"함께하면 이겨낼 수 있습니다" 코로나 상생 국민지원금	**보 도 자 료**	**행정안전부 디지털안전정책과** 과 장 이상민(044-205-2741) 사무관 부 미(044-205-2752)
관계부처 합동	2021년 9월 6일(월) 조간 (9. 5. 12:00 이후)부터 보도하여 주시기 바랍니다.	**과학기술정보통신부 사이버침해대응과** 과 장 최미정(044-202-6460) 사무관 김남승(044-202-6461) **방송통신위원회 이용자보호과** 과 장 이소라(02-2110-1540) 주무관 김효나(02-2110-1542)

코로나 상생 국민지원금 안내 관련 문자 결제 사기(스미싱) 주의하세요

- 정부·카드사 공식문자 확인 및 결제 사기 의심 문자 118신고 -

□ 정부는 '코로나 상생 국민지원금(이하 국민지원금)' 신청·지급 시기와 맞물려 **국민지원금 지급대상·금액 안내, 카드 사용 승인, 지원금 충전** 등의 내용으로 **정부·카드사를 사칭한 스미싱*이 증가할 것으로 예상**되어 **이용자들의 주의를 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

□ 이용자는 스미싱 피해예방을 위해 **국민비서 사전 알림서비스를 적극 활용**하고, **국민비서·카드사 외에 출처가 불분명한 안내문자**를 받은 경우 또는 **정부·카드사를 사칭한 의심스러운 인터넷 주소가 포함된 문자**를 받은 경우 한 번 더 **유심히 살펴보아야** 한다.

○ **의심 문자**로 판단한 경우 **클릭하지 말고 바로 삭제**하고, 문자를 열람하였다면 **문자 내 인터넷주소(URL) 클릭에 신중**해야 한다.

< 스미싱 문자 예시 (인터넷주소(URL) 클릭을 유도함) >

❑ 안내 사칭
[OO부 지원금 신청 안내] 귀하는 국민지원금 신청대상자에 해당되므로 온라인 센터(http://kr.center.com)에서 지원하시기 바랍니다.
❑ 신청 사칭
귀하는 국민지원금 대상자입니다. 신청하기를 클릭 하세요. 신청하기 -> http://kr-hw.com
❑ 접수 사칭
지원금 신청이 접수되었습니다. 다시 한번 확인 부탁 드립니다. https://url.kr/25yp3q

□ 아울러, 이용자들은 평상시 **'10대 스마트폰 보안수칙[붙임1]'을 실천**할 필요가 있으며, **스미싱 의심 문자를 수신**하였거나 **악성앱 감염 등이 의심**되는 경우 **24시간 무료**로 운영하는 **118상담센터(☎118)에서 상담**받을 수 있다.

□ 정부는 국민지원금 신청·지급이 시작되는 **9월 6일부터** 각 통신사 명의로 **'스미싱 피해예방 문자를 순차 발송'**하는 등 다양한 창구를 활용하여 스미싱에 대한 이용자의 경각심을 높이고자 하며,

○ **24시간 모니터링**을 실시하고, 신고·접수된 스미싱 정보를 분석하여 **악성앱 유포지를 즉시 차단**하는 등 **이용자의 피해를 최소화**하기 위해 총력을 다한다는 방침이다.

붙임1 **10대 스마트폰 보안수칙**

일상에서 지켜주세요

스마트폰 보안수칙 10



01

스마트폰 운영체제와 모바일 백신 최신으로 업데이트하기



02

공식 앱 마켓이 아닌 다른 출처의 앱 설치 제한하기
(출처를 알 수 없는 앱)



03

스마트폰 앱 설치 시 과도한 권한을 요구하는 앱은 설치하지 않기



04

문자 또는 SNS 메시지에 포함된 URL 클릭하지 않기



05

스마트폰 보안 잠금을 설정하여 이용하기
(비밀번호 또는 화면 패턴)



06

스마트폰 WiFi 연결 시 제공자 불분명한 공유기 이용하지 않기



07

루팅, 탈옥 등을 통한 스마트폰 플랫폼의 구조 임의변경 금지



08

스마트폰에 중요정보 저장하지 않기
(주민등록증, 보안카드 등)



09

스마트폰 교체 시 개인정보 등 데이터 완전삭제 혹은 초기화 적용



10

스마트폰, SNS 등 계정 로그인 2단계 인증 설정하기



과학기술정보통신부

KISA 한국인터넷진흥원

붙임2 스미싱 피해예방 대응요령 및 피해발생 시 행동요령

1 스미싱 피해예방 대응요령 및 피해사례

<대응요령>



<피해사례>

□ 문서나 이미지 등을 가장한 파일, 정부기관이나 거래처 등을 사칭한 문자 또는 이메일을 통해 사용자의 PC나 휴대폰 등에 악성앱, 악성코드 등을 설치하는 사례 증가

<질병관리청 예방접종증명서 관련 스미싱 사례>



① "[질병관리청COOV]코로나19 전자예방접종증명서 발송 완료" 등의 **사칭 문자 내부 URL 클릭** 시 **검진모아 사칭 사이트 등으로 연결**되며 피해자 **전화번호 입력 시 악성 앱 설치**

② 악성 앱은 **정상 COOV앱을 사칭**하고 악성 앱 실행 시 피해자 **스마트폰 번호·문자메시지 등을 탈취, 개인·금융정보 입력을 유도**하여 **추가정보 탈취**

2 스미싱 피해발생 시 행동요령

⇨ **【행동요령】**

① 한국인터넷진흥원 118상담센터**(국번없이 118) 상담**

② 문자메시지 등으로 수신된 **금융회사 및 공공기관의 홈페이지**는 반드시 **인터넷 검색 등을 통해 정확한 주소**인지 **확인**

③ 금융 및 증권 등 **인증서 즉시 폐기** 및 **재발급**받기

④ 사용 중인 **이동통신사**에서 제공하는 문자결제사기 **예방서비스 (App 등)** 설치 및 활용

⑤ 이동통신사에 **모바일 결제내역** 여부 **확인**

⑥ **주변 지인**들에게 문자결제사기 피해 사실을 즉시 알려 **2차 피해 발생 사전 방지**

⑦ 악성파일 삭제 : **스마트폰 내 '다운로드' 앱 실행** → 문자를 클릭한 시점 이후, 확장자명이 apk인 파일 저장여부 확인 → 해당 **apk 파일 삭제**

※ 삭제되지 않는 경우, 휴대전화 서비스센터 방문 또는 스마트폰 초기화

* 자료 : 과기정통부(한국인터넷진흥원)

붙임3 스미싱 주요 사례

[사례 1] 지원금 사칭

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

① 귀하는 국민지원금 대상자입니다. 신청하기를 클릭하세요. 신청하기 -> http://kr-hw.com

② 지원금 신청이 접수되었습니다. 다시 한번 확인부탁드립니다. https://url.kr/25yp3q

[사례 2] 택배 사칭

[C J대한통운] 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 http://tinyurl.com/yk4lalqs

② 우.체국화물 반송처리중 바로확인부탁드립니다 https://tinyurl.com/yjot7w3q

[사례 3] 백신 관련 사칭

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

① [방역센터]방역증명서 발급완료, 개인정보 인증 바랍니다. http://reurl.kr/337126CB5MK

② [코로나19예약시스템] 전자예방접종증명서 발송 완료 http://t2m.kr/MnDS

[사례 4] 공공기관 사칭

<국가건강검진>진단결과상세보기:baie.gsiw.zone

① [건강관리협회]신체검사 통지서확인:aac.gspw.mba

② [교통민원24(이파인)] 면허 벌점 과태료 통지 진정서 https://vki.kr/d2eec

[사례 5] 지인 사칭

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

① [Web발신](광고)저희 결혼식에 참석해 주시길 바랍니다. han.gl/ILSz7무료거부 0808781572

② 사랑하고 아끼면서 잘살겠습니다. 일시: 9월 11일 오후 1시, 청첩장: http://me2.do/x6j0DUji

붙임4 국민지원금 관련 스미싱 주의 안내사항

□ 이동통신 3사 (문자메시지 발송)

[국민지원금 관련 스미싱 주의 안내]

국민지원금 신청·지급시기와 맞물려 정부나 카드사를 사칭하거나 지원금 지급 대상·금액, 카드 사용 승인, 지원금 충전 등 국민지원금 안내 정보를 가장하여 의심스러운 인터넷 주소 클릭을 유도(앱 설치 유도)하는 스미싱 시도가 빈번하게 일어날 것으로 예상됩니다. 문자 속 인터넷 주소(URL)을 클릭하거나, 전화를 할 경우 피해를 입을 수 있으니 각별히 주의하시기 바라며 아래 유의 사항을 반드시 숙지하시기 바랍니다.

① 발신인이 불명확하거나 의심스러운 인터넷 주소(URL)를 포함한 문자는 절대 클릭하지 마세요.

② 의심 문자를 받았거나, 악성앱 감염이 의심되는 경우, 118센터(☎118)로 신고하시기 바랍니다.