seoul energy

랜섬웨어
피해 예방 수칙

랜섬웨어(Ransomware)란?

Ransom(몸값)+ Software(소프트웨어)의 합성어

시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 한 뒤,

이를 인질삼아 금전을 요구하는 **악성 프로그램입니다.**

랜섬웨어 감염 경로

랜섬웨어가 지정한 기간 내에 금전 지불 등 요구사항을 처리하지 않으면 요구 금액이
증가할 수 있고 감염 시스템과 암호화된 데이터는 사용할 수 없거나 삭제될 수 있습니다.

1

홈페이지 방문

랜섬웨어가 유포중인 홈페이지 방문

2

이메일·SNS 유포

첨부 파일 다운로드·링크 실행시 감염

3

웜(자가전파)

컴퓨터 부팅시 자동 감염

4

타킷형(APT) 공격

서버 침투 및 악성코드 설치

www.i-se.co.kr

| 랜섬웨어 예방수칙

파일 복구가 어려운 랜섬웨어는 감염 전 예방하는 것이 중요합니다.

랜섬웨어 피해 예방 수칙

모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.

매월 세 번째 주 수요일 사이버보안진단의 날 시행시 윈도우, 응용프로그램 소프트웨어 업데이트를 반드시 수행해주세요. (내 PC지키미 100점 만들기)

- 보안 업데이트가 제공되는 최신버전의 운영체제 사용 및 매달 발표되는 보안 업데이트 적용
  ※ 윈도우즈 XP·비스타 등 보안 지원이 중단된 운영체계는 최신 버전으로 교체
- 직접적인 공격 수단인 인터넷 익스플로러가 아닌 마이크로소프트 엣지, 구글 크롬, 모질라 파이어폭스 등 다른 브라우저 사용
- 브라우저, 자바, 플래시 플레이어, 아크로뱃리더 등 사용하고 있는 소프트웨어를 항상 최신 버전으로 유지
- 그 외 응용소프트웨어에서 업데이트를 제공하는 경우 즉시 적용
- 사용하지 않는 불필요한 소프트웨어는 삭제

업데이트 하기 or 건너뛰기

Start 오전 11:59

랜섬웨어 피해 예방 수칙

백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.

매일 낮 12시 V3 백신 검사가 진행됩니다. 이상징후가 발견되면 전산정보부로 연락주세요.

- 최신 업데이트를 유지하고 실시간 감시 이용기능 활성화 등 백신 소프트웨어가 정상적으로 동작하도록 설정
- 주기적으로 PC 악성코드 검사 수행

업데이트 하기 or 건너뛰기

랜섬웨어 피해 예방 수칙

출처가 불분명한 이메일과 URL 링크는 실행하지 않습니다.

업무와 관련되지 않거나, 알 수 없는 사람이 보낸 이메일과 URL 링크는 실행하지 않습니다.

- 수상한 이메일 열람과 첨부파일 실행, URL 클릭을 자제
- 이메일에 첨부되어 있는 MS오피스(DOC, XLS 등) 파일의 매크로 기능 허용하지 않음
- 이메일에 첨부되어 있는 스크립트(JS, JAVA 등)나 실행파일(EXE, SCR, VBS 등)은 실행하지 않음

연결하기 or 건너뛰기

Chrome

Start

오후 12:00

랜섬웨어 피해 예방 수칙

파일 공유 사이트 등에서 파일 다운로드 및 시행에 주의합니다.

외부에서 파일을 다운로드하여 시행할 경우 악성코드일 수 있으니 신뢰할 수 있는 사이트에서 업무에 필요한 파일만 다운로드 및 실행해야 합니다.

- 공짜 사이트는 악성코드의 온상임을 기억

연결하기 or 건너뛰기

파일 2

서에 다

파일 3

Chrome

랜섬웨어 피해 예방 수칙

중요 자료는 정기적으로 백업합니다.

중요한 일부 자료는 암호화하여 별도 저장매체로 백업하는 것이 안전합니다.

- 업무 및 기밀문서, 각종 이미지 등 중요 파일은 주기적으로 백업
- 중요 파일은 PC 외에 일부 저장장치 등을 이용한 2차 백업을 하거나 보안백업 SW 등을 통해 쉽게 접근하기 어렵도록 설정

확인 or 취소

Start

오후 12:01

ESC F11 F12

《 랜섬웨어 감염 시 피해 최소화를 위한 긴급조치 》

ONE STEP 외부 연결장치 연결 해제

>>> 랜섬웨어는 공유폴더, PC에 연결되어 있는 이동식 저장장치(USB)나 외장하드 등에 저장되어 있는 파일에도 접근해서 암호화할 수 있기 때문에 기존에 백업해둔 파일까지 암호화 될 수 있음

TWO STEP PC 전원 유지

>>> PC가 종료된 경우 부팅까지 불가능하게 되는 경우도 있으므로 PC의 전원은 끄지 말 것

THREE STEP 네트워크 차단

>>> 네트워크를 통해 랜섬웨어가 확산 될 가능성이 있으므로, 감염 사실 확인 즉시 네트워크 차단

FOUR STEP 복구 방법 확인

>>> 랜섬웨어의 유형 파악(감염 알림 창, 암호화된 파일 등)후, 백신소프트웨어 제조사 홈페이지 등을 통해 제공하는 복구 툴이 있는지 확인

Start 오후 12:02

나의 소중한 정보 보호를 위한 랜섬웨어 피해 예방 수칙을 꼭! 지켜주세요.

랜섬웨어 신고 방법

- 홈페이지 신고 : KISA 인터넷보호나라 & KrCERT
  (https://www.boho.or.kr)
- 전화 신고 : 118

출처: KISA인터넷보호나라 & KrCERT '랜섬웨어 대응 가이드라인'