

05 스마트폰 10대 안전수칙

- ① 의심스러운 애플리케이션 다운로드하지 않기
- ② 신뢰할 수 없는 사이트 방문하지 않기
- ③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
- ④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
- ⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기
- ⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기
- ⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기
- ⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기
- ⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기
- ⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

06 어떤 행위를 하면 처벌 받나요?

☞ 개인정보가 누설된 사정을 알면서 부정한 목적으로 개인정보를 제공받는 경우

정보통신망법 제28조의2(개인정보의 누설 금지) ② 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니 된다.

☞ 위반시 5년 이하의 징역 또는 5천만원 이하의 벌금

☞ 인터넷상 명예훼손

정보통신망법 제70조의(벌칙) ① 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처한다.
 ② 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

☞ 타인의 주민등록 번호 도용

주민등록법 제37조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

8. 다른 사람의 주민등록증을 부정하게 사용한 자
10. 다른 사람의 주민등록번호를 부정하게 사용한 자

이용자용

개인 정보 보호 !! 이것만은 꼭 알아두세요



01 개인정보란?

- 살아있는 개인에 관한 정보로서, 그 개인을 “알아볼 수 있는 정보”를 말합니다.
- 그 정보만으로는 특정 개인을 알아볼 수 없더라도, 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있다면 개인정보에 포함됩니다.
- ⇒ 예를 들어, 주민등록번호는 개인마다 고유한 것이므로 개인을 손쉽게 식별할 수 있으나, 이름의 경우에는 동명이인(同名異人)이 많아 그 정보 하나만으로는 개인정보로 보기 어렵습니다. 그러나 이름이 전화번호나 주소 등의 정보와 결합하는 경우에는 특정 개인을 식별할 수 있게 되어 개인정보로 볼 수 있습니다.

※ 개인정보의 유형

- 일반정보 - 성명, 주민등록번호, 주소, 연락처 등
- 경제정보 - 소득, 재산상황, 신용, 부채 등
- 사회정보 - 학력, 성적, 병역, 직업, 자격 등
- 통신정보 - 전자우편, 통화내용, 인터넷 접속 IP, 로그(log) 등
- 민감정보 - 사상, 신념, 노동조합·정당의 가입탈퇴, 정치적 견해, 건강, 성생활정보 등

02 “보이스피싱” 무섭죠?

보이스피싱이란?

- ‘전화를 통해 개인정보를 낚아 올린다’는 뜻으로 음성(voice)+개인정보(Private Data)+낚시(Fishing)를 합성한 신조어
- 기망행위로 타인의 재산을 편취하는 사기범죄의 하나로 전기통신수단을 이용한 비대면거래를 통해 금융 분야에서 발생하는 일종의 특수사기범죄

보이스피싱 예방 요령

- 금융거래정보 요구는 일절 응대하지 말 것
- 현금지급기로 유인하면 100% 보이스피싱
- 자녀납치 보이스피싱에 미리 대비
- 개인·금융거래정보를 미리 알고 접근하는 경우에도 내용의 진위를 확인
- 피해를 당한 경우 신속히 지급정지를 요청
- 유출된 금융거래정보는 즉시 폐기
- 예금통장 및 현금(체크)카드 양도 금지
- 발신 (전화)번호는 조작이 가능함에 유의
- 금융회사 등의 정확한 홈페이지 여부 확인 필요
- “전자금융사기 예방서비스” 적극 활용

03 “스미싱” 알고 미리 대처하자

스미싱이란?

- SMS와 Phishing의 결합어로 문자메시지를 이용하여 피싱하는 방법을 말합니다. 웹사이트 링크가 포함된 문자 메시지를 보내 휴대폰 사용자가 링크를 클릭하면 트로이목마를 주입해 범죄자가 휴대폰을 통제할 수 있게 합니다.
- 햄버거, 아이스크림 등 외식상품 무료쿠폰을 가장해 특정 URL이 포함된 문자메시지를 소비자에게 보내고, 이를 소비자가 클릭하면 악성코드가 휴대폰에 설치가 되어 소액결제가 자동으로 되는 등 피해가 발생합니다.

스미싱 예방 요령

- 각 통신사 고객센터에 전화하거나 통신사 인터넷 홈페이지를 이용하여 소액결제를 원천적으로 차단하거나 결제 금액을 제한
- 스마트폰용 백신프로그램을 설치하고 주기적으로 업데이트하여 악성코드 설치를 차단
- 확인되지 않은 앱(App)이 함부로 설치되지 않도록 자신이 보유한 스마트폰의 보안설정을 강화
- 쿠폰, 상품권, 무료, 조회, 공짜 등으로 스팸 문구를 미리 등록하여 내 스마트폰에 스미싱 문자가 전송되는 것을 사전에 차단
- T스토어·올레마켓·U+앱마켓 등 공인된 오픈마켓을 통해 앱(App)을 설치
- 출처가 확인되지 않은 링크를 클릭하지 않도록 하고, 인터넷상에서 apk파일을 다운받아 스마트폰에 저장하지 말 것

04 개인정보 피해예방 10계명

- ① 회원가입을 하거나 개인정보를 제공할 때에는 개인정보취급방침 및 약관을 꼼꼼히 살핍니다.
- ② 회원가입시 비밀번호를 타인이 유추하기 어렵도록 영문/숫자 등을 조합하여 8자리 이상으로 설정합니다.
- ③ 가급적 안전성이 높은 주민번호 대체수단으로 회원가입을 하고, 꼭 필요하지 않은 개인정보는 입력하지 않습니다.
- ④ 자신이 가입한 사이트에 타인이 자신인 것처럼 로그인하기 어렵도록 비밀번호를 주기적으로 변경합니다.
- ⑤ 타인이 자신의 명의로 신규 회원가입 시 즉각 차단하고, 이를 통지받을 수 있도록 명의도용 확인서비스를 이용합니다.
- ⑥ 자신의 아이디와 비밀번호, 주민번호 등 개인정보가 공개되지 않도록 주의하여 관리하며 친구나 다른 사람에게 알려주지 않습니다.
- ⑦ 인터넷에 올리는 데이터에 개인정보가 포함되지 않도록 하며, P2P로 제공하는 자신의 공유폴더에 개인정보 파일이 저장되지 않도록 합니다.
- ⑧ 금융거래 시 신용카드번호와 같은 금융정보 등을 저장할 경우 암호화 하여 저장하고, 되도록 PC방 등 개방 환경을 이용하지 않습니다.
- ⑨ 인터넷에서 아무 자료나 함부로 다운로드 하지 않습니다.
- ⑩ 개인정보가 유출된 경우 해당 사이트 관리자에게 삭제를 요청하고, 처리되지 않는 경우 즉시 개인정보침해신고센터(국번없이 118, www.118.or.kr)에 신고합니다.