
 관계부처 합동	보 도 자 료		 대한민국 대전환 한국판뉴딜
보도		2022.1.21.(금) 조간 부터 보도 온라인 1.20(목) 12:00	배 포 2022. 1.20(목) 09:00
책 임 자	과기정통부 사이버침해대응과장 최 미 정(044-202-6460)	담 당 자	김 남 승 사무관 (044-202-6461)
	과기정통부 통신이용제도과장 이 정 순(044-202-6650)		이 호 철 사무관 (044-202-6657)
	금융위원회 전자금융과장 김 중 훈(02-2100-2970)		안 영 비 사무관 (02-2100-2975)
	경찰청 사이버범죄수사과장 이 병 귀(02-3150-1605)		이 성 일 경정 (02-3150-1658)
	금감원 불법금융대응단 국장 박 중 수(02-3145-8150)		곽 원 섭 팀장 (02-3145-8521)
	한국인터넷진흥원 침해대응단 단장 이 동 근(02-405-6610)		박 순 태 팀장 (02-405-5421)

설 명절 택배 배송, 정부 지원금 등을 사칭한 문자결제사기(스미싱)·사기전화(보이스피싱) 주의보 발령!!

- 출처가 불분명한 문자내 인터넷주소(URL) 및 전화번호 클릭 주의
- 정부 지원금은 전화 또는 문자메시지로 신청 받지 않음
- 스마트폰 소액결제 차단기능 이용하기(통신사 고객센터)
- 스마트폰 악성코드 감염 의심 시 '내컴퓨터(PC)돌보미 서비스'로 점검 받기
- 이통3사 협력 문자결제사기·사기전화 피해예방 문자메시지 발송

□ 과학기술정보통신부(장관 임혜숙, 이하 '과기정통부'), 금융위원회(위원장 고승범), 경찰청(청장 김창룡), 금융감독원(원장 정은보), 한국인터넷진흥원(원장 이원태, 이하 'KISA')은 설 연휴를 앞두고 선물(택배) 배송 확인, 코로나19 관련 정부 지원금 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 앱 설치하도록 유도하는 공격

- 지난해('21년) 스미싱 신고(접수)·차단 20.2만여건 중 설 명절 등 택배를 많이 주고받는 시기를 악용한 택배사칭 스미싱이 17.5만여건으로 전체대비 87%를 차지하는 것으로 분석되어 택배관련 스미싱에 대한 이용자들의 각별한 주의가 요구된다.

< 최근 3년간 스미싱 유형별 신고(접수)·차단 현황 >

구분	2019	2020	2021
택배사칭	324,269	782,013	175,753
공공기관사칭	36	12,208	16,513
지인사칭	35,568	1,043	25
기타	4,713	155,579	9,985
합계	364,586	950,843	202,276

< 택배 사칭 스미싱 사례(예시) >

<p>[OO 택배] 택배 배송 불가 * 주소 불완전함 즉시 변경 부탁드립니다:< dokdo.in/V0h ></p>	<p>① 주문한 상품이 OO 택배에서 배송되었으나 주소가 확인되지 않아 반송되었으니 주소 확인 부탁드립니다. <URL> ② 미수령 택배가 있습니다. 앱다운 설치 후 확인해주세요 <인터넷주소></p>
<p>OO님 명절 선물로 모바일 상품권을 보내드립니다 확인 바랍니다. http://hpbl.are/nbaBl</p>	<p>① OO님 설 명절 선물로 모바일 상품권을 보내드립니다. 확인 바랍니다. <URL> ② 설 선물 50% 할인쿠폰 지급완료! 즉시 사용가능! 확인 <인터넷주소></p>

- 아울러, 코로나19 장기화에 따라 정부가 소상공인 등을 대상으로 하는 다양한 지원 사업을 사칭한 스미싱도 증가할 것으로 예상됨에 따라 주의가 요구된다.

- 정부는 각종 지원금 신청을 전화 또는 문자메시지를 통해 받지 않으며 신분증 등 개인정보도 요구하지 않음에 따라, 이를 요구하는 행위에 이용자는 응하지 말아야 하며, 의심이 되거나 확인이 필요한 경우는 지원금 지급 관련 정부기관에 직접 확인을 해 줄 것을 권고하였다.

< 정부지원금 사칭 스미싱 사례(예시) >

<p>[OO부 지원금 신청 안내] 귀하는 국민지원금 신청대상자에 해당되므로 온라인 센터 (http://kr.nnillida.com) 에서 지원하시기 바랍니다.</p>	<p>① 귀하는 국민지원금 신청대상자에 해당이되므로 온라인센터 <인터넷주소>에서 지원하시기 바랍니다. ② 손실보상금 지원을 위해 아래에 접속 후 신청해주시요. <인터넷주소></p>
<p>지원금 신청이 접수되었습니다. 다시 한번 확인 부탁드립니다. http://kr-jiwon.com</p>	<p>① 지원금 신청이 접수 되었습니다. 다시 한번 확인 부탁드립니다. <인터넷주소> ② 긴급 희망회복 자금 신청접수 실시('21.11.~) <인터넷주소></p>

- 스미싱을 통해 전송된 문자내 인터넷주소(URL)을 클릭할 경우, 스마트폰에 악성앱이 설치되고 악성앱을 통해 유출된 개인정보를 악용한 보이스피싱 사기 등 금전적 피해가 발생할 수 있어 이용자의 보안수칙 준수 등 각별한 주의가 필요하다.
- 이용자가 스미싱(보이스피싱) 사기 피해를 사전에 예방하기 위해 기본적으로 지켜야할 보안수칙으로는
 - △ 택배 조회, 모바일 상품권 증정, 정부 지원금 신청 등의 문자 속에 출처가 확인되지 않은 인터넷주소(URL) 또는 전화번호를 클릭하지 않고 바로 삭제하기
 - ※ 지인 등이 보낸 문자의 경우라도 반드시 전송 여부 등을 확인하기
 - △ 이벤트 당첨, 선물 배송 조회, 정부 지원금 신청 등의 명목으로 본인인증, 신분증 및 개인정보·금융정보를 요구하는 경우, 절대 입력하거나 알려주지 않기
 - △ 스마트폰 보안설정에 백신프로그램을 설치하고 업데이트 및 실시간 감시 상태 유지와 소액결제 차단 기능을 설정하기
 - ※ 스마트폰 소액결제 차단은 각 통신사 고객센터를 통해 신청
 - △ 악성앱 클릭 등 감염이 의심되는 경우 ☎ 118 신고 또는 '내PC 돌보미' 서비스 신청을 통해 스마트폰 악성코드 유·무 점검 받기
 - ※ 내PC돌보미 서비스 이용방법 : 붙임1 참조

□ 아울러, 정부는 설 명절을 앞두고 관계 부처간의 협업을 통해 국민 피해가 발생하지 않도록 스미싱·보이스피싱 주의문자 발송, 스미싱 모니터링 및 사이버 범죄 단속 강화 등을 중점적으로 실시할 계획이다.

○ 과기정통부와 KISA는 설 연휴기간 동안 스미싱 유포 등에 신속하게 대응할 수 있도록 24시간 모니터링을 실시하고,

- 신고·접수된 스미싱 정보를 분석하여 악성앱 유포지 차단 등 신속한 조치를 통해 이용자 피해를 최소화할 계획이며,
- 또한, 이통3사(SKT, KT, LGU+)와 협력하여 각 통신사 명의로 「스미싱·보이스피싱 주의문자(붙임 2)」를 순차 발송하여 국민들의 주의를 당부할 계획이다.

○ 금융위원회와 금융감독원은 설 명절 기간 동안 금융업권과의 협조를 통해 각 고객들에게 코로나19 관련 손실보상금 또는 피해회복 특별대출 등을 빙자한 사기문자에 대해 각별히 유의하도록 안내하는 등 보이스피싱 예방홍보를 집중적으로 실시하고,

○ 경찰청은 보이스피싱·스미싱 등 사이버범죄 피해 예방을 위해 경찰청 홈페이지와 모바일 앱인 '사이버캡'을 통해 예방 수칙·피해 정보 등을 제공하고,

- 설명절 연휴 기간 전후로 발생하는 보이스피싱·스미싱, 직거래 사기 등 서민생활을 침해하는 사이버범죄에 대해 단속을 강화할 계획이며,
- 사이버범죄 피해를 입었을 경우 사이버범죄 신고시스템(ECRM)을 이용해 신고를 접수해달라고 당부했다.

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

□ 정부는 코로나19 지속에 따른 사회적 이슈를 악용한 스미싱과 보이스피싱 범죄가 지능화하고 있어, 이를 예방하기 위해서는 이용자의 보안수칙* 준수와 함께 피해 발생(의심) 시, 스미싱은 한국인터넷진흥원(☎118), 보이스피싱 피해발생시, 해당 금융회사 콜센터, 경찰청(☎112) 또는 금감원(☎1332)에 즉시 신고하고 계좌의 지급정지 등을 신청을 해 줄 것을 당부하였다.

* 10대 스마트폰 보안수칙 : 붙임 3 참고

붙임 1 내PC 돌보미 스마트폰 점검 서비스 받기

□ 내PC 돌보미 서비스란?

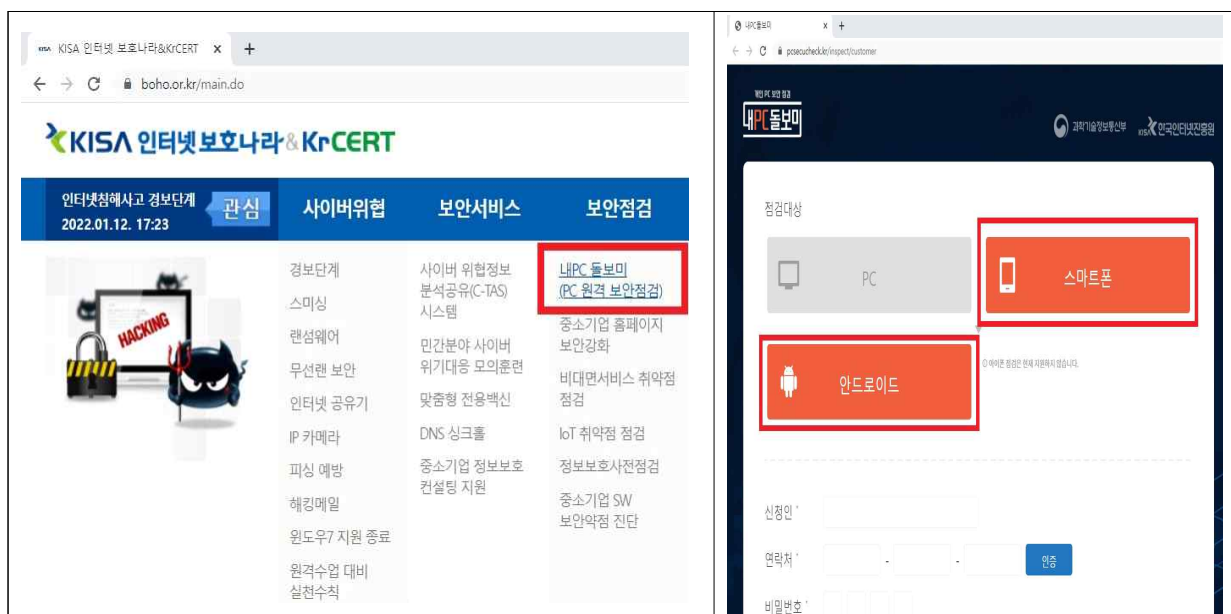
- 사이버 위협에 즉각적으로 대응이 어려운 대국민 PC·스마트폰(안드로이드) 이용자를 대상으로 원격 보안점검을 통해 안전조치를 지원



- (스마트폰 보안점검) 악성코드 유·무 점검, 잠금 설정, 최신 보안 업데이트, 앱 권한 관리, 백신 설치 및 실시간 감시기능 활성화 등
- (서비스 시간) 평일 08시~22시, 토·공휴일 09시~18시(일요일 휴무)
- (이용안내) ☎ 1899-3313, ☎ 118(ARS 2번), 보호나라 홈페이지 참조

□ 서비스 신청 방법

- 한국인터넷진흥원 보호나라 홈페이지(www.boho.or.kr)에서 보안점검 → 내PC 돌보미 → 스마트폰 → 안드로이드 선택 후 서비스 신청



과기정통부, 금융위, 경찰청 합동으로 설 명절에 앞서 택배 배송조치, 정부지원금 신청 등을 빙자한 스미싱·보이스피싱 피해가 예상되니 예방을 위해 대응 요령을 안내 드립니다.

▶ 이런 경우 스미싱·보이스피싱을 의심하고 대응하세요.

- ① 검·경·금감원은 어떤 경우에도 금전의 이체를 요구하거나 금융거래정보를 수집하지 않습니다. 이런 경우 공신력 있는 전화번호 등을 이용하여 사실 여부를 다시 확인하세요.
- ② 불법 스팸문자를 보고 연락하지 마세요. 신용등급 상향, 저금리 전환, 대출수수료 명목의 금전 및 개인정보 요구는 거절하세요. 또한, 이를 위한 금융상담원의 앱 설치 요구는 100% 보이스피싱입니다.
- ③ 가족의 긴급상황(전화고장, 납치 등)이라며 연락받은 경우, 전화통화 등으로 해당 가족이 보낸 사실이 맞는지 확인하세요.
- ④ 가까운 사이라도 메시지로 신분증, 카드·계좌 비밀번호를 요구하면 거절하고, 출처 불명의 인터넷 주소(URL)는 절대로 클릭하지 마세요.
- ⑤ 피해가 의심된다면 스미싱의 경우, 한국인터넷진흥원(☎ 118), 보이스피싱의 경우, 해당 금융회사 콜센터, 경찰청(☎112) 또는 금감원(☎1332)에 즉시 전화하여 확인하고 피해 발생시 계좌의 지급정지 등을 신청하세요.

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 인터넷주소(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

한국인터넷진흥원

* 자료 : 과학기술정보통신부, 한국인터넷진흥원

- 7 -