

2023-1

2023년 상반기

사이버 보안 소식

경기교육사이버안전센터(GECSC)



경기도교육정보기록원

▪ INDEX

1

해킹메일 사고 사례 / 예방 방법

2

랜섬웨어 감염 경로/증상 및 예방/대응

3

샤오치잉 관련 침해사고와 대응 방안

4

P2P!! 사용 금지 해야된다!

5

2023년 상반기 보안 이슈 동향

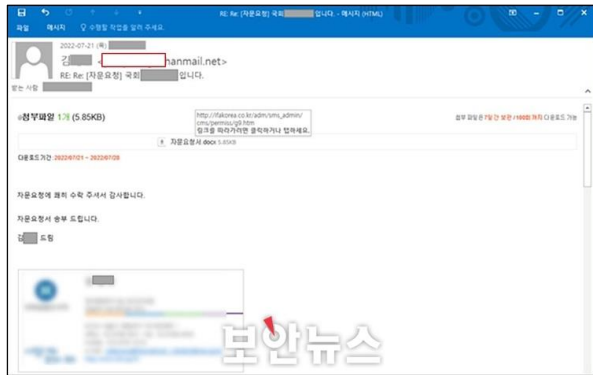
별첨1) 경기교육사이버안전센터(GECSC) 사이버침해사고 대응

별첨2) 개인정보 유출사고 위험진단 / 최고의 개인정보취급자



해킹메일 사고 사례

□ “자문요청서” 파일첨부형 해킹메일 및 피해 사례

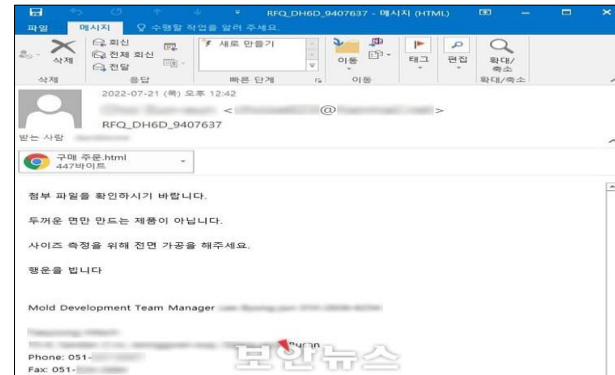


“자문요청서” 등 업무와 관련이 높은 문서 파일을 첨부하는 방식의 해킹메일을 발송

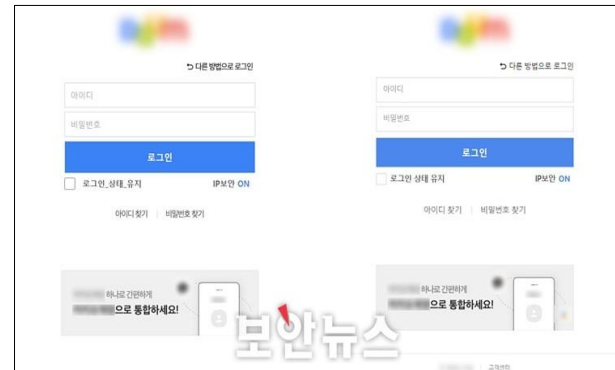


첨부된 문서 파일 실행 시 “콘텐츠 사용 알람” 발생, 해당 알람을 실행 하면 악성코드가 다운로드됨 (랜섬웨어, 가상화폐채굴 등)

□ “구매주문”으로 위장한 해킹메일 및 피해 사례



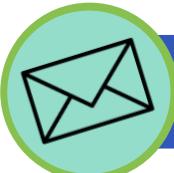
“구매주문 수정” 등 업체 직원을 사칭하는 방식의 첨부 파일 삽입형 해킹메일을 발송



첨부된 파일 실행 시 미리 만들어진 위장페이지(피싱사이트)로 연결되어 포털 및 SNS 계정 정보 등 탈취 유도

- 출처: 과학기술정보통신부, 법무처 사이버보안 사고사례 홍보

<https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&searchWrd=%EB%B2%94%EB%B6%80%EC%B2%98&menuNo=205021&pageIndex=1&categoryCode=&nttd=67085>



해킹메일 예방 방법



해킹메일이란?

Q. 해킹(피싱) 메일이란 무엇인가요? (#해킹메일, #피싱메일)

- ✓ 개인정보(Pprivate data)와 낚시(Fishing)의 합성어로
- ✓ 메일을 통해 이용자의 PC를 악성코드로 감염시키거나 임의의 URL로 접속을 유도하여 주요 정보를 탈취하는 해킹 기법입니다.

Q. 어떻게 악성코드 감염 등 피해가 발생하게 되나요? (#감염경로)

- ✓ 메일의 본문에 포함된 신뢰할 수 없는 URL 링크를 클릭하거나 악성행위가 포함된 첨부파일을 실행할 경우 감염되게 됩니다.

Q. 해킹메일을 통해 어떠한 피해가 발생하게 되나요? (#해킹메일 피해)

- ✓ URL 링크 또는 첨부된 파일을 통해 악성코드에 감염되거나 웹페이지로 정보 입력을 통해 정보가 외부로 유출되게 됩니다.

Q. 해킹 메일이 주로 사용되는 내용, 유형이 있나요? (#해킹메일 유형)

- ✓ 개인의 경우 쇼핑·택배안내·연말연시 행사·이벤트 등 일상생활과 밀접한 정보로 위장하여 발송되고 있습니다.
- ✓ 기업의 경우 사업제안서·견적서 등 업무와 관련되거나, 협력업체 직원 등을 사칭하여 발송되고 있습니다.

- 출처: 과학기술정보통신부, 법무처 사이버보안 사고사례 홍보

<https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&searchWrd=%EB%B2%94%EB%B6%80%EC%B2%98&menuNo=205021&pageIndex=1&categoryCode=&ntId=67085>



해킹메일 수신 시 유의 사항

:: 이메일 수신 시 유의사항 ::



- 출처: KISA 인터넷보호나라&Krcert > 사이버위협 > 자세히 알아보기

<https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000030&ntId=70087&menuNo=205027>



사이버침해사고신고 : 경기교육사이버안전센터(GECSC) 031-240-6599

E-mail : goeboan@korea.kr



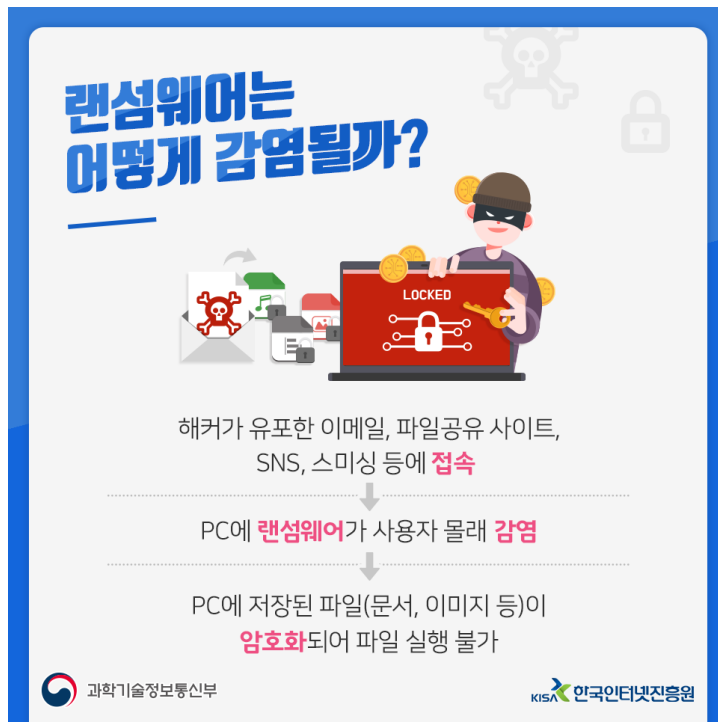
경기도교육정보기록원
Gyeonggi-do Education Information Archive



랜섬웨어 감염 경로 및 증상



랜섬웨어 감염 경로



- ▶ 이메일, 파일 공유 사이트, SNS 등에 접속
- ▶ 악성코드 감염 이후 랜섬웨어 추가 감염
- ▶ PC내 저장된 파일이 암호화됨(문서, 이미지등)



랜섬웨어 감염 증상



- ▶ 감염 파일 실행 불가 (파일 암호화)
- ▶ 화면 잠금, 키보드/마우스 동작 불가
- ▶ 시스템파일 손상, PC 재부팅 불가

- 출처: 한국인터넷진흥원 블로그 <https://blog.naver.com/kisa118/221218861926>





랜섬웨어 피해 예방 및 대응 절차



랜섬웨어 피해 예방 수칙

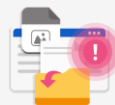
피해를 예방하기 위한 수칙①



모든 소프트웨어와 백신은
최신 버전으로 업데이트하여 사용

※ 업데이트 방법은 「보호나라(www.boho.or.kr)」에서 확인 가능

피해를 예방하기 위한 수칙②



출처가 불명확한
이메일과 파일 공유 사이트 등에서
파일 **다운로드** 및 **실행**에 주의

피해를 예방하기 위한 수칙③



PC에 저장된 **중요 자료**는
정기적으로 **백업**

※ 백업 방법은 「보호나라(www.boho.or.kr)」에서 확인 가능

- ▶ 최신 버전 업데이트
- ▶ 출처가 불명확한 파일 다운로드 및 실행 주의
- ▶ 중요자료 정기적 백업



랜섬웨어 감염시 대응 절차

랜섬웨어 감염시 대응절차!

01 증상 확인하기

- 파일 열람 불가, 화면 잠금, 금전요구 문구 등이 출력되는지 확인

02 신고하기 [관련기관 신고]

※ 경기도교육정보기록원 사이버안전센터

전화. 031) 240-6599

이메일. goeboan@korea.kr



랜섬웨어 감염시 대응절차!

03 데이터 복구

• 백업된 파일이 있는 경우

1. PC 포맷 및 운영체제 재설치
2. 기존 백업매체 연결 및 데이터 복구

• 백업된 파일이 없는 경우

공개용 랜섬웨어 복구 도구 활용

※ NAR(www.nomoreransom.org), 국내 백신사 등에서 제공하는 복구 프로그램

- ▶ 증상 확인
- ▶ 관련기관 신고
- ▶ 데이터 복구



- 출처: 한국인터넷진흥원 블로그 <https://blog.naver.com/kisa118/221218861926>



사이버침해사고신고 : 경기교육사이버안전센터(GECSC) 031-240-6599

E-mail : goeboan@korea.kr



경기교육정보기록원
Gyeonggi-Do Education Information Archive

사오치잉 관련 침해사고와 대응 방안

해커 해커그룹
**사오치잉(晓骑营) 관련
침해사고와 대응 방안**

PHISHING ALERT

1

해커조직 사오치잉은 2023년 1월부터 2월말까지
국내 웹사이트를 공격하고 정보 유출, 웹페이지 변조 등의
피해 상황을 공개했습니다.

한국인터넷침해를 선포합니다.

2

사오치잉 침해사고 타임라인
2023년

- 1.7 A기업 내부자료 유출 주장 1차
- 1.20-21 B기업 해킹사실 공개
C기업 해킹사실 공개 1차
- 1.22 KISA 보호나라 공지
- 1.24-26 다음 목표로 KISA 예고
C기업 해킹사실 공개 2차
- 2.14 D, E, F기업 웹페이지 변조
- 2.18 A기업 내부자료 유출 주장 2차

3

사오치잉 공격기법

보안이 취약한 웹 서비스*를 통해 내부 침투

*SQL Injection, 외부에 노출된 계정정보, 오래된 버전의 WAS(Web Application Server) WebLogic 등

4

사오치잉 침해사고 사례

- 1. 내부 정보 탈취**
서버 내부 자료에 직접 접근하거나
웹셀, 백도어 등을 업로드해 정보 탈취
- 2. 웹사이트 변조 및 무단생성**
해킹 사실을 과시하거나 새로운 멤버를 모집하는
웹페이지를 메인 페이지와 교체 또는 추가로 업로드
- 3. 자료 삭제**
데이터베이스 탈취 후 삭제

5

**사오치잉 침해사고?
대응할 수 있어요!**

- ✓ SQL Injection 공격 예방
- ✓ 계정정보 관리
- ✓ 운영체제 및 소프트웨어 버전 업그레이드
- ✓ 중요 자료 백업
- ✓ 로그 설정
- ✓ 한국인터넷진흥원 정보보호 서비스 활용

6

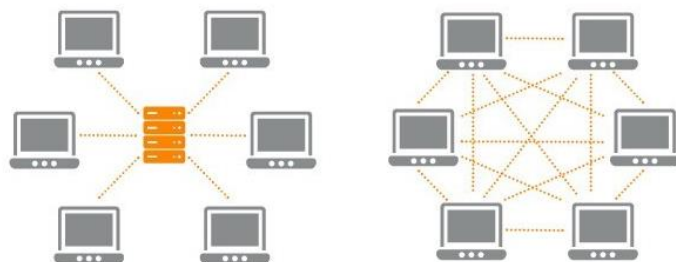
- 출처: 한국인터넷진흥원 블로그 <https://blog.naver.com/kisa118/223085396557>



P2P!! 사용 금지 해야된다!



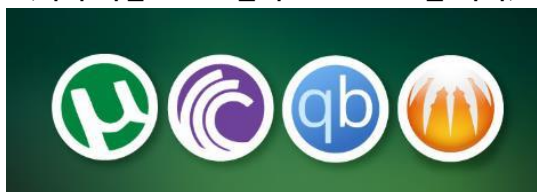
P2P(Peer To Peer)에 대한 이해



Server-Based

P2P

(서버 기반 프로토콜과 P2P프로토콜 차이)



(다양한 종류의 토렌트 프로그램)

▲ 출처: <https://focuskr.tistory.com/426>

▶ P2P(Peer To Peer)는 ?

- 사용자 연결 구조로 서로 간 데이터 공유
- 기존 서버 환경 구조보다 빠른 데이터 전송
- 서로 간 데이터 공유 전달로 인한 연결 유지성 탁월
- 공유 파일의 조각 별 다운로드로 매우 빠른 다운로드 속도

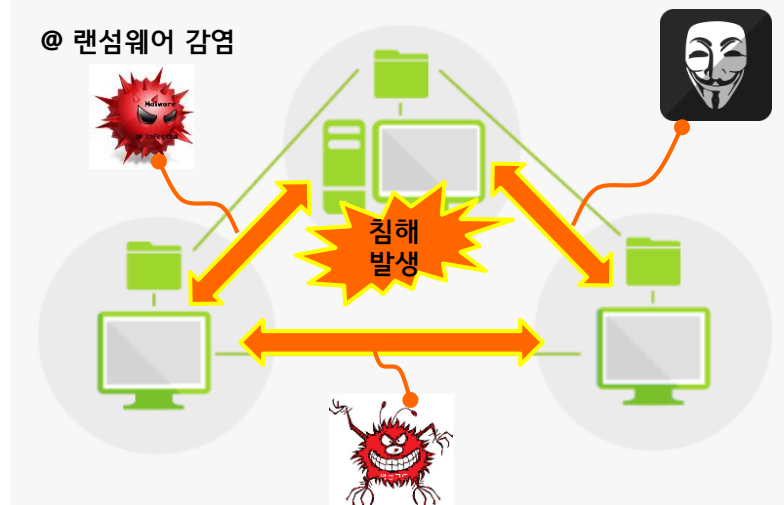


사용 시 발생하는 문제점

- 서로 간 연결구조로 인한 **악성코드 감염 증가**
- 불완전한 파일 다운로드 시 **랜섬웨어 / 해킹 위협에 노출**
- **불법** 파일 다운로드로 인한 **저작권 침해**
- 지속적인 연결 유지로 인한 내부 **네트워크 부하 발생**

@ 해킹, 정보유출

@ 랜섬웨어 감염



@ 악성코드 감염

? 2023년 상반기 보안 이슈 동향



2023년 1월 보안 이슈

- [보안뉴스] [넷서포트 RAT 악성코드, 포켓몬 게임으로 위장](#)
- [보안뉴스] [구글 홈 스마트스피커, 도청 가능 취약점 발견](#)
- [보안뉴스] [중국의 해킹 단체, 동아시아 단체들 공격](#)
- [보안뉴스] [중국발 해킹 '디페이스 공격', 홈페이지가 바뀜](#)



2023년 2월 보안 이슈

- [보안뉴스] [수강신청 페이지 해킹 시도, 컴퓨터공학과 학생들](#)
- [보안뉴스] [중해커조직 추가공격예고 "다음 달 28일부터 韓공격"](#)
- [보안뉴스] [URL 단축 서비스인 지오링크를 피싱에 악용](#)
- [보안뉴스] [작년 전국학력평가 응시생 성적 유출, 해킹 여부 수사](#)



2023년 3월 보안 이슈

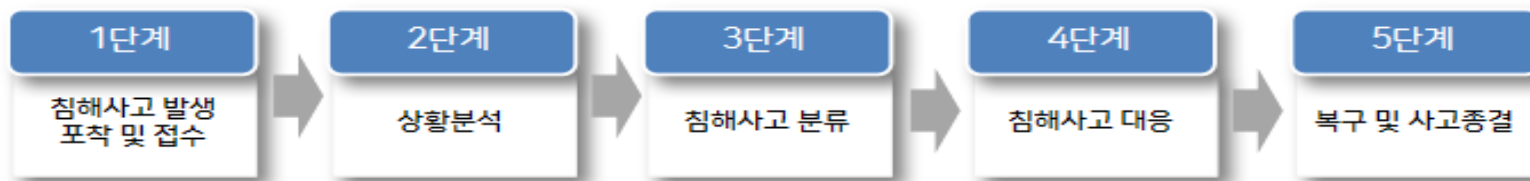
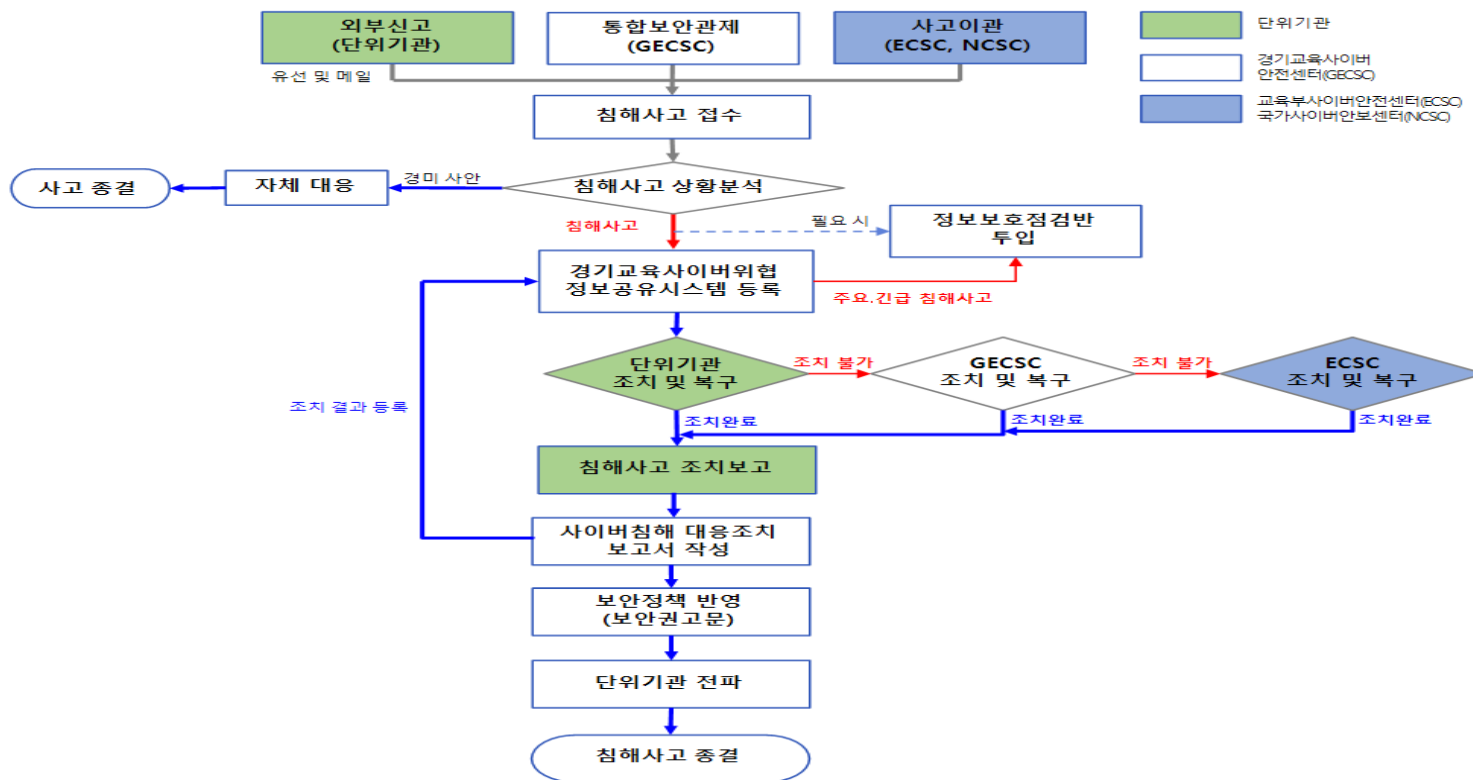
- [보안뉴스] [미국 연방보안청, 랜섬웨어 공격에 당해](#)
- [보안뉴스] [금융정보 탈취 악성코드 이모택, 이메일로 유포](#)
- [보안뉴스] [MS 스마트스크린 기능, 제로데이 통해 랜섬웨어 퍼져](#)
- [보안뉴스] [김수키 해킹그룹, 사례비 지급 위장한 악성코드 퍼뜨려](#)



2023년 4월 보안 이슈

- [보안뉴스] [트리고나 랜섬웨어, 관리 미흡 MS-SQL서버 통해 유포](#)
- [보안뉴스] [보안인증프로그램 취약점 악용 해킹사건, 북한 소행](#)
- [보안뉴스] [미국 CISA, 크롬과 맥OS서 발견된 취약점을 KEV에 추가](#)
- [보안뉴스] [레드아이즈 공격그룹, 록랫 악성코드 링크 파일 통해 유포](#)

[별첨1] 경기교육사이버안전센터(GECSC) 사이버침해사고 대응



◆ 출처: 경기도교육청 정보보호 업무 추진 계획 및 사이버분야 위기대응 실무 매뉴얼

[별첨2] 개인정보 유출사고 위험진단 / 최고의 개인정보취급자

개인정보 유출사고 위험진단

당신은 **안전** 유형? **위험** 유형?

☒ 권한은 많이 주고 계정은 공유하고 비밀번호는 간단하게 사용하시나요?

위험 유형입니다! 접근권한 관리가 필요합니다

- 권한은 '최소'로, '차등' 부여
- 회직 등 인사정보 변경 시 '지체 없이(5일 이내) 반영'
- '계정 공유'는 곧 '개인정보 유출'이라는 인식 가지기
- 비밀번호 작성규칙 적용과 입력횟수 제한은 필수

☒ "개인정보처리시스템"을 "개인정보 공유 서비스"로 방치하고 계신가요?

위험 유형입니다! 엄격한 접근통제가 필요합니다

- 비인가자는 IP, MAC으로 제한
- 외부접속은 '안전한 접속수단(가상사설망, VPN)' 또는 '인증수단(2-factor)' 적용
- 업무용PC 보안은 '유해사이트, P2P, 공유설정, 공개된 무선망 사용 제한'부터 시작
- 최대접속시간 제한(idle timeout) 설정은 기본!

☒ 아직까지 MD5로 비밀번호를 암호화 하시나요?

위험 유형입니다! 개인정보는 안전하게 암호화해야 합니다

- 고유식별정보*, 생체인식정보*, 비밀번호는 암호화 필수
- 고유식별정보 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호
- 생체인식정보 특정 개인을 인증·식별할 목적으로 사용되는 정보(지문, 얼굴, 홍채 등)
- 안전한 암호 알고리즘 사용 (MD5, SHA-3)
- ※ 권고 암호 알고리즘은 개인정보의 암호화 조치 안내서(교육부 개인정보보호 포털-(자료실) 참고
- 암호 KEY는 철저한 계획 수립을 통해 생성부터 파괴까지 안전하게 관리

☒ 접근권한 ☒ 접근통제 ☒ 암호화

3가지 모두 잘 지키고 계신다면 당신은 "안전 유형"입니다 😊

교육부 KERIS 한국교육학술정보원

개인정보취급자 편

교육부 KERIS 한국교육학술정보원

최고의 개인정보취급자가 되는 비법이 궁금해?



(따라만 하면 되는) 지금부터 나도

- 최** 소한의 개인정보만을 수집하고
- 고** 유식별정보 등의 개인정보는 철저히 암호화하며
- 의** 무(안전조치)는 반드시 지키는

"개인정보취급자,,

최고의 개인정보취급자가 실천하는 업무습관

01 PC 부팅 시 CMOS 및 Windows 비밀번호는 필수로 설정해요



02 5분 이상 자리를 비울 때는 잠금화면 설정 [Window] + [L] 또는 시스템 종료를 꼭꼭 하고 가요



03 운영체제와 SW (백신, 한컴오피스 등)는 항상 최신 버전을 유지해요



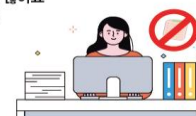
04 엑셀파일에서 작업할 땐 숨기기 처리된 행·열이 있는지 항상 확인하고 게시할 땐 PDF로 변환해요!



05 개인정보가 담긴 문서는 업무처리 후 바로바로 파쇄해요



06 비밀번호나 중요한 개인정보는 메모하여 붙여놓지 않아요 (클린데스크 실천!)



07 인쇄 또는 복사 후 프린터에 출력물을 방치하지 않아요



이것만 실천하면 나도 최고의 개인정보취급자

◆ 출처: 교육부 개인정보보호 홍보용 자료

https://privacy.moe.go.kr/cop/pds/selectEduDataList.do?bbsId=BBSMSTR_000000000005