철통보안 프로젝트_정보보안교육

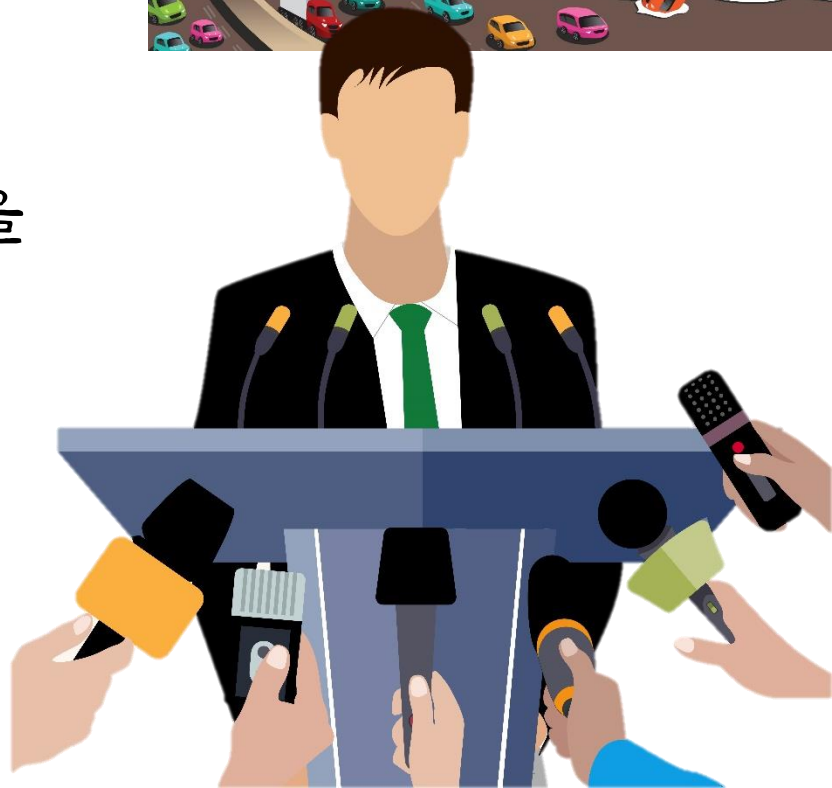
정보보안 교육 자료

1. 물리적 보안 시스템 확보의 중요성

▌물리적 보안 위반 사례

대규모 산업단지에 태풍과 폭우 피해가 발생했습니다.
수많은 회사들이 누전, 침수 등으로 인해 주요 시스템들이 먹통이 되었고,
수많은 정보가 날아가는 사건이 발생했는데요.

전혀 피해를 입지 않은 회사가 딱 1군데 있었다고 합니다.
많은 기업 대표들이 그 회사에 찾아가 정보 피해를 입지 않은 비결을
물었다고 하는데요.
비결은 바로, 정보보안의 기본수칙을 준수했다는 겁니다.



1. 물리적 보안 시스템 확보의 중요성

▌물리적 보안 위반 사례

물리적 보안이란?

회사의 자원, 데이터 장치, 시스템, 시설 자체의 위약점과 이를 이용한 내/외부의 공격으로부터 보호하여 안전한 상태를 유지하는 활동

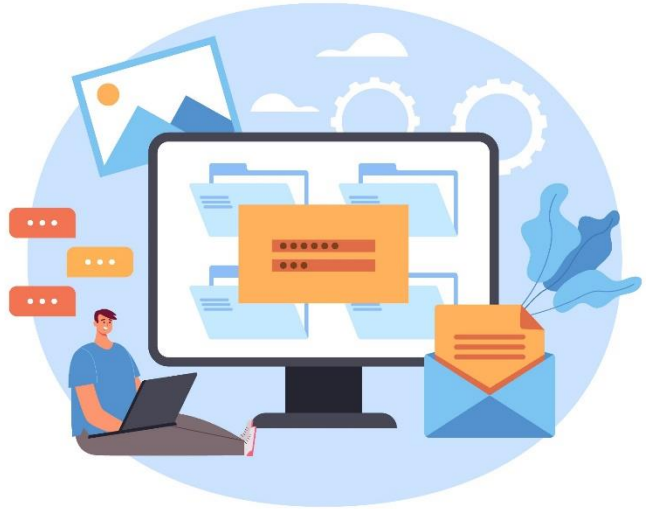
물리적 보안을 위협하는 상황

1	**자연 환경적 위협**	홍수나 지진, 폭풍, 화재와 같은 자연재해(누수, 습도, 먼지 등 포함)
2	**악의적 위협**	물리적 공격, 도난, 절취, 파괴, 테러 등
3	**사고적 위협**	승인 받지 않은 접근, 직원의 실수, 단순 사고, 보안 의무사항의 간과 등

2. 개인 업무 좌석의 물리적 보안조치

▌개인좌석 정보보안 조치

- 업무용 PC의 부팅 시 부팅암호 및 윈도우 암호 설정
- 사용 시 파일암호 설정
- 공석 시 화면보호기 암호 설정



- 중요한 문서 캐비닛 등에 보관
- 복사기, 프린터기, 팩스기, 복합기 등 사무실 안쪽에 배치

2. 개인 업무 좌석의 물리적 보안조치

▌개인좌석 정보보안 조치

Q. 회사 PC에 ID/패스워드가 적혀 있어서 접속했을 뿐인데, 잘못된 건가요?

정답은 O 입니다.
네 당연히 잘못된 일입니다. 우연히 알게 된 타인의 ID/패스워드로 승낙 없이 접속하는 행위는 권한 없는 접근에 해당하며 개인정보 안전성 확보조치기준 위반 사례입니다. 또한 과거 직무상 알게 된 패스워드로 퇴직 후에 접속하거나, 동료직원의 패스워드를 이용하여 접속하는 것도 위반 사례입니다.

2. 개인 업무 좌석의 물리적 보안조치

▌업무용 컴퓨터 및 시스템 비밀번호 작성 – 안전한 비밀번호 작성을 위한 규칙

1. 시스템별, 사이트별, 계정별 **동일 비밀번호 사용 제한**
2. **예측이 어려운 비밀번호**로 설정(아이디와 동일한 번호 또는 연속된 숫자 제한)
3. 문자와 숫자, 한글과 영문, 대문자와 소문자 등 **두 가지 이상의 규칙 적용**
4. 비밀번호가 **노출 시 비밀번호를 변경**해야 하며, **주기적으로 새로운 비밀번호**로 변경

2. 개인 업무 좌석의 물리적 보안조치

▌인사 변경 시의 보안 조치

정보 취급 인력, 관련부서 자산 반납

계정 회수 및 접근권한 조정

정보보호 및 비밀유지 서약서 징구

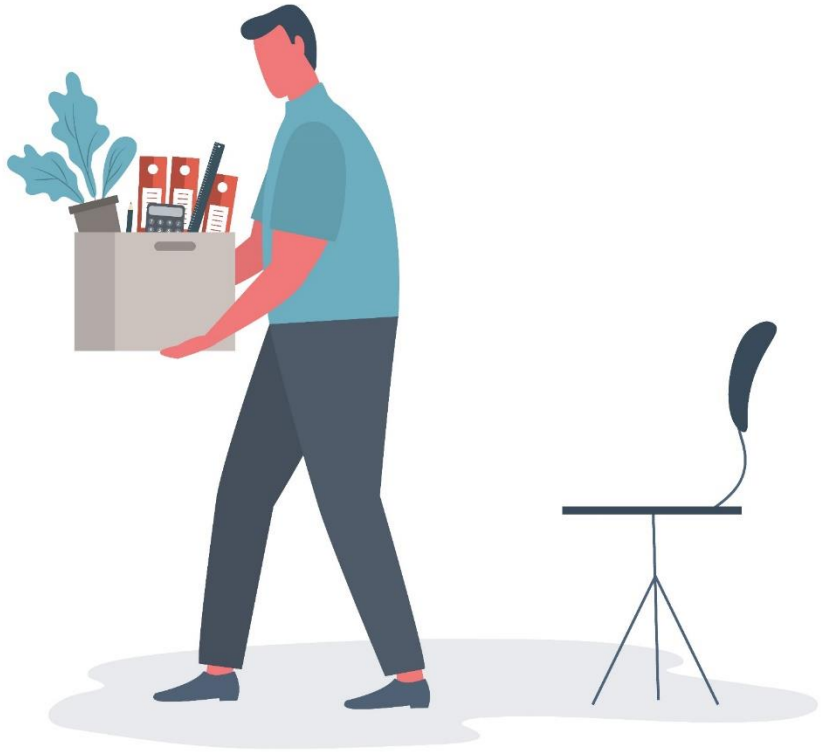
2. 개인 업무 좌석의 물리적 보안조치

▌인사 변경 시의 보안 조치

사내 정보처리 시스템과 인사 시스템 연동
계정 정보 동기화

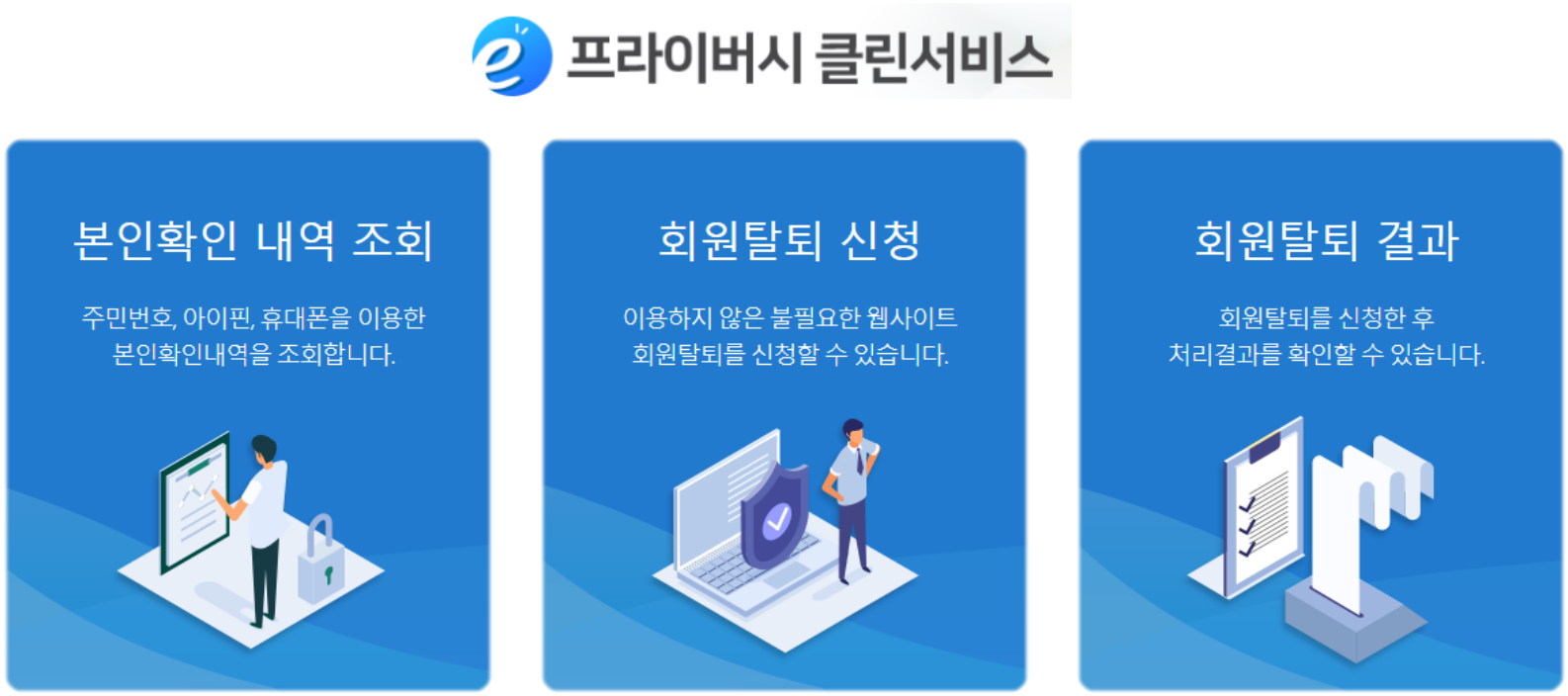
협력사 인원에 대한 통합 계정
시스템 구축 및 계정 동기화

퇴직 프로세스 내
퇴직자 정보 공유



2. 개인 업무 잔석의 물리적 보안조치

▌e 프라이버시 클린 서비스



- 인터넷에서 회원가입, 연령확인(성인인증), 실명인증 등을 위해 실시된 주민번호 및 아이핀, 휴대폰, 신용카드 등의 주민번호 대체수단을 통한 본인확인 내역을 통합적으로 조회 및 제공함
- 명의도용이 의심되거나 아이디 및 비밀번호 등을 알지 못해 회원탈퇴에 어려움이 있는 경우, 더 이상 이용을 원하지 않는 불필요한 웹사이트에 대한 회원탈퇴 처리를 대행함

3. 물리적 보관장소 관리

▌전산실과 자료보관실 보안설정

물리적 장소의 출입통제

- 별도의 물리적 보관 장소 통제구역 지정
- 잠금장치 등으로 출입통제 절차 수립
- 비인가된 외부인의 출입 제한 RFID 태그
- 인터록킹 포탈도어 기업 내부의 진입 구분
- 외부인 방문 시 신원 확인 및 임시 출입증 발급
- 직무와 직급에 따라 통제구역에 들어갈 수 있는 지정 및 인가된 인원을 지정하여 출입 허용
- 통제구역 출입 시 카메라나 스마트폰 반입 금지

출입자 로그 기록

- 사원증과 같은 아이디 카드를 이용하거나 지문 · 홍채와 같은 생체정보인식시스템 또는 CCTV나 출입대장 관리 등을 통해 이용 기록 관리
- 전산실 및 자료보관실은 기업에서 가장 중요한 정보가 모여 있는 곳이니 만큼 최상위의 보안대책이 마련되어 있어야 함

3. 물리적 보관장소 관리

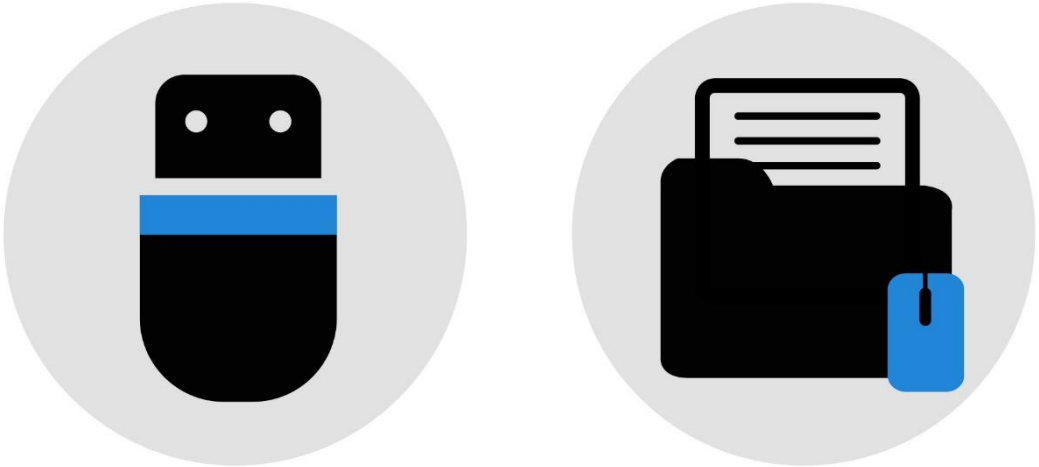
▌전산실과 자료보관실 보안설정

Q. 정보보안 규정에 따라 방문차량과 인원을 감시카메라로 확인하고 차량 번호판을 인식하는 시스템을 마련해야 한다고 하는데, 저희 회사는 중소기업이라 이런 시스템 설치가 어렵습니다. 어떻게 하는 게 좋을까요?

방문하는 모든 차량과 인원을 감시해 혹시 모를 사고를 미연에 방지해야 하는데요. 기업의 재정능력에 따라 구축이 곤란한 경우가 발생할 수 있습니다. 이럴 경우에는 보안 요원을 두어 관리하는 것을 대안으로 삼을 수 있습니다.

3. 물리적 보관장소 관리

▌보조저장매체 잠금장치



USB나 외장하드, CD 등의 보조 저장매체
정보 유출 가능성이 높아짐

반드시 안전장치 사용

- 비밀번호 설정 가능한 외장하드 등 사용
- 관리자 외 열람 금지

3. 물리적 보관장소 관리

▌서류 및 저장매체 반출입

외부 보조저장매체 통제절차 수립

내부 보조저장매체 보관절차 이행

사내 컴퓨터에는 외부 USB 등 사용 불가

주요 정보 서류 등 물리적 보관시설 이용

서류와 보조 저장매체는 잠금장치가 있는 캐비닛 등에 보관

4. 검색엔진 위험 및 삭제 방법

▌검색엔진의 위험

인터넷 정보 수집

데이터베이스에 저장

검색 시 좋은 결과 제공

4. 검색엔진 위험 및 삭제 방법

▌검색엔진의 위험

정보를 어떻게 수집하고 저장할까?

웹 크롤러 웹 페이지를 돌아다니며 정보를 수집

'저장된 페이지'의 위험

중요한 정보라면 웹 크롤러의 접근을 사전 차단 또는 주기적 삭제 필요

검색엔진에 노출 정보 URL이나 노출된 값을 입력하여 검색결과 값 확인,
검색결과 캐시페이지에서 개인정보 존재 시 해당 페이지 삭제 요청

4. 검색엔진 위험 및 삭제 방법

▌검색엔진의 위험

네이버 웹마스터 도구

- 네이버의 경우는 웹마스터 도구라는 메뉴를 통해 요청 가능
- https://help.naver.com/support/home.nhn
- 네이버 고객센터에 방문하여 신고센터 메뉴 내 유해게시물 신고 버튼 클릭
- 네이버 게시물 신고접수에서 신고 사유로 “개인정보 노출” 선택
- 개인정보 노출이 발생한 게시물이 어디에서 노출되고 있는지 선택하여 검색엔진에서 노출되는 게시물을 검색 제외하기 위해 '검색 제외 요청하기‘ 메뉴 선택
- 게시물 작성자를 선택한 뒤 게시물의 상태를 선택하여, 마지막으로 신청자 정보를 입력 후 신청 완료

4. 검색엔진 위험 및 삭제 방법

▌검색엔진의 위험

구글 내 저장 페이지 삭제

- 구글에서 캐시페이지를 삭제하기 위해서는 오래된 콘텐츠 삭제 요청 선택
- https://www.google.com/webmasters/tools/removals
- 구글 웹 마스터를 방문하여 화면 중 해당되는 경우로 진행하고 노출된 콘텐츠를 입력한 뒤 접수 상태 확인

다음 내 저장 페이지 삭제

- 다음은 권리침해신고를 통해 캐시페이지 삭제 가능
- https://cs.daum.net/redbell/top.html
- 다음 고객센터에 접속하여 검색결과 제외를 선택한 뒤 검색결과 제외 신청 선택
- 개인정보가 포함된 게시글이 검색되는데 삭제할 수 있나요? 라는 제목으로 다음 고객센터에 문의한 뒤, 제외 신청 접수 완료

4. 검색엔진 위험 및 삭제 방법

▌검색엔진의 위험

Google

오래된 콘텐츠 삭제

구글 웹 마스터

∨

URL 입력

∨

삭제 요청

NAVER

웹 마스터 도구

네이버 고객센터

∨

신고센터

∨

유해게시물 신고 버튼

DAUM

권리침해 신고

고객센터의 검색 탭

∨

검색결과 제외

∨

검색결과 제외 신청

5. 문서 내 정보보안 방법

▌한글 파일 이용 시 정보보안

Case 한글 문서 내에 고객 주민등록번호가 너무 많아 다 지우지 못했을 때

주민등록번호는 검색도 잘 되지 않다 보니, 파일 내용이 길면 가끔 빠뜨리기도 합니다.
하지만 이런 부분을 고려하여 한글에서는 개인정보가리기 기능을 사용할 수 있는데요.
개인정보의 구체적인 항목을 선택하면, 모두 자동으로 암호화 됩니다. 또한 한글 내에
들어있는 다양한 정보에서의 취약점을 방지하기 위하여 PDF로 저장하기 기능을 이용하여
PDF로 변환하여 사용하는 것이 권장됩니다.

5. 문서 내 정보보안 방법

▌엑셀 파일 이용 시 정보보안

Case1 엑셀 배경색과 동일하게 설정된 글자색으로 인한 정보 유출

주요 정보에 대해서 배경색과 동일한 글자색을 설정하는 방법으로 화면에 내용이 나타나지 않게 처리된 파일이 있을 수 있습니다. 파일의 보관 시, 셀을 전체 선택하여 배경색 채우기 없음 및 글자색을 변경하여 모든 정보를 확인 후 삭제 또는 마스킹 처리 해야 합니다.

Case2 엑셀 숨겨진 부분에 있었던 주요 정보 노출

엑셀 파일에서 숨겨진 시트 또는 숨겨진 행열 안에 주요 정보가 숨어 있었던 사례도 적발되고 있습니다.

Case3 엑셀 외부파일 참조 기능에 의한 정보 유출

한 기업에서 공개채용을 진행하면서, 외부파일 참조 기능을 이용해 면접 안내 파일을 작성했습니다. 헌데 상단의 파일명을 복사한 뒤 함수창에 입력하자, 지원자 전체의 정보가 모두 나타난다는 것을 알게 되었습니다.

5. 문서 내 정보보안 방법

▌문서 정보 파기법

안전하게 보관한 정보

회사의 **큰** 자산

보유기간 경과 시 **파기**

잘못된 파기로
정보 복원 · 유출
사고 발생!

가장 중요한 것은, 완전한 파괴

5. 문서 내 정보보안 방법

▌문서 정보 파기법

완전 파괴 방법

오래된 콘텐츠 삭제

전용 소자 장비 이용

초기화 또는 덮어쓰기 수행

전자적 파일의 형태인 경우 정보를 삭제한 후 복구 및 재생되지 않도록 관리 감독

기록물, 인쇄물, 서면의 경우 마스킹 처리, CD나 저장장치는 천공 등으로 파기

6. 영상정보 처리기기 관리법

▌영상정보 처리기기의 설치

영상정보처리기기의 설치 및 운영이 가능한 경우

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄 예방 및 수사
3. 교통단속
4. 교통정보의 수집 · 분석 및 제공

6. 영상정보 처리기기 관리법

▌영상정보 처리기기의 설치

영상정보처리기기의 설치 및 운영 시 주의사항

목욕실, 화장실, 탈의실 등과 같이 내부를 볼 수 있는 장소의 설치 및 운영 금지

- 2020년에 충주의 한 목욕탕의 남자 탈의실에 설치되어 있는 CCTV가 발각되어 행정처분을 받은 사례
  → **5천만원 이하의 과태료**

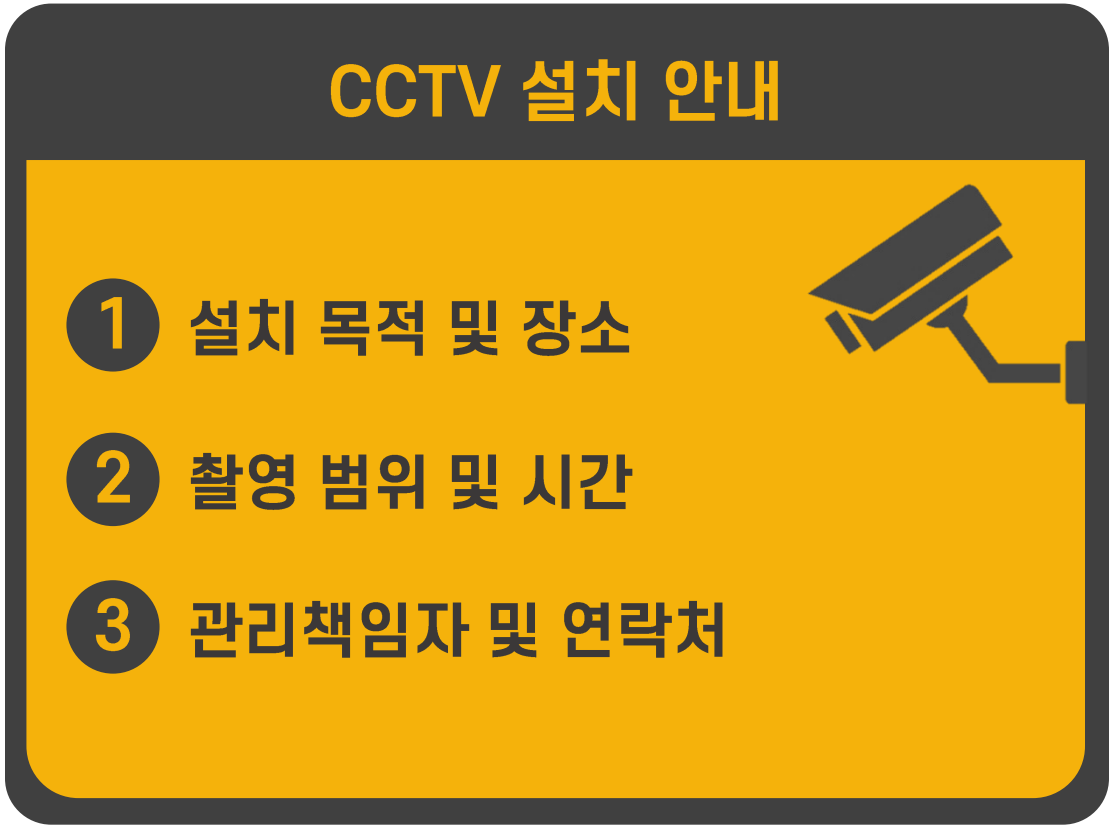
영상정보처리기기 임의 조작 또는 각도 조절 및 녹음 기능 사용 금지

- 임의 조작하거나 각도 조절 시 사생활 침해의 우려
- 녹음 기능 사용 시 통신비밀보호법 제14조 타인의 대화비밀 침해금지 조항에 위배되기 때문에, 영상정보 만을 처리해야 하며, 음성 정보는 수집 및 이용 금지

6. 영상정보 처리기기 관리법

▌영상정보 처리기기의 안내

안내판 기재사항



6. 영상정보 처리기기 관리법

▌영상정보 처리기기의 안내

Q. 저희 회사에 CCTV가 수십 대인데 설치된 곳마다 안내판을 설치해야 하나요?

정답은 X 입니다.
물론 공개된 장소에 설치된 영상정보처리기기마다 안내판을 설치하는 것이 원칙이지만, 건물 안에 다수의 영상정보처리기기를 운영하는 경우 출입구 등 정보주체가 출입하면서 잘 볼 수 있는 곳에 시설 또는 장소 전체가 영상정보처리기기 설치 지역임을 표시하는 안내판을 설치할 수 있습니다. 또한 안내판에는 설치 목적 및 장소, 촬영 범위 및 시간, 관리책임자 성명 및 연락처 등을 표기해야 합니다.

7. 기업이미지 추락하는 해킹 사고

▌사례 1) A 쇼핑몰 가입자 정보 해킹

**지난 2008년 A 쇼핑몰에서 천만 명이 넘는 정보가 유출된 어마어마한 해킹 사건이 있었습니다.
한국인이 중국 해커에게 의뢰하여 사건을 일으켰습니다. 사실상 전 국민의 정보가 유출된 첫 대형사고여서
수많은 고객들이 이에 대해 소송을 제기했지만, 결과는 원고 패소 판결이었습니다. 해당 기업의 과실이 입증되지
않는다는 것이 이유였습니다.**

예전에는 정보관리가 취약해서 어처구니없이 보안이 뚫린 기업이 많았지만 지금은 반대라고 할 수 있습니다.
보안을 철저히 했음에도 불구하고 신종 해킹 기법을 막지 못해 일어나는 사고가 많습니다. 그러다 보니, 이런
사건들을 계기로 법안이 계속 강화되고 있습니다. 게다가 업계의 선두를 달리던 A 쇼핑몰, 이제는 고객들의 무너진
신뢰를 예전으로 회복하지 못하고 있는 상황입니다.

7. 기업이미지 추락하는 해킹 사고

▌사례 2) B여행사 고객 신분증 이미지 해킹 사례

B여행사는 홈페이지를 통해 고객의 여권 사진을 접수 받고 있습니다. 하지만 자동 마스킹 시스템으로 고객들에게서 필요한 주요 정보 외에는 잘 가려져 있고, 고객 당사자의 개인 페이지에서만 확인 되기 때문에 안전한 관리라고 생각했는데요. 그런데 문제는 인터넷 검색엔진에서 조금만 쉽게 검색하면 전체 고객의 여권 이미지 파일이 검색되었던 겁니다.

검색엔진에는 캐시데이터라는 것이 존재하기 때문에, 모든 페이지를 임시로 저장해 둡니다. 이 내용은 접근이 되지는 않지만, 미리보기 등을 통해서 확인이 가능한데요. 그러다 보니, 홈페이지를 통해서 접수 받은 파일이 통으로 다운받아지거나 미리보기 화면을 통해서 확인 되는 경우가 종종 있습니다.
이 경우에도 나름의 보안조치를 했다고 생각했지만, 생각지 못한 곳에서 정보유출이 발생한 건데요. 이런 사고가 발생할 때마다 고객들의 신뢰는 바닥까지 내려가게 됩니다. 한번 실추된 기업이미지는 회복될 수 없겠지요.

8. 종류별 해킹 및 악성코드 대응법

▌악성프로그램이나 악성코드의 유입 경로

웹사이트 방문

이동형 저장장치

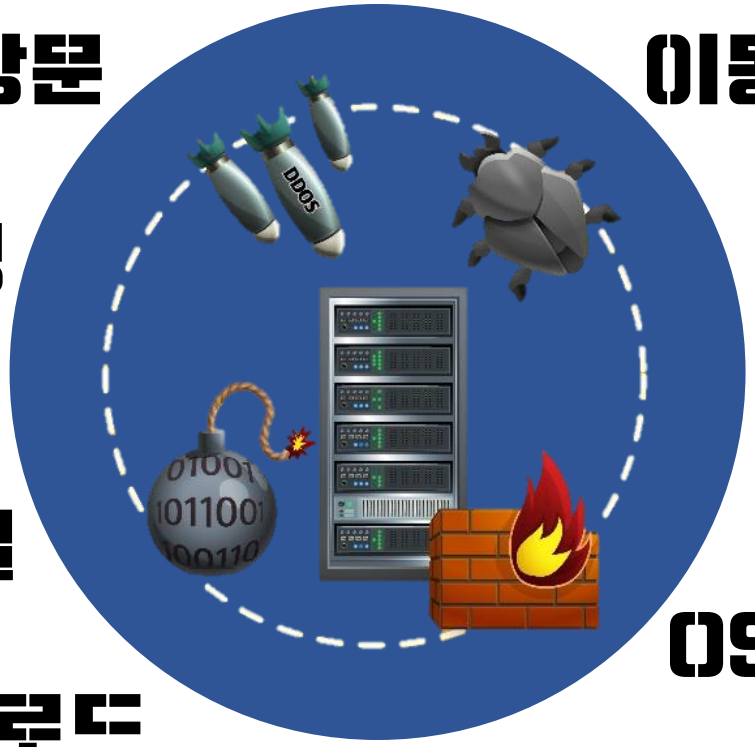
인스턴트 메시징 프로그램

P2P프로그램

전자메일

OS의 취약한 보안설정

인터넷 파일 다운로드

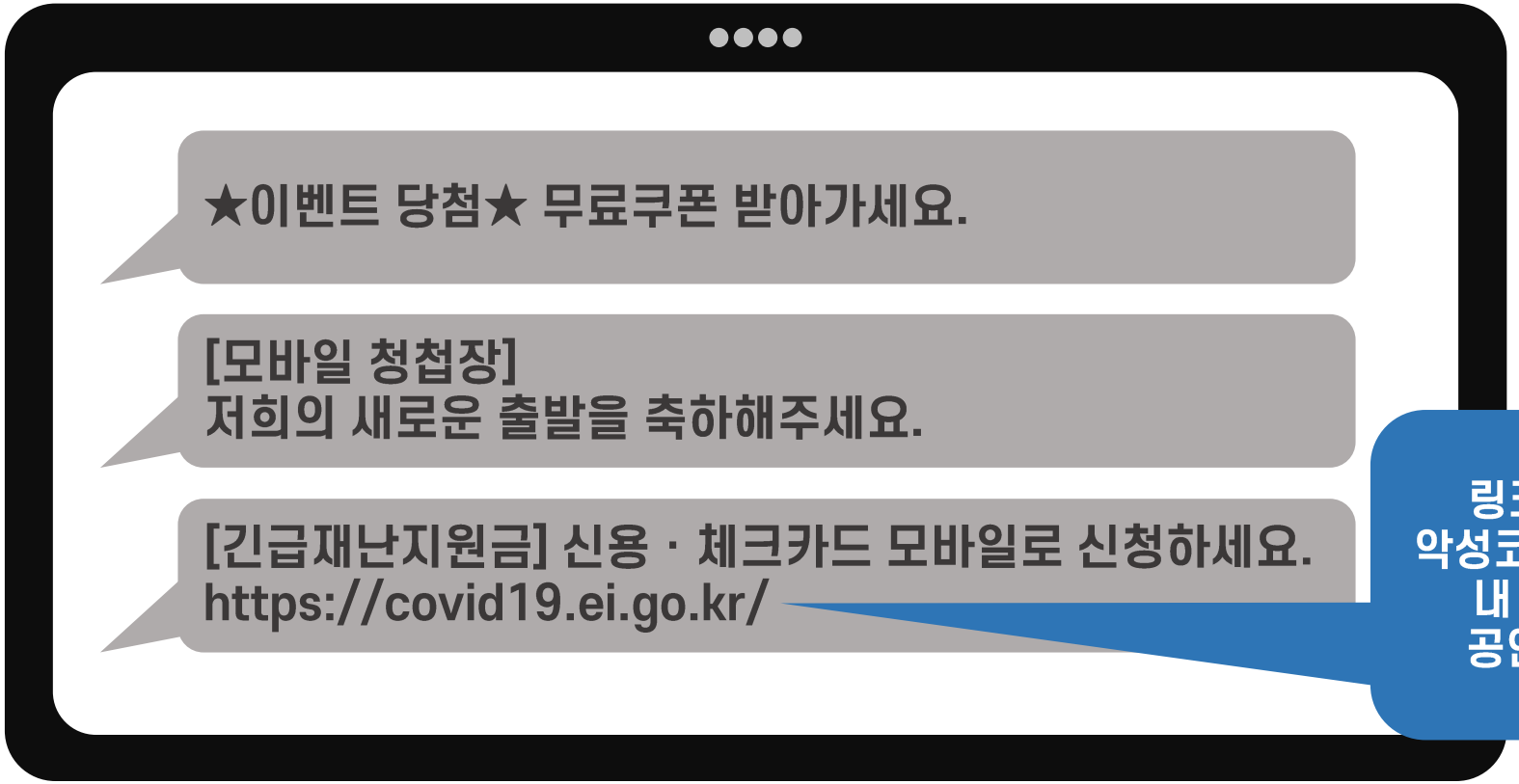


8. 종류별 해킹 및 악성코드 대응법

▌스미싱 (문자메시지 피싱)

Smishing = SMS + Phising

스미싱 | 문자메시지 | 낚시



8. 종류별 해킹 및 악성코드 대응법

▌스미싱 (문자메시지 피싱)

스미싱을 받았다면?

경찰청 사이버안전지킴이로 신고
(http://cyberbureau.police.go.kr, 182)

통신사에 소액결제서비스 차단 신청

8. 종류별 해킹 및 악성코드 대응법

▌보이스피싱(Voice Fishing)

‘자녀 인질형 피싱’

아동의 경우

유괴범이나 학교 사칭

성인의 경우

사고나 병원 사칭

학원, 보험상품,
인터넷 쇼핑몰 등
개인정보 유출

가입한 사이트에서 대량의 개인정보 유출 시
부모님 및 가족에게 개인정보 유출 사실 고지!

8. 종류별 해킹 및 악성코드 대응법

▌랜섬웨어(Ransomware)

Ransomware = Ransom + Software

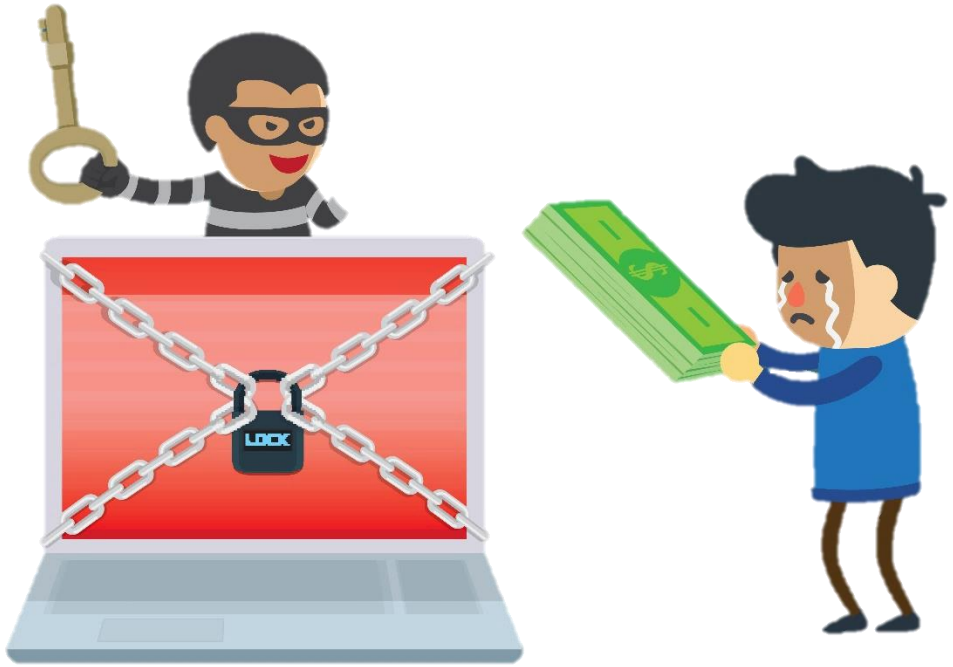
랜섬웨어 = 몸값 + 소프트웨어

시스템을 잠그거나 데이터를 암호화해
사용할 수 없도록 한 뒤,
이를 인질로 삼아 금전을 요구하는 악성 프로그램

8. 종류별 해킹 및 악성코드 대응법

▌랜섬웨어(Ransomware)

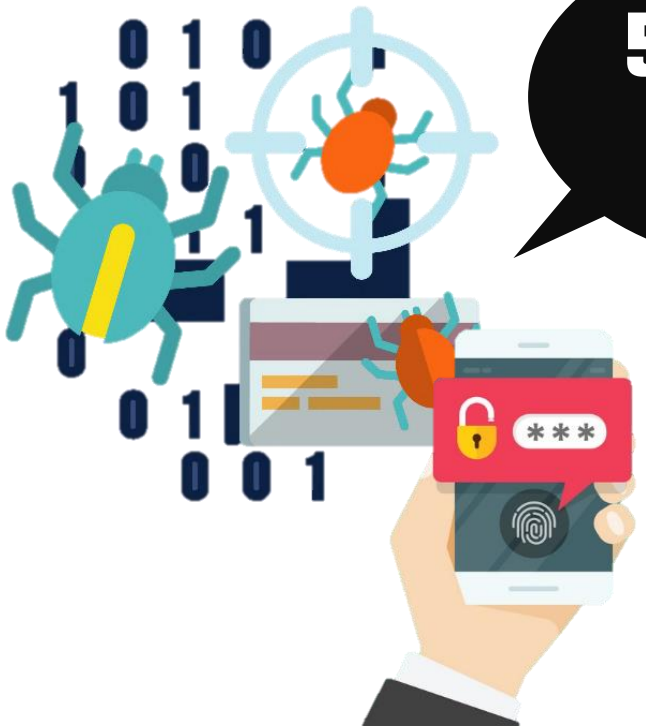
2015년 4월, 특정 인터넷 사이트에 방문한 사람들의 컴퓨터가 갑자기 먹통이 되는 일이 발생했습니다.
컴퓨터 뿐 아니라 컴퓨터에 연결된 외장형 하드 드라이브, 네트워크 연결 서버, 보조저장장치까지 모두
바이러스에 감염되었으며, 이를 풀어주는 대가로 파일 복원 비용을 요구하여 논란이 일어난 적이 있었습니다.



8. 종류별 해킹 및 악성코드 대응법

▌랜섬웨어(Ransomware)

개인 공격에서 공공기관과 기업 등으로 피해가
전세계적으로 늘어나고 있는 추세



50종이 넘는
랜섬웨어

다양한 유포 방식
이메일, 메신저, SNS 등

정기적
백업 및 클라우드
서버 이용

8. 종류별 해킹 및 악성코드 대응법

▌랜섬웨어(Ransomware)

랜섬웨어에 감염됐다면?

신속하게 컴퓨터 전원 강제 종료

컴퓨터 선과 인터넷 선 분리하고 경찰에 신고

8. 종류별 해킹 및 악성코드 대응법

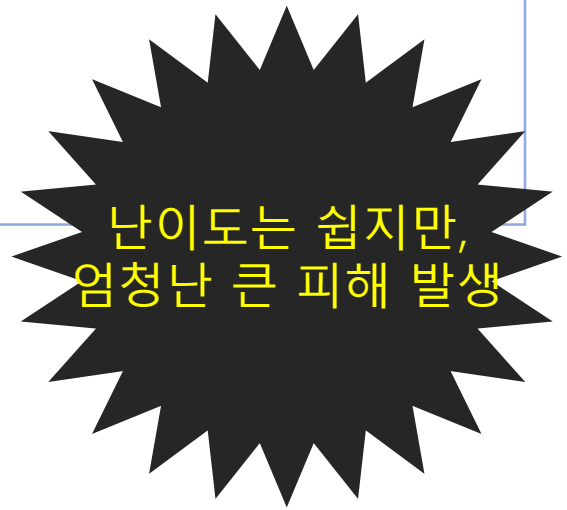
▌SQL 인젝션 공격

SQL (Structured Query Language)

데이터베이스를 구축하고 활용하기 위해 사용하는 언어

SQL 인젝션 (SQL Injection)

SQL문구를 의도적으로 삽입해서 데이터베이스가 비정상적인 동작을 하도록 조작하는 행위



8. 종류별 해킹 및 악성코드 대응법

▌SQL 인젝션 공격

SQL 인젝션 공격 방지

웹 방화벽 등의
구축 및 운영

SQL 인젝션 공격
탐지 및 차단

DB 사용자의 계정
권한 제한 및
최소한의 권한 부여

8. 종류별 해킹 및 악성코드 대응법

▌APT 지능형 지속 공격

APT(Advanced Persistent Threat)

- 지능형 지속 공격으로 불리는 이 해킹 공격은 최근 몇 년간 기업과 보안 관계자들을 끈질기게 괴롭힌 공격 수단
- 하나의 분야나 대상을 정해 그 타깃을 다양한 공격방법으로 꾸준히 공격하는 행위
- 개인, 단체, 기업, 국가, 정치단체까지 APT의 공격대상 표적이 됨
- 가능한 모든 수단을 동원해 표적의 허점을 파고들기 때문에 종합적인 방어체계 구축 필요

최신 공격 기법이 동원

8. 종류별 해킹 및 악성코드 대응법

▌APT 지능형 지속 공격 사례

2011년 APT공격을 받은 한 금융사의 경우 서버의 유지보수업체 직원이 서버관리용 노트북에 영화를 불법다운로드 한 것이 화근이었습니다.

모든 직원들이 가장 기본적인 것을 지키지 않을 때 공격의 틈이 벌어진다고 볼 수 있는데요.
보안 업데이트는 제 때 자주 해주고, 백신 소프트웨어를 이용하여 발견된 악성프로그램 등에 대해 빠른 삭제와 조치가 큰 사고를 막을 수 있습니다.

9. 상황별 긴급조치 및 시스템 설정

▌사례 1) 외부 해킹의 사례

회사의 서버가 다운되었는데, 문의해보니 해킹에 의한 침해사고 같다고 하네요. 그런데 저희 회사는 중소기업이라 내부에 전문성을 가진 인력이 없어, 긴급조치가 어렵습니다. 어떻게 하면 좋을까요?

해킹에 의한 정보유출 사고를 당하셨을 때는 추가 피해를 막기 위한 대책을 마련하셔야 합니다. 유출된 시스템을 분리 및 차단 조치하고 관련 로그 등 증거자료를 확보한 뒤 피해 원인을 분석해야 합니다. 그 외에도 이용자 및 관리자 비밀번호 변경, 기술적 보호조치 강화, 시스템 변경 같은 긴급조치를 시행해야 하는데요. 내부에 전문인력이 없는 경우에는 긴급조치가 어려울 수 있죠. 이 경우에는 한국인터넷진흥원에 기술지원을 요청할 수 있습니다.

9. 상황별 긴급조치 및 시스템 설정

▌사례 2) 내부자에 의한 정보보안 사고 사례

회사 시스템 내에서 대량의 정보 다운로드가 있어서 살펴보니, 이미 퇴사를 한 직원이 접속하여정보를 다운로드 하였습니다.

내부자에 의한 정보보안 사고가 일어났군요. 우리나라에서 발생한 '내부자'에 의한보안사고 중 대부분이 이러한 악의적인 내부자에 의해 발생한 대량의 정보 유출사고들인 만큼 가장 조심해야 하는 경우입니다. 대부분 정상적으로 근무하지만, 어느 순간 동료에게 앙심을 품거나, 연봉 인상 등이 되지 않는다는 이유로 악의를 갖게 되는 경우가 많습니다. 이들은 주로 재직 중에는 사고를 일으키지 않지만, 회사 시스템과 보안 프로그램 등을 파악하며 계획을 세웁니다. 그러다 퇴사하기 전 날이나, 퇴사를 한 후에 여전히 남아있는 계정과 권한으로 회사의 시스템에 접속하여 정보 유출 등의 보안사고를 일으킵니다.

기본적으로 퇴직자의 경우 퇴직 즉시 계정과 권한을 즉각 회수 및 삭제하는 등의 계정 라이프 사이클 관리가 이루어져야 이러한 유형의 내부자 위협에 대응할 수 있습니다. 회사의 인사관리 시스템에 계정의 권한 관리를 연동하는 것도 한 방법입니다. 퇴사를 하기 전부터 단계적으로 권한을 줄여나가면서 퇴사 이전에 모든 권한을 막아, 업무의 필요한 최소한의 조회만 가능하도록 하는 것도 방법 중 하나입니다.

9. 상황별 긴급조치 및 시스템 설정

▌사례 3) 이메일 오발송에 의한 사고 사례

고객정보가 들어있는 파일을 팀장님께 발송한다는 게, 실수로 전체 고객에게 단체메일을 보내버렸어요. 고객 리스트부터 연락처 같은 정보가 다 들어있는데 어쩌면 좋을까요?

의외로 종종 일어나는 실수 중 하나입니다. 이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일의 삭제를 요청하도록 합니다. 만약 메일 서버 외 첨부파일서버를 이용하는 경우에는 첨부파일서버 운영자에게 관련 파일의 삭제를 요청해야 합니다.

9. 상황별 긴급조치 및 시스템 설정

▌잘못된 대응 사례

Q. 해킹에 의해 정보가 유출되었습니다. 경찰청에서 해커를 검거할 때까지 신고를 보류해달라고 하여 30일 후에 유출 통지를 하였습니다.

경찰청의 요청으로 인해 개인정보 유출 통지를 미루셨군요. 공적기관에서 요청하면 별도의 절차없이 미뤄도 된다고 생각하기 쉽지만 결코 그렇지 않습니다. 해커 검거를 통해 유출된 개인정보를 회수하기 위하여 경찰청으로부터 필요한 최소한의 기간 동안 유출 통지 보류를 요청 받은 경우에는 우선 개인정보보호위원회에 고객정보에 대한 유출 신고를 한 후 협의하여야 하고 그 사유를 소명해야만 합니다.

Q. 거래처 직원에게 실수로 고객정보 2명의 인적사항이 담긴 파일을 발송했습니다. 거래처 직원에게 바로 삭제해 달라고 요청하고 마무리 하였습니다.

거래처 직원 1명에게 유출된 내용이라, 당사자에게만 요청하면 된다고 생각하셨군요. 게다가 고객정보가 2명 분이어서 안일하게 생각하셨던 것 같습니다. 하지만, 단 1명의 정보라 할지라도 유출되는 경우에는 통지 및 신고를 해야 합니다.

9. 상황별 긴급조치 및 시스템 설정

▌잘못된 대응 사례

Q. 고객 정보가 유출되었지만, 고객의 연락처가 없어 통지 절차를 이행하지는 않았습니다.

고객의 연락처를 몰라서 통지를 하지 않으셨군요. 고객에게 유출 통지를 할 때에는 정보주체가 실제 확인 가능하도록 이용 빈도가 높은 방법을 우선 활용하여 통지하는 것이 바람직하기는 합니다. 우선 휴대전화번호를 보유하고 있는 경우에는 전화통화 및 문자 등을 활용하고 곤란한 경우에는 이메일, 팩스, 우편 등의 방법을 활용해야 합니다. 하지만, 그조차 알 수 없거나, 대규모 유출로 24시간 이내 전체 통지가 기술적으로 불가능한 경우에는 홈페이지 팝업창 등을 이용하여 방문하는 이용자가 모두 알 수 있도록 현재까지 파악된 유출 사실 등을 게시하여야 합니다.

Q. 고객정보가 유출되어 통지하려 하였지만, 어떤 사항이 유출되었는지 구체적인 내용이 확인되지 않아 통지를 할 수 없습니다.

유출 통지하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 통지하고, 추가로 확인되는 내용은 확인되는 즉시 통지해야 합니다. 구체적 사실관계 파악을 이유로 정보주체에게 유출 사실 통지를 지연하는 경우에는 3천만원 이하의 과태료가 부과될 수 있으니 주의가 필요합니다.

10. 홈페이지 관리법

▌대표적인 홈페이지 해킹 유형

1 홈페이지를 변조하는 공격

- 원래의 홈페이지 메인 화면이 아니라 해커가 올린 사진으로 홈페이지 메인 화면이 바뀌는 등의 공격
- 일반적으로 해커가 자신의 실력을 과시하기 위해 사용하거나 정치적 비판 메시지를 전파하기 위해 사용하는 홈페이지 해킹 유형
- 기업의 보안이미지에도 치명적인 영향을 줄 수 있기 때문에, 기업의 위상을 위해서라도 반드시 막아야 하는 공격 유형 중 하나임

2 악성코드 유포

- 해커가 홈페이지를 해킹 하여 악성코드를 홈페이지에 심으면, 다른 사용자가 홈페이지 접속 시 사용자의 컴퓨터에 악성코드가 심어지는 방식
- 랜섬웨어를 심는 공격도 많이 이루어지고 있음
- 최근 사용자들도 기업의 보안에 아주 많은 관심을 보이고 있기 때문에 기업 홈페이지를 통한 악성코드 유포는 여러모로 치명적인 결과를 낳게 됨

10. 홈페이지 관리법

▌대표적인 홈페이지 해킹 유형

3 디도스 공격

- 분산 서비스 거부 공격이라고도 함
- 해커가 사전에 다른 사용자 컴퓨터를 대량으로 감염시켜 놓고 특정 홈페이지를 공격할 때 감염시켰던 많은 좀비 컴퓨터를 이용하여 타깃 웹 서버에 비정상적으로 많은 요청 패킷을 보내 홈페이지 서비스 장애를 유발하는 공격

10. 홈페이지 관리법

▌홈페이지의 보안을 취약하게 만드는 4가지 경우

1 홈페이지 소스코드 보안설정

- 홈페이지 설계 오류로 홈페이지 소스코드에 노출되는 경우
- 홈페이지에서 마우스 오른쪽 버튼을 눌러 [소스보기] 기능을 이용했을 때 소스 안에 가려졌던 정보가 나오는 경우가 있음
- 불필요한 정보는 소스코드에서 삭제하고 꼭 필요한 정보는 암호화하거나 개인 식별용 구분자를 변경하는 것도 좋음

2 홈페이지 URL 설정

- 홈페지이 접속경로와 관련된 오류
- 홈페이지의 URL을 교묘하게 바꿨을 때 타인의 정보가 노출되거나 보안상 가려졌던 페이지가 드러날 때 파라미터 값이 보이지 않게 포스트 방식을 사용하는 것이 좋음
- 이용자 자신의 정보만을 조회할 수 있도록 접근제어를 하고 회원 구분 값을 개인정보로 활용한다면 이에 대한 변경 필요

10. 홈페이지 관리법

▌홈페이지의 보안을 취약하게 만드는 4가지 경우

3 임시저장 페이지 관리

- 브라우저를 사용할 때는 일부 웹사이트 정보는 캐시 및 쿠키 형태로 저장됨
- 캐시 및 쿠키를 주기적으로 삭제하여 임시로 저장된 페이지에 대한 정보 유출을 막을 수 있음

4 디렉터리 리스팅 보안설정 미흡

- 서버 관리자가 사이트 테스트 목적으로 사용하는 설정으로 인터넷 사용자에게 웹 서버 내 디렉터리와 파일 목록을 보여주는 기능
- 웹 서버의 URL로 '도메인 네임+디렉터리' 경로를 입력했을 때, 웹 브라우저에 해당 디렉터리 내 모든 파일 목록이 노출되는 보안 취약점
- 운영체제 등 서비스 환경에 맞도록 디렉터리 리스팅 취약점 조치가 필요하며 접근 제어를 설정하는 것이 좋음

11. 재발 방지를 위한 과제

▌정보 주체에 대한 피해 구제 방법

1 유출 여부를 조회할 수 있어야 한다.

- 정보 주체가 개인정보 유출 여부 등을 확인 가능하도록 별도의 홈페이지 등을 제공해야 함
- 본인 확인 수단으로 핸드폰, 이메일 인증 등을 활용할 수 있지만, 주민등록번호는 활용하지 않도록 주의해야 함

2 민원 대응이 가능해야 한다.

- 개인정보 유출로 인해 정보주체의 피해 신고가 접수되어 상담 및 문의를 원한다면 각종 민원 대응을 위한 방안을 모색해야 함
- 개인정보 유출 문의에 신속히 대응할 수 있도록 상담 스크립트를 운영하고 전화, 이메일, 홈페이지, SNS 등 다양한 채널을 통해 개인정보 유출 사실, 경위 등을 확인할 수 있는 창구를 마련해야 함

11. 재발 방지를 위한 과제

▌정보 주체에 대한 피해 구제 방법

3 현장 혼잡을 최소화 해야 한다.

- 유출 대응 현장에서의 긴급 상황 또는 돌발 상황이 발생한다면 그에 따른 혼란 최소화를 위한 방안도 강구해야 함
- 현장에서 물리적 시스템 장애, 파괴 그리고 불필요한 인력 등으로 인하여 개인정보가 분실, 도난, 훼손 되지 않도록 주의해야 함

4 고객 불안을 해소해 주어야 한다.

- 보이스피싱 등 2차 피해 방지를 위한 유의사항을 사전 안내하고 유출 및 피해 대응 현황 등을 실시간으로 정확하고 투명하게 공개하는 등 고객 불안 해소를 위해 노력해야 함

5 피해구제에 힘써야 한다.

- 정보주체의 피해 구제 계획을 마련하고 개인정보 분쟁조정 위원회, 손해배상제도 등도 함께 안내하도록 해야 함

11. 재발 방지를 위한 과제

▌재발 방지 대책 마련

개인정보 유출 원인과 취약점 등에 대한 적절한 대책을 마련하고 개인정보 취급자를 대상으로 개인정보보호교육을 정기적으로 실시해야 함

개인정보 유출 상황에 대비하여 대응 시나리오를 작성하고, 모의훈련 등을 실시하여 우리 회사의 유출 대응 체계를 점검하고 지속적으로 보완해야 함

홈페이지가 취약한 부분이 있어 유출 사고가 일어났다면 이를 예방하기 위해 안전조치를 강화해야 함

11. 재발 방지를 위한 과제

▌재발 방지 대책 마련

홈페이지 취약점 예방을 위해서는 연 1회 이상 정기 점검하고, 개인정보 노출을 방지하기 위해 인증 절차 추가 및 로봇 배제 규칙을 적용하여 홈페이지 접근을 제한해야 함

홈페이지에 첨부파일을 포함한 게시글 작성 시 개인정보 포함 여부를 확인하도록 해야 하며, 게시판 등에 정보주체가 글 작성 시 개인정보가 노출되지 않도록 주의 안내가 필요함

관리자 페이지에 접근하는 IP를 제한하거나 아이디, 비밀번호 외 추가적인 인증 수단을 사용하여 접속할 수 있는 시스템 마련이 필요함