『2018년 정보보안 및 개인정보보호 교육 자료』

전직원이 실천할 수 있는
정보보안 및 개인정보보호

2018. 12.

서울교통공사

정보보안처

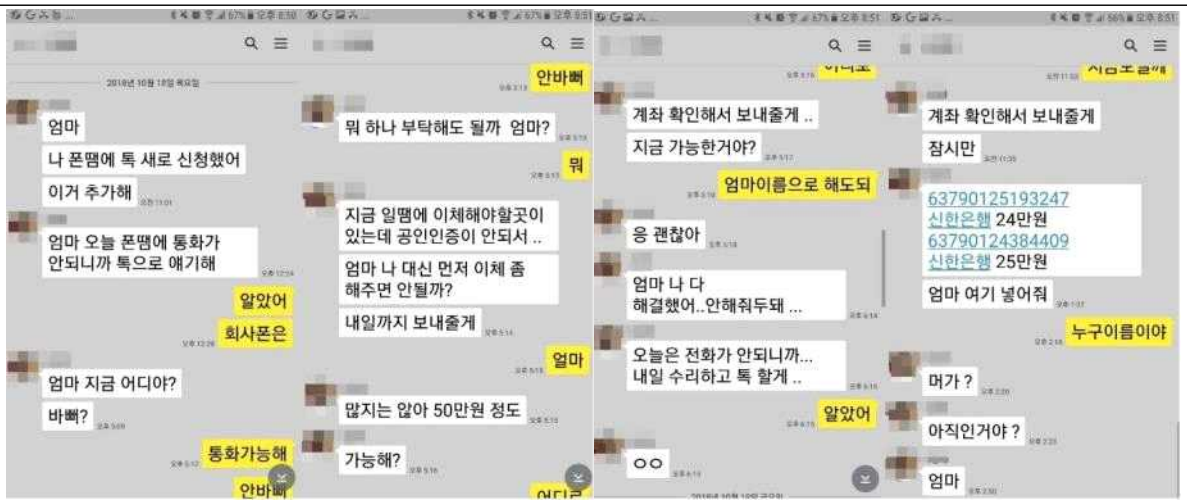
Ⅰ. 정보보안

1. 최신 사이버 공격 유형

✔ 카카오톡 피싱(지인사칭)

“오빠, 급하게 돈 좀ㅠㅠ” ‘카톡 피싱’ 안 당하려면?
중앙일보 | 입력 2018.11.11 15:41

카카오톡에서 가족이나 지인을 사칭해 대화하면서 돈을 보내 달라고 하는 ‘메신저 피싱’ 범죄가 기승이다. 메신저 피싱은 메신저 아이디(ID)를 도용해 지인을 사칭하고 카카오톡·네이트온 등 대화창을 통해 돈을 요구해 가로채는 수법을 일컫는다. (생략)



〈실제 카카오톡 피싱 내용〉

대 처 방 안	① 지인이 메신저로 돈을 요구할 시 직접 통화하기 ② 주소록 연동 되어있는 계정 2차 인증 로그인 설정(ex. 핸드폰 인증)

✔ 크립토재킹

PC 6천대 감염시켜 가상화폐 채굴 동원…'크립토재킹' 첫 적발
'크립토재킹' 국내 첫 적발…경찰, 20대 일당 4명 입건
연합뉴스 | 2018-11-08 12:00

(생략) 작년 10월부터 12월까지 온라인 구인구직 사이트에서 기업체 인사담당자 등의 이메일 아이디 3만2천435개 계정을 수집, 악성코드를 탑재한 메일을 보내 PC 6천38대를 감염시킨 뒤 가상통화 채굴에 이용한 혐의를 받는다. (생략)

크립토재킹이란 암호화폐를 뜻하는 크립토커런시(Cryptocurrency)와 납치를 뜻하는 하이재킹(Hijaking)을 합친 신조어로 **사용자의 PC나 스마트폰에 악성코드를 심어 CPU나 GPU를 사용자 모르게 암호화폐(가상화폐) 채굴에 이용하여 부당이득을 취하는 공격**을 말한다.

대 처 방 안	① 출처가 불분명한 메일에 있는 첨부파일 혹은 링크 접근 지양 ② 검증되지 않은 파일 실행 전 백신프로그램 활용 악성 여부 검사 ③ 출처가 불분명한 앱 설치 지양 ④ 지나치게 많은 권한 혹은 서비스와 관련 없는 권한을 요구하는 앱 설치 지양

2. 전직원이 실천할 수 있는 정보보안

가. 안전한 비밀번호 설정하기

국가 정보보안 기본지침 제39조(비밀번호 관리)

③ 비밀번호는 다음 각 호 사항을 반영하여 **숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기별로 1회 이상 주기적으로 변경 사용**하여야 한다.

- PC부팅 비밀번호(1차), 윈도우 비밀번호(2차), 보안USB 비밀번호(3차) 설정
- 최대 90일 사용(분기별 변경)
- 비밀번호 부여 원칙 준수
  - 숫자, 영문, 특수문자 혼합 9자리 이상
  - '내 패스워드는 얼마나 안전한가?' 확인하는 방법
    · https://howsecureismypassword.net/ 에 접속하여 패스워드 입력하면 크래킹 (무작위 대입으로 패스워드를 찾아내는 방법) 시간을 확인할 수 있다(참고)

[접속시 메인화면]

[패스워드 입력시 크래킹 시간 확인가능]

나. Windows 방화벽 설정하기

- 제어판 > 모든 제어판 항목 > Windows 방화벽 > [권장 설정 사용] 버튼 클릭

[Windows 방화벽 설정 전]

[Windows 방화벽 설정 후]

다. 사이버보안진단의 날 참여하기(매달 세 번째 수요일)

- 내PC지키미 실행(취약점 제거) 후 결과 등록
  · 등록메뉴 : 메트로넷 > 업무시스템 > 일반관리 > 공통(사이버보안)

라. 전자메일 열람 시 주의하기

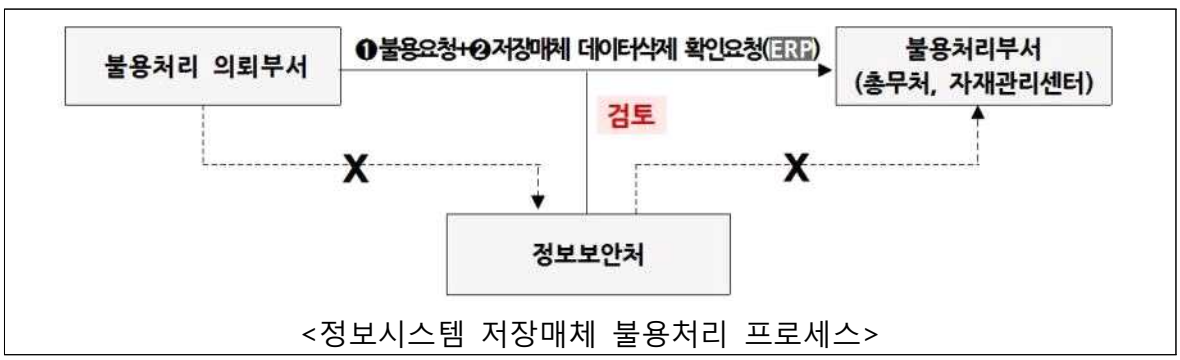
- 모르는 사용자로부터의 메일 열람 주의
- 첨부파일 열람 주의(각종 바이러스/랜섬웨어 주요 감염 경로)
  - 특히 확장자가 .exe인 파일(실행파일)은 각별한 주의 요망
- 분기별 실시중인 해킹메일 훈련 적극 참여

마. 업무용 컴퓨터 철저히 관리하기

- 개인소유의 PC를 업무용으로 사용금지
- 결재권자 인가 없이 임의로 업무용 컴퓨터 반출입 금지
  - 업무용 컴퓨터 반출입시 전산장비 반입·반출대장(정보보안처리규정 별지 제5호 서식) 작성
- 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제

바. 정보시스템 자산 불용 시 데이터 삭제(파기)하기

- 저장매체 데이터삭제(파기) 후 ERP 불용요청 시 관련 증빙자료 첨부



<정보시스템 저장매체 불용처리 프로세스>

- **1차 결재선** :

결재라인 추가

기안자(요청) → 해당 소속장(검토) → **정보보안처 담당자(검토)** → **정보보안처장(결재)**

Ⅱ. 개인정보보호

1. 개인정보란?

"개인정보"란 **살아있는** 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 **개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함**한다)를 말한다.

2. 개인정보 라이프 사이클에 따른 처리단계별 주의사항

가. 개인정보 수집 단계

- 수집항목의 타당성 검토(수집항목 최소화)
- 개인정보 수집·이용 동의서 받기(별도 법령 근거가 있는 경우 생략)
  - 필수항목(4가지) : 개인정보의 수집·이용 목적, 수집하려는 개인정보 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익 내용
- 주민등록번호는 법령근거가 있어야지만 수집가능(동의 수집 불가)

나. 개인정보 보관·저장 단계

- 개인정보 보유 문서(서류)를 보관하고 있는 물리적 보관 장소 출입통제 철저
- 개인정보처리시스템 접근권한 관리 철저(내역 3년 이상 보관)
- 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보(지문 등)는 암호화하여 저장(미 이행시 과태로 5천만원 이하)

  ※ 주민등록번호가 분실·도난·유출·위조·변조·훼손된 경우 5억원 이하의 과징금 부과

다. 개인정보 이용·제공 단계

- 개인정보 파일은 수집 목적 외에 다른 용도로 이용하거나 제공해서는 안 됨 (단, 다른 법률에 근거가 있는 경우 예외로 함)
- 수집 목적 외 처리가 가능한 경우는 개인정보보호법 제18조 제1항, 제2항 각 호에 해당하는 경우로 정보주체 또는 제3자의 권익을 부당하게 침해하지 않는 최소한의 범위에 한정함

라. 개인정보 파기 단계

- 보유기간경과, 개인정보 처리 목적 당성 등 개인정보가 불필요하게 되었을 때 지체 없이 파기. 타 법령에 따라 보존해야하는 경우는 제외.
- 담당자는 개인정보 파기 이력을 개인정보파기대장에 관리해야 함

3. 전직원이 실천할 수 있는 개인정보보호

가. PC내 주요 개인정보(주민등록번호) 암호화하기

- PC개인정보암호화 솔루션 PCFILTER를 활용하여 주민등록번호 암호화

※ 5-8호선 구간 2018.12월 설치 예정

나. ‘전자문서 개인정보보호 가이드라인’ 준수하기

- 원칙 : 전자문서 작성시 개인정보 미 포함(첨부파일 포함)
- 불가피한 경우

① 마스킹 처리 등 비식별화 조치

② 업무에 필요한 최소한의 개인정보만 기재하고 열람범위 **‘결재선 공개’(내부 열람 제한)** 및 **‘대시민 비공개(6호)’(외부 열람 제한)**로 설정

다. 개인정보 관련 문의가 있을 경우 개인정보보호담당자 적극 활용하기

개인정보보호담당자	
정보보안처	
이덕기	백지윤
02-6311-9396	02-6311-9399
ldkdream@seoulmetro.co.kr	bjy0817@seoulmetro.co.kr