
[슬기로운 보안생활]
언택트 시대에 필요한
정보지킴 매뉴얼

개인 정보를 대하는 우리의 자세
타사 사례에서 우리는 뭘 배울까?

개인 정보를 대하는 우리의 자세
타사 사례에서 우리는 뭘 배울까?

1. Who are you?
2. 이런 사고, 저런 이유
3. 업무에서 만나는 개인 정보

Who are you?

Who are you?

두 개의 정체성

시민, 정보주체

개인 정보 유출사고 발생

기업, 개인정보취급자

또 사고야!!

손해배상 소송을 걸어야지

제재가 너무 약해

우리 회사는 문제 없나?

아, 큰일 났다!

형사처벌은 심하지

Who are you?

두 개의 정체성

시민, 정보주체

기업, 개인 정보취급자

개인정보취급자

임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘 · 감독을 받아 개인 정보를 처리하는 자

또 사고 났어!

손해배상 소송을 걸어야지

제재가 너무 약해

아, 큰일 났다!

형사처벌은 심하지

이런 사고, 저런 이유

사례1. 지인을 가장한 피싱 메일을 통해 외부에서 해킹

사고 경위	범인이 I사를 표적으로 하여 I사 직원의 지인의 계정을 해킹하고, 화면보호기로 위장한 악성 프로그램을 첨부한 메일을 지인을 가장하여 직원에게 메일을 보냈음. 이를 클릭한 직원 PC를 기점으로 개인 정보 DB에 이르는 경로를 찾아내 2일 만에 1,030만 명의 개인 정보 유출함 (I사, 2016.07.)
회사 영향	• 과징금 44억 8,000만원 • 과태료 2,500만원 • 브랜드에 악영향
원 인	• 지인 명의로 온 피싱 메일의 첨부 파일(악성 프로그램) 클릭 • 서버 계정의 비밀번호를 파일에 평문으로 저장 • 최대 접속 시간 제한 미조치
대 책	• 피싱(phishing) 메일 조심해요! 첨부 파일은 특히!! • 비밀번호를 파일에 써서 PC에 저장할 때는 파일 암호화 기능을 써야 해요! • 보안솔루션은 구축하는 것도 중요하지만, 잘 운영하는 것이 매우 중요해요!

이런 사고, 저런 이유

사례2. 웹사이트 보안취약점에 대한 보안 공격

해커가 데이터베이스 질의어를 조작해 데이터베이스에서 원하는 자료를 유출해가는 보안 공격 기법

사고 경위	범인은 P사의 웹사이트 중 취약한 웹페이지를 대상으로 SQL 인젝션(Structured Query Language Injection) 공격을 통해 195만여 건의 아이디, 암호화된 비밀번호, 생년월일, 이메일 등 8개 항목을 유출 (P사, 2015.09.)
회사 영향	• 과징금 1억 200만원 • 과태료 1,500만원 • 민사소송 1인당 20만원 배상 판결(2심, 2019.05.) - 최초로 법정손해배상제 적용
원 인	• 웹사이트 보안취약점 점검을 하지 않음 • 기본적인 네트워크 보안 장비를 설치, 운용하지 않음
대 책	• 개발자는 기능과 성능뿐 아니라 소프트웨어 보안취약점을 생기지 않도록 개발해야 해요 • (외주) 개발팀에게 업무 요청하는 부서에서는 기능과 일정뿐 아니라 보안취약점을 최소화하는 것도 요청하세요. • 다만 사람이 하는 일은 적절한 인력, 일정, 예산이 투입되어야 적절한 품질의 결과물이 나온다는 것은 만고불변의 진리!!

이런 사고, 저런 이유

사례3. 모바일 이벤트 페이지 개발 오류로 개인 정보 노출

사고 경위	이벤트 페이지 개발 과정에서 직원의 캐시 정책 적용 오류로 인하여 타인의 주문 정보가 노출되었음. 유출 건 수는 20건, 유출 항목은 아이디, 성명, 휴대폰, 배송지 주소 (W사, 2018.11.)
회사 영향	• 과징금 18억 5,200만원 • 과태료 1,000만원 • 수사기관에 고발
원 인	• 모바일 이벤트 페이지에 오류 존재
대 책	• 이벤트 페이지 개발에도 적절한 개발기간 확보 • 이벤트 페이지에도 품질 관리 필요 • 이벤트 페이지에도 개발 프로세스 적용

이런 사고, 저런 이유

사례4. 메일 발송 시 타인의 정보를 파일에 첨부하여 발송

사고 경위	N사가 광고수익 지급 원천징수 영수증을 블로거에게 메일로 보내면서 타인의 원천징수 영수증을 포함하여 발송하여 이름, 주소, 주민번호 등 약 2,200여 명의 개인 정보가 타인에게 노출 (N사, 2019.05.)
회사 영향	• 과징금 2,720만원, 과태료 1,300만원 등 총 4,020만원 • 브랜드에 악영향
원 인	• 시스템 오류
대 책	• 시스템 개발 오류 대책 • 시스템 운영 오류 대책

이런 사고, 저런 이유

사례5. 여러 수신인에게 메일 발송 시 타인의 이메일 주소 노출

사고 경위	공채 서류 전형 합격 여부 안내 메일을 보내면서, '개별 발송' 설정 누락으로 수신인에게 다른 수신인들의 이름과 메일 주소 노출 (S사, 2018.11.)
대 책	• 책상 앞에 중요 메일 발송 매뉴얼을 부착해요! • 4 eyes principle - 중요한 일은 두 사람이 하세요!!

업무에서 만나는 개인 정보

개인 정보의 종류

일반적 정보

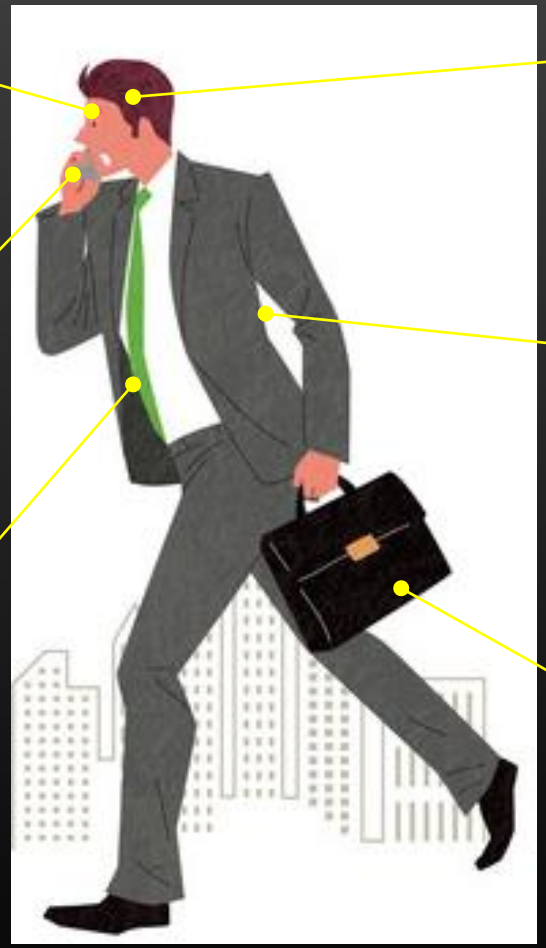
- 주민등록번호
- 이름, 주소

통신 · 위치 정보

통화 · 문자 내역, IP 주소,
화상 정보

사회적 정보

- 교육 정보
- 근로 정보
- 자격 정보



정신적 정보

- 기호, 성향
- 신념, 사상

신체적 정보

- 의료 · 건강 정보
- 생체인식 정보
- 신체 정보

재산적 정보

- 개인 금융정보
- 개인 신용정보

업무에서 만나는 개인 정보

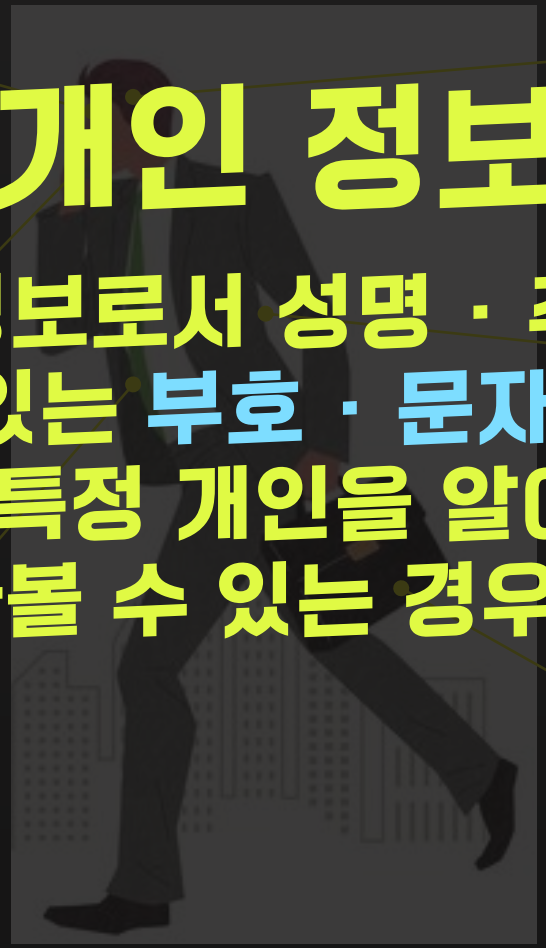
개인 정보의 종류

일반적 정보

- 주민등록번호
- 이름, 주소

정신적 정보

- 기호, 성향
- 신념, 사상



개인 정보

살아있는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보, 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함

사회적 정보

- 교육 정보
- 근로 정보
- 자격 정보

재산적 정보

- 개인 금융정보
- 개인 신용정보

업무에서 만나는 개인 정보

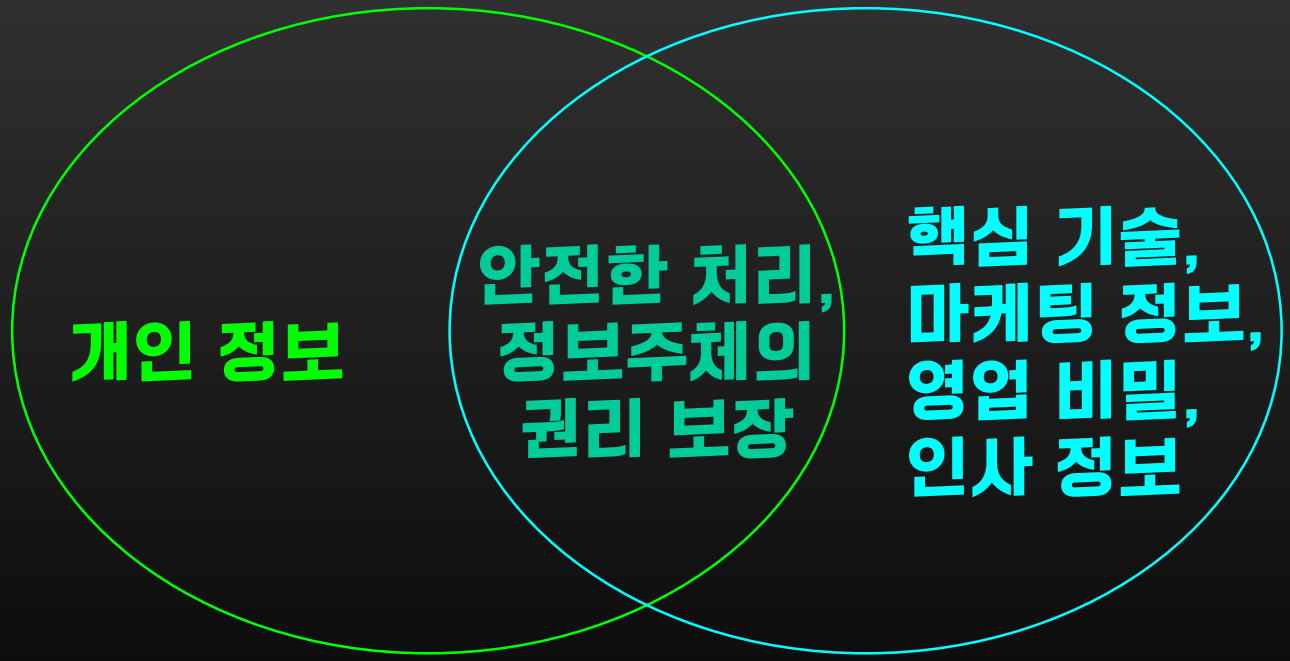
개인 정보의 특성

고객과 비(非)고객(임직원, 주주, 기자, 협력업체 직원 등)을 포함
- 14세 미만 어린이의 개인 정보는 반드시 법정 대리인의 동의를 받아 처리

정보주체

개인정보처리자 (사업자)

개인 정보를 처리하는 개인, 단체, 법인, 공공기관



업무에서 만나는 개인 정보

개인 정보의 특성

개인 정보 보호법의 목적

개인 정보를 안전하게 처리하고,
정보주체의 권리를 보장

업무에서 만나는 개인 정보

내 업무와 개인 정보

부서	개인 정보 처리 업무
영업	• 협력업체 협업 • 고객사 영업, 관리
마케팅	• B2C 마케팅 • B2B 마케팅 • 고객DB 관리

부서	개인 정보 처리 업무
서비스 기획	• 서비스 기획 및 운영
개발	• 서비스 테스트
품질	• 서비스 테스트
IT운영	• 서버, DB서버 운영
R&D	• 기술 개발, 테스트

부서	개인 정보 처리 업무
개인 정보보호	• 개인 정보 처리, 보호
정보보안	• 개인 정보 기술적 · 관리적 보호
물리적 보안	• 출입통제, 시설보안

부서	개인 정보 처리 업무
인사	• 임직원 정보 관리 • 인사 평가, 급여
재무	• 급여, 계좌정보
회계	• 계좌정보

부서	개인 정보 처리 업무
대외	• 대관업무, 대외업무
IR	• 주주 등 투자자 관리

사례를 통한
개인 정보 처리 단계별 보호 업무

▌사례를 통한 개인 정보 처리 단계별 보호 업무

1. 개인 정보 처리 단계 보호 업무
2. 개인 정보 수집 단계 보호 업무
3. 개인 정보 이용 · 제공 단계 보호 업무
4. 개인 정보 파기 단계 보호 업무
5. 정보주체의 권리 보장 업무

개인 정보 처리 단계 보호 업무

개인 정보 처리 단계 보호 업무

개인 정보 처리 단계별 보호 업무

1. 수집

- 최소 수집
- 명시적 동의
- 14세 미만, 법정 대리인 동의
- <처리 제한> 민감 정보, 고유식별정보, 주민등록번호
- 영상정보처리 기기 설치·운영

2. 이용

3. 제공

- 목적 외 이용·제공 제한
- 제3자 제공
- 처리 위탁
- 가명 정보 처리
- 영업 양·수도 국외 이전

4. 관리 (보관)

- 안전조치 의무
- 처리방침, 보호책임자(CPO)
- 개인 정보 유출 시 통지·신고
- 개인 정보파일 등록(공공)
- 개인 정보영향 평가(공공)

5. 파기

- 파기

개인 정보 처리 단계 보호 업무

개인 정보 처리 단계별 보호 업무

1. 수집

- 최소 수집
- 명시적 동의
- 14세 미만, 법정 대리인 동의
- <처리 제한> 민감 정보, 고유식별정보, 주민등록번호
- 영상정보처리 기기 설치·운영

2. 이용

3. 제공

- 가명 정보 처리
- 영업 양·수도 국외 이전

4. 관리

- 안전조치 의무
- 처리방침
- 개인정보보호책임자(CPO)
- 개인 정보파일 등록(공공)
- 개인 정보영향 평가(공공)

5. 파기

- 파기

정보주체의 권리 보장

- 개인 정보의 열람
- 개인 정보의 정정·삭제
- 개인 정보의 처리 정지
- 권리행사의 방법 및 절차
- 손해배상, 법정손해배상

개인 정보 처리 단계 보호 업무

사례. (위반) 선택 항목 미입력으로 서비스 거부

위반 내용	정유사에서 멤버십 카드 가입을 위해 개인 정보를 수집하면서 군 복무 정보를 필수항목으로 요구하고, 미 기재 시 멤버십 가입 불허

- 필수입력항목에 멤버십과 무관한 ‘군복무 여부’ 포함
- 기재하지 않을 경우 멤버십 가입 불허

개인 정보 수집 단계 보호 업무

사례1. (준수) 선택 항목 미입력으로 서비스 거부

준수 내용	회원 가입 시 수집하는 개인 정보를 '필수'와 '선택' 사항으로 구분하여 수집 동의를 받고, 선택사항은 입력하지 않아도 회원가입 허용

개인 정보 수집 단계 보호 업무

사례2. (위반) 인사 정보의 과다 수집

위반 내용	인사 정보 수집 시에도 반드시 필요한 정보만 수집 채용 계약 시 반드시 필요하지 않은 신체사항, 종교, 가족사항 등을 수집

사진	이름							
	생년월일							
	전화	집전화			E-mail			
		휴대전화			비상 연락처			

채용 계약 시 신체사항, 가족사항 등 개인 정보 수집은 불필요함

신체사항	신장	체중	혈액형	시력	기타	종교	취미	특기

가족사항	관계	성명	연령	학력	직업	직위	동거 여부

개인 정보 수집 단계 보호 업무

사례2. (위반) 인사 정보의 과다 수집

위반 내용	인사 정보 수집 시에도 반드시 필요한 정보만 수집 채용 계약 시 반드시 필요하지 않은 신체사항, 종교, 가족사항 등을 수집

사진	이름	
	생년월일	
	전화	
신체사항	신장	

(준수)

- **종교는 민감 정보이므로 수집 시 별도 동의 필요**
- **연말 정산을 위해 필요한 가족 정보는 해당 업무 수행 시 수집**

가족사항	관계	성명	연령	학력	직업	직위	동거 여부

개인 정보 수집 단계 보호 업무

사례3. (위반) 만 14세 미만 어린이 정보 수집 시 법정 대리인 동의

위반 내용	틱*은 개인 정보 처리 방침에 만 14세 미만 어린이를 대상으로 서비스하지 않는다고 밝혔으나, 이용자의 나이를 확인하는 절차를 운영하지 않았고, 법정대리인의 동의도 받지 않음

(준수)

- **회원 가입 시 휴대폰 본인 인증 등을 통해 만 14세 미만인지 확인**
- **만 14세 미만 어린이의 개인 정보를 수집할 때에는 문자 메시지, 공인인증서 등을 통한 법정대리인의 동의 획득**

개인 정보 수집 단계 보호 업무

사례4. (위반) 민감 정보 수집 제한

위반 내용	이동통신사가 요금감면을 위해 민감 정보(신체 장애 정보)를 수집하면서 정보주체의 동의를 받지 않거나 일반 개인 정보와 구분하여 별도의 동의를 받지 않음

개인 정보 수집 단계 보호 업무

사례5. (준수) 민감 정보 수집 제한

준수 내용	민감 정보를 수집할 때에는 민감 정보의 수집 · 이용 목적, 수집 항목, 보유 · 이용 기간, 이용자 권리를 일반 개인 정보 수집과 구분하여 별도로 고지하고 별도의 동의 획득

개인 정보 수집 동의

- 개인 정보의 수집 및 이용 목적
  - 회원관리 및 결혼 서비스에 관한 상담 및 자료요청 확인
  - 결혼 관련 서비스 상담
- 수집하는 개인 정보의 항목
  - 성명, 아이디, 비밀번호, 휴대폰번호, 이메일, 거주지 주소
- 이용 및 보유 기간

☐ 동의함 ☐ 동의하지 않음

민감 정보 수집에 대한 별도 동의 획득

민감 정보 수집 동의

- 민감 정보 수집 목적
  - 결혼 상대 추천 시 추가 서비스 제공
  - ** 정보 주최 이벤트 정보 제공
- 수집하는 민감 정보의 항목
  - 신체 정보, 종교

민감 정보 수집 항목

- 이용 및 보유 기간
  - 회원 탈퇴 시까지 보유

☐ 동의함 ☐ 동의하지 않음

개인 정보 수집 단계 보호 업무

사례6. (위반) 주민번호 수집 제한

위반 내용	주민번호 체계를 유지하면서 생년월일을 수집하면 주민번호를 이용하는 것에 해당 법령의 근거 없이 주민번호 수집 또는 주민번호를 수집 목적과 다른 목적으로 이용

주민등록번호 일부 정보(앞자리 + 뒷자리 첫째 숫자) 사용

Q 저희 회사는 고객으로부터 주민등록번호 앞자리와 뒷자리 첫째 숫자까지만 수집하여 사용하려고 합니다.
이런 방식은 허용되는지요?

A 주민등록번호 13자리 체계를 유지하면서 주민등록번호의 일부를 기호로 처리하는 것도 주민등록번호 처리를 허용하는 구체적 법령 근거가 없으면 금지됩니다. 다만, 주민등록번호 13자리 체계가 아닌 생년월일과 성별을 별도로 수집하는 것은 허용됩니다.

(준수)

생년월일과 성별을 별도로 수집하는 것은 주민번호로 간주되지 않음

개인 정보 수집 단계 보호 업무

사례6. (위반) 주민번호 수집 제한

위반 내용	주민번호 체계를 유지하면서 생년월일을 수집하면 주민번호를 이용하는 것에 해당 법령의 근거 없이 주민번호 수집 또는 주민번호를 수집 목적과 다른 목적으로 이용

법령상 주민등록번호 수집 근거가 있는 업무처리를 위해 홈페이지 회원가입 시 주민등록번호 수집

Q 저희 기관은 법령의 구체적인 근거 규정에 따라 주민등록번호를 수집 이용하고 있습니다. 이러한 경우 홈페이지에서 회원가입을 받는 절차에서 주민등록번호를 받아도 되는 것 아닌지요?

A 법령에 구체적 근거가 있지 않는 한 단순 회원가입 목적으로 주민등록번호를 수집할 수 없습니다. 아이핀, 휴대전화번호 등 다른 수단으로 본인 여부를 확인해야 합니다.

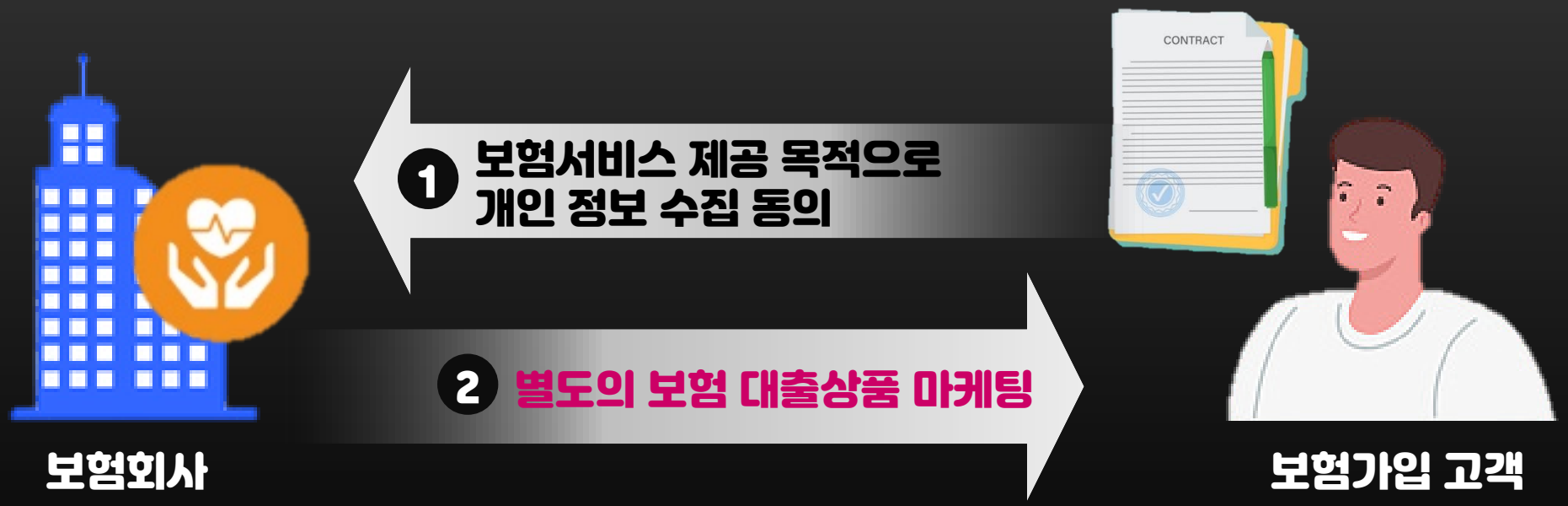
(준수)

주민번호 수집의 법적 근거가 있다 하더라도 수집 목적의 범위 내에서만 사용

개인 정보 이용 · 제공 단계 보호 업무

사례1. (위반) 수집 시 동의 받은 목적 외 이용 금지

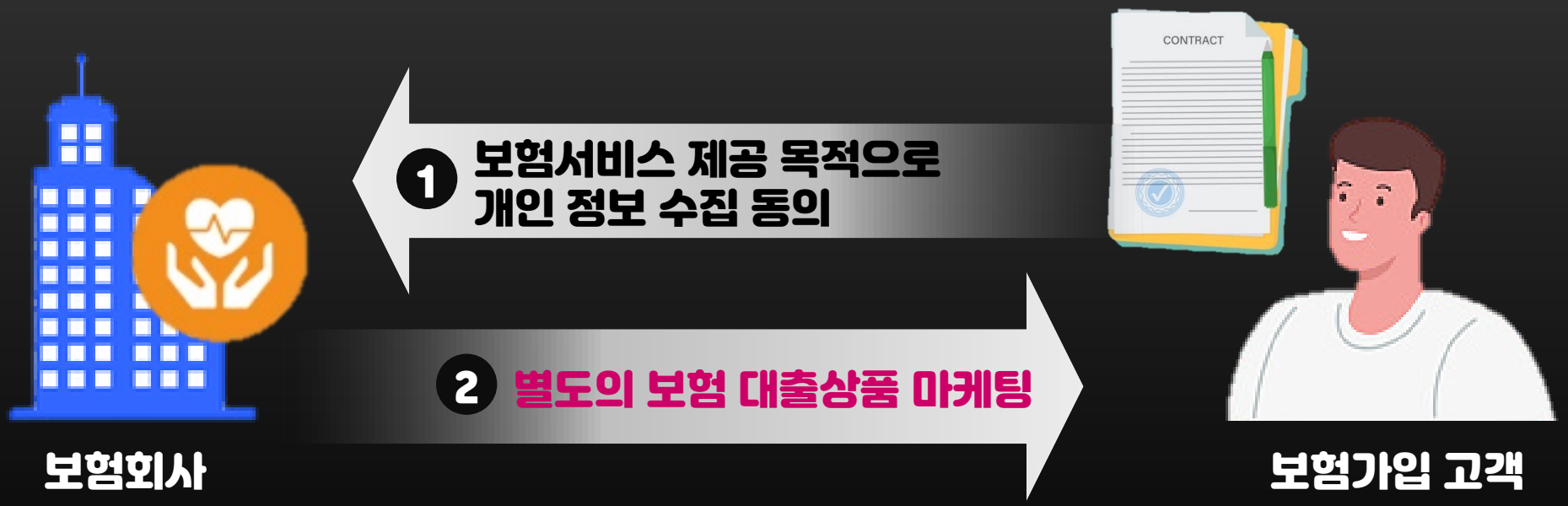
위반 내용	보험 서비스를 제공할 목적으로 보험가입자의 개인 정보를 수집하였으나, 정보주체의 동의 없이 보험상품 홍보 및 판매를 위해 개인 정보 이용



개인 정보 이용 · 제공 단계 보호 업무

사례2. (준수) 수집 시 동의 받은 목적 외 이용 금지

준수 내용	당초 동의 받은 목적 외에 이벤트 등 다른 목적으로 개인 정보 이용 시, 변경된 수집·이용 목적, 수집 항목, 보유 · 이용기간 등을 다시 고지하여 동의 획득



개인 정보 이용 · 제공 단계 보호 업무

참고. (준수) 별도 고지, 별도 동의를 통해 수집하는 개인 정보

개인정보 수집 시, 필수항목과 선택 항목, 고유식별정보, 민감 정보, 제3자 제공 등에 대하여 반드시 별도로 고지하고 별도로 동의 획득

A사의 개인 정보 수집 및 이용

회사는 회원가입, 고객상담, 서비스 제공을 위해 최초 회원가입 시 아래와 같은 개인 정보를 수집하고 있습니다.

<필수 정보> 성명, 생년월일, 성별, 아이디, 비밀번호, 필수 연락처, 가입 인증 정보

수집한 개인 정보는 회원 유지기간 및 A/S 기간 동안 보관합니다.

회원께서는 개인 정보 수집 동의를 거부하실 수 있으며 다만 이 경우 회원가입이 제한됩니다.

개인 정보 수집 및 이용에 동의하십니까	☐ 동의함	☐ 동의하지 않음	일반 동의

(필요 시) 고유 식별 정보 처리 동의 (수집 또는 제공 시의 고지사항 고지) [주민등록번호 제외]

고유 식별 정보 처리에 동의하십니까	☐ 동의함	☐ 동의하지 않음	별도 동의

(필요 시) 민감 정보 처리 동의 (수집 또는 제공 시의 고지사항 고지)

민감 정보 처리에 동의하십니까	☐ 동의함	☐ 동의하지 않음	별도 동의

(필요 시) 목적 외 제공 동의 시 (목적 외 제공 시의 고지사항 고지)

개인 정보 목적 외 이용에 동의하십니까	☐ 동의함	☐ 동의하지 않음	별도 동의

<선택 정보> 기혼 여부, 기념일, 병력, 취미, 소득 수준, 자녀 정보

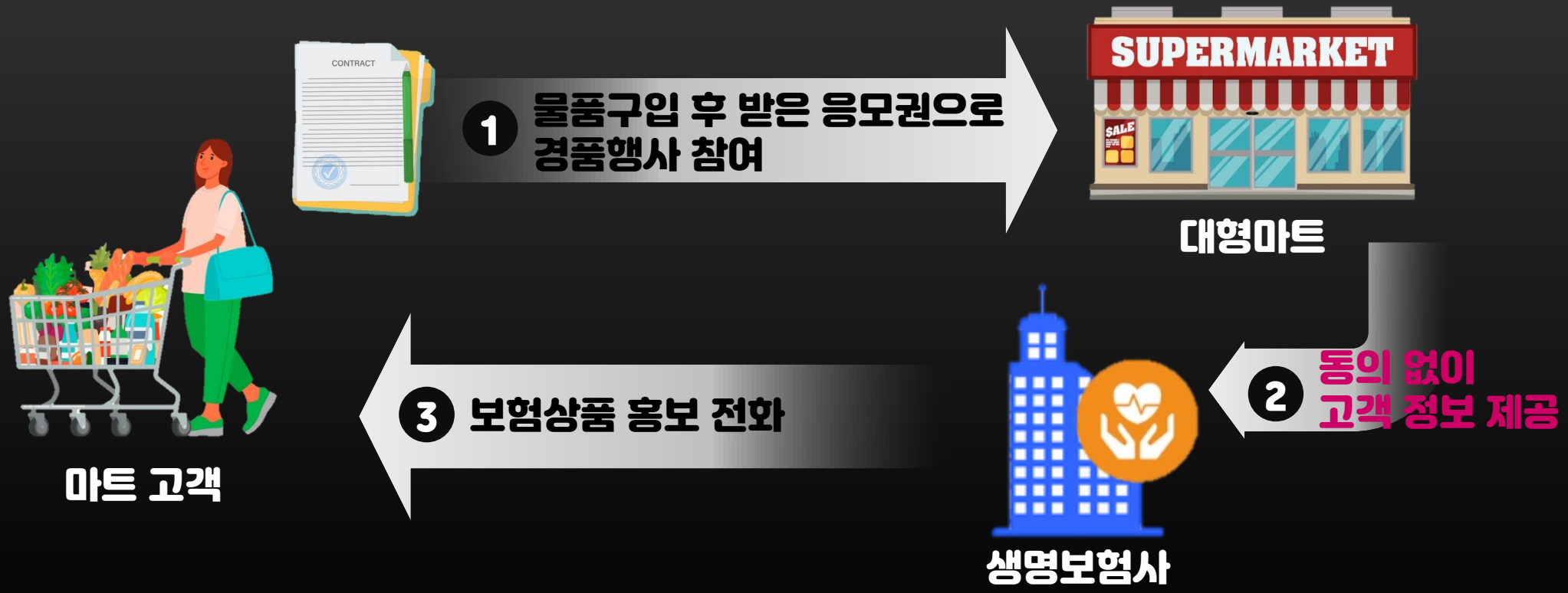
※ 선택 정보 사항을 획득하지 못한 사유로 인해 서비스 제공을 거부할 수 없습니다.

선택적 개인 정보 수집 및 이용에 동의하십니까	☐ 동의함	☐ 동의하지 않음	별도 동의

개인 정보 이용 · 제공 단계 보호 업무

사례3. (위반) 제3자 제공 시 동의

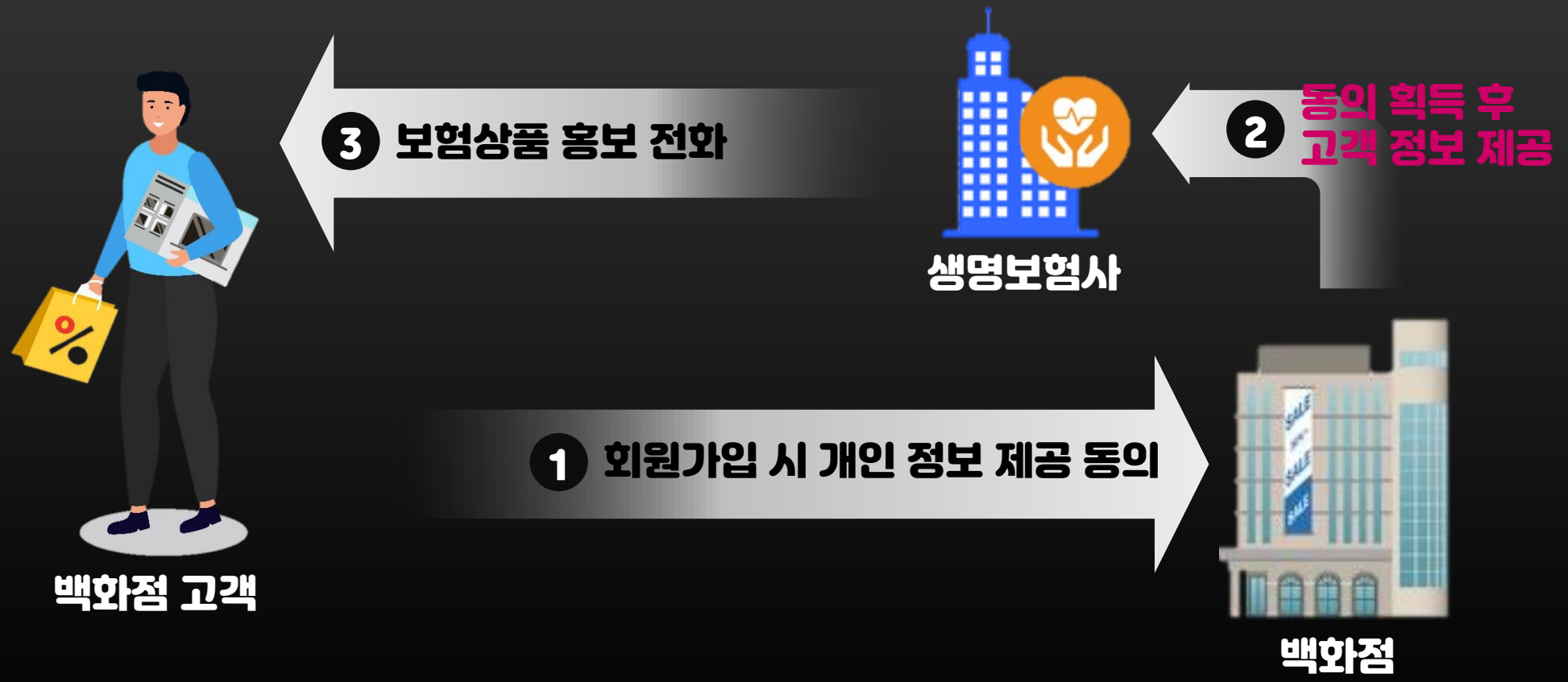
위반 내용	대형마트가 경품 행사에 응모한 정보주체의 개인 정보를 동의 없이 생명보험사에 제공



개인 정보 이용 · 제공 단계 보호 업무

사례4. (준수) 제3자 제공 시 동의

준수 내용	백화점이 보험업체와의 마케팅 제휴를 통해 회원 개인 정보 제공 시, 제공 받는 자, 제공 목적, 제공 항목 및 이용 기간 등을 명시하고 별도 동의 필수



개인 정보 이용 · 제공 단계 보호 업무

개인 정보 보호법 동의 없이 개인정보의 이용 또는 제3자 제공이 가능한 경우

- 제15조(개인정보의 수집 · 이용) 제3항

  개인정보처리자는 **당초 수집 목적과 합리적으로 관련된 범위**에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

- 제17조(개인정보의 제공) 제4항

  개인정보처리자는 **당초 수집 목적과 합리적으로 관련된 범위**에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.

- 시행령 제14조의2(개인정보의 추가적인 이용 · 제공의 기준 등) 제1항

  개인정보처리자는 법 제15조 제3항 또는 제17조 제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.

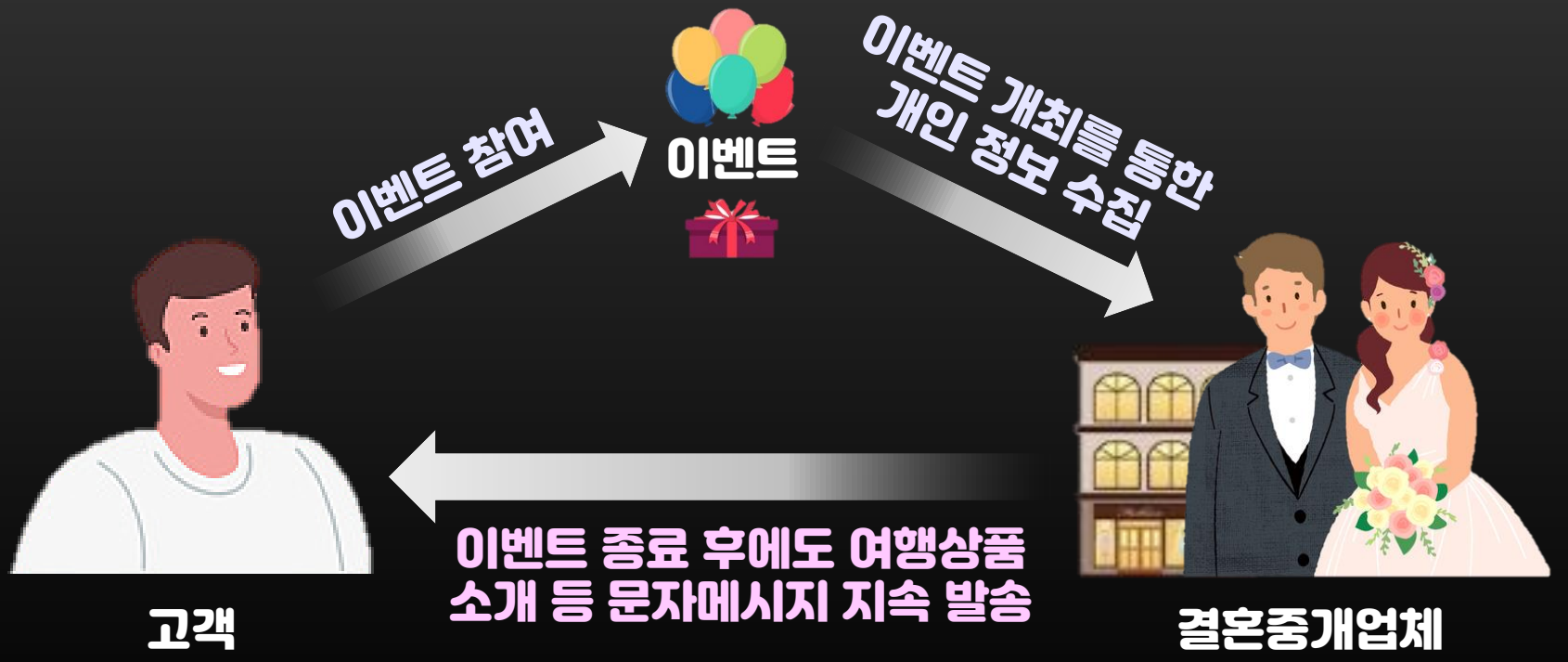
  1. 당초 수집 목적과 관련성이 있는지 여부
  2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 **예측 가능성**이 있는지 여부
  3. 정보주체의 이익을 부당하게 침해하는지 여부
  4. 가명 처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

  (2020.08.05 시행)

개인 정보 파기 단계 보호 업무

사례5. (위반) 개인 정보 파기

위반 내용	결혼중개업체가 이벤트 행사 목적으로 수집한 개인정보를 이벤트 종료 후에도 파기하지 않고 홍보 목적으로 사용



(준수)

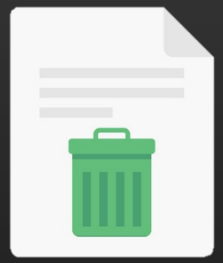
이벤트 종료 또는 회원 탈퇴 등 목적 달성, 보유기간이 만료된 개인정보는 지체 없이 복구 재생할 수 없는 방법으로 파기

개인 정보 이용 · 제공 단계 보호 업무

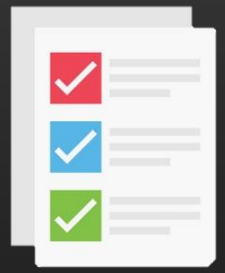
사례6. (준수) 개인 정보 파기

전체 파기

완전 파괴
(소각 · 파쇄 등)



전용 소자 장비
이용하여 삭제



데이터가
복원되지 않게
초기화 또는
덮어쓰기

일부 파기

전자적 파일 형태인 경우

개인 정보를 삭제한 후 복구 및 재생되지
않도록 관리 및 감독

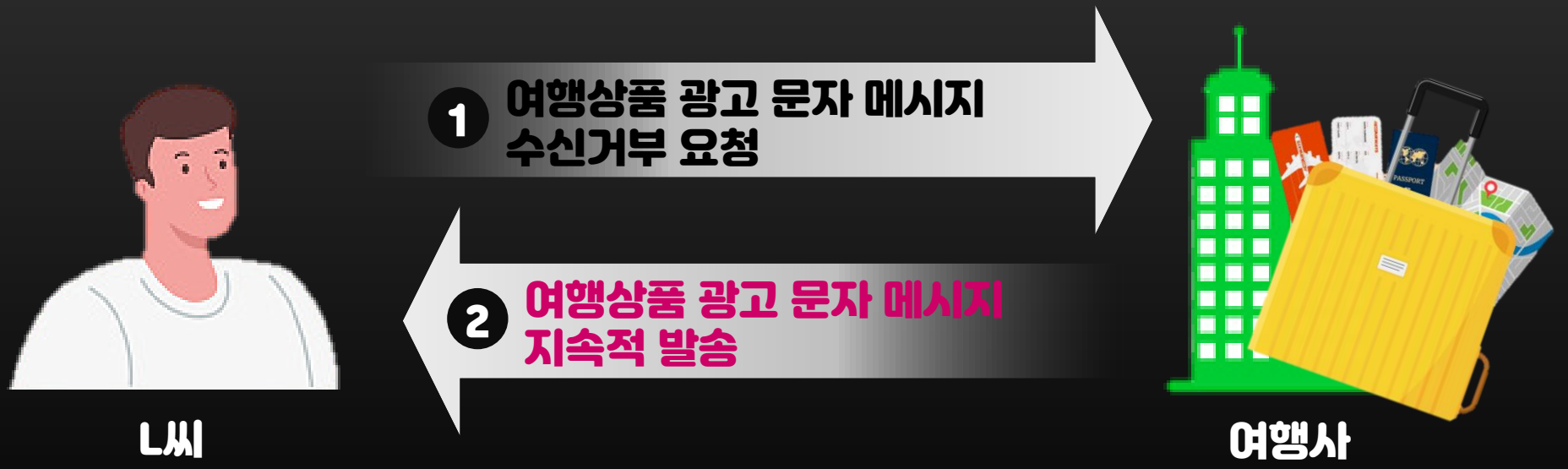
**제1호 외의 기록물, 인쇄물,
서면, 그 밖의 기록 매체인 경우**

해당 부분을 마스킹, 천공 등으로 삭제

정보주체의 권리 보장 업무

사례1. (위반) 동의 철회에 따른 개인 정보 파기

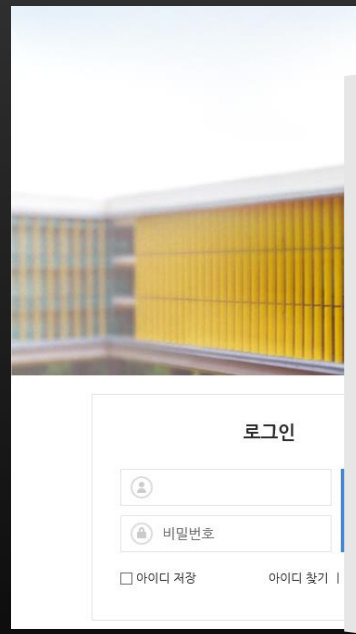
위반 내용	정보주체의 개인 정보 이용 동의 철회 및 광고 문자 수신 거부에도 불구하고 광고 문자를 수 차례 발송



정보주체의 권리 보장 업무

사례2. (준수) 동의 철회에 따른 개인정보 파기

준수 내용	개인 정보 수집 방법보다 쉽게 동의 철회를 할 수 있도록 홈페이지에서 회원 탈퇴 메뉴를 제공하고, 탈퇴 시 지체 없이 해당 개인 정보를 파기



회원서비스

- 회원가입
- 회원로그인
- 회원탈퇴
- ID 확인 / 비밀번호 확인
- 비밀번호 변경

정보주체의 동의철회 요구를 즉시 처리할 수 있도록 메뉴 지원

(준수)

개인정보처리자는 정보주체 또는 그 법정대리인이 개인정보를 열람, 정정, 삭제, 처리 정지(동의 철회)를 요구할 수 있는 통로 마련, 요구 시 법정 시일 내 조치를 취하여야 함

언택트 시대의 정보 보안

언택트 시대의 정보 보안

1. 공격과 수비
2. 안전한 원격 근무
3. 기업의 중요 정보 보호

공격과 수비

러시아 월드컵 독일전 승리의 주역, 조현우

러시아월드컵 F조 경기에서 대한민국이 세계 최강팀 독일을 2대 0으로 이김

수 많은 공격을 받았으나, 한 골도 허용하지 않은 수문장 조현우 선수가 이 경기 최우수 선수상을(MOM)을 받음 (2018.06.)

수비 가담하는 손흥민

대한민국 남자 축구대표팀과 호주와의 평가전에서 세계적인 공격수 손흥민 선수가 호주 코너킥 공격 때 최종 수비선까지 내려와 호주 선수의 헤더 공격을 차단하고 있음 (2019.06.)

공격과 수비

기업에서의 공격과 수비

1997년 IMF 외환위기, 2008~2009년 세계 금융위기에서 리스크 관리를 하지 못한 기업은 살아남지 못함

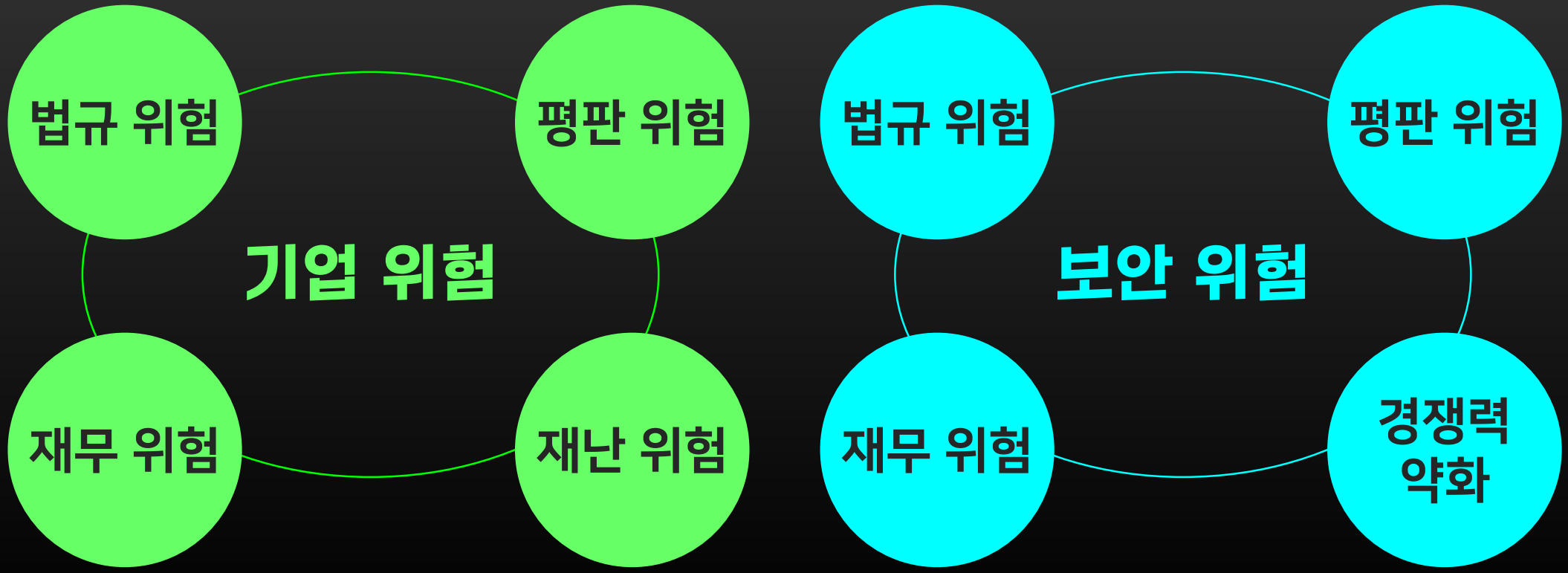
공격수	매출, 영업이익에 기여하는 부서			
	영업	마케팅	개발	R&D

수비수	회사와 사업의 리스크 관리에 기여하는 부서			
	경영지원, 재무, 인사	법무	홍보	보안 개인정보

공격과 수비

기업차원의 위험

기업 차원에서 관리해야 할 대표적인 리스크로는 법규 위험, 평판 위험, 재무 위험, 재난 위험 등이 있음. 보안 위험은 기업의 경쟁력 약화뿐 아니라, 다른 기업 차원의 위험의 원인이 되었음



공격과 수비

정보 보안 = 정보 보안 조직의 업무?

기업 차원의 위험인 보안 위험을 관리하기 위해서는 정보보안 조직뿐 아니라 경영진과 관련 부서, 모든 임직원이 수행해야 할 정보보안 활동과 업무가 있음

	정보보안 조직	비(非)정보보안 조직
정보 보안 업무	정보보호 관리체계 보안 기술 정보보안 운영, 분석 보안사고 대응	계정 및 권한 관리 인적 보안 생활 보안 외주 보안 비밀번호 관리
비(非) 정보 보안 업무	인사 총무	영업, 마케팅 개발, IT운영, 인사, 총무

안전한 원격 근무

사례1. 재택 근무 PC 해킹을 통해 외부에서 해킹

사고 경위	범인은 H사의 외주 인력 A씨의 자택 PC에 악성코드를 유포하고, 이를 통해 H사의 원격 접속 프로그램을 통해 회사 내부에 접근한 뒤 A씨의 사무실 PC와 서비스용 DB, 개발용 DB에 저장되어 있는 43만여 명의 주민등록번호를 포함하여 총 49만여 명의 개인정보를 유출함 (H사, 2017.09.)
회사 영향	• 과징금 3억 2,725만원 • 과태료 1,800만원 등 총 약 3억 4,500만원 • CEO와 개인정보보호책임자(CPO)의 징계
원 인	• 외주 인력이 자택에서 회사 내부의 업무망에 접속하여 작업 • 회사 외부에서 내부의 개인정보처리시스템에 접속 시 일회용 비밀번호(OTP) 등 다중 인증 미비
대 책	• IT용역 사용 부서에서는 외주 인력이 일하는 장소를 알고, 정보보안팀과 협의하세요. • IT외주 인력이 정보보안 서약서를 비롯한 보안 가이드를 준수하도록 해야 해요. 가이드가 혹시 없다면? 정보보안팀에 요청하세요!! • (조금 귀찮더라도) 회사 외부에서 내부로 접속할 때에는 반드시 일회용 비밀번호 같은 다중 인증을 사용해요. 가성비 높은 보안 수단이예요.

안전한 원격 근무

사례2. 무선랜을 통한 회사 기밀 자료 유출

사고 경위	무선랜은 회사나 집에서 인터넷을 접속할 때 가장 많이 사용하는 네트워크인데, 보안이 취약하여 아이디, 비밀번호, 회사의 중요 자료가 유출되는 주요 통로임. 무선랜을 이용한 인터넷 전화를 사용하면 통화 내용이 유출될 수 있음
원 인	• 무선 AP(Access Point)에 비밀번호가 설정되어 있지 않거나 추정하기 쉬운 것으로 설정되었음 • 정상 AP와 유사한 이름으로 더 강력한 무선 신호를 보내 사용자 PC가 정상 AP로 오인하여 접속할 수 있음 → 무선랜 위장 공격(wifi phishing)
대책(AP)	• 무선 AP의 비밀번호는 예측하기 어려운 문자와 숫자를 섞어서 만들어요. • 외부 방문자용 무선 AP는 별도로 구축하고 비밀번호를 설정해요 (이 비밀번호는 예측하기 쉬원도 괜찮음) • 공유기의 관리자 페이지에 접속하여 관리자 계정을 변경하고 비밀번호를 설정해요
대책(PC)	• PC 등 업무용 단말기에서는 자동으로 접속하는 AP를 최소화해요 • 중요 정보는 암호화 통신을 이용하여 전송해요(웹 브라우저에서 자물쇠 확인) • PC에서 무선랜 암호화방식은 WPA2를 선택해요

안전한 원격 근무

코로나19에 따른 원격 근무의 증가와 보안위협

코로나19 이전에도 출장, 휴가, 이동 중에 긴급한 업무를 처리하기 위해 원격 근무를 하였으나, 코로나19 상황에서 직장의 일시 폐쇄 등의 이유로 원격 근무가 지속적 · 간헐적 발생 가능

물리적 위협

- 근무 장소가 회사가 제공하는 수준의 안전한 환경이 되기 어려움
- 불특정 다수가 모이는 카페, 도서관 또는 이동 중 단말기 분실 또는 도난의 위험이 있음

인적 위협

- 사회공학적 공격에 노출되고, 의도하지 않은 비정상 작업이 발생 가능
- 원격근무 단말기를 통해 회사 중요 정보 유출될 수 있음
- 재택근무 시 가족 및 방문자 업무용 단말에 접근하여 자료 훼손 가능

물리적 위협

- 사용자 단말기가 악성 프로그램에 감염될 경우 아이디, 비밀번호가 노출되고, 해커가 이를 이용해 회사 내부망에 침입할 수 있음
- 원격 근무에 사용한 무선랜(네트워크)이 안전하지 않을 경우 비밀번호, 회사 자료 등 중요 정보가 유출될 수 있음
- 회사 업무 처리 시스템의 인증 절차가 부실한 경우, 해커가 내부망에 침입할 수 있음

안전한 원격 근무

원격 근무자 보안 수칙 (1/2)

1 주민등록번호 일부 정보(앞자리 + 뒷자리 첫째 숫자) 사용

- 카페, 공원 등 공개된 장소는 안 좋아요.
- 아무나 못 들어오는 전용 공간이 좋아요.

2 단말기 보안은 원격 근무 보안의 핵심이에요

- 회사 단말과 동일한 보안 시스템이 설치되는 게 가장 안전해요.
- 단말기를 가족이나 지인 등이 사용하지 않도록 해요.
- 운영체제, 백신, 웹 브라우저를 자동 업데이트를 통해 최신으로 유지해요.
- 가능한 한 USB를 통해 자료를 복사하지 말아요. 악성 프로그램이 단말기에 설치될 수 있어요.

안전한 원격 근무

원격 근무자 보안 수칙 (2/2)

3 무선랜을 이용할 때 조심해요

- 공항, 컨퍼런스룸 등 공개된 장소의 무선랜은 업무에 사용하지 마세요.
- 집 공유기의 관리자 계정을 변경하고 비밀번호를 설정해요.

4 비밀번호를 안전하게 관리해요

- 업무에 사용하는 계정 아이디와 비밀번호는 개인적으로 사용하는 것과 꼭 구분해요.
- 브라우저에 비밀번호를 자동 저장하지 마세요. 악성 프로그램이 유출할 수 있어요.
- PC방 등 공개된 장소의 PC는 악성 프로그램이 설치되기 쉬워요. 중요한 정보를 입력하지 마세요.

안전한 원격 근무

원격 근무 환경 운영자(관리자) 보안 수칙

IT운영팀, 정보보안팀 등 회사의 원격 근무 환경이나
도구, 정책을 관리하는 부서에서는
다음 문서를 참고하세요.

「비대면 업무환경(원격근무, 영상회의) 도입·운영을
위한 보안 가이드」, (한국인터넷진흥원, 2020.06.)

기업의 중요 정보 보호

유출된 기술 정보 종류 및 수단

기술 정보

제품, 설계 도면, 연구 결과 데이터,
최종 연구결과 순으로 많이 유출

비기술 정보

영업 정보, 원가 정보, 사업추진계획,
재무 정보 순으로 많이 유출

수단

- USB, 외장하드 등 휴대용 저장장치가 가장 많았고,
  인력 스카우트, 복사·절취, 이메일, 스마트폰, 컴퓨터 해킹 순
- 온-오프 방식에 관계 없이 해당 기업의 취약한 지점을
  공격함

기업의 중요 정보 보호

기술 정보 유출 범인은?

기술정보 유출은 전 직원에 의해 발생하는 경우가 다른 경우에 월등하게 많은 상태가 계속되고 있음

현 직원, 협력업체 지원 역시 내부 사정을 잘 아는 사람들

비기술정보의 유출 역시 이와 비슷하리라 추정

대책

주로 내부 사정을 잘 아는 사람들에 의해 유출되므로
퇴사한 직원이나 협력업체 직원 역시 외부자 보안 관리
기준과 절차에 따라 관리해야 해요.

기업의 중요 정보 보호

개인 정보 유출 사고 주요 원인 외부 공격이 압도적으로 많음

외부 공격	시스템 오류	내부 직원 유출	관리자 부주의	기타
80.5%	6.9%	1.8%	9.0%	1.8%
291건	25건	7건	33건	7건

- 웹셸 업로드, 파라미터 변조, 지능형 지속공격, SQL 인젝션 등 해킹 공격
- 이메일 오발송, 인트라넷 게시글이 구글 검색엔진에 노출, 접근통제 등 보안조치 미흡
- 퇴사 시 USB로 유출 미 마케팅에 활용, 흥신소를 통한 구매, 지자체 공무원이 이장에게 무단 제공 등
- 약국 처방전이나 개인정보가 담긴 서류를 미파기 및 방치 등
- 확인 불가 등 원인 미상

보안 위협 3종 세트
(악성메일, 랜섬웨어, 스미싱)
대응하기

▌보안 위협 3종 세트(악성 메일, 랜섬웨어, 스미싱) 대응하기

1. 악성 메일 대응하기
2. 랜섬웨어 대응하기
3. 스미싱 대응하기

악성 메일 대응하기

악성 메일이란?

악성 메일은 악의적인 목적으로 갖고 배포되는 이메일로서 많은 보안 공격의 출발점이 되는 메일로, 메일에 다른 파일로 위장한 악성 프로그램을 첨부하거나 이를 유포하는 사이트의 링크를 본문에 포함

악성 프로그램 유포

원격제어, 키로거, 가상화폐 채굴, 다른 악성 프로그램을 설치하는 악성 프로그램 다운로드

피싱메일

수신인을 속여서 금융정보, 비밀번호, 개인정보 등 탈취하거나 탈취하기 위한 피싱 사이트로 유도

랜섬웨어 유포

랜섬웨어를 유포하여 이를 통해 금전 요구

악성 메일 대응하기

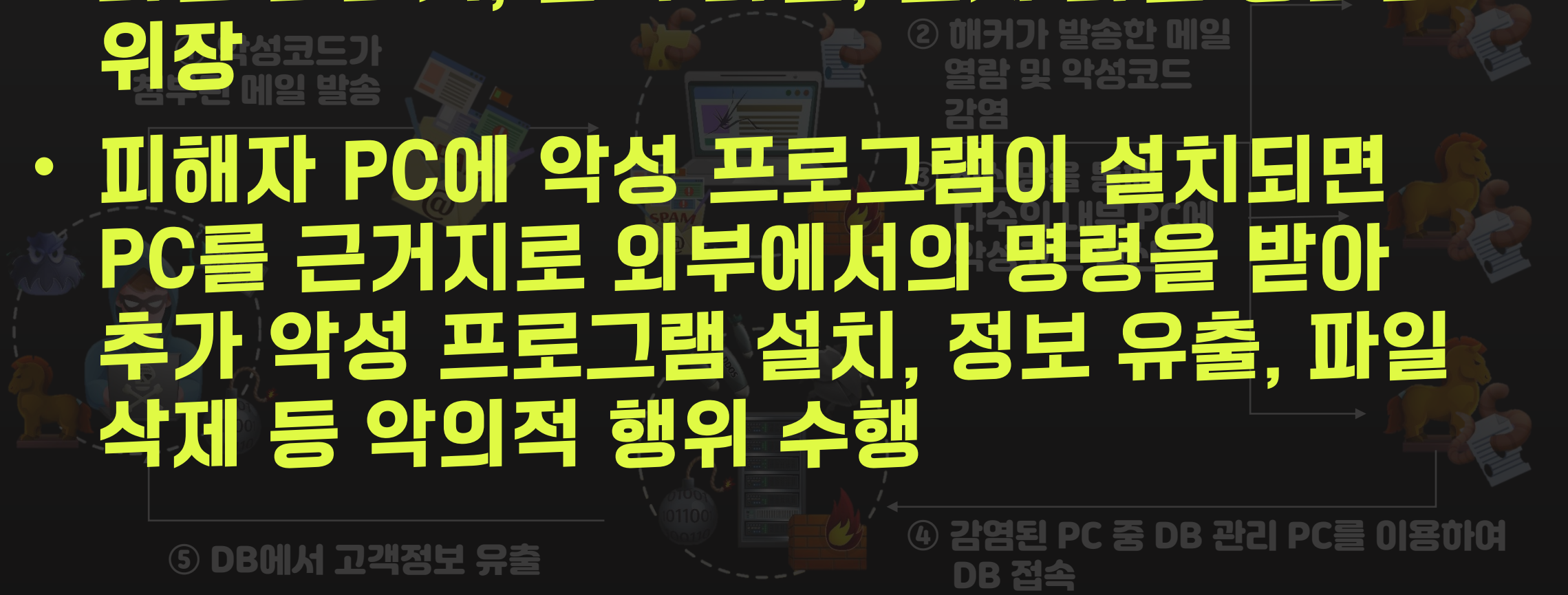
악성 메일을 통한 악성 프로그램 유포

악성 메일의 링크나 첨부파일을 통해 악성 프로그램이 설치되면, PC 이용자의 비밀번호 유출, PC에 있는 파일의 유출, 다른 악성 프로그램의 설치, 가상화폐 채굴 등 악성 행위가 이뤄짐

악성 메일 대응하기

악성 메일을 통한 악성 프로그램 유포

- 악성 프로그램의 주요 유포 수단
- 화면 보호기, 압축 파일, 문서 파일 등으로 위장
- 피해자 PC에 악성 프로그램이 설치되면 PC를 근거지로 외부에서의 명령을 받아 추가 악성 프로그램 설치, 정보 유출, 파일 삭제 등 악의적 행위 수행



악성 메일 대응하기

피싱 메일(Phishing email)

유명 기업 등 사칭할 기관의 홈페이지와 외관상 똑같은 위장 홈페이지를 사전에 준비한 뒤, 불특정 다수의 인터넷 이용자들 또는 표적으로 한 특정 이용자에게 이메일을 발송하여 비밀번호, 개인정보 등을 입력 받은 뒤 이를 금융사기 등 다른 범죄에 악용함

1. 시스템 해킹 후 위장 홈페이지 준비
2. 피싱 메일 발송
3. 메일 내용에 현혹되어 본문의 링크 클릭
4. 위장 홈페이지에 개인 정보 입력
5. 수집한 개인 정보로 사기

악성 메일 대응하기

피싱 메일(Phishing email)

유명 기업 등 사칭할 기관의 홈페이지와 외관상 똑같은 위장 홈페이지를 사전에 준비한 뒤, 불특정 다수의 인터넷 이용자들 또는 표적으로 한 특정 이용자에게 이메일을 발송하여 비밀번호, 개인[illegible] 사기 등 다른 범죄에 악용함

1. 시스템 해킹 후 위장 홈페이지 제작
2. 피싱 메일 발송
3. 메일 이용자 개인정보 유출 및 탈취
4. 위장 홈페이지에 개인 정보 입력
5. 수집한 개인 정보로 사기

피싱(Phishing)

Private data와 fishing(낚시)의 합성어로서
상대방을 속여서 비밀번호, 금융정보, 개인정보 등
중요 정보를 획득하려는 공격 방법,
이용 수단에 따라 피싱 메일(이메일), 피싱 사이트(웹사이트), 메신저 피싱(메신저), 보이스 피싱(전화), 스미싱(문자메시지)으로 부름

악성 메일 대응하기

사례1. 악성 메일을 기점으로 개인정보 유출, 가상 화폐 출금

사고 경위	범인은 B사의 직원 채용 기간 중에 B사와 자문계약 관계에 있는 A씨에게 악성코드가 포함된 이력서 파일을 첨부한 스피어피싱 메일을 발송하였고, 이를 실행한 A씨의 PC가 해당 악성코드에 감염되어 이를 통해 3만 6천여 명의 고객 개인정보 유출, 260여 계정에서 가상 화폐 출금됨 (B사, 2017년 6월)
회사 영향	• 과징금 4,350만원, 책임자 징계 권고 • 출금된 고객에게 보상 또는 민사소송 대응, 민원 대응을 위한 비용 • 가상화폐거래소에 대한 불안감 확산
원 인	• 임직원 PC에 개인정보를 암호화하지 않은 채 저장 • 외부 인력인 자문계약자에게 회사의 고객 개인정보 전달 & 통제 안됨 • 출금 시 다중 인증을 도입했으나 관리 상 허점 존재
대 책	• 외부자에게 고객정보 전달을 금지하고 및 개인정보 유출방지 대책을 세워요. • 다중 인증이 잘 작동하도록 관리체계를 수립해요. • 임직원 PC에 개인정보 저장을 제한하고 필요한 경우 반드시 암호화한 뒤 저장하도록 해요.

악성 메일 대응하기

특정한 대상을 표적으로 하여, 그 표적이 속을 수 있도록 발신자, 내용, 형식 등을 정교하게 꾸며서 보내는 메일

사례2. 표적 피싱 메일을 통한 무역 대금 사기(1)

사고 경위	범인은 L사의 담당자를 겨냥한 표적 피싱(Spear phishing) 메일을 보내 입금계좌가 바뀌었다고 속여 범인 계좌로 무역대금 240억원을 송금함 (L사, 2016년 3월)
회사 영향	• 240억원 손실(?) - 거래 은행에 소송을 건 뒤 취하 (2017.04.) • 대기업의 역량에 대한 신뢰 저하
원 인	• 거래 상대방 메일 계정이 해킹 됐을 가능성이 있음 • 거래계좌 변경 등 주요한 거래 조건의 변경, 거래 액수가 큼에도 추가 확인 하지 않음
대 책	• 주요 거래조건 변경은 전화, 영상회의 등을 통해 거래 상대방과 직접 소통하여 확인해요.

악성 메일 대응하기

(개인) 악성 메일 예방법

이런 메일 열어보지 마세요!

- 스팸 메일
- 발신자나 제목에서 업무상 필요하지 않은 것이 분명한 메일
- 제목에서 돈을 벌게 해 준다는 등 사람의 호기심이나 궁금증을 자극하는 메일
- 평소 업무와 관계가 없는 관공서나 은행, 기타 기업이나 단체가 보낸 메일
- 가입하지 않은 사이트에서 온 단체 메일

이메일 보안 솔루션이 필요해요!

이런 메일의 첨부 파일 절대 클릭하지 마세요!!

- 메일에 첨부된 실행 파일 (*.exe 등)
- 메일에 첨부 된 압축 파일 (*.zip, *.egg 등)
- 모르는 사람이 보낸 메일에 딸려온 첨부 파일
- 평소 업무와 관계가 없는 관공서나 은행, 기타 기업이나 단체가 보낸 메일의 첨부 파일
- 본인이 요청하지 않은 첨부파일

의심스러운 메일이라도 반드시 확인을 해야 한다면, PC보다는 악성 프로그램이 상대적으로 적은 스마트폰을 사용하는 것이 좋다. 하지만, 스마트폰을 사용하더라도 메일 본문에 있는 링크나 첨부 파일은 클릭하지 말아야 한다.

악성 메일 대응하기

악성 프로그램 예방법

악성 프로그램을 예방하려면 백신 프로그램을 설치하여 적절한 설정을 해서 사용하는 것도 중요하지만, 악성 프로그램이 많이 유포되는 프로그램과 사이트를 이용하지 않는 것이 매우 중요함

1 이런 사이트 방문하지 마세요!

- 파일 또는 콘텐츠 공유 사이트
- 도박 또는 성인 사이트
- 보안이 취약한 소규모 사이트

2 이런 프로그램과 콘텐츠 사용하지 마세요!

- P2P 프로그램
- 불법 동영상 및 불법 콘텐츠

악성 메일 대응하기

악성 프로그램 예방법

3 백신(안티바이러스) 프로그램에서 다음 설정은 꼭 해 주세요!

- 자동 업데이트 : 새로운 악성 프로그램을 탐지할 수 있어요
- 실시간 감시 : 악성 프로그램이 다운로드되면 차단할 수 있어요
- 주 1회 이상 정밀 검사 : 차단되지 않아 PC에 저장된 악성 프로그램을 탐지, 제거할 수 있어요

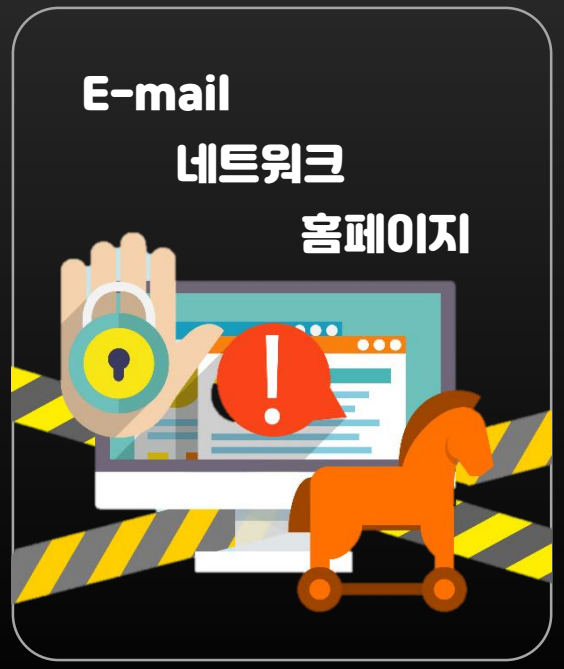
4 악성 메일 예방법은 악성 프로그램 예방법에도 적용돼요!

랜섬웨어 대응하기

랜섬웨어(Ransomware)란?

Ransom(몸값) + Software(소프트웨어)의 합성어로서 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 한 뒤, 이를 인질로 삼아 금전을 요구하는 악성 프로그램

① 여러 경로를 통한 랜섬웨어 감염



② 암호화 대상을 검색하고 파일(문서파일/이미지 등)을 암호화

③ 감염 사실을 알리고 가상 화폐로 복호화 대가 요구

랜섬웨어 대응하기

사례. 미리 알아낸 관리자 계정을 통해 원격접속, 랜섬웨어 배포

사고 경위	범인은 사전에 알아낸 관리자 계정 정보를 이용하여 웹 호스팅 업체의 관리자 PC에 원격에서 접속, 4일 동안 작업을 통해 서버에 랜섬웨어를 설치하고 일시에 랜섬웨어를 작동시켜 서버에 있는 데이터를 암호화하고, 백업 데이터는 삭제함 (I사, 2017년 6월)
회사 영향	• I사가 운영하던 약 5,500개의 고객사 홈페이지가 1달 이상 중단 • 데이터 복호화를 위해 범인과 협상하여 약 13억원 지불 • 일부 복구하지 못한 홈페이지 이용자에게 무료 서비스 등 보상
원 인	• 외부에서 관리자 PC 접속 시 가상사설망에 일회용 비밀번호(OTP) 등 다중 인증 사용하지 않음 • 서버들의 계정 정보가 평문으로 저장됨 • 백업 서버가 항상 서버에 접속되어 있어서 랜섬웨어에 취약
대 책	• 회사 외부에서 내부로 접속할 때에는 반드시 일회용 비밀번호 같은 다중 인증을 사용해요. 가성비 높은 보안 수단이에요. • 백업은 랜섬웨어뿐 아니라 다른 이유로 데이터가 삭제, 훼손되는 데 대응하는 좋은 방법이에요. • 백업 서버나 저장장치는 인증을 통해 접속하거나 백업할 때에만 접속되도록 운영해요.

랜섬웨어 대응하기

(개인) 랜섬웨어 피해 예방 5대 수칙

1. 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.
2. 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.
3. 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.
4. 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.
5. 중요 자료는 정기적으로 백업합니다.

랜섬웨어 대응하기

(개인) 랜섬웨어 피해 예방 5대 수칙

일반 사용자 역시 PC에 있는 사진, 문서 등 중요 파일이 암호화되는 등 랜섬웨어의 피해를 많이 입음

- 랜섬웨어는 악성프로그램의 일종이므로 악성프로그램 예방법과 비슷해요.
- PC에 있는 중요 자료를 외장하드 등 오프라인 매체에 정기적으로 백업해요.
- 백업 또는 복원할 때에만 백업매체를 PC에 접속해요.

랜섬웨어 대응하기

Q 랜섬웨어에 감염되면 어떤 증상이 나타나나요?

A (파일 사용불가)
평소에 잘 쓰던 파일들이 안 열리거나 열려도 이상한 문자로 가득해요.

(확장자 변경)
.txt, .hwp 등 확장자 뒤에 이상한 확장자가 덧붙거나 바뀌어 있어요.
파일 이름이 바뀌기도 해요.

(부팅 불가능)
평소 사용하던 운영체제로 부팅이 안 돼요.

(바탕화면 변경 및 감염 알림 창)
사용자의 파일이 암호화됐고, 이를 복호화하기 위한 비용을 요구하는 알림창이 보여요.

랜섬웨어 대응하기

랜섬웨어 감염됐을 때 이렇게 하세요 - 2가지 방법

- 네트워크 단절
  - 랜섭 뽑기
  - 와이파이 끄기

- 윈도우 재설치
  - 포맷

- 보안 패치 및 백신
  - 윈도우 보안 패치
  - 백신 프로그램 설치

- 백업 자료 존재 시
  - 패치 완료 후 복구

- 데이터 복구 시도
  - 복구 업체 의뢰

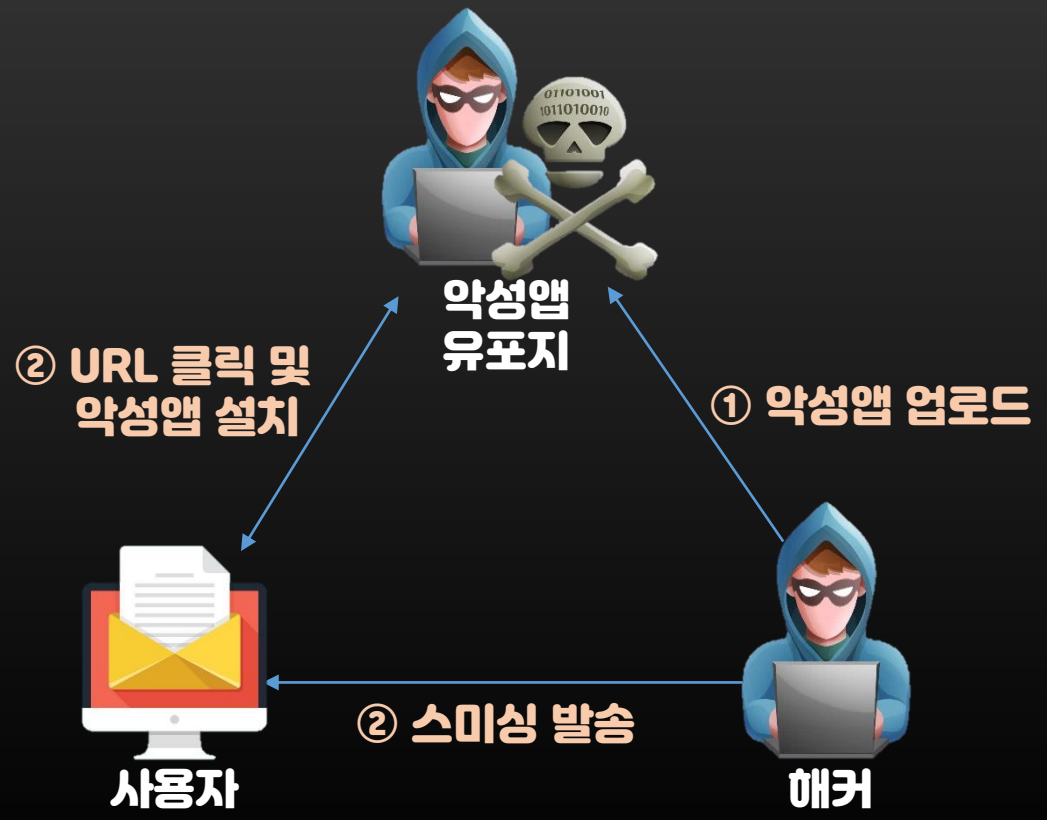
- 직접 복구 시도(권장하지 않음)
  - 해커에게 비용 지불
  - 지불 후에 복구되지 않는 경우 다수
  - 미국(97%), 독일(78%), 영국(42%) 등 대부분 복구 비용을 지불하지 않음

- 랜섬웨어는 예방과 백업이 최고의 대책이에요.
- 감염된 것을 알면 PC 운영체제를 재설치한 다음에 백업했던 자료를 복원해요.
- 복구 업체에서 랜섬웨어로 암호화된 파일을 복구하는 것은 기술적으로 어려워요.

스미싱 대응하기

스미싱(Smishing)이란?

문자메시지(SMS)와 피싱(Phising)의 합성어로 악성 모바일 앱 주소가 포함된 휴대폰 문자(SMS)를 대량으로 전송 후 이용자가 악성 앱을 설치하도록 유도하여 금융정보 등을 탈취하는 사기수법임

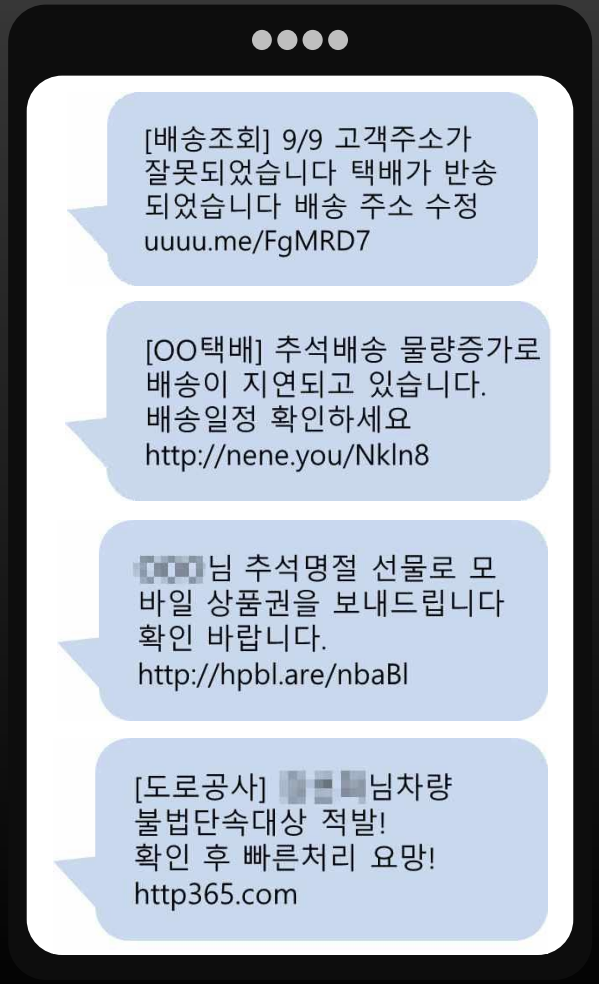


1. 해커가 유포지에 악성 모바일앱을 업로드
2. 불특정 다수에게 악성코드를 설치할 수 있는 인터넷주소가 포함된 문자메시지를 발송
3. 문자를 수신한 사용자가 인터넷주소를 클릭하면 악의적으로 만들어진 피싱 사이트로 접속되거나 악성 앱을 설치하는 설치 파일이 다운로드 됨

스미싱 대응하기

스미싱 문자 사례 및 현황

택배를 사칭한 스미싱이 압도적으로 많으므로 이용자들이 이에 유의할 필요가 있음

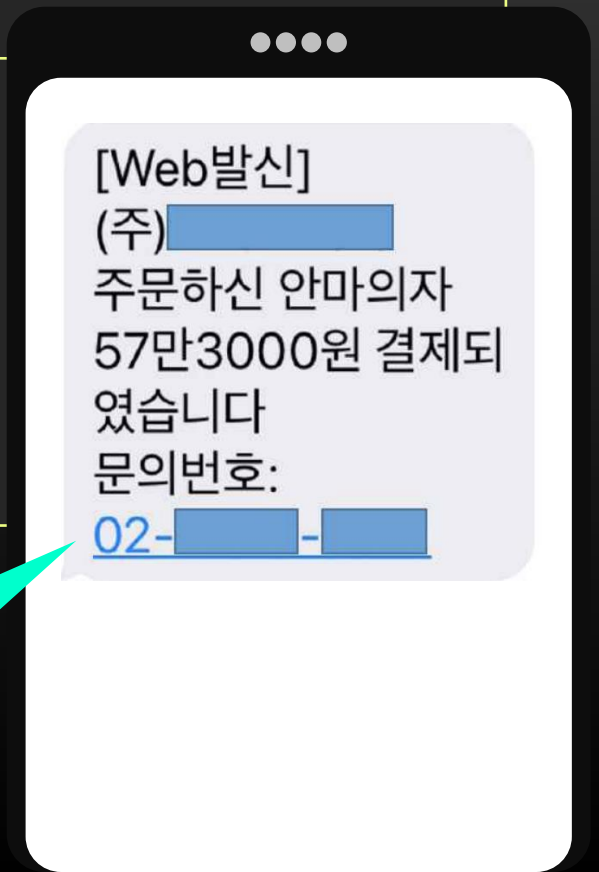


구분	2016	2017	2018	2019(~7월)
택배 사칭	267,274	317,618	191,038	139,645
지인 사칭	17,413	15,080	14,372	34,160
공공기관 사칭	75	6,156	8,549	30
기타	27,149	163,173	28,881	2,385
합계	311,911	502,207	242,840	176,220

스미싱 대응하기

사례. 스미싱과 보이스 피싱을 결합한 금융 사기

사고 경위	사기범은 허위 문자를 받고 연락한 A씨에게 보이스피싱 방식으로 진행. A씨의 은행 계좌 해킹 여부를 점검해 준다는 명목으로 A씨 PC에 원격조종 프로그램을 설치하게 한 후 인터넷뱅킹에 접속하여 A씨에게 각종 인증정보를 직접 입력하게 하여 2천만원 상당의 예금을 편취 (2019년 3월)
대 책	• 출처가 불분명한 문자메시지 링크는 클릭하지 마세요 • 공식 앱스토어에 있는 앱만 설치해요 • (안드로이드) “출처를 알 수 없는 앱 설치”를 차단해요 • 개인정보나 금융정보를 절대(!) 입력하거나 알려주지 말아요 • 모바일 백신 프로그램을 설치해요 • 소액결제를 차단해요 - 통신사 콜센터(114), 앱, 웹에서 쉽게 할 수 있어요



피해자가 받은 허위 결제 문자

스미싱 대응하기

스미싱 피해 발생 시 대응 방법

매우 중요

1 관할 경찰서에 신고하여 사건사고 사실 확인원을 받아요.

2 금융기관 콜센터 전화 : 경찰서에서 발급받은 '사건사고 사실 확인원'을 이동통신사, 게임사, 결제대행사 등 관련 사업자에 제출해서 환불을 요구해요.

3 악성파일 삭제 : 스마트폰 내 '다운로드' 앱 실행 → 문자를 클릭한 시점 이후, 확장자명이 apk인 파일 저장여부 확인 → 해당 apk파일 삭제
※ 삭제되지 않는 경우, 휴대전화 서비스센터 방문 또는 스마트폰 초기화

4 한국인터넷진흥원 불법스팸대응센터(국번없이 118) 신고해요.

스미싱 대응하기

스미싱 피해 발생 시 대응 방법

5 금융 및 증권 등 공인인증서 즉시 폐기 및 재발급 받아요.

6 사용 중인 이동통신사에서 제공하는 스미싱 예방서비스(App 등) 설치해요.

7 주변 지인들에게 스미싱 피해 사실을 즉시 알려 2차 피해 발생을 예방해요.

스미싱 대응하기

스미싱 피해 발생 시 대응 방법

정보통신망법 제58조(통신과금서비스 이용자의 권리 등) 제3항

통신과금서비스 이용자는 통신과금서비스가 자신의 의사에 반하여 제공되었음을 안 때에는 통신과금서비스 제공자(통신사)에게 이에 대한 정정을 요구할 수 있으며(통신과금서비스 이용자의 고의 또는 중과실이 있는 경우는 제외한다), 통신과금서비스 제공자는 이용자의 정정 요구가 이유 있을 경우 판매자에 대한 이용 대금의 지급을 유보하고 그 정정 요구를 받은 날부터 2주 이내에 처리 결과를 알려 주어야 한다.