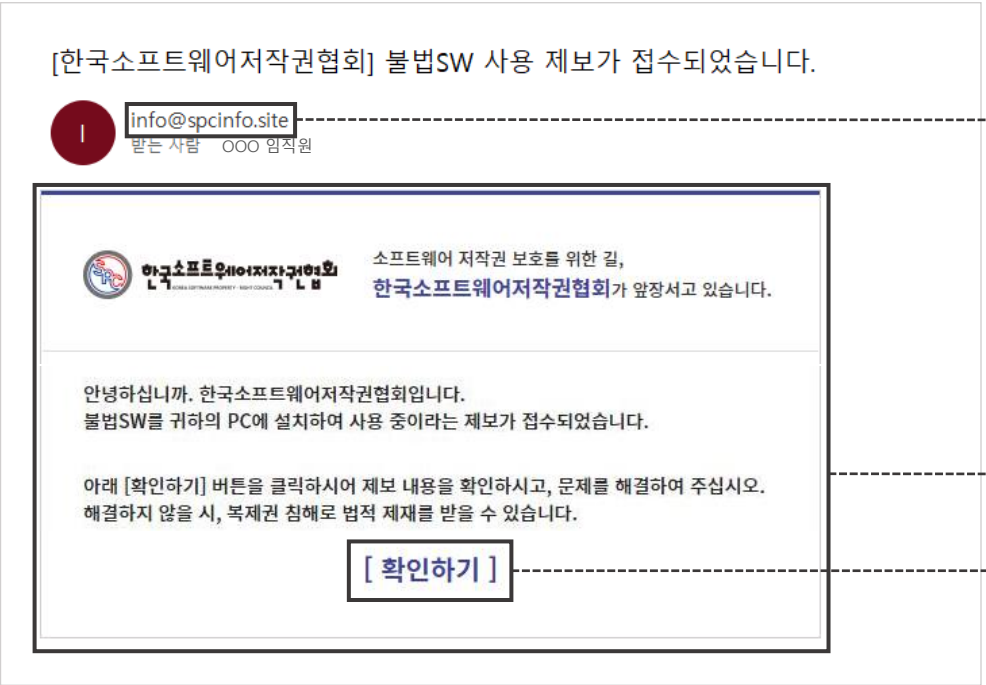
단계	위치	시나리오 내용	평가 항목
1	메일 본문	신뢰할 수 있는 단체를 사칭한 URL 버튼 포함 메일 수신	**메일 열람 여부** : 출처를 알 수 없는 메일을 열람했는지 평가 ※ 메일 열람 여부는 'URL 클릭 여부'와 동일하게 평가됩니다.
			URL 클릭 여부 : 악성 행위가 발생할 수 있는 URL을 클릭하였는지 평가
2	피싱사이트	URL 버튼과 연결되는 피싱사이트에서 개인 정보 입력	**정보 입력 여부** : 메일과 연결되는 사이트에서 민감한 정보를 요구하는 경우, 요구 정보를 입력했는지 평가
3	피싱사이트 결과 페이지	[Case 1] 정보 입력 결과 페이지와 사칭 메일에 답장 유도 [Case 2] 모의훈련 안내 페이지	**악성 메일 답장 여부** : 출처를 알 수 없는 메일(답장 받는 주소가 변경되는 변조 메일)에 답장을 했는지 평가

| 02 | 훈련 시나리오 상세

KIWONTECH

▪ 예시 : 한국소프트웨어저작권협회 사칭

단계	위치	시나리오 내용	위험 요소	예상 피해
1	메일 본문	신뢰할 수 있는 단체를 사칭한 URL 버튼 포함 메일 수신	① 사칭 단체의 실제 사용 도메인 혹은 유사한 도메인 사용 ② 사칭 단체의 디자인 양식을 이용하여 메일 제작	신뢰할 수 있는 단체를 사칭하여 공격 요소에 쉽게 피해를 입을 수 있음
			③ 메일 주소, IP 등의 정보를 수집하는 스크립트 자동 실행	악성 URL 클릭 시, 악성코드(랜섬웨어)가 자동으로 실행되어 PC 감염



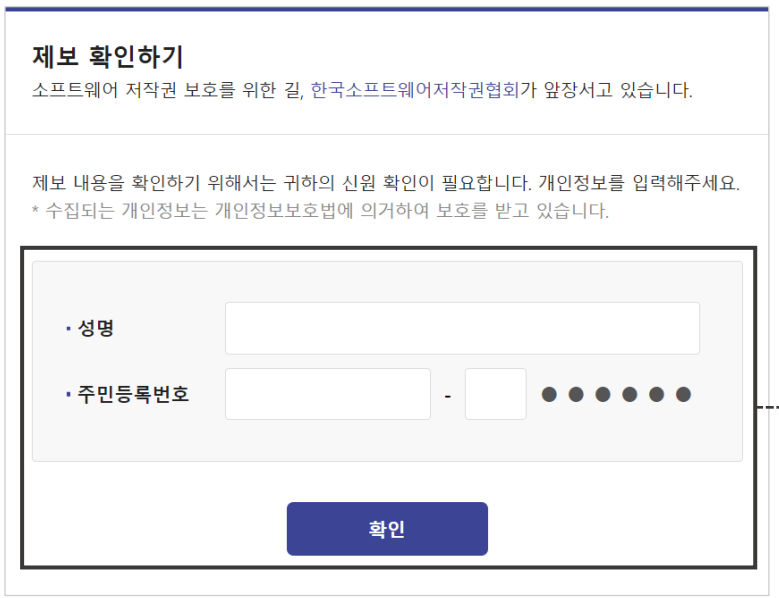
[그림] 임직원이 '받은 메일함'에서 열어본 악성메일 **(예시)**

| 02 | 훈련 시나리오 상세

KIWONTECH

▪ 예시 : 한국소프트웨어저작권협회 사칭

단계	위치	시나리오 내용	위험 요소	예상 피해
2	피싱사이트	URL 버튼과 연결되는 피싱사이트에서 개인 정보 입력	① 개인 정보 입력 유도	입력한 정보를 이용한 명의 도용, 계정 탈취, 금전적 피해 등이 발생



1 정보 입력 후, '확인' 버튼 클릭 시, 입력한 정보 수집

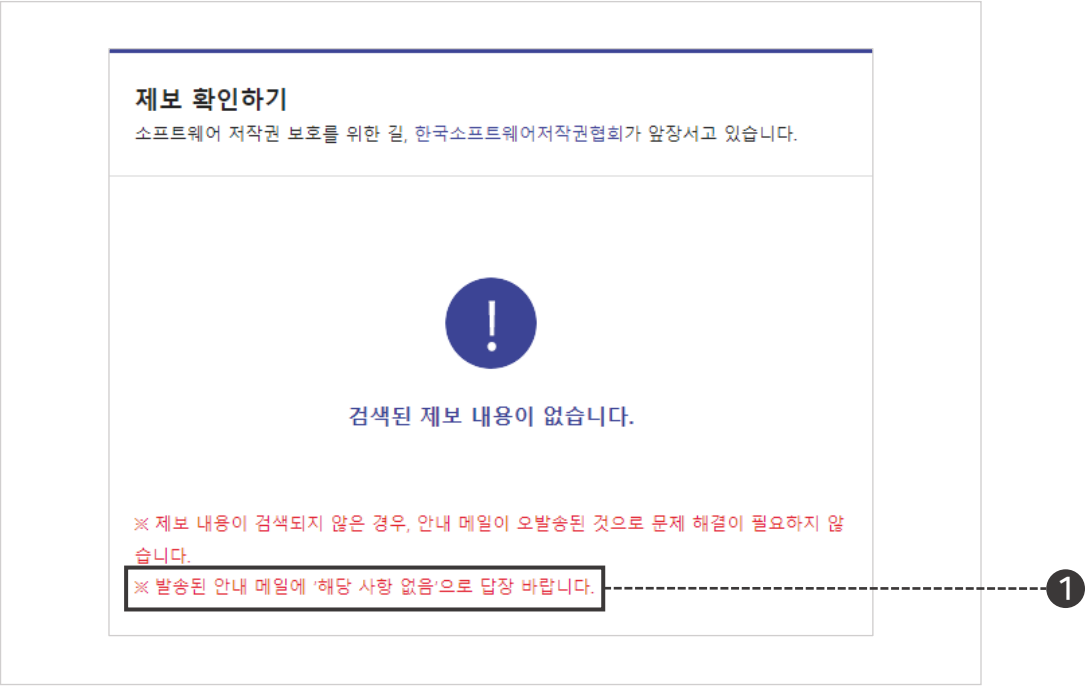
[그림] **[확인하기]** 클릭 시, 연결되는 피싱사이트

| 02 | 훈련 시나리오 상세

KIWONTECH

- 예시 : 한국소프트웨어저작권협회 사칭

단계	위치	시나리오 내용	위험 요소	예상 피해
3	피싱사이트 결과 페이지	**[Case 1] 정보 입력 결과 페이지와 사칭 메일에 답장 유도** [Case 2] 모의훈련 안내 페이지 (8p 참고)	① 답장 유도	메일에서 요구하는 정보나 파일을 첨부하여 답장 시, 기업/개인 정보 유출



[그림] **[Case 1]** 정보 입력 후, **[확인]** 클릭 시 결과 페이지

[그림] 악성메일에 답장하기 클릭 시, 메일 쓰기 화면 **(예시)**

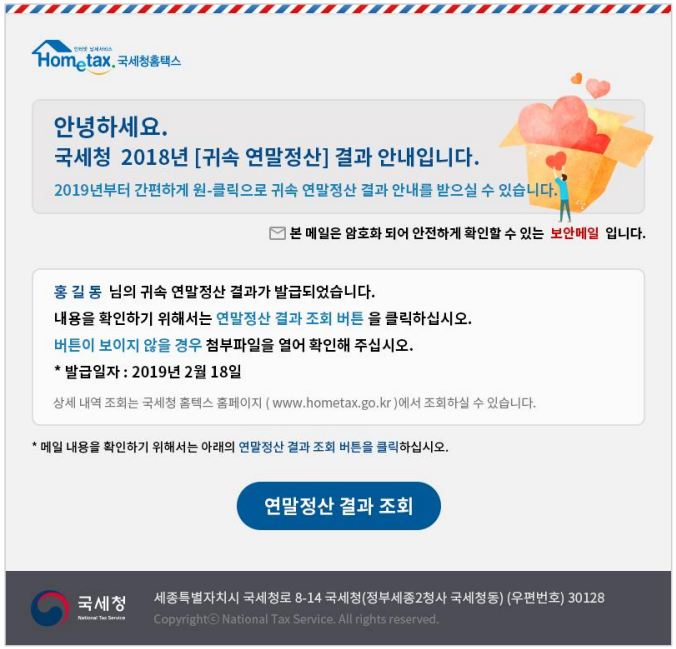
| 01 | 국가 기관 사칭 - 홈택스

KIWONTECH

- 시나리오 내용 : 연말정산 결과 조회

[1단계] 메일 본문

홈택스 사칭 및 링크 클릭 유도 메일 발송

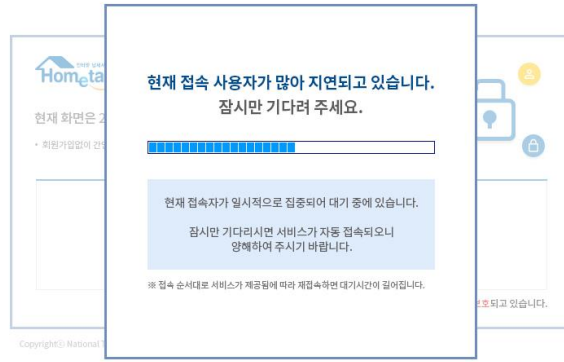


[2단계] 피싱사이트

개인정보 입력 유도 피싱사이트

[3단계] 피싱사이트 결과 페이지

접속 지연 페이지



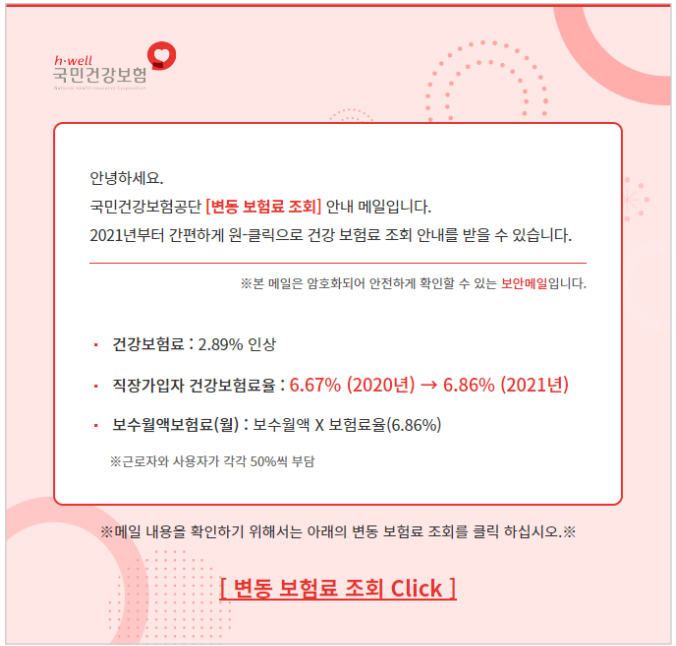
| 02 | 국가 기관 사칭 - 국민건강보험

KIWONTECH

- 시나리오 내용 : 변동 보험료 조회

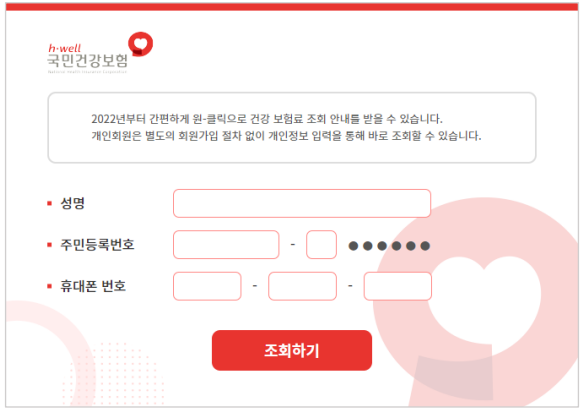
[1단계] 메일 본문

국민건강보험 사칭 및 링크 클릭 유도 메일 발송



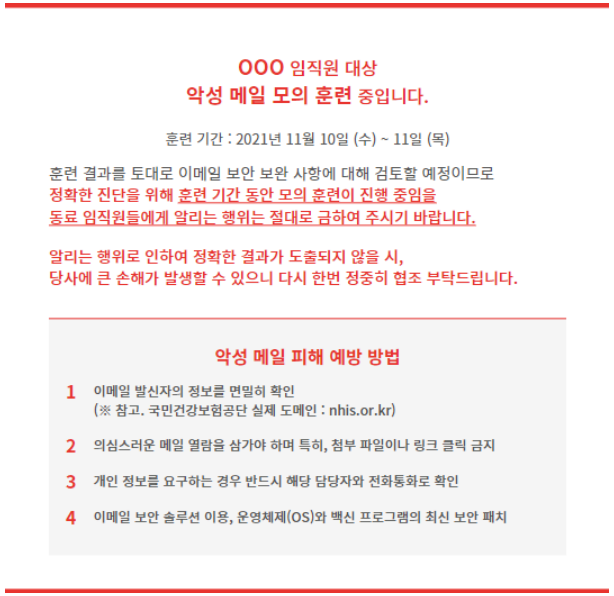
[2단계] 피싱사이트

개인정보 입력 유도 피싱사이트



[3단계] 피싱사이트 결과 페이지

모의훈련 안내 페이지



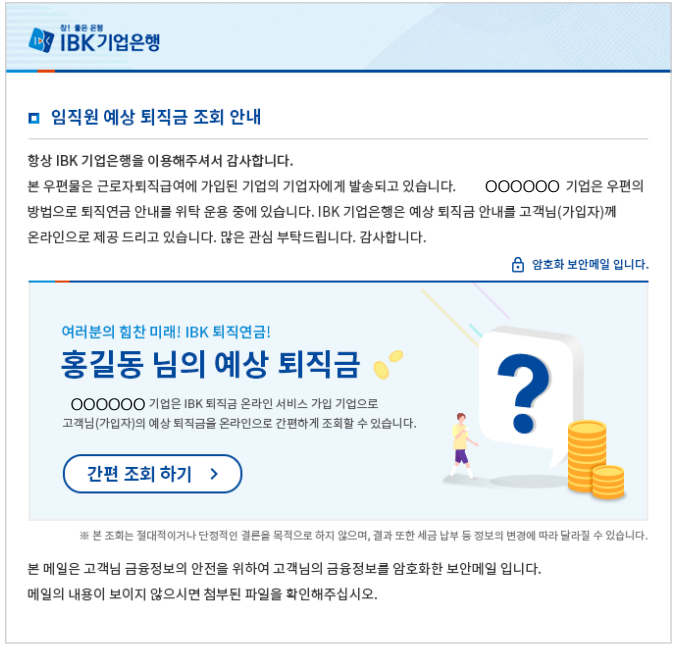
| 03 | 기업 주거래 은행 사칭

KIWONTECH

- 시나리오 내용 : 퇴직 연금 조회

[1단계] 메일 본문

기업 주거래 은행 사칭 및 링크 클릭 유도 메일 발송

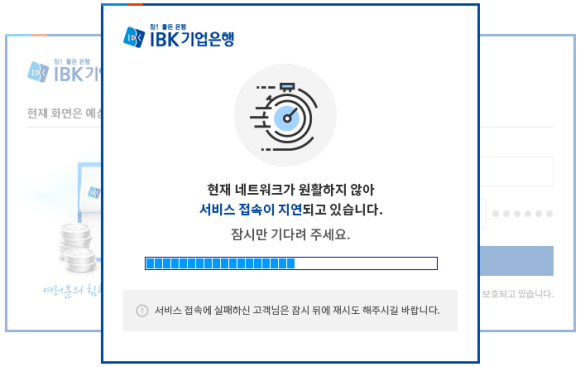


[2단계] 피싱사이트

개인정보 입력 유도 피싱사이트

[3단계] 피싱사이트 결과 페이지

접속 지연 페이지



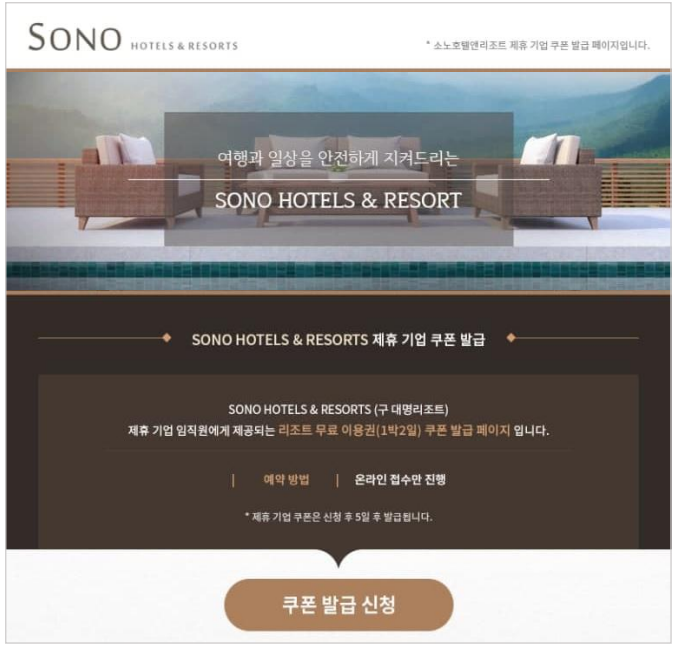
| 04 | 기업 제휴 호텔 사칭

KIWONTECH

- 시나리오 내용 : 무료 이용권 쿠폰 발급

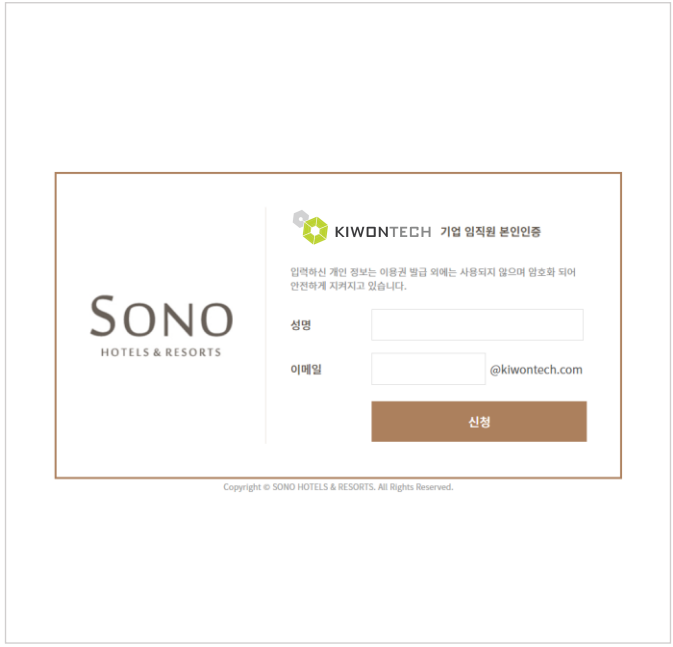
[1단계] 메일 본문

기업 제휴 호텔 사칭 및 링크 클릭 유도 메일 발송



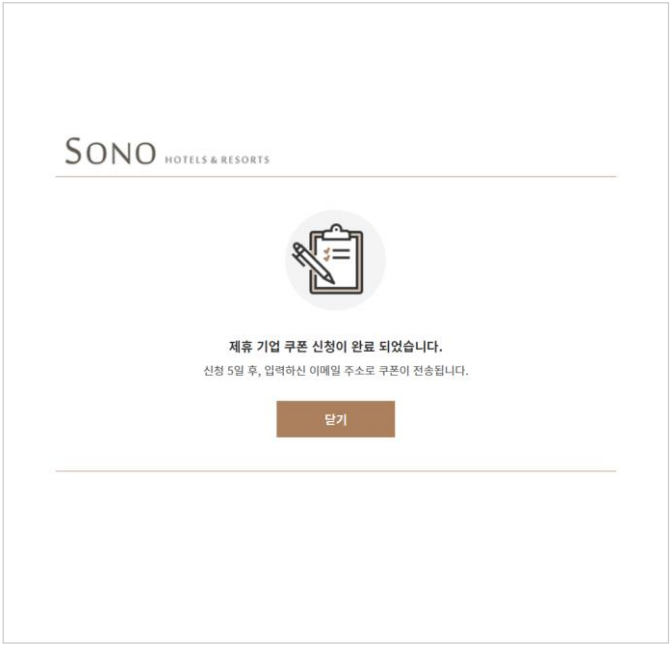
[2단계] 피싱사이트

개인정보 입력 유도 피싱사이트



[3단계] 피싱사이트 결과 페이지

정보 입력 결과 페이지



감 사 합 니 다

KIWONTECH