

빗썸 오지급 보상 안내의 URL링크는 사기입니다.

- 빗썸 오지급 사고 관련 스미싱 소비자경보 발령 -

■ 소비자경보 2026 - 7호

등급	주의 경고 위험
대상	금융소비자 일반

소비자경보 내용

- 최근 빗썸의 오지급 사고 관련 보상금 지급 발표로 국민들의 관심이 높아지면서 스미싱* 피해 우려도 커지는 상황

* 문자메시지(SMS)+피싱(Phishing)의 합성어로 악성앱 주소(url)이 포함된 휴대폰 문자(SMS)나 카카오톡 등 메시지를 대량 전송 후 이용자가 클릭하도록 유도, 개인정보, 금융거래정보 등을 탈취

- 빗썸은 보상금 지급 관련 개별 안내를 아직 실시하지 않았으며, 향후 고객 안내시 인터넷 주소(URL)를 절대 포함하지 않을 예정

- 빗썸 등을 사칭한 메시지의 URL 클릭시 개인정보 노출 및 금융 피해가 발생할 수 있으므로 **절대로 클릭 금지**

<소비자 유의사항 및 대응요령>

- 1) 빗썸 오지급 보상금 관련 URL 링크는 100% 사기이므로 **클릭 금지**
- 2) '보상', '피해사실 조회' 등 키워드는 **일단 의심**
- 3) 스미싱이 의심되면 **보호나라 서비스**를 이용하여 확인
- 4) 피해 발생시 신속한 **신고** 및 **지급정지** 요청

I 소비자경보 배경

- 최근 빗썸이 오지급 사고 관련 일부 고객에 보상금을 지급하겠다고 밝혀 국민들의 관심이 높아지면서, 스미싱 피해가 우려되는 상황입니다.
- 이에 금융당국은 그간 사회적 이슈가 발생할 때마다 이를 악용하는 스미싱 사기가 단기간에 확산된 점을 고려하여
 - 빗썸 오지급 사고를 미끼로 접근하는 스미싱 사기에 대해 **소비자 유의사항**을 안내하고 **소비자경보(주의)**를 발령하였습니다.

II 금융당국의 대응

- 금융당국은 빗썸이 보상금 지급 관련 고객 안내시 메시지에 **인터넷 주소(URL 링크)**를 **절대** 포함하지 **않도록** 하였고,
 - 이와 유사한 기능을 하는 **배너 링크, 앱푸쉬 기능**도 제공하지 **않도록** 하였습니다.
 - 아울러 빗썸도 스미싱 유의사항에 대해 추후 대고객 안내를 실시하도록 하였습니다.

III 소비자 유의사항

① 빗썸 오지급 보상금 관련 URL 링크는 100% 사기이므로 클릭 금지

- 문자·카톡 메시지에 포함된 출처가 의심스러운 인터넷 주소(URL)를 클릭할 경우 악성앱이 설치되어 개인정보 유출 및 금융피해 등이 발생할 수 있습니다.
- 특히 빗썸 오지급 보상금 안내 메시지에 URL 링크가 포함되어 있다면 100% 사기이므로 절대 클릭하면 안 됩니다.

* 알 수 없는 출처의 앱 설치 차단을 위한 휴대폰 보안설정 방법 : <붙임1> 참조

□ 악성앱이 설치되면 사기범이 휴대폰에 저장된 메시지, 통화내역, 사진, 연락처 등을 볼 수 있고, 발신번호를 빗썸 고객센터 번호 등으로 변작 표시하여 전화를 걸 수도 있습니다.

○ 또한 피해자가 도움을 요청하려고 112, 1332 등에 연락을 해도 사기범이 전화를 받을 수도 있습니다(일명 '통화 가로채기').

○ 악성앱이 설치되었다면 비행기 모드 실행 및 휴대폰 초기화 등을 진행하고, 경찰서에 직접 방문하여 피해를 신고하세요.

※ (참고) 2.11일 현재까지 보상금 지급 절차 등이 확정된 바 없으며, 보상금 지급에 대한 개별 안내를 이미 받았다면 사기일 가능성이 높습니다.

② '보상', '피해사실 조회' 등 키워드는 일단 의심

□ 메시지에 '보상', '피해사실 조회', 등 키워드가 있다면 일단 스미싱을 의심할 필요가 있고

○ 메시지에 기재된 고객센터 번호도 사기범 번호일 가능성이 있으니 반드시 고객센터 공식 번호(1661-5566)로만 전화를 걸어야 합니다.

※ 스미싱 문자 예시(가상의 사례)

[빗썸 고객센터]
보상금 지급 대상자로 선정되었습니다. 관련 절차 안내를 위해 상담이 필요합니다. 1500-XXXX

전산 오류로 인한 코인 오지급 가능성이 확인되었습니다. 대상 여부를 확인하시기 바랍니다.
<https://bithumb.check/>

[빗썸]
코인 오지급 관련 보상금 지급 안내입니다. 지금 바로 확인하세요.
(이미지 클릭)

③ 스미싱이 의심되면 보호나라 서비스를 이용하여 확인

□ 스미싱이 의심되는 메시지를 받은 경우 한국인터넷진흥원(KISA)의 보호나라 서비스 등을 통해 스미싱 여부를 확인할 수 있습니다.

※ 스미싱 문자 제보 방법 (1) - 경찰청 통합대응단 홈페이지 이용

전기통신금융사기 통합대응단 통합제보 전기통신금융사기란? 예방 및 조치 알람 소식 기관소개 로그인 보이스피싱 제보를 한 번에!!

아너도? 아나도!

전기통신금융사기 통합제보하기

제보방법 안내

통합 제보하기

보이스피싱으로 의심되는 연락처를 제보하세요.

보이스피싱으로 실제 피해를 받았다면? 즉시 112로 제보하세요

보이스피싱 제보

피싱(사기)로 인한 피해 금액을 신고하면, 해당 금액을 환불받을 수 있습니다. (통화내역 등 관련 자료를 첨부할 수 있습니다.)

스미싱 문자 제보

악성 앱 설치 등 의심되는 문자를 신고하면, 해당 문자를 삭제할 수 있습니다.

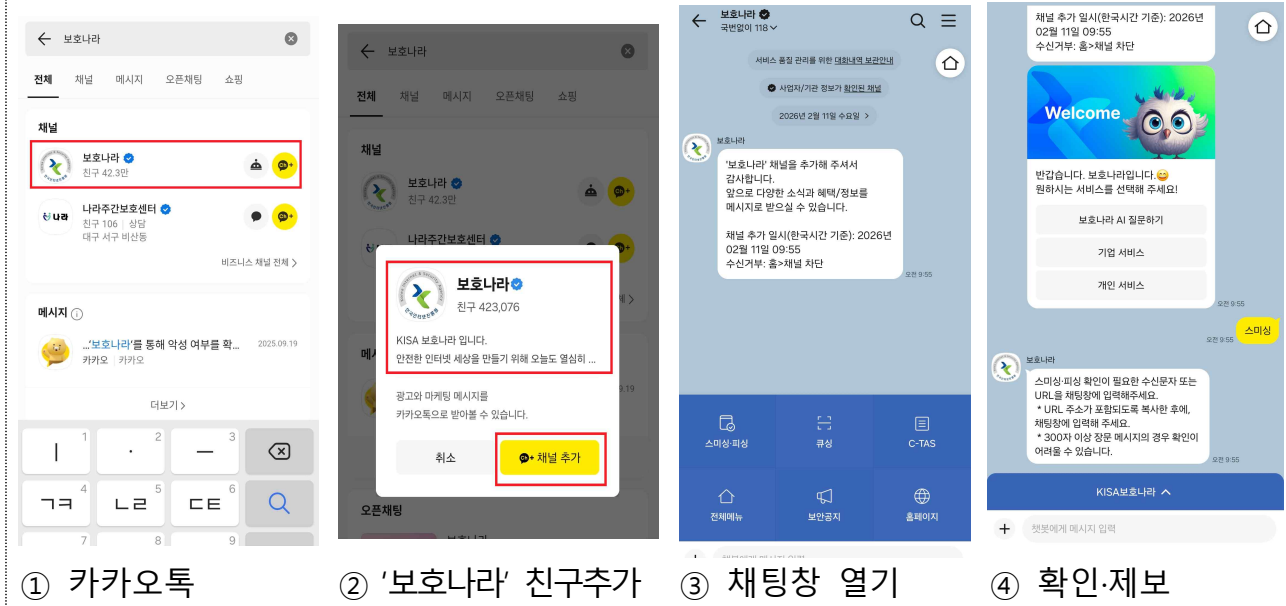
발신번호 거짓표시 제보

가장먼저(가장) 발신번호로 표시하는 행위를 제보할 수 있습니다.

① 통합대응단 홈페이지 > '통합 제보하기' ② '스미싱 문자 제보' 클릭

* 경찰청 전기통신금융사기 통합대응단 홈페이지 : <http://counterscam112.go.kr>

※ 스미싱 문자 제보 방법 (2) - KISA 보호나라 이용 (<붙임2> 참조)



④ 피해 발생시 신속한 신고 및 지급정지 요청

○ 자금 이체 등 금융 피해가 발생한 경우 ①본인 또는 사기범 계좌의 금융회사나 ②보이스피싱 통합신고대응센터(112)로 지체없이 신고 하여 지급 정지를 요청하세요.

○ 개인정보 유출로 인한 추가 피해 예방을 위해 『개인정보 노출자 사고예방 시스템*』, 『본인계좌 일괄지급정지 서비스**』를 활용하세요.

* 금융감독원 홈페이지 파인(pd.fss.or.kr)에서 신청 가능, 신청시 신규 계좌개설 카드 발급 등이 제한

** 금융결제원 홈페이지 야카운트인포(www.payinfo.or.kr)에서 신청 가능, 본인계좌에서의 모든 출금거래 정지

IV 향후 계획

□ 금융당국은 향후 빗썸 보상금 등 관련 금융사기 피해 여부를 면밀히 모니터링 하고

○ 피해사례 발생시 소비자 경보 상향(주의→경고) 등을 검토할 예정입니다.

담당 부서	금융위원회	책임자	과 장	김태훈 (02-2100-2970)
	금융안전과	담당자	사무관	유은지 (02-2100-2974)
	금융감독원	책임자	팀 장	정윤미 (02-3145-8130)
	금융사기대응총괄팀	담당자	수 석	한유섭 (02-3145-8522)

< 차단 기능 설정 방법(안드로이드) >



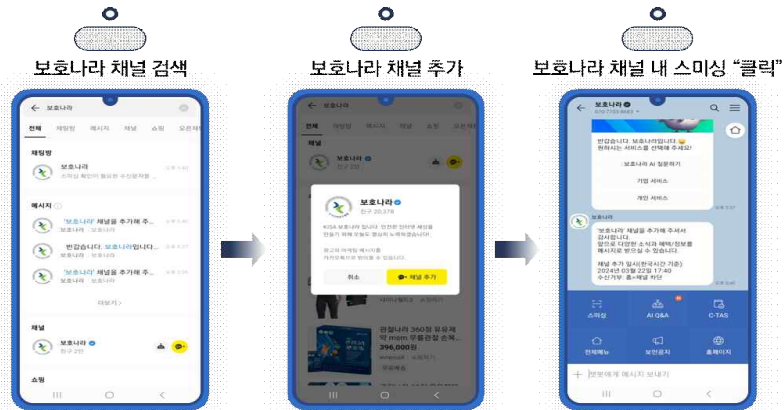
1. 스마트폰 '설정' 앱 클릭

2. '보안 및 개인정보 보호' 메뉴 접속

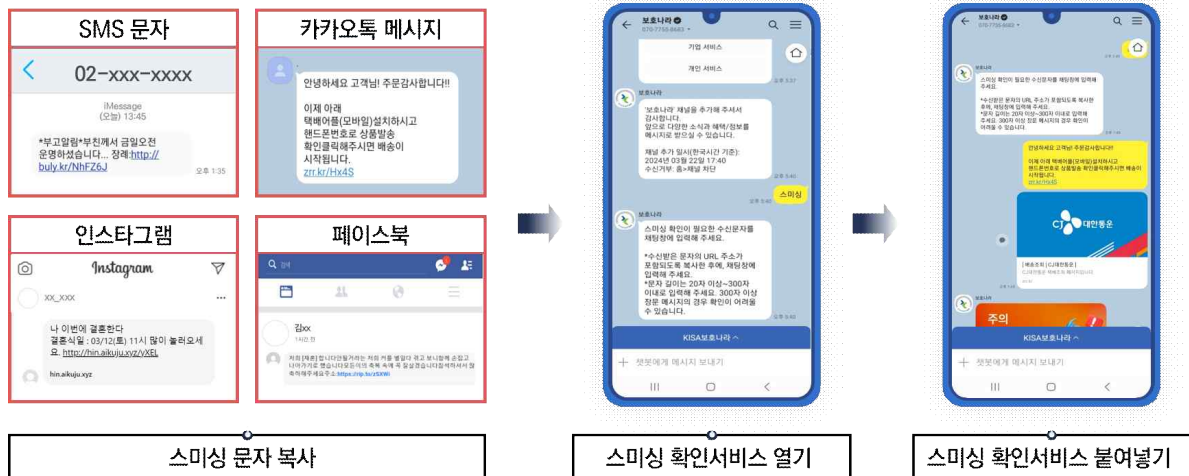
3. '보안 위험 자동 차단' 활성화

※ 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