[정보통신서비스 제공자등을 위한]

개인정보 유출 대응 매뉴얼

2016. 8. 31.

방송통신위원회 KISA 한국인터넷진흥원

◇ 개인정보 유출 대응 매뉴얼은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조제1항제1호(개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행), 같은 법 시행령 제15조제1항, 개인정보의 기술적·관리적 보호조치 기준(방통위 고시) 제3조제6호(개인정보의 분실·도난·누출·변조·훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항)를 기반으로 정보통신서비스 제공자등이 자사의 개인정보가 유출된 사실을 알게 된 후 준수해야 할 조치사항을 안내하고 있습니다.

◇ 정보통신서비스 제공자등은 매뉴얼을 참고하여 자사의 상황에 맞게 「개인정보 유출 대응 매뉴얼」을 마련하고, 내부관리계획에 매뉴얼을 포함하여 보호조치 이행을 위한 세부적인 추진방안을 수립·시행하여야 합니다.

◇ 이 매뉴얼은 유출사고 발생 직후 정보통신서비스 제공자등이 신속한 조치를 통해 개인정보의 추가 유출을 막고, 유출로 인한 이용자 피해를 최소화하기 위한 필수조치를 설명하고 있습니다.

◇ 따라서, 정보통신서비스 제공자등은 평상 시에 개인정보 보호조치 및 웹 취약점 점검 등을 통해 개인정보가 안전하게 보호될 수 있도록 자사의 환경에 맞는 보호조치 수준을 설정하고 유지하여야 합니다.

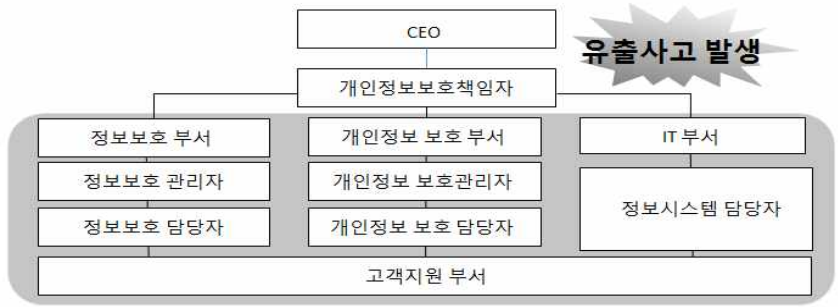
◇ 추가적으로 개인정보 보호와 관련한 규정에 대하여는 「정보통신서비스 제공자를 위한 개인정보보호 법령 해설서」, 「개인정보의 기술적·관리적 보호조치 기준 해설서」 등을 참조해 주시기 바랍니다.

☞ 자료 : 개인정보보호 포털(www.i-privacy.kr) / 자료실 / 안내서 및 해설서

목 차

< 개인정보 유출 대응 절차(요약) >

1 개인정보 유출 신속 대응팀 구성



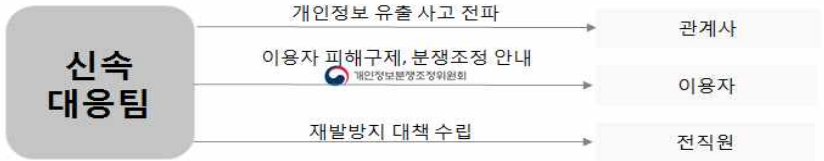
2 유출 원인 파악 및 추가 유출 방지조치

신속 대응팀

- 개인정보 침해사고 접수 및 사실 여부 확인
- 개인정보 유출 사고 원인 파악
- 접근통제, 모니터링 강화
- 유출된 개인정보 회수

3 개인정보 유출 신고 및 통지

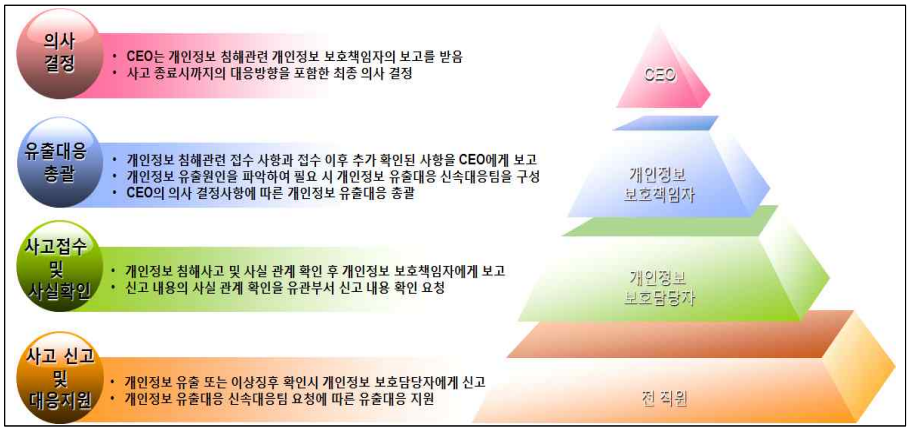
4 이용자 피해구제 및 재발방지 대책 마련



Ⅰ. 개인정보 유출 신속대응체계 구축

◇ 개인정보 유출 사실을 알게 된 경우, 개인정보보호책임자는 **즉시 CEO**에게 **보고**하고 개인정보보호·정보보호 부서를 중심으로 **「개인정보 유출 신속대응팀」**을 **구성**하여, **추가 유출 및 이용자 피해발생 방지**를 위한 **조치**를 강구하여야 함

1. 개인정보 유출사실 CEO 보고



o **(전직원)** 개인정보 유출사실을 발견하거나 의심스러운 정황을 알게된 경우에는 즉시 개인정보보호 담당자에게 전화, 이메일 등으로 신고

o **(개인정보보호 담당자)** 신고를 받은 후 즉시 유출사실을 확인할 수 있는 부서에 유출사실, 규모, 경로 등 확인을 요청하고, 개인정보보호 책임자에게 전화, 이메일 등으로 신속하게 유출사실과 대응상황을 보고

o **(개인정보보호 책임자)** 현재까지 파악된 상황을 CEO에게 신속하게 보고하고 새로운 상황이 발생될 때마다 수시로 보고해야 하며, 개인정보 유출이 확인되면 즉시 「개인정보 유출 신속대응팀」을 소집하여야 함

o **(CEO)** 전체 대응방향을 결정하고 「개인정보 유출 신속대응팀」을 중심으로 유관부서가 유기적으로 대응하여 추가 피해가 발생하지 않도록 지휘

2. 「개인정보 유출 신속대응팀」 구성·운영

o **(구성)** 내·외부 개인정보 유출 사고 발생 시 사고의 분석, 처리, 사후 복구 및 예방 조치 등을 위해 「개인정보 유출 신속대응팀」을 운영

정보통신 서비스제공자 등		
개인정보 유출 신속대응팀	개인정보보호 책임자	· 개인정보 유출 대응 총괄 지휘 · 개인정보 유출대응 신속대응팀 구성·운영
	개인정보보호 담당자	· 유관기관에 개인정보 유출 신고 · 이용자에게 개인정보 유출 통지
	정보보호 담당자	· 유관기관에 침해사고 신고 · 사고경위 분석, 시스템 복구 등 침해대응
	고객지원 부서	· 정부, 언론사, 이용자 민원 대응 · 이용자 피해구제 및 분쟁조정 기구 안내
전직원	· 개인정보 유출 확인 시 부서장 또는 개인정보보호 부서에 신고 · 침해사고 발생 확인 시 부서장 또는 정보보호 부서에 신고 · 개인정보 유출 신속대응팀 요청에 따른 유출대응 지원	

o **(역할)** '개인정보보호책임자'를 중심으로 사업자 내부 조직 및 인력을 효율적으로 재구성하여 유출원인 분석 및 대응, 유출신고·통지, 이용자 피해구제 등 고객지원 등으로 세분화하여 신속히 대응

- 개인정보 유출 관련 사항에 대하여는 CEO에게 보고하여야 함

※ 정보통신망법 제27조제4항 : 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 정보통신서비스 제공자등의 사업주 또는 대표자에게 개선조치를 보고하여야 한다.('16.9.23.시행)

Ⅱ. 유출 원인 파악 및 추가 유출 방지 조치

◇ 개인정보 유출원인을 파악한 후 추가 유출 방지를 위해 **유출 원인 별 보호조치** 실시

1. 해킹의 경우

o **(긴급 조치)** 해킹 등 침해사고 발생으로 인해 개인정보가 유출된 사실을 알게 된 경우에는 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치를 강구하여야 함

- 추가 유출 방지를 위해 시스템 일시정지, 이용자 및 개인정보취급자 비밀번호 변경*, 유출 원인 분석, 기술적 보안조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급조치를 시행하여야 함

  * 일방향 암호화되지 않은 비밀번호가 유출된 경우에는 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해 예방에 노력하여야 함

- 개인정보 유출의 직접·간접적인 원인을 즉시 제거하고, 미비한 보호조치 부분을 파악하여 보완하여야 함

o **(필요시 기술지원 요청)** 기술력 등의 한계로 자체 긴급조치가 어려운 경우 한국인터넷진흥원에 기술지원을 요청할 수 있음

기술지원 내용
▶ 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제·변경 또는 폐쇄 조치 지원
▶ 네트워크, 방화벽 등 대·내외 시스템 보안점검 및 취약점 조치 지원
▶ 향후 수사 등에 필요한 접속기록 등 증거 보존 조치 지원

☞ **참고1 : 해킹에 의한 개인정보 유출 시 조치사항**

2. 내부자 유출의 경우

o 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역을 확인하여야 함

o 개인정보 유출자의 개인정보처리시스템에 대한 접근형태가 정상인지 비정상인지 여부를 확인하고, 비정상적인 접속인 경우 우회경로를 확인하여 접속을 차단하여야 함

o 개인정보취급자의 개인정보처리시스템 접속계정, 접속권한, 접속기록 등을 검토하여 추가적인 유출 여부를 확인하여야 함

o 개인정보 유출에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수하고, 수사기관과 협조하여 유출된 개인정보를 회수하기 위한 모든 방법을 강구하여야 함

3. 이메일 오발송의 경우

o 이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일의 삭제를 요청하여야 함

o 메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 첨부파일 서버 운영자에게 관련 파일의 삭제를 요청하여야 함

4. 개인정보가 외부에 노출된 경우

o **(외부 검색엔진을 통한 노출의 경우)** 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 필요시 로봇배제 규칙을 적용하여 외부 검색엔진의 접근을 차단하여야 함

o **(관리자 페이지에 접속하여 노출된 경우)** 관리자의 접속 IP를 제한하고, 소스코드를 수정하여 사용자 인증 절차를 추가하여야 함

o **(개인정보취급자 부주의로 인한 노출의 경우)** 게시글 및 첨부파일 내 개인정보 노출 부분을 마스킹(* 처리)하여 다시 게시하여야 함

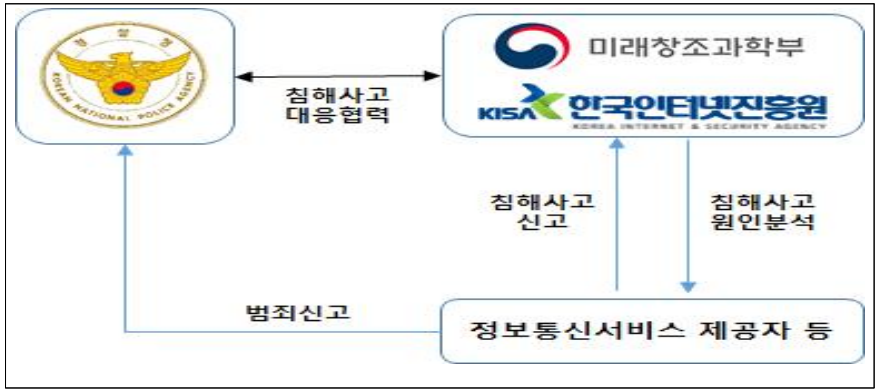
Ⅲ. 개인정보 유출 신고 및 통지

◇ **(신고)** 개인정보 유출사실을 알게 된 경우 **즉시(24시간 이내)** 해커 등 유출자 검거를 위해 **경찰청 사이버안전국**에 **수사 요청**하고, **미래창조과학부·한국인터넷진흥원**에 **침해사고 신고** 및 **방송통신위원회·한국인터넷진흥원**에 **개인정보 유출 신고**

◇ **(통지)** 유출된 개인정보로 추가 피해가 발생하지 않도록 개인정보 유출을 알게 된 후 **즉시(24시간 이내)** 해당 이용자에게 개인정보 **유출사실**을 **통지**

1. 침해사고 신고

<침해사고 대응 체계>

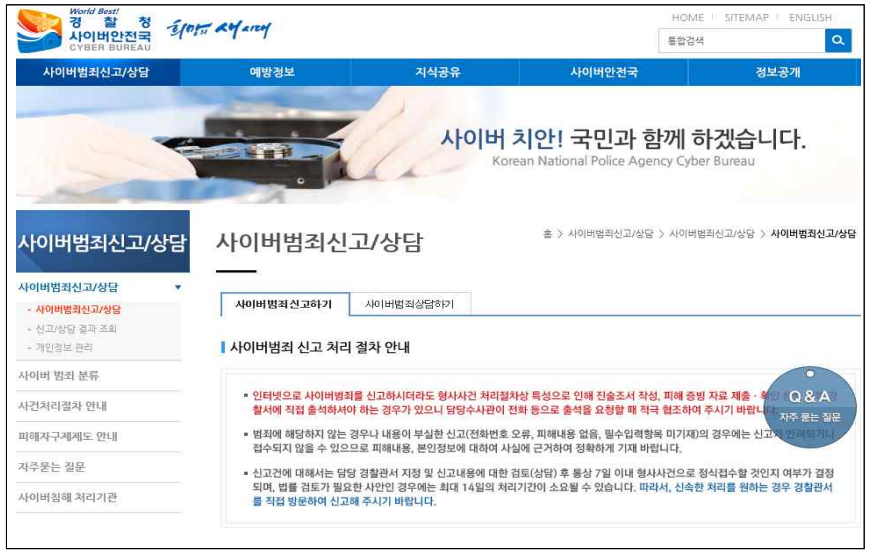


가. 경찰청(사이버 안전국)에 수사 요청

o 개인정보 유출로 인한 피해를 막기 위해서는 해커 등 개인정보 유출자 검거 및 개인정보 회수를 위한 조치가 선행되어야 함

o 따라서, 개인정보 유출사실을 알게 된 경우에는 즉시 경찰청 사이버안전국에 범인 검거를 위한 수사를 요청하고 유출된 개인정보 회수를 위한 조치 실시

※ 사이버범죄 신고 : 경찰청 사이버안전국 / 사이버범죄신고·상담 / 사이버범죄신고하기



나. 미래창조과학부·한국인터넷진흥원(보호나라)에 침해사고 신고

o 인터넷 상 침해사고가 발생하면 즉시 미래창조과학부 또는 한국인터넷진흥원에 신고하여 침해사고 원인분석 및 취약점 보완조치 등을 실시하여야 함

※ 침해사고 신고 : KISA 보호나라 / 상담 및 신고 / 해킹 사고, ☏ 국번없이 118

2. 개인정보 유출 신고

o **(신고 시점)** 개인정보의 유출사실*을 알게 된 경우 즉시(24시간 이내) 개인정보 유출사실을 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 함

* 개인정보보호법(1만건 이상)과는 달리 개인정보 유출 규모와 관계없이 신고하여야 함

- 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 신고하고, 추가로 확인되는 내용은 확인되는 즉시 신고

※ 구체적 사실관계 파악을 이유로 신고를 지연하는 경우에는 3천만원 이하의 과태료가 부과될 수 있음

o **(신고 항목)** 개인정보 유출 신고를 할 때에는 ① 유출된 개인정보 항목, ② 유출이 발생한 시점, ③ 이용자가 취할 수 있는 조치, ④ 정보통신서비스 제공자등의 대응조치, ⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처를 명시하여야 함

신고 항목	유의사항
① 유출된 개인정보 항목	· 유출된 개인정보 항목을 모두 기재해야 하며, '등'과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 '전화번호'로 기재하여서는 안됨 · 유출된 개인정보의 모든 항목을 적어야 하며, 유출 규모도 현 시점에서 파악된 내용을 모두 작성
② 유출이 발생한 시점	· 유출시점, 인지시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출경위와 인지경위를 작성해야 함
③ 이용자가 취할 수 있는 조치	· 개인정보 유출로 발생 가능한 스팸 문자, 보이스 피싱, 금융사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재(예: 비밀번호 변경 등)
④ 정보통신서비스 제공자등의 대응조치	· 유출사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재 ex) 경찰에 신고, 일시적 홈페이지 로그인 차단(홈페이지 해킹일 경우) 등
⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처	· 실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재
⑥ 기타	· 유출된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 기재

o **(신고 방법)** 방송통신위원회와 한국인터넷진흥원이 운영 중인 "개인정보보호 포털"(www.i-privacy.kr)*을 통해 해당 시점까지 확인된 내용을 중심으로 신고

- 전화, 팩스, 이메일, 우편 등의 방법을 이용하는 경우에는 정확한 신고 접수 여부를 반드시 확인하여야 함(신속한 신고-접수를 위해 "개인정보보호 포털" 활용)

* 유출 신고 : 개인정보보호 포털 / 개인정보 신고 / 개인정보 누출 신고 / 사업자

<개인정보 유출 및 침해사고 신고 경로>

구 분		전화번호	팩스번호	전자우편주소	인터넷 사이트
한국인터넷진흥원	개인정보 유출	118	02-405-5229	118@kisa.or.kr	www.i-privacy.kr
	침해사고				www.krcert.or.kr

☞ **참고2 : 개인정보 유출 신고서 양식**

3. 개인정보 유출 통지

o **(통지 시점)** 개인정보 유출시 침해사실을 인지한 시점으로부터 즉시(24시간 이내) 개인정보 유출사실을 이용자에게 통지하여야 함

- 온라인의 경우 유출된 개인정보의 확산 속도가 빨라 피해가 가중될 수 있으므로 먼저 파악한 유출사실을 신속하게 통지하여 추가 피해를 방지하는 것이 중요함

- 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 개별 통지하고, 추가로 확인되는 내용에 대해서는 확인되는 즉시 개별 또는 홈페이지를 통해 신속히 통지하여야 함

  ※ 구체적 사실관계 파악을 이유로 이용자 통지를 지연하는 경우에는 3천만원 이하의 과태료가 부과될 수 있음

- 유출된 개인정보가 대규모여서 24시간 이내에 전체 통지가 기술적으로 불가능한 경우에는 우선적으로 홈페이지 팝업창 등을 통해 방문하는 이용자가 모두 알 수 있도록 현재까지 파악된 유출사실을 게시한 후 개별 통지를 병행하여야 함

  ※ 개인정보가 유출된 이용자가 유출사실을 신속히 인지한 후 대비할 수 있도록 가능한 모든 방법을 병행하여야 함

☞ **잘못된 대응사례①**

o OO사는 이상 징후를 인지하고 5일 후, 개인정보 유출사실을 확인하고 2일 후부터 유출 통지를 실시함

o 침해사고로 추정되는 이상 징후를 알게 된 경우에는 즉시 미래창조과학부·한국인터넷진흥원에 침해신고를 하여야 하고, 개인정보가 유출된 사실을 알게 된 경우에는 24시간 이내에 해당 이용자에게 유출 통지를 이행하여야 함

☞ **잘못된 대응사례②**

o OO사는 해커에 의해 개인정보가 유출된 사실을 확인한 후 경찰청에 신고하였으나, 수사관으로부터 해커가 검거될 때까지는 유출 통지를 유보해 달라는 구두 요청을 받고 30일 이상 통지를 지연

o 해커 검거를 통해 유출된 개인정보를 회수하기 위해 반드시 필요한 경우로서 경찰청으로부터 공식 문서로 반드시 필요한 최소한의 기간 동안 유출통지 보류를 요청받은 경우에는 방송통신위원회에 유출 신고 후 협의하여야 하고 사유를 소명하여야 함

o **(통지 대상)** 개인정보가 유출된 사실을 알게 된 경우에는 유출된 이용자 수, 유출된 개인정보의 유형에 관계없이 유출 통지 절차를 운영하여야 함

☞ **잘못된 대응사례①**

o OO사는 개인정보 유출을 알게 된 후 유출된 이용자를 대상으로 유출통지를 실시하였으나, '아이디', '아이디+일방향 암호화된 비밀번호'만 유출된 이용자에 대하여는 별도의 통지절차를 이행하지 않음

o 유출된 개인정보의 유형이 '아이디+비밀번호'만이더라도 별도 분리 보관되어 있는 연락처 정보 등을 활용하여 유출 통지를 진행해야 하고, 연락처가 없는 경우에는 홈페이지를 통해 30일 이상 게시하여야 함

☞ **잘못된 대응사례②**

o OO사는 개인정보취급자가 업무상 e-메일을 보내면서 붙임 파일로 이용자 10여명의 인적사항이 담긴 파일을 다른 사람에게 잘못 보냈으나, 해당 파일에 담긴 이용자에게 별도의 유출 통지절차를 이행하지 않음

o 정보통신망법 제27조의3의 규정은 유출된 경우이면 그 수량과 관계없이 통지·신고하여야 함

o **(통지 방법)** 통지를 할 때에는 이용자가 실제로 확인 가능하도록 이용빈도가 높은 방법*을 우선 활용하여 통지하는 것이 바람직함

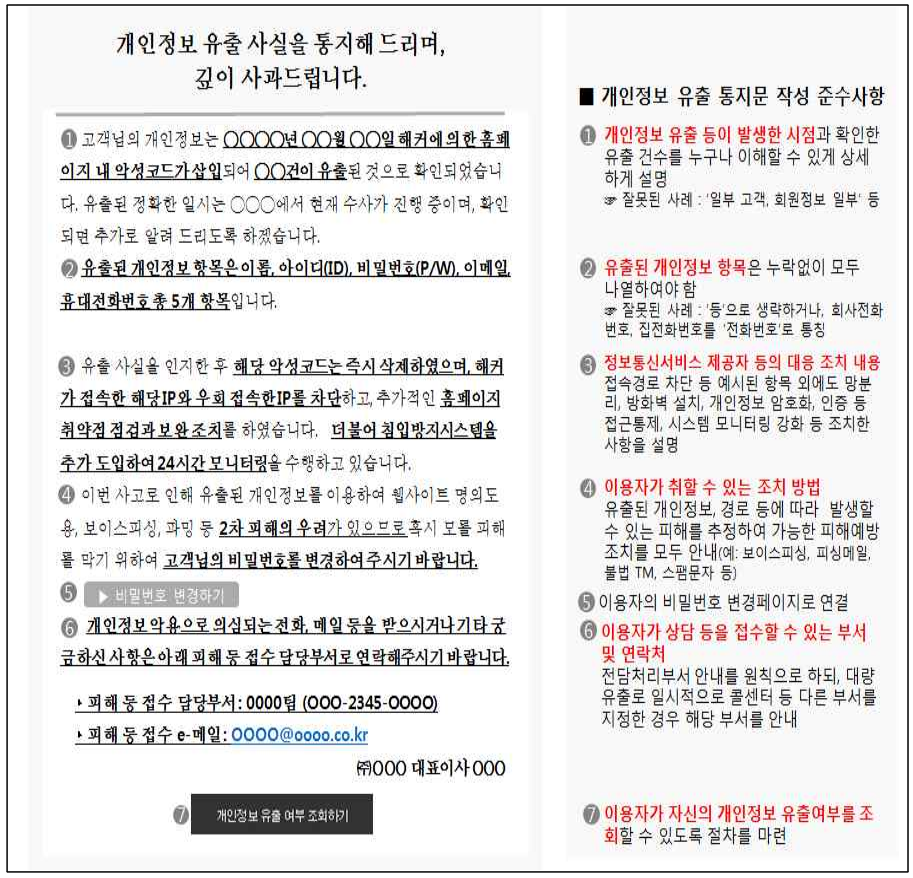
  ※ (예) 휴대전화번호를 보유하고 있는 경우에는 전화통화 및 문자를 통해 우선 통지하고, 곤란한 경우에는 이메일, 팩스, 우편 등의 방법을 활용

- 이용자의 연락처를 알 수 없는 등 정당한 사유가 있어 통지가 불가능한 경우에는 자신의 인터넷 홈페이지에 30일 이상 게시하여 접속하는 이용자가 알 수 있도록 유지하여야 함

  ※ 홈페이지에 게시할 때에는 '사과문', '개인정보 유출 안내' 등의 제목을 사용하되, 법정 통지사항이 모두 포함되어야 함

- 천재지변이나 그 밖에 정당한 사유로 홈페이지 게시조차 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고하여야 함

<홈페이지 개인정보 유출 통지문(예시)>



개인정보 유출 사실을 통지해 드리며,
깊이 사과드립니다.

❶ 고객님의 개인정보는 ○○○○년 ○○월 ○○일 해커에 의한 홈페이지 내 악성코드가 삽입되어 ○○건이 유출된 것으로 확인되었습니다. 유출된 정확한 일시는 ○○○에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.

❷ 유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호 총 5개 항목입니다.

❸ 유출 사실을 인지한 후 해당 악성코드는 즉시 삭제하였으며, 해커가 접속한 해당IP와 우회 접속한IP를 차단하고, 추가적인 홈페이지 취약점 점검과 보완조치를 하였습니다. 더불어 침입방지시스템을 추가 도입하여 24시간 모니터링을 수행하고 있습니다.

❹ 이번 사고로 인해 유출된 개인정보를 이용하여 쉽사이트 명의도용, 보이스피싱, 파밍 등 2차 피해의 우려가 있으므로 혹시 모를 피해를 막기 위하여 고객님의 비밀번호를 변경하여주시기 바랍니다.

❺ ▶ 비밀번호 변경하기

❻ 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나기타 궁금하신사항은아래 피해 등 접수 담당부서로 연락해주시기 바랍니다.

‣ 피해 등 접수 담당부서: 0000팀 (000-2345-0000)
‣ 피해 등 접수 e-메일: 0000@oooo.co.kr

㈜000 대표이사 000

❼ 개인정보 유출 여부 조회하기

■ 개인정보 유출 통지문 작성 준수사항

❶ 개인정보 유출 등이 발생한 시점과 확인한 유출 건수를 누구나 이해할 수 있게 상세하게 설명
☞ 잘못된 사례 : '일부 고객, 회원정보 일부' 등

❷ 유출된 개인정보 항목은 누락없이 모두 나열하여야 함
☞ 잘못된 사례 : '등'으로 생략하거나, 회사전화번호, 집전화번호를 '전화번호'로 통칭

❸ 정보통신서비스 제공자 등의 대응 조치 내용
접속경로 차단 등 예시된 항목 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명

❹ 이용자가 취할 수 있는 조치 방법
유출된 개인정보, 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예: 보이스피싱, 피싱메일, 불법 TM, 스팸문자 등)

❺ 이용자의 비밀번호 변경페이지로 연결

❻ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내

❼ 이용자가 자신의 개인정보 유출여부를 조회할 수 있도록 절차를 마련

o **(유출 확인절차 마련)** 홈페이지 등을 통해 개인정보 유출사실을 확인할 수 있는 절차를 마련하여 운영하는 것이 바람직함

- 홈페이지 구성 시에는 확인 과정에서 추가적인 개인정보 유출이 발생하지 않도록 웹 취약점을 제거한 후 운영하고, 전송구간 암호화(보안서버 구축 등)를 이행하는 등의 조치를 하여야 함

- 본인확인을 명목으로 주민등록번호를 입력하도록 유도하는 것은 인터넷 상 주민번호 사용 제한에 반할 수 있음을 유의해야 함

☞ **잘못된 대응사례**

o ○○사는 개인정보 유출을 알게 된 후 자사 홈페이지를 통해 이용자가 자신의 개인정보가 유출되었는지 여부를 확인하는 페이지를 운영하였으나,

– 본인확인을 위해 이름과 주민등록번호를 입력하도록 하고, 전송구간 암호화 조치를 취하지 않음

o 본인확인을 위해 유출된 정보를 입력하도록 하는 것과 개인정보와 인증정보 전송구간 암호화 조치를 하지 않은 경우 추가적인 개인정보 유출의 위험이 발생할 수 있으므로,

– 유출 확인 페이지를 운영할 때에는 **주민등록번호를 활용하지 않도록 하고, 전송구간 암호화 조치(보안서버 구축 등)**를 반드시 이행하여야 함

Ⅳ. 이용자 피해구제 및 재발방지 대책 마련

◇ 이용자 피해구제 방법을 안내하고, 유사 사고의 재발방지를 위해 대책 마련

1. 개인정보 유출 사고 전파

o 개인정보 침해 발생을 인지한 경우 임직원 및 이해관계가 있는 사업자에게 개인정보 유출 상황을 전파하여 유사 피해가 발생할 수 있음을 전파하여야 함

o 전파 시에는 한국인터넷진흥원과 협의를 통해 기 구축되어 있는 사업자 핫라인을 활용

2. 이용자 피해구제 관련 민원 대응 강화

o 이용자 개인정보 유출 문의에 신속히 대응할 수 있도록 스크립트와 유출통지문을 작성하고 필요시 이용자 상담 회선을 증설

o 전화, 이메일, 홈페이지, SNS 등 다양한 채널을 통해 이용자의 개인정보 유출사실, 유출경위를 확인할 수 있는 창구를 마련

o 이용자에게 피해 발생에 따른 구제절차를 안내하고, 이용자의 요청이 있는 경우에는 별도의 "개인정보 유출 확인서" 발급 절차를 운영

- **(개인정보 분쟁조정위원회)** 개인정보보호위원회에 설치되어 있는 개인정보 분쟁조정위원회를 통해 개인정보 유출에 따른 분쟁조정 절차가 있음을 안내

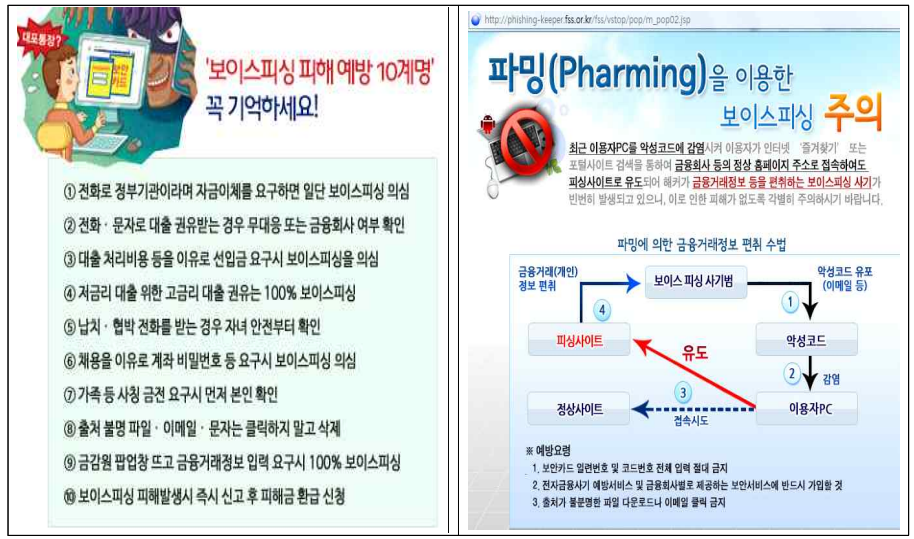
  ☞ 홈페이지(www.kopico.go.kr) 및 분쟁조정위원회에 우편(03171 서울특별시 종로구 세종대로 209 정부서울청사 4층 개인정보 분쟁조정 위원회) 또는 FAX(02-2100-2485) 이용

- **(손해배상제도 안내)** 법정손해배상제도, 징벌적 손해배상제도 등 민사소송을 통해 피해구제 절차를 진행할 수 있음을 안내

  ☞ 참고3 : 개인정보 유출에 따른 2차 피해 유형 및 대응요령 안내

o 이용자에게 개인정보 유출로 인해 보이스피싱, 파밍 등 추가 피해가 발생할 수 있으므로 피해 방지를 위한 유의사항을 안내

- 금융감독원과 경찰청에서 합동으로 운영 중인 보이스피싱 지킴이 홈페이지의 대처요령, 을 참조하여 안내



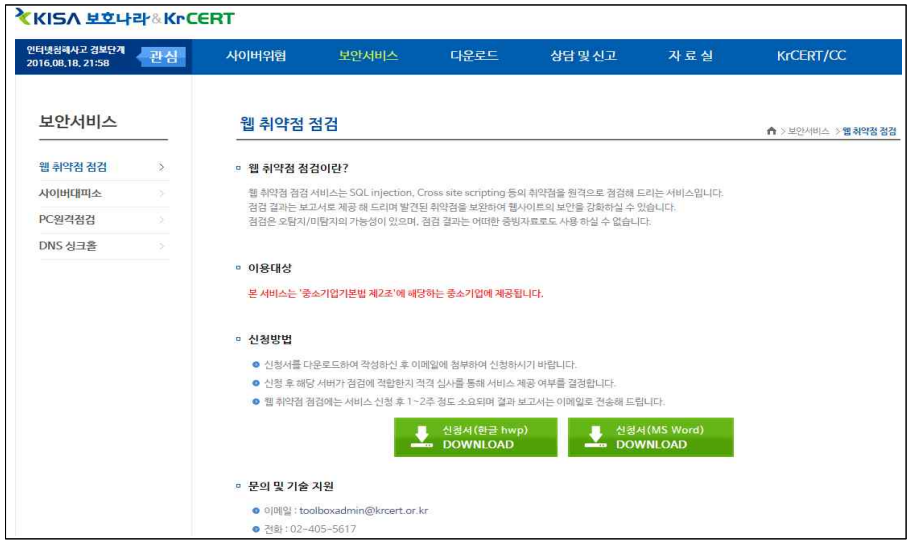
3. 유출 원인분석 및 재발방지 대책 마련

o 개인정보 유출 원인에 맞는 대책을 마련하고, 유사 사고 재발 방지를 위해 개인정보보호 교육을 실시하여야 함

o 개인정보 유출사고 시나리오 작성 및 모의훈련을 실시하여 개인정보 유출 대응체계를 점검

o 홈페이지의 취약점을 연 1회 이상 정기적으로 점검하여야 하며, 중소기업의 경우에는 한국인터넷진흥원에서 제공하는 웹 취약점 점검 서비스를 이용할 수 있음

※ 웹취약점 점검 신청 페이지 : KISA 보호나라 → 보안서비스 → 웹취약점 점검



o 유출사고 취약점을 반영하여 전사적으로 개인정보 취급자 대상 개인정보보호 및 정보보호 인식 제고 교육을 실시

※ 개인정보 교육 페이지 : KISA 개인정보보호 포털 / 개인정보보호교육 / 온라인 교육 / 사업자 대상

o 개인정보가 인터넷 상에 노출되는 것을 방지하기 위해 검색엔진의 로봇배제 규칙을 적용하여 홈페이지 접근을 제한하고,

- 홈페이지에 첨부파일을 포함한 게시글 작성시 개인정보 포함여부를 확인하여야 하며,
- 이용자에게 게시글 작성시 개인정보가 노출되지 않도록 주의할 것을 안내하고,
- 관리자 페이지에 접근하는 IP제한 또는 VPN 등 안전한 접속수단을 사용하여야 함

<로봇배제 규칙 예시>

참고 1 해킹에 의한 개인정보 유출 시 조치사항

□ 해커가 삽입한 악성코드 확인 및 삭제

o 한국인터넷진흥원에서 배포중인 '휘슬'을 활용하여 웹서버에 삽입된 악성코드와 웹쉘 파일을 찾아서 삭제

※ 악성코드 탐지도구 제공 페이지 : KISA 보호나라 → 다운로드 → 휘슬 / 캐슬

□ 침해 발생 시스템의 계정, 로그 등을 점검하여 침해 현황 확인

점검 항목	점검 내용	비고
계정	· 사용하지 않는 계정 및 숨겨진 계정 확인 - 윈도우 : [관리도구]→[컴퓨터 관리]→ [로컬사용자 및 그룹]→[사용자] 정보 확인 - 리눅스 : /etc/passwd 확인	· $ 문자가 포함된 계정 확인 · 패스워드 미설정 계정 확인 · /bin/bash 설정 계정 확인
로그파일	· 이벤트 로그 및 시스템 로그 변조 유무 확인 - 윈도우 : [관리도구]→[컴퓨터 관리]→ [이벤트뷰어] 확인 - 리눅스 : /var/log/secure, message 등 확인 · 윈도우 웹로그 경로 및 변조 유무 확인 - [관리도구]→[인터넷정보서비스(IIS)관리]에서 · 리눅스 웹로그 경로 확인 - /usr/local/apache/logs 확인	· 웹로그 생성/수정 시간 확인
웹쉘	· 확장자별 웹쉘 패턴 점검 - asp, aspx, asa, cer, cdx, php, jsp, html, htm, jpg, jpeg, gif, bmp, png	· 휘슬 사용
백도어	· 네트워크 상태 확인 - nmap -sV 침해사고시스템IP · 비정상 포트 및 외부연결 확인 - 윈도우 : netstat, TCPView 등 사용 - 리눅스 : netstat -nlp, lsof -i	· 6666, 6667 등 의심 Port 확인 · 의심 Port를 사용하는 프로세스 확인
루트킷	· 숨겨진 프로세스 및 비정상 프로세스 확인 · 변조된 파일 및 시스템 명령어 확인 - Windows : IceSword, GMER 등 사용 - Linux : Rootkit Hunter, Check Rootkit 등 사용	· Rootkit Hunter 업데이트 필수

□ 로그분석 결과에 따른 접속경로 차단 등

o 로그 분석 결과 침입자 접속경로가 확인된 경우 접속경로를 차단하고 경유한 시스템은 추가적인 분석

구분	접속 경로 차단 방법	비고
서버	· 윈도우 [제어판]→[Windows 방화벽]→[일반]방화벽 사용→[예외]→원격데스크톱→편집→범위변경→사용자 지정 목록 설정(허용할IP)	특정 IP에 원격데스크톱 서비스를 허용하고 나머지 IP접속은 차단
	· 리눅스 iptables -A INPUT -p TCP --dport 22 -s 허용할IP -j ACCEPT iptables -A INPUT -p TCP --dport 22 -s -j DROP	특정 IP에 ssh 서비스를 허용하고 나머지 IP접속은 차단
네트워크	· 방화벽/라우터/스위치 access-list 101 permit tcp 허용할IP host 접근서버IP eq 22 interface ethernet 0 ip access-group 101 in	특정 IP에 ssh 서비스 허용정책을 ethernet 0 인터페이스에 인바운드 정책 적용

□ 기타 조치사항

o 서버, PC 등 정보처리시스템의 백신을 최신으로 업데이트하고 전체 디렉토리를 점검

o 직원 PC의 운영체제, 오피스 프로그램의 보안 업데이트를 실시

o 가능한 경우 침해사고 원인을 식별하고 재발방지를 위해 개인정보 유출 시스템의 휘발성 및 비활성 정보 수집

- 기술적인 사항은 한국인터넷진흥원이 배포하는 「침해사고 분석절차 안내서」 참조

※ 제공 페이지 : 한국인터넷진흥원 / 자료실 / 관련법령·기술안내서 / 기술안내 가이드 / 침해사고 분석절차 안내서

o 수사시관과 협조하여 유출된 개인정보를 회수하기 위한 조치를 강구

참고 2 개인정보 유출 신고서 양식

☞ 내려받기 : 개인정보보호 포털(www.i-privacy.kr/개인정보유출신고/신고안내/서면신고)

사업자 개인정보 유출 신고서

(필수)가 표시되어있는 항목을 꼭 기재 부탁드리며, 부족한 내용이 있을 경우 연락이 갈 수 있습니다.

기관명**(필수)**		사업자번호**(필수)**	
사업자주소 (사업자등록기준)		웹 사이트 주소	
누출된 개인정보의 항목 및 규모**(필수)**			
누출이 발생된 시점, 누출 인지 시점 및 경위**(필수)**			
이용자가 취할 수 있는 조치**(필수)**			
정보통신서비스 제공자등의 대응조치**(필수)**			

이용자가 상담 담당부서·담당자 및 연락처**(필수)**		성명	연락처	이메일
	개인정보 보호책임자			
	개인정보 보호담당자			

※ 하단은 접수기관에서 기재하는 부분이므로 신고자는 기재하실 필요가 없습니다.

신고접수 기관	기관명(지역)	접수자명	연락처	이메일	접수일자

참고 3 개인정보 유출에 따른 2차 피해 유형 및 대응요령

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
금전적	온라인 사기쇼핑	주민등록번호, 카드번호, 유효기간 등	① 카드번호, 유효기간으로 온라인 결제가 가능한 국내외 홈쇼핑 사이트에 접속 ② 홈쇼핑 홈페이지, ARS를 통한 온라인 사기 결제·주문	• 신용카드 정지 및 재발급 신청 ※ 신고기관 : 각 카드사, 한국소비자원 소비자 상담센터(☏1372) 등
	명의도용을 통한 통신서비스 가입	이름, 주소, 주민등록번호 등	① 유출된 개인정보를 이용하여 휴대전화, 인터넷전화 등 가입 ※ 통신서비스 가입 시 본인확인절차가 있으므로 주민등록증 위조 등 추가적인 불법 행위 수반이 예상됨 ② 불법 가입한 전화번호로 스팸을 발송하여 금전적 이익을 취득함 ※ 명의를 도용당한 사람은 서비스 이용제한을 당하거나 명의도용 소명절차를 밟는 등 피해를 당함	• 한국정보통신진흥협회(KAIT)의 명의도용방지서비스(M-Safer)를 통한 불법 통신서비스 신규가입 여부 확인 ※ 신고기관 : 통신민원조정센터(msafer.or.kr) ※ 명의도용방지서비스(M-Safer) : 통신서비스 신규가입시 이메일·문자로 가입여부 통보
	명의도용을 통한 신용카드 복제	이름, 신용카드 번호, 유효기간 등	① 유출된 개인정보를 이용하여 신용카드 불법 복제 ※ 특수장비를 이용하여 카드번호, 유효기간, 이름 등으로 복제 가능	• 신용카드 정지 및 재발급 신청, 이용내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☏1332)

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			② 불법 복제된 카드를 국내외에서 활용하여 상품 결제 등에 악용 ※ 국내외 POS단말기의 경우 마그네틱 부분만을 이용하여 결제 가능	
	스미싱	휴대전화번호	① '정보유출 확인 안내' 등 금융기관을 사칭하는 문자메시지에 악성코드(인터넷주소)를 삽입하여 발송 ② 금융기관 사칭 메시지를 받은 피해자가 인터넷주소(URL)를 클릭하면 악성코드에 감염되어 소액결제 피해 및 개인·금융정보 탈취	• 수상한 문자메시지 삭제 및 메시지 상 링크 클릭하지 않기 또는 카드사 공지 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
비금전적	보이스피싱	신용카드번호, 휴대전화, 집전화번호, 집주소 등	① 경찰, 금융감독당국 또는 금융회사 직원을 사칭하여 전화 ② 금융관련 업무 목적 사칭을 통한 개인정보·금융정보 탈취(비밀번호, 보안카드번호 등) ③ 유출된 금융사를 사칭, 개인정보 유출 확인을 빙자하여 ARS를 통해 계좌번호/비밀번호 등 금융정보 입력 요청	• 수상한 전화 거부 및 각 카드사에서 공지한 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름, 이메일	• e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십 여개의 웹사이트 가입하여 개인정보 불법 이용	※ 신고기관 : 경찰, 불법스팸대응센터(☎118) ※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가
	휴대전화/이메일 스팸발송	휴대전화 번호, 이메일 주소 등	① 유출된 개인정보를 이용해 불특정 다수에게 스팸 발송 ※ 유출된 모든 휴대전화, 이메일로 도박 등 스팸 무작위 발송 가능 ※ 신용정보, 연소득등 활용 대출 스팸 발송, 자동차 보유여부를 활용한 보험 스팸 발송 등 특정유형의 개인에 대한 타겟 마케팅 가능 ② 휴대전화, 이메일 서비스 이용자는 원치 않는 홍보·마케팅 광고 수신	• 지능형 스팸차단서비스를 이용한 스팸 차단, 수신 스팸 적극 신고 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118) ※ 지능형 스팸차단서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단해주는 서비스
	사회공학적 기법을 활용한 악성코드 유포메일 발송	이메일주소 등	① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도 URL이 포함된 이메일 발송 ② 수신자들이 이메일에 포함된 첨부파일 및 URL을 클릭 ③ 해커가 수신자의 PC를 장악하여 기밀 및 개인정보를 빼냄	• 의심가는 이메일을 받은 경우 함부로 열람하지 않고 바로 삭제 • 사용자 PC의 바이러스 백신을 항상 최신버전으로 유지 및 정기적 검사 수행 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118)