

# 의료기관 해킹메일 모의훈련이란?

이메일은 주요 사이버 공격(랜섬웨어, 정보탈취 등)의 핵심 공격통로로 악용되어 실제공격과 동등한 수준의 메일훈련으로 피해를 최소화하고 보안인식 제고·대응역량 강화를 위한 예방서비스

## 훈련 대상

- 의료기관 종사자 누구나
- (추천) 메일수신 업무가 많은 의료기관
- (추천) 보안인식 점검 의료기관

## 훈련 항목

- 해킹메일 열람율
- 열람된 메일내부 링크(파일) 클릭율
- 해킹메일 열람 후 신고율

## 훈련 기간

- 약 3주 소요
- 1~2주 : 대상기관별 훈련(메일발송)
- 1주 : 기관별 결과보고서 작성

사전준비

일정협의·훈련 시나리오 등

훈련 및 결과보고

훈련실시 및 결과리뷰

보안교육

(의료기관) 임직원 보안교육

정기훈련

차년도 정기훈련 실시

## 해킹메일 모의훈련 절차

### 훈련 방법

실제 발생한 해킹메일 사례와 동등한 수준의 메일발송을 통해 임직원의 해킹메일 식별·대응역량 점검  
발송된 해킹메일에 대한 열람율, 내부링크(파일) 클릭율, 열람 후 신고율 종합 측정

### 훈련 결과

의료기관은 훈련결과 보고서 수신 후 해킹메일 대응역량 파악, 이후 임직원 대상 보안교육 등 시행  
센터는 의료기관에 대한 체계적인 지원을 위해 차년도 정기훈련 계획수립

### 기타 사항

점검비용 : 의료기관 대상 무상 서비스  
관련문의 : 02-6360-6500 / [cert@hisc.or.kr](mailto:cert@hisc.or.kr)

서비스 신청하기([hisc.or.kr](http://hisc.or.kr))

