
 관계부처 합동	보 도 자 료				 정부혁신 보다 나은 정부
	보도	배포시점부터 보도	배포	2019. 9. 4.(수) 14:00	

책 임 자	과기정통부 사이버침해대응과장 황 큰 별(044-202-6430)	담 당 자	김 남 승 사무관 (044-202-6431)
	방송통신위원회 이용자보호과장 천 지 현(02-2110-1540)		정 성 혜 주무관 (02-2110-1542)
	금융위원회 전자금융과장 이 한 진(02-2100-2970)		유 원 규 사무관 (02-2100-2974)
	금감원 불법금융대응단 팀장 이 성 호(02-3145-8521)		장 종 현 선임조사역 (02-3145-8534)
	경찰청 사이버안전과장 유 재 성(02-3150-2208)		김 상 순 경정 (02-3150-0252)

추석 택배, 소액결제 등을 사칭한 스미싱 피해 주의!

- 이통3사와 협업하여 스미싱 피해예방을 위한 문자메시지 발송 -

- 과학기술정보통신부(장관 유영민), 방송통신위원회(위원장 이효성), 금융위원회(위원장 최종구), 금융감독원(원장 윤석현), 경찰청(청장 민갑룡)은 추석 연휴를 앞두고 택배 배송 확인, 소액 결제 문자 등을 사칭한 스미싱*이 증가할 것으로 예상되어 이용자들의 주의를 당부했다.

* 스미싱(smishing): 문자메시지(SMS)와 피싱(Phishing)의 합성어로 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량 전송 후 이용자가 악성 앱을 설치하거나 전화를 하도록 유도하여 금융정보·개인정보 등을 탈취하는 수법(보이스피싱, 전자상거래 사기, 기타 다양한 사기에 광범위하게 이용)

- 올해 7월까지 스미싱 탐지 건수는 전년 동기간 대비 21.5% 증가하였으며('18.1~7월 145,093 → '19.1~7월 176,220건), 지인을 사칭한 스미싱이 크게 증가(357.3%, '18.7월 7,470건 → '19.7월 34,160건)하고 있어 이용자의 각별한 주의가 요망된다.

□ 이용자가 이러한 스미싱 사기 피해를 예방하기 위해서는

△ 택배 조회, 명절 인사, 모바일 상품권·승차권·공연예매권 증정 등의 문자 속에 출처가 확인되지 않은 인터넷주소(URL)는 클릭하지 않을 것

※ 스미싱 문자 사례, 스미싱 문자를 이용한 보이스피싱 피해사례 : 붙임 1, 2 참고

△ 알 수 없는 출처의 앱이 함부로 설치되지 않도록 스마트폰의 보안 설정을 강화하고, 앱을 다운로드 받을 경우 문자 속 링크를 통해 받지 않고 공인된 오픈마켓을 통해 앱을 설치할 것

△ 이통사 등에서 제공하는 백신프로그램을 설치하여 업데이트 및 실시간 감시상태를 유지할 것

※ 스미싱 피해예방 수칙 및 피해발생 시 행동요령 : 붙임 3 참고

△ 보안강화 및 업데이트 명목으로 개인정보·금융정보를 요구하는 경우 절대 입력하거나 알려주지 않는 것이 중요하다.

□ 정부는 추석을 앞두고 「전기통신금융사기(보이스피싱) 방지 종합 대책」의 일환으로 관계부처 간의 협업을 통해 다양한 피해예방 활동을 추진할 예정이다.

○ 방송통신위원회는 한국정보통신진흥협회(KAIT), 이통3사(SKTEL, KT, LGU+)와 협력하여 9월 5일부터 총 5,360여만 명을 대상으로 「스미싱 피해예방 문자」를 발송하여 국민들의 주의를 당부할 계획이다.

<문자 내용>

추석 스미싱 주의! 택배, 소액결제문자 속 의심되는 인터넷주소 클릭 금지

※ 9.5.(목)부터 각 회사 명의로 문자메시지 발송 예정

- 과학기술정보통신부(한국인터넷진흥원)는 추석 연휴기간동안 스미싱 유포 등에 신속하게 대응할 수 있도록 24시간 모니터링을 실시하고,
 - 신고·접수된 스미싱 정보를 분석하여 악성앱 유포지 차단 및 스미싱에 이용된 번호중지·차단 등 이용자 피해를 최소화할 계획이다.
- 금융위원회와 금융감독원은 추석연휴 기간 동안 금융업권의 협조를 통해 KTX객실, 고속버스터미널, 지하철역 등 유동 인구가 많은 장소에서 보이스피싱 예방홍보를 집중적으로 실시하고,
 - 스미싱 피해예방을 위하여 휴대폰 문자메시지 분석을 통한 스미싱 문자 경고·차단이 가능한 인공지능(AI) 기반의 앱이 출시될 수 있도록 추진할 계획이다.
- 경찰청은 사이버범죄 예방을 위해 개발·운영 중인 모바일 앱 ‘사이버캡’을 통해 스미싱 탐지, 피해경보 발령 기능과 스미싱 예방수칙 정보 등을 제공하고 있다.

□ 명절 연휴 중 스미싱 의심 문자를 수신하였거나 악성앱 감염 등이 의심 되는 경우 **국번없이 118**로 불법스팸대응센터에 신고하면, 다른 사람에게 유사한 내용의 스미싱을 발송하는 등의 2차 피해예방 및 악성코드(앱) 제거 방법 등을 24시간 무료로 상담 받을 수 있다.

※ 자세한 정보는 방송통신이용자정보포털(와이즈유저, www.wiseuser.go.kr), 보호나라(www.boho.or.kr) 및 경찰청(<https://www.police.go.kr/main.html>), 보이스피싱지킴이(<http://phishing-keeper.fss.or.kr/fss/vstop/main.jsp>) 홈페이지 참조

① 택배 관련 스미싱

<p>[배송조회] 9/9 고객주소가 잘못되었습니다 택배가 반송되었습니다 배송 주소 수정 uuuu.me/FgMRD7</p>	<p>[OO택배] 추석배송 물량증가로 배송이 지연되고 있습니다. 배송일정 확인하세요 http://nene.you/Nkln8</p>
---	--

② 공공기관 사칭 스미싱

<p>[생활불편신고] 귀하에게 민원이 접수되어 통보드립니다. 민원확인 http://bit.ly/2Hh9vp9</p>	<p>[도로공사] ■■■님차량 불법단속대상 적발! 확인 후 빠른처리 요망! http365.com</p>
--	--

③ 지인 사칭·선물 관련 스미싱

<p>☞(^o^)-~★ 추석 잘 보내시고 2019년 남은 시간 모두 모두 행복하세요. ^.^~ http://woz.kr/mhgd</p>	<p>■■■■님 추석명절 선물로 모바일 상품권을 보내드립니다 확인 바랍니다. http://hpbl.are/nbaBl</p>
<p>추석선물 도착 전 상품 무료 배송! 할인쿠폰 지급완료! 즉시 사용가능! 확인 http://vno.kr/ncnqbH</p>	<p>추석에 찾아뵈어야 하는데 영상으로라도 인사드립니다. 즐거운 한가위 보내세요! http://mnon.it/Pnti1</p>

- 2019년 3월 피해자 A(52세, 교사)는 본인이 사용한 적이 없는 결제 문자메시지를 받고 사실 여부를 확인하기 위해 **문자메시지에 안내된 전화번호로 전화**
- 전화 상담원은 피해자 A에게 “명의를 도용된 것 같으니 **고객(피해자)을 위해 대신 경찰에 신고해 주겠다**”며 **피해자를 안심** 시킴
- 잠시 후 서울지방경찰청 지능범죄수사대 최OO 경감이라는 사기범의 전화가 와서 피해자 A에게 “당신의 신용카드가 해외에서 발생한 명의도용 사기범죄에 이용되었으니 범죄 수사에 협조하면 당신에게 직접적인 불이익은 없을 것”이라며 **피해자에게 자신의 지시를 따를 것을 요구**
- 사기범은 피해자 소유의 은행 계좌 해킹 및 바이러스 감염 여부를 점검해준다는 명목으로 **피해자 소유 컴퓨터에 원격조종 프로그램을 설치하게 한 후** OO은행 인터넷뱅킹에 접속하여 **피해자에게 이체 비밀번호, 공인인증서 비밀번호, OTP생성번호를 직접 입력**하게 하여 2천만원 상당의 예금을 편취

피해자 A가 받은 허위 결제 문자메시지

[Web발신]
 (주) [redacted]
 주문하신 안마의자
 57만3000원 결제되
 였습니다
 문의번호:
 02-[redacted]-[redacted]

① 스미싱 피해예방 수칙

- 

(링크 클릭주의) 출처가 미확인 문자메시지의 링크주소(숫자열 포함) 클릭 주의
 ※ 지인에게서 온 문자도 인터넷주소가 포함된 경우 클릭 前 확인
- 

(스마트폰 보안설정 강화) 알 수 없는 출처의 앱 설치 제한
 ※ 설정방법 : 환경설정 > 보안 > 디바이스 관리 > '알 수 없는 출처'에 V체크 해제
- 

(백신프로그램 설치) 업데이트 및 실시간 감시상태 유지
 ※ (스미싱 방지앱 설치) 이통사 · 보안업체 제공
- 

(소액결제 차단·제한)
 자신의 스마트폰으로 114를 눌러 상담원과 연결
- 

(금융정보 입력제한)
 보안등급 명목으로 요구하는 보안카드번호 입력 금지
 ※ 스마트폰 등 정보저장장치에 보안카드 사진 · 비밀번호 등 저장 금지
- 

(전자금융사기 예방서비스 가입) 공인인증서 PC지정, SMS 사전인증 등 금융회사 제공 보안강화 서비스 적극 가입

* 자료 : 경찰청

② 스미싱 피해발생 시 행동요령

⇒ 【행동요령】

- ① 금융기관 콜센터 전화 : 경찰서에서 발급받은 '**사건사고 사실 확인원**'을 이동통신사, 게임사, 결제대행사 등 관련 **사업자에 제출**
- ② 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
- ③ 한국인터넷진흥원 **불법스팸대응센터(국번없이 118)** 신고
- ④ 금융 및 증권 등 **공인인증서 즉시 폐기 및 재발급받기**
- ⑤ 사용 중인 **이동통신사에서** 제공하는 스미싱 **예방서비스(App 등)** 설치 및 활용
- ⑥ **주변 지인들에게** 스미싱 피해 사실을 즉시 알려 **2차 피해 발생 사전 방지**

* 자료 : 경찰청, 한국인터넷진흥원

(단위: 건)

구분	2016	2017	2018	2019(~7월)
택배사칭	267,274	317,618	191,038	139,645
공공기관사칭	75	6,156	8,549	30
지인사칭	17,413	15,080	14,372	34,160
기타	27,149	163,173	28,881	2,385
합계	311,911	502,027	242,840	176,220

* 자료 : 과학기술정보통신부, 한국인터넷진흥원