관계부처 합동	보 도 자 료			정부혁신 보다나은 정부
	보도	2021.9.13.(월) 부터 보도 온라인 9.12(일) 12:00	배포	2021. 9.10(금)14:00

책 임 자		담 당 자	
	과기정통부 사이버침해대응과장 최 미 정(044-202-6460)		김 남 승 사무관 (044-202-6461)
	금융위원회 전자금융과장 이 한 진(02-2100-2970)		이 영 우 사무관 (02-2100-2811)
	경찰청 사이버범죄수사과장 최 종 상(02-3150-1605)		이 성 일 경정 (02-3150-1658)
	한국인터넷진흥원 침해대응단 단장 이 동 근(02-405-6610)		이 재 형 팀장 (02-405-5421)
	금감원 불법금융대응단 국장 김 미 영(02-3145-8150)		곽 원 섭 팀장 (02-3145-8521)

추석 명절, 선물 배송 등을 사칭한 스미싱 주의!

- 출처가 불분명한 문자내 URL 및 전화번호 클릭 주의 -

□ 과학기술정보통신부(장관 임혜숙, 이하 '과기정통부'), 금융위원회(위원장 고승범), 경찰청(청장 김창룡), 한국인터넷진흥원(원장 이원태, 이하 'KISA'), 금융감독원(원장 정은보)은 추석 연휴를 앞두고 **선물**(택배) **배송 확인, 국민지원금 등을 사칭한 스미싱*이 증가**할 것으로 **예상**되어, **이용자**들의 **주의**를 **당부**했다.

* 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 8월까지 **스미싱 신고(접수)·차단 건수**는 전년 동기간 대비 74% 감소하였으나('20.1~8월 700,783건 → '21.1~8월 184,002건), 추석 명절 기간 **선물 배송 등**에 악용될 수 있는 **택배 사칭 스미싱 유형**이 **93%**를 **차지**하고 있어 **이용자**의 **각별**한 **주의**가 **요구**된다.

〈 스미싱 신고(접수)·차단 현황 〉

구분	2017	2018	2019	2020	2021(~8월)
택배사칭	317,618	191,038	324,269	782,013	171,391
공공기관사칭	6,156	8,549	36	12,208	9,814
지인사칭	15,080	14,372	35,568	1,043	24
기타	163,173	28,881	4,713	155,579	2,773
합계	502,027	242,840	364,586	950,843	184,002

□ **이용자**가 **스미싱**(보이스피싱) **사기 피해**를 **사전**에 **예방**하기 위해서는

△ 택배 조회, 명절 인사, 모바일 상품권·승차권·공연예매권 증정 등의 **문자** 속에 **출처**가 **확인되지 않은 인터넷주소(URL) 또는 전화번호를 클릭하지 않을 것**

※ 스미싱 문자 사례, 스미싱 문자를 이용한 보이스피싱 피해사례 : 붙임 1, 2, 3 참고

△ **알 수 없는 출처의 앱이 함부로 설치되지 않도록 스마트폰의 보안 설정**을 **강화**하고, 앱을 다운로드 받을 경우 문자 속 링크를 통해 받지 않고 **공인**된 **오픈마켓**을 **통해 앱**을 **설치할 것**

△ **백신프로그램을 설치**하여 **업데이트** 및 **실시간 감시 상태를 유지**할 것

△ **본인인증, 재난지원금 및 백신예약 조회 등의 명목**으로 신분증 및 **개인정보·금융정보를 요구**하는 경우 절대 **입력하거나 알려주지 않는 것**이 **중요**하다.

※ 10대 스마트폰 보안수칙 : 붙임 5 참고

□ 아울러, 정부는 추석을 앞두고 **관계부처 간**의 **협업**을 통해 스미싱으로 인한 국민 피해가 발생하지 않도록 **스미싱 모니터링 및 사이버 범죄 단속 강화** 등을 **중점적**으로 **실시**할 계획이다.

○ **과기정통부와 KISA**는 추석 연휴기간 동안 **스미싱 유포 등**에 **신속하게 대응**할 수 있도록 **24시간 모니터링을 실시**하고,

- 신고·접수된 **스미싱 정보를 분석**하여 **악성앱 유포지 차단 등 신속한 조치**를 통해 **이용자 피해**를 **최소화**할 **계획**이며,

- 또한, **이통3사(SKT, KT, LGU+)**와 **협력**하여 각 통신사 명의로 「**보이스피싱 주의문자**(붙임 4)」를 **순차 발송**하여 **국민들**의 **주의**를 **당부**한다.

○ **금융위원회**와 **금융감독원**은 추석연휴 기간 동안 금융업권과의 협조를 통해 각 고객들에게 **코로나19 관련 국민지원금 또는**

재난지원금 등을 **빙자**한 **사기문자에 대해 각별히 유의하도록 안내**하는 등 **보이스피싱 예방홍보를 집중적으로 실시**하고,

○ **경찰청**은 스미싱 피해 예방을 위해 경찰청 홈페이지와 모바일 앱인 '사이버캅'을 통해 **예방 수칙·피해 경보 등을 제공**하고,

- 추석 연휴 기간 전후로 발생하는 스미싱, 직거래 사기 등 서민생활을 침해하는 사이버범죄에 대해 **단속을 강화**할 계획이며,

- 사이버범죄 피해를 입었을 경우 **사이버범죄 신고시스템(ECRM)**을 이용해 **신고**를 접수해달라고 **당부**했다.

※ 경찰청(https://www.police.go.kr) 및 사이버범죄신고시스템(ecrm.cyber.go.kr) 홈페이지 참조

□ **명절 연휴** 중 **스미싱 의심 문자**를 **수신**하였거나 **악성앱 감염** 등이 의심 되는 경우 **국번없이 118 상담센터**에 신고하면 **24시간 무료로 상담** 받을 수 있다.

※ 보호나라(https://www.boho.or.kr) 홈페이지 참조

붙임1 스미싱 문자 사례

[사례 1] 추석 명절 사칭

☞(^o^)~★ 추석 잘 보내시고 2021년 남은 시간 모두 모두 행복하세요. ^.~ http://woz.kr/mhgd

① OO님 추석명절 선물로 모바일 상품권을 보내드립니다. 확인 바랍니다. <URL>

② 추석선물 도착 전 상품 무료 배송! 할인쿠폰 지급 완료! 즉시 사용가능! 확인 <URL>

[사례 2] 택배 사칭

[OO 택배] 택 배배 송 불 가 * 주* 소 불 완 전 함 즉 시 변 경 부 탁 드 립 니다:< dokdo.in/V0h >

① 상품 거래번호는 틀려서 보낼수 없습니다. 앱다운로드 다?시 확인해주세요 <URL>

② 우.체국화물 반송처리중 바로확인부탁드립니다 <URL>

③ 주문한 항목은 CJ 익스프레스에서 배송되었습니다. 배송 주소를 확인하십시오. <URL>

④ 상품 거래번호는 틀려서 보낼수 없습니다. 앱다운로드 다 시 확인해주세요 <URL>

⑤ 물품.이 우편으로 발송되었으므로 분실을 방지하기 위해 제 시간.에 픽.업하십시오 <URL>

[사례 3] 지원금 사칭

[OO부 지원금 신청 안내]
귀하는 국민지원금 신청대상자에 해당되므로 온라인 센터 (http://kr.center.com)에서 지원하시기 바랍니다.

① [Web발신] (광고) "「○○은행」" 9월 귀하는『재난지원금』대출신청 대상이니 확인 부탁드립니다.
상담문의 : 02-000-0000

② 지원금 신청이 접수되었습니다. 다시 한번 확인 부탁드립니다. <URL>

③ 재난 지원금 신청 및 지급:<URL>

④ (광고)「OO희망론」『2021년 정부 특별지원금 대출 시행 안내』 안녕하세요. 『OO새희망론』의 새로운 소식을 전합니다. [지원절차]- 상담 및 접수(신청인) → 한도조회 → 가결시 대출약정체결 → 대출금 입금 무료거부 080-000-0000

⑤ O월에 추가 보조금이 지급 되었으니 시간 내에 철회하십시오 <URL>

[사례 4] 공공기관 사칭

<국가건강검진>진단결과상세 보기:baie.gsiw.zone

① [Web발신] [금융감독원]명의계좌가 신고되었습니다. <URL>

② [Web발신] [질병관리청 COOV]코로나19 백신 예약 확인 요청 <URL>

③ 【사이버 검찰청】.사건 처리통지서입 니 다상세내용 확인 <URL>

④ [국민건강보험] OOO님의 영유아검진표가 우편 발송되었습니다. <URL>

⑤ [경찰청교통민원]교통법규위반 사실확인통지서(통지): <URL>

[사례 5] 백신 관련 사칭

[질병관리청] 8/5 코로나19 백신 예약 인증 본인확인 https://ya.mba/3Pm

① [방역센터]방역증명서 발급완료, 개인정보 인증 바랍니다. <URL>

② [코로나19예약시스템] 전자예방접종증명서 발송 완료 <URL>

③ [질/병/관/리/청]2021년 9월 코/로/나 19 백/신접/종 예 약고지 서 발송 완료 <URL>

④ 백 신 접 종 고 지 서 발송 완료본인확인 예 약 <URL>

⑤ 전 자 예 방 접 종 증 명 서 발송 완료 <URL>

[사례 6] 지인 사칭

내일 결^혼 선^발 웨딩^드레^스 사진 보여^드릴^까요 goo.gl/xxxxxx?$$^^

① "엄마, 딸인데, 핸드폰 액정이 깨져서 대리점에서 임시 폰 받았어. 전화통화 안되니까 카톡 친구 추가해줘"

② "신분증과 계좌번호, 비밀번호 보내줘. 엄마 폰으로 할 게 있어. 보내주는 앱 깔아줘" <URL>

③ (광고)저희 결혼식에 참석해 주시길 바랍니다. <URL> 무료거부 0808781572

④ 전 v기억나s세o요? 동창i인데r요 여기n에 같w이 찍은 사l진 있어요 <URL>

⑤ 예식시간:2021.O.OO 오전 11시 15분 확인 <URL>

붙임2 스미싱 문자를 이용한 보이스피싱 피해사례 1(재난지원금 빙자)

□ '21.3월 피해자 A(52세, 개인사업자)는 ○○은행을 사칭하여 **정부의 4차 재난지원금 대출을 빙자**한 **문자**를 받고, 전화를 걸어 **대출상담을 요청**

□ 전화 상담원은 피해자 A에게 "제가 보내는 앱을 설치해야 대출신청이 가능하다"며 앱 설치용 인터넷주소(URL)를 보냈고, 피해자 A는 이를 클릭하여 앱 설치*

* 피해자가 설치한 것은 휴대폰 원격조종앱 및 전화 가로채기앱 (대출신청용 앱이 아님)

□ 또한, 피해자 A는 전화 상담원이 보낸 전자 대출신청서 작성용 인터넷 주소(URL)를 클릭하였으며, 그 후 사기범은 피해자 A의 폰을 원격조종하여 허위 대출신청서를 작성

□ 피해자 A는 전화 상담원의 지시에 따라 본인 명의의 B은행 계좌번호 2개를 전화로 알려주고, 동 계좌의 체크카드*를 전화 상담원이 지시하는 주소로 택배 발송

* 사기범은 피해자가 대출받기 위해서는 계좌 입출금 내역을 부풀려 신용등급을 높여야 한다며 체크카드를 요구 (실제로는 입출금 내역과 신용등급은 아무런 관련이 없음)

□ 피해자 A가 자신의 계좌에서 타인 자금 6천만원이 입금된 후 인출* 되어 지급정지된 사실을 알고 전화를 걸어 문의하자, 전화 상담원은 거래실적을 부풀리는 과정에서 문제가 발생한 것이라고 하면서,

* 사기범은 피해자가 알려준 2개 계좌를 대포통장으로 이용하여, 다른 피해자로부터 6천만원의 피해금이 동 통장으로 입금되게 한 후 바로 인출

○ 금감원에 보증금 1천만원을 내면 지급정지도 풀리고 대출도 정상 진행된다고 하면서 금감원 콜센터(☎1332)에 문의해보라고 답변

□ 피해자 A가 1332로 전화하자 금감원 직원*이라는 사람이 전화를 받아서 사기범 말이 맞으니 □□은행의 D씨 계좌로 1천만원을 입금하라고 하여 그대로 입금하였으나, 사기범은 1천만원을 인출 후 잠적

* 피해자는 금감원에 전화하였지만, 동 전화는 사기범에게 연결 (전화 가로채기앱 때문)

붙임3 스미싱 문자를 이용한 보이스피싱 피해사례 2(자녀 사칭)

□ ‘21.7.31. 09:40경에 피해자 B(64세)는 자녀를 사칭하여 “휴대폰이 고장나 임시 폰을 발급받았으며 인증이 필요하다”는 문자를 수신

□ 피해자 B는 사기범의 요구대로 신분증과 ▢▢은행 계좌번호와 비밀번호를 보내고, 사기범이 보낸 앱 인터넷주소(URL)*를 클릭하여 설치

* 피해자가 설치한 것은 휴대폰 원격조종앱

○ 공교롭게도 피해 2주 전 자녀의 휴대폰이 실제로 바닷물에 침수되어 수리가 필요한 상황이었기 때문에 피해자 B는 의심하지 않았음

□ 사기범은 같은 날 19:30분경 ‘인증이 실패했으니 내일 다시 해보자’라는 메시지를 남기고 잠적

□ 피해자 B는 같은 날 19:52경 다른 자녀와 통화하면서 메신저피싱임을 알게 되었으며, 계좌번호와 비밀번호를 유출한 ▢▢은행 계좌를 확인한 결과 아무런 피해가 없었음

□ 그러나, 다음 날 10:00경, 피해자 B는 거래중인 신협 고객센터로 전화했을 때 7.31. ◈◈계좌에서 1억원이 ○○○○증권, △△은행, ◇◇은행 총 3곳으로 분산 이체된 사실을 알게 됨

○ 사기범은 피해자 B의 ▢▢은행 계좌번호와 비밀번호를 이용하여 ▢▢은행에 접속 후 오픈뱅킹을 통해 ◈◈계좌에 1억원이 있는 것을 확인

○ ◈◈은행의 간편비밀번호서비스 인증 시에 ‘타행 계좌로 인증 받는 방법’을 이용(피해자 B의 ▢▢은행 계좌에 보낸 1원의 입금내역 및 인증번호를 입력)하여 새로운 간편비밀번호를 발급받고, 디지털OTP를 발급

○ ‘21.7.31. 12시경 타인 명의 ○○○○증권 계좌로 3,600만원(900만원×4번), ◎◎법인 명의 ◇◇은행 계좌로 1,400만원(900만원×1번, 500만원×1번)을 이체하고

○ 같은 날 16시경 정기예금(5천만원)을 해지하여 법인 명의 △△은행 계좌로 이체(900만원×5번, 500만원×1번)

붙임4 보이스피싱 주의문자 안내문

추석 명절에 앞서 코로나19 정부지원 대출, 택배 배송조회 등을 빙자한 보이스피싱 문자가 예상되오니 피해예방을 위해 다음 유의 사항을 안내드립니다.

▶ 이런 경우 보이스피싱을 의심해 주세요

① 전화로 검찰 등을 사칭하여 범죄에 연루되었다며 접근
② 문자로 금융회사를 사칭하여 저리대출 제공하겠다며 접근
③ 문자로 가족·지인을 사칭하며 접근
④ 출처를 알 수 없는 앱 설치 또는 인터넷 주소(URL) 클릭 유도

▶ 의심될 때 이렇게 대응하세요

- 검찰, 경찰 등은 어떠한 경우에도 금전의 이체를 요구하거나 금융거래정보를 수집하지 않습니다. 이런 전화를 받은 경우, 해당 기관의 공신력 있는 전화번호 등을 이용하여 사실 여부를 확인하세요

- 신용 등급 상향, 저금리 전환, 대출 수수료 명목의 금전 및 개인정보 요구는 거절하고, 문자메시지를 이용한 대출광고에 연락하지 마세요

- 가족·지인의 긴급 상황(사고, 휴대폰고장 등)이라며 연락받은 경우, 전화통화 등으로 해당 가족·지인이 보낸 메시지가 맞는 지 확인하세요

- 가까운 사이라도 메시지로 신분증 및 신용카드, 계좌·비밀번호 등을 요구하면 반드시 거절하고, 절대로 URL을 터치하지 마세요

- 피해가 의심된다면 즉시 해당 금융회사 콜센터, 경찰청(☎112) 또는 금감원(☎1332)에 전화하고 계좌의 지급정지 등을 신청하세요

보이스피싱은 예방이 최선입니다.

붙임5 10대 스마트폰 보안수칙

○ 10대 스마트폰 보안수칙



* 자료 : 과학기술정통부, 한국인터넷진흥원