



보도시점 온라인 : 2024. 9. 8.(일) 12:00
지면 : 2024. 9. 9.(월) 조간

배포 2024. 9. 6.(금) 14:00

정부, 추석명절 보이스피싱 등 사이버사기 대응 요령 안내

- 출처가 불분명한 문자의 인터넷주소(URL)나 전화번호 클릭 주의 -

과학기술정보통신부(장관 유상임, 이하 ‘과기정통부’), 방송통신위원회(위원장 직무대행 김태규, 이하 ‘방통위’), 금융위원회(위원장 김병환, 이하 ‘금융위’), 경찰청(청장 조지호), 한국인터넷진흥원(원장 이상중, 이하 ‘KISA’), 금융감독원(원장 이복현, 이하 금감원)은 추석 연휴를 앞두고, 보이스피싱, 교통법규 위반 범칙금, 쓰레기 무단투기 과태료 조회 등 공공기관 사칭, 명절 선물을 위한 쇼핑물을 사칭하여 대금을 갈취하는 문자사기(스미싱*) 등 다양한 사이버사기에 대한 국민 피해 최소화를 위한 주의를 당부했다.

* 문자메시지(SMS)와 피싱(Phishing)의 합성어. 악성 앱 주소가 포함된 휴대폰 문자를 전송하여 이용자가 악성 앱 설치 또는 통화를 유도하여 금융정보·개인정보 등을 탈취하는 수법(보이스피싱, 전자상거래 사기 등에 악용)

스마트폰 사용이 일반화되면서 금전적 이익 또는 개인정보 등의 탈취를 목적으로 하는 문자 발송이 크게 증가하고 있으며, 특히 국민들이 속기 쉽도록 공공기관, 지인 등을 사칭하는 문자 발송의 비중이 매우 높다.

관계 당국에서 탐지한 문자사기 현황('22년~ '24.상반기)을 살펴보면, 공공기관을 사칭하는 유형이 합계 116만여 건(71.0%)에 이르고, 청첩장, 부고장 등 지인 사칭형도 27만여 건(16.8%)으로 꾸준히 증가하고 있으며, 올해는 주식·가상자산 투자 유도, 상품권 지급 등 투자·상품권 사칭형이 2만여 건(1.3%)으로 전년에 비해 크게 증가하였다.

< 문자사기(스미싱) 신고(접수)차단 현황 >

(단위: 건)

구 분	2022년	2023년	2024년8월	합 계
전 체	37,122	503,300	1,092,838	1,633,260
기관사칭유형(%)	17,726(47.8%)	350,010(69.5%)	792,496(72.5%)	1,160,232(71%)
지인사칭유형(%)	4(0.0%)	59,565(11.8%)	214,589(19.6%)	274,158(16.8%)
투자·상품권 유형(%)	110(0.3%)	164(0.1%)	20,975(1.9%)	21,249(1.3%)
택배유형(%)	19,214(51.8%)	91,159(18.1%)	7,304(0.7%)	117,677(7.2%)
기타(%)	68(0.2%)	2,402(0.5%)	57,474(5.3%)	59,944(3.7%)

※ 자료출처 : 과기정통부·KISA

정부는 이번 추석 명절 전후에도 범칙금, 과태료, 지인의 부고, 명절 선물 등을 사칭하여 명절 분위기에 들뜬 국민들이 쉽게 속아 넘어갈 수 있는 상황을 악용하는 문자가 다량 유포될 수 있어서 국민들의 각별한 주의를 당부했다.

이와 같은 문자 사기 외에도 정상문자처럼 속인 후 메신저앱으로 유도해 금전이나 상품권, 금융거래 정보 등을 요구하는 메신저 피싱* 피해가 증가하는 추세를 보이고 있어서 이에 대한 주의도 필요하다.

* 휴대전화 고장, 신용카드 도난·분실, 사고 합의금, 상품권 대리 구매 등

특히, 유포된 미끼 문자를 통해 원격조종이 가능한 악성 앱이 스마트폰에 설치되면 재산상 피해가 발생할 수 있으므로 전화, 영상통화 등으로 상대방을 정확하게 확인하기 전에는 악성 앱 설치를 유도하는 상대방의 요구에 응하지 말아야 한다.

정부는 다문화, 고도화되는 사이버사기에 대한 국민 피해를 사전에 예방하기 위해서는 다음과 같은 보안 수칙을 생활화할 필요가 있다고 강조하였다.

< 사이버사기 피해 예방을 위한 보안수칙 >

- ① 택배 조회, 명절 인사, 모바일 상품권·승차권·공연예매권 증정, 지인사칭 문자에 포함된 출처가 불명확한 인터넷주소(URL) 또는 전화번호를 클릭하지 않을 것
- ② 출처를 알 수 없는 앱은 함부로 설치되지 않도록 스마트폰 보안설정을 강화하고, 앱 다운로드를 받은 문자의 링크를 통해 받지 말고 공인된 열린시장(오픈마켓)을 통해 설치할 것
- ③ 스마트폰에 백신프로그램을 설치하여 주기적으로 업데이트 하고, 실시간 감시 상태를 항상 유지할 것
- ④ 본인인증, 재난지원금 및 백신예약 조회 등의 명목으로 신분증 등 개인정보·금융정보를 요구하는 경우, 절대 입력하거나 알려주지 않을 것
- ⑤ 대화 상대방이 개인·금융정보나 금전을 요구하거나 앱 설치를 요구하는 경우 반드시 전화, 영상통화 등으로 상대방을 정확하게 확인할 것
- ⑥ 신분증 사진 등이 유출되지 않도록 스마트폰 내에 저장된 주민등록증, 운전면허증, 여권 사진을 바로 삭제할 것

정부는 국민들이 안심하고 추석 명절을 보낼 수 있도록 관계부처들이 협력해 24시간 사이버 안전 대응체계를 마련하고, 스미싱 등 다양한 사이버 사기에 대한 감시와 사이버 범죄 단속을 중점적으로 실시할 계획이다.

< 추석 전 기관별 사이버사기 예방활동 현황 >

정부	주요내용	협력기관
과기정통부	24시간 탐지체계 운영, 스미싱 확인서비스, 피싱사이트 및 악성 앱 유포지 등 긴급차단, 사이버사기 주의 SNS 홍보 등	KISA
방통위	「스미싱 문자 주의 안내」 문자 메시지 발송	이통3사, KAIT
금융위	소포·택배상자 활용 사이버사기 예방 홍보, 여신거래 안심차단 서비스 및 휴대폰 기기 내 보안강화 기능 활용방법 홍보	금융감독원, 금융사, 우정사업본부, 전국상인협회
경찰청	사이버사기 예방수칙 제공, 인터넷 사기 의심 계좌조회 서비스 제공, 사이버범죄 피해신고(112, 경찰청 사이버범죄 신고시스템)	

< 사이버사기 예방 홍보 추진 >

과기정통부와 KISA는 추석 연휴기간 동안 문자사기에 신속하게 대응할 수 있도록 24시간 탐지체계를 운영하고, 스미싱확인서비스* 등을 통해 신고·접수된 문자사기 정보를 분석하여 피싱 사이트, 악성 앱 유포지 등에 대한 긴급 차단조치를 지원하여 국민들의 피해를 최소화할 계획이다.

* 카카오톡앱에서 채널 친구로 '보호나라'를 추가, '스미싱' 메뉴를 통해 의심되는 문자메시지를 입력하면 메시지 분석 후 10분 이내 '주의', '악성', '정상' 답변 제공

방통위는 이동통신 3사(SKT, KT, LGU+), 한국정보통신진흥협회(KAIT)와 협력하여 9월 2일부터 각 통신사 명의로 가입자에게 『스미싱 문자 주의 안내』 문자 메시지를 순차 발송한다. <붙임 4 참고>

금융위원회와 금융감독원은 우정사업본부 및 (주)한진·전국상인연합회와 공동으로 서울과 수도권 지역의 우체국 소포상자(10만개)에 스미싱 주의 메시지를 인쇄하고, 전국 66개 전통시장에서는 각지로 배송되는 택배상자에 스미싱 예방문구를 담은 스티커(1만장)를 부착함으로써 소포·택배 이용자가 일상에서 스미싱의 위험성을 쉽게 인식할 수 있도록 지원하고 있다.

또한, 금융소비자들이 「여신거래 안심차단」 서비스(8.23일부터 시행)*와 휴대폰 기기 내 보안 강화 기능**을 보이스피싱 피해예방 수단으로 적극 활용할 수 있도록 서비스 이용 방법을 금융회사 영업점에서 적극 안내하고, 객장 모니터를 통해 홍보영상을 송출하는 한편, 금융앱(알림톡)이나 자체 운영중인 SNS 채널 등을 통해서도 고객에게 전파하고 있다.

* 금융소비자가 본인이 원하지 않는 여신거래로 인한 피해를 입지 않도록 신용대출, 카드론 등 개인의 신규 여신거래를 사전에 차단할 수 있도록 신청할 수 있는 서비스
☞ 「여신거래 안심차단」 서비스 이용방법 : <붙임5> 참조

** 알 수 없는 출처의 앱이 휴대폰에 설치되는 것을 제한하여 악성앱 설치를 미연에 방지
☞ 알 수 없는 출처의 앱 설치 차단 방법 : <붙임6> 참조

경찰청은 추석 연휴 기간 전후 발생하는 사이버사기 및 스미싱 범죄에 대한 단속을 강화하고 피해 예방을 위해 누리집과 사회관계망(SNS)을 통해 예방수칙을 제공할 계획이다. 또한, 연휴 중에는 택배 미운영 기간이 길어 사기피해 확인이 늦을 수 있는 만큼 가급적 비대면 거래를 지양하고, 거래에 앞서 경찰청 누리집에서 제공하는 『인터넷 사기 의심·계좌번호 조회』 서비스를 통해 사기피해 발생 여부를 확인할 것을 당부하였다.

< 사이버사기 피해 또는 의심되는 경우 조치방법 >

악성앱 설치 등으로 금융정보 유출이 의심되는 경우, 본인이 거래하는 금융회사 영업점을 방문하거나 콜센터에 전화하여 본인 계좌에 대해 일괄 지급정지를 요청함으로써 피해를 최소화하고, 특히 보이스피싱 사기범에게 속아 피해금을 계좌로 송금한 경우에는 경찰청(☎112)에 피해사실을 신고하고 범인이 돈을 옮기지 못하도록 즉시 지급정지를 신청*할 것을 당부했다.

* 돈이 출금되거나 입금된 은행 콜센터 연락하여 지급정지를 신청하는 것도 가능

명절 연휴 중 스미싱 등 사이버범죄 피해를 입은 경우, 경찰청(☎112)에 신고하거나 『경찰청 사이버범죄 신고시스템(ECRM)』을 통해 온라인으로 피해신고를 접수할 수 있다.

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

또한 문자사기 의심 문자를 수신하였거나, 악성 앱 감염 등이 의심되는 경우 ‘보이스피싱지킴이’에 신고하거나, 국번없이 118 상담센터(KISA운영)에 연락하면 24시간 무료로 상담 받을 수 있다.

< 사이버사기 피해 또는 의심되는 경우 신고방법 등 >

사이버사기 사례(의심)	조치방법
○ 보이스피싱 사기범에게 속아 피해금을 계좌로 송금한 경우	경찰청(☎112) 신고 및 송금계좌에 대한 지급 정지 요청 ※ 돈이 출금되거나 입금된 금융회사 콜센터에 연락하여 지급정지 신청하는 것도 가능
○ 악성앱 설치 등으로 개인정보 유출이 의심되어 보이스피싱 우려	금융회사 영업점을 방문하거나 콜센터에 전화하여 본인 계좌에 대해 일괄 지급정지를 요청
○ 사이버사기 범죄 피해 시	경찰청(☎112)에 전화신고 또는 사이버범죄 신고센터(ECRM)에 온라인 신고
○ 문자사기 의심문자 수신 또는 악성 앱 감염 의심 시	① 보호나라 스미싱확인서비스 이용 악성 확인 ※ 카카오톡 채널에 '보호나라'를 검색하여 접속 ② KISA(☎118) 상담센터에 상담 ③ 보이스피싱지킴이에 신고(금감원) ※ 네이버에 '보이스피싱지킴이'를 검색하여 접속

담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	최광기	(044-202-6460)
		담당자	사무관	김성환	(044-202-6461)
	방송통신위원회 디지털이용자기반과	책임자	과 장	고남현	(02-2110-1520)
		담당자	사무관	김상엽	(02-2110-1527)
	금융위원회 금융안전과	책임자	과 장	이진호	(02-2100-2970)
		담당자	사무관	유은지	(02-2100-2974)
	경찰청 사이버범죄수사과	책임자	과 장	함영욱	(02-3150-1605)
		담당자	경 정	이여정	(02-3150-1658)
	한국인터넷진흥원 국민피해대응단	책임자	단 장	이동연	(02-405-6640)
		담당자	팀 장	김은성	(02-405-5363)
	금융감독원 금융사기대응단	책임자	국 장	임정환	(02-3145-8150)
		담당자	팀 장	정재승	(02-3145-8130)



[사례 1] 추석 명절 사칭

추석 잘 보내시고 2024년 남은 시간 모두 행복한 시간 되시길 바랍니다. ▼x.xx/xxxx

- ① 추석 돈 나갈 일 많으시죠? 하루 30분이면 충분합니다. <URL>
- ② 추석선물 도착 전 상품 무료 배송! 할인쿠폰 지급 완료! 즉시 사용가능! 확인 <URL>

[사례 2] 택배 사칭

고객님의 주소가 정확하지 않아 귀하의 상품을 배달할 수 없습니다. 주소를 정확히 입력해 주세요:xxx.xxxx

고객님 택배 배송주소 불일치로 물품이 취소되었습니다.배송주소 확인 http://xxxx.xxx

- ① 고객님의 택배 배송주소 불일치로 물품이 취소되었습니다.배송주소 확인 <URL>
- ② 운송장번호(5*****19): 물품지연 확인하시기바랍니다. <URL>
- ③ 우편번호 오류로 인해 배송이 보류되었습니다. 최대한 빨리 작성하여 다시 보내주세요 <URL>
- ④ 고객님의주소가정확하지않아귀하의상품을발송할수없습니다주소를정확히입력해주세요 <URL>
- ⑤ 주문하신 물품 O/OO 배달예정, 주소재확인바람 <URL>

[사례 3] 상품권 사칭

【OO 이벤트 현금 문화상품권 1만원권 당첨 축하드립니다.▶아래 링크 당첨인: 간편 입력하고 현금상품권 1만원-최대50만원까지 받기▶ https://xxx.xxxx※ 수신된 번호는 문자발송 전용이므로 간편 응모시 【카OO】으로 안내 해드립니다.

- ① 【OOOOO/이벤트 현금문화상품권 당첨 축하드립니다】《대기업 와 함께하는뱅크샐러드 이벤트》OO VS OO 제품
- ② [OO]에서 전달된 소식입니다!▶세배는 마음으로▶세뱃돈은 [OO]에서▶설날 이벤트 50000원 모두에게 지급
- ③ 대기업전자제품현금문화상품권당첨축하드립니다.간편 입력하고현금받기<URL>

[사례 4] 리딩방

억을 모으는 방법 300만 ▶1984만 소요기간 단 3일 xx.xx/xxxxxx 상담▲ 광고거부

- ① 추석 여유자금"이것"으로마련하세요 ↓↓↓↓↓<URL>
- ② 이번 수익율 28% 종목 무료수령!! <URL>
- ③ 전문가는 또 다른 두 가지 급등 주식을 추천할 예정입니다. 기회는 눈앞에 있으니 주식 시장에서 성공적으로 투자할 수 있도록 도와드립니다. <URL>
- ④ 억을 모으는 방법 300만▶1984만 소요기간 단 3일 <URL> 상담

[사례 5] 공공기관 사칭

귀하께 음식물분리수거 위반으로 신고되었습니다.내용확인:
http: xxx.xxxx/xxx

2024/07/18 층간소음행위 1건 신고되었습니다- 이의제기 관할경찰서 방문내역 : xxx.xx/xxx

- ① [Web발신] 도로교통위반 벌금고지서 <URL>
- ② 2024/07/18 층간소음행위 1건 신고되었습니다- 이의제기 관할경찰서 방문내역 : <URL>
- ③ 2024/07/13 지하철 불법촬영물소지 1건 신고 접수되었습니다- 수사협조 통지안내 :<URL>
- ④ [서울지방청] (7**6) 06/10 폭력/스토킹관련 접근금지명령 접수되었습니다상세 : <URL>
- ⑤ [국민건강보험]건강검진결과서 발송완료상세보기 <URL>
- ⑥ 쓰레기분리 위반대상으로 민원이 신고 되어 안내드립니다. 신고내용 보기 <URL> 민원24

[사례 6] 지인 사칭

①24일 박OO 자녀 결혼식에 초대합니다. 식장 : xxx.xx/xxx

8월 22일, 어머니가 심장마비로 22시에 돌아가셨습니다 빈소:< xxx.xx/xxx >

- ① 저희 아버지께서 어젯밤 22시에 심혈관 및 뇌혈관 질환으로 돌아가셨습니다..추도식 :<URL>
- ② 아바님께서 오늘 별세하셨기에 삼가 알려드립니다. 장례식장 <URL>
- ③ [玆以(상보)]6월26일 [노환으로]부친께서 별세.삼가 故 人의 冥福을 .빈소<URL>
- ④ 3월30일(토) 저희 이쁜 손녀딸 첫돌을 맞이하게 되었습니다. <URL>

[사례 7] 기타

[국제발신]OOOOOO id에 연체된 청구서가 있습니다. 로그인하여 확인해 주십시오: http://xxx.xxxx

[OO프]한국소비자보호원 중재를 통해 즉시 환불이 지급됩니다신청 : xxx.xx/xxx

- ① [Web발신][O팡]신규상품 사용 해보시고 리뷰도 하시면제품과 포인트 팡팡~!!안내상담 링크 연결하기: <URL> ※ 원하시는 시간대 자율근무 가능 / 교육비,위탁비,수수료 절대 없음
- ② [텔OO램]회원님의 계정 로그인이 비정상적입니다. 본인인증을 완료해 주세요. <URL>
- ③ 일반 영상은 가라이젠 AI기술로 연예인/옆집누나의 사생활을 감상해보세요 <URL>
- ④ 귀하의 계정은 휴면 상태입니다. 최대 절전 모드를 방지하려면12시간 이내에 <URL>를 확인하세요

- '22. 8월 피해자 A는 “엄마 내꺼 핸드폰 떨어트려서 화면이 깨져 수리 맡겼어 이 번호로 특친구 추가하고 특취”라는 문자를 수신
- 문자 발송 전화번호를 메신저앱에 등록하고 메시지를 보내자 “가족명의로 핸드폰 액정 보험에 가입하면 수리비가 공짜라는데 가족명의 인증이 필요해, 엄마 주민등록증사진, 계좌번호랑 비밀번호 보내줘, 빗반사 없이 네면 잘보이게”라며 개인정보, 금융거래정보 요구
- 피해자가 개인·금융정보를 보내자 다시 “인증이 안되네, 내가 엄마폰 연결해서 할게, 눌러서 설치하고 열면 귀하의 아이디 9자리라고 나오면 나한테 보내줘”라며 인터넷주소(URL)를 보내 원격제어앱* 설치를 유도
 - * 원격제어앱 이용은 휴대전화로 할 수 있는 비대면 계좌개설, 이체, 대출 등 모든 행위를 상대방이 할 수 있게 해준다는 의미로, 반드시 제어 상대방 신분 확인 필요
- 피해자 인터넷 주소(URL)를 클릭해 앱 설치 후 접속정보를 알려주자 “내가 폰 다 사용하고 얘기할게, 폰 그냥 가만히 놔둬”라고 하며 사기범이 피해자 휴대전화를 제어, 은행·증권앱 등을 이용해 수십 회에 걸쳐 약 1억 5천만 원을 다수의 대포계좌로 이체하고,
 - ※ 휴대전화로 신청 가능한 비대면 대출을 이용, 대출금까지 편취해가는 사례 다수 발생
- 온라인 쇼핑몰, 게임앱 등에서 전자지급결제대행 (PG) 서비스를 이용해 약 1천만 원 상당의 상품권(기프트 카드), 게임 아이템 등을 구매함
- 범행 중간에 이상함을 느낀 피해자가 전화통화를 요청하거나 출신학교, 지인들의 이름 등을 물어봤지만 사기범은 “엄마 왜 그래, 아들이라니까, 지금 거의 다 했어 끝나고 전화할게, 컴퓨터 메신저라 전화 못해”라며 통화 및 답변을 회피, 시간을 끌며 계속 범행을 이어감

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

□ **이동통신3사 [문자메시지 발송]**

[추석 연휴 스미싱 문자 주의 안내]

추석명절을 앞서 코로나19 정부지원금 지급대상, 택배 배송조회 등을 사칭한 스미싱 문자가 예상되오니 피해예방을 위해 다음 유의사항을 안내 드립니다.

1. 출처가 불분명한 문자를 받은 경우 인터넷주소(URL)나 전화번호는 절대 누르지 마시고 '스팸으로 신고' 또는 경찰청(☎112)으로 신고하시기 바라며, 카카오톡 「보호나라」 채널 '스미싱확인서비스'에 의심문자의 '정상' 여부를 확인하시기 바랍니다.
2. 출처를 알수 없는 앱은 함부로 설치되지 않도록 스마트폰 보안 설정을 강화해 주시기 바랍니다.

<안드로이드폰 설정 방법>

스마트폰 '설정' 앱 클릭 → '보안 및 개인정보 보호' 메뉴 접속 → '보안 위험 자동 차단' 활성화

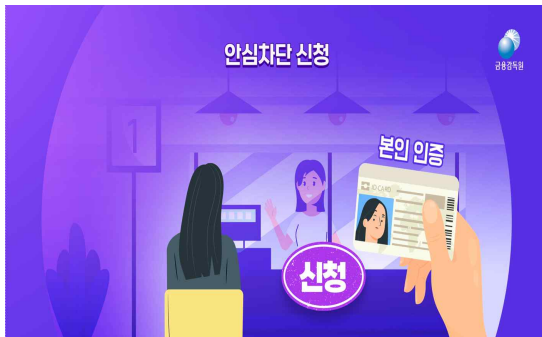
3. 개인정보 유출로 인해 본인이 원하지 않는 여신거래가 발생하여 피해를 입지 않도록 금융회사를 방문하여 '여신거래 안심차단 서비스'를 신청하시기 바랍니다.
4. 사이버사기 범죄피해를 입은 경우 112 또는 경찰청 홈페이지 신고창구로 즉시 신고하여 주시기 바랍니다.

※ 9월2일부터 순차적으로 이통 3사를 통해 문자발송 예정

붙임5

「여신거래 안심차단」 이용방법

① 여신거래 안심차단 신청(은행, 저축은행, 농·수협, 새마을금고, 신협, 산림조합, 우체국)



- ▶ 이용자는 현재 거래 중인 금융회사 영업점을 방문하여 본인확인 후 여신거래 안심차단을 신청
- ▶ 안심차단 신청 즉시, 금융권의 신규 여신거래가 차단됩니다.



② 차단되는 여신거래



- ▶ 안심차단 신청시, 금융회사의 신용대출, 카드로, 신용카드 발급, 할부금융, 예·적금 담보대출 등 개인의 여신거래가 실시간 차단됩니다.



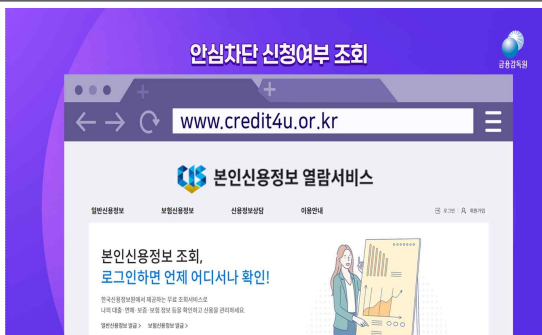
③ 여신거래 안심차단 해제(은행, 저축은행, 농·수협, 새마을금고, 신협, 산림조합, 우체국)



- ▶ 기존 거래여부와 무관하게 가까운 금융회사 영업점을 방문하여 본인확인 후 손쉽게 해제 가능
- ▶ 이용자는 필요한 여신 실행 이후, 안심차단의 재신청도 가능합니다.



④ 여신거래 안심차단 신청여부 조회 및 통지


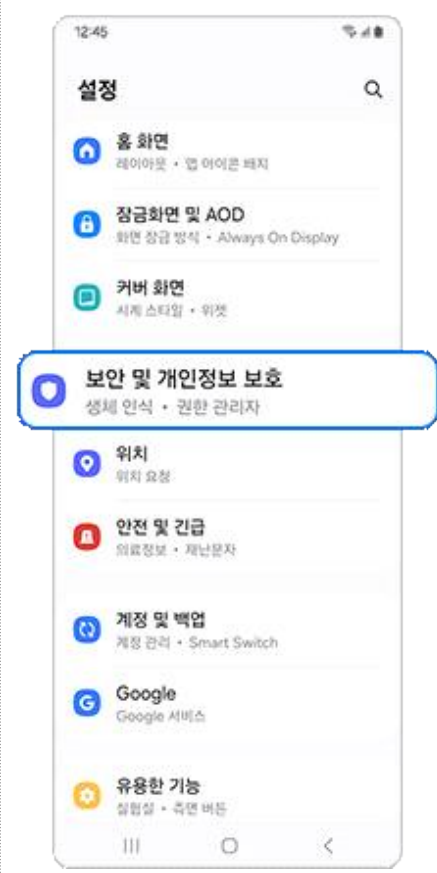


- ▶ 이용자는 본인의 안심차단 신청여부에 대해 한국신용정보원 홈페이지*를 통해 직접 조회 가능(신청 및 해제 상태 확인가능)

* www.credit4u.or.kr

- ▶ 안심차단을 신청한 금융회사에서 반기 1회 안심차단 신청사실을 이용자에게 통지합니다.

< 차단 기능 설정 방법(안드로이드) >

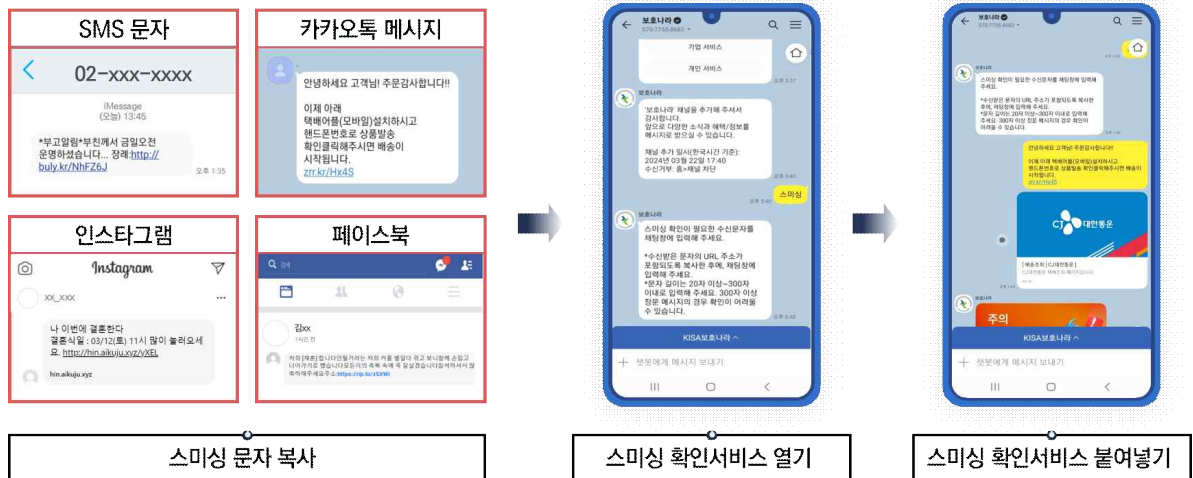
		
<p>1. 스마트폰 '설정' 앱 클릭</p>	<p>2. '보안 및 개인정보 보호' 메뉴 접속</p>	<p>3. '보안 위험 자동 차단' 활성화</p>

※ 차단 방법은 스마트폰에 탑재된 안드로이드 OS 버전에 따라 다를 수 있음

1. 카카오톡 채널 검색 후, ‘보호나라’ 채널추가



2. 채널 창내 ‘스미싱’ 클릭 후 메시지 복사 및 붙여넣기



3. 결과 확인



☑ ‘주의’ : 10분 후에 ‘접수결과확인’ 클릭하여 재확인, 링크 클릭 자제

☑ ‘악성’ : 해당 메시지를 삭제·차단

권역	기관	콜센터 번호	권역	기관	콜센터 번호
은행	산업	1588-1500	증권사	DB금융투자	1588-4200
	농협	1661-3000 1522-3000		K B	1588-6611
	신한	1577-8000 1599-8000 1544-8000		L S	1588-2428
	우리	1588-5000 1599-5000 1533-5000		NH투자	1544-0000
	기업	1566-2566 1588-2588		S K	1588-8245 1599-8245
	국민	1588-9999 1599-9999 1644-9999		교보	1544-0900
	SC제일	1588-1599		다올투자	1588-3100
	하나	1588-1111 1599-1111		대신	1588-4488
	씨티	1588-7000		메리츠	1588-3400
	수협	1588-1515 1644-1515		미래에셋	1588-6800
	아이엠	1566-5050 1588-5050		부국	1588-7744
	부산	1544-6200 1588-6200		삼성	1588-2323
	광주	1588-3388 1600-4000		신영	1588-8588
	제주	1588-0079		신한투자	1588-0365
	전북	1588-4477		아이엠	1588-7171
	경남	1600-8585 1588-8585		유안타	1588-2600
	케이	1522-1000		유진투자	1588-6300
	카카오	1599-3333		케이프투자	1544-7600
	토스	1661-7654		키움	1544-9000 1544-9911
제2금융	농협중앙회	1661-2100 1588-2100		하나	1588-3111
	수협중앙회	1588-1515 1644-1515		한국투자	1544-5000
	산림조합중앙회	1544-4200		한화투자	080-851-8282
	신협중앙회	1566-6000 1644-6000		현대차	1588-6655
	저축은행중앙회*	02-3978-800			
	새마을금고중앙회	1599-9000			
	우정사업본부	1588-1900			

* 영업시간 중에는 개별 저축은행 콜센터에서 일괄지급정지 신청 접수