피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	정보주체 대응 방안
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)
명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름, 이메일, 연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십여개의 웹사이트 가입하여 개인정보 불법 이용	• e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118) ※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가

피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	정보주체 대응 방안
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)