



금융감독원

# 보도자료



금융은 튼튼하게 소비자 행복하게

보도	배포시	배포	2024.2.15.(목)	
담당부서	금융감독원 금융사기대응단	책임자	팀장	장종현 (02-3145-8140)
		담당자	선임조사역	이다은 (02-3145-8137)

## 민생금융지원 이자환급·대환대출을 미끼로 한 보이스피싱 소비자경보 발령!!!

### □ 소비자경보 2024 - 9호

등급	주의	경고	위험
대상	금융소비자 일반		

### 소비자경보 내용

- ◆ 최근 대출을 빙자한 보이스피싱 피해액이 전년동월 대비 5배 가까이 급증한('23.1월 27억원 → '24.1월 130억원) 가운데
  - ◆ 은행권이 '24.2.5. 취약계층에 대한 2.1조원+a 규모의 대출이자 환급 등 민생금융지원액을 집행하기 시작하고
    - 중소기업권이 3월말부터 소상공인에 대한 3천억원 규모의 대출 이자지원 혜택을 신청자에 대해 집행할 예정임에 따라
    - 사기범이 금융회사를 사칭하여 이자환급(캐시백) 신청 등을 명목으로 개인정보를 요구하거나, 대출상환 및 추가대출을 요구하는 등 보이스피싱 사기수법이 기승을 부릴 것으로 예상
- ⇒ 이러한 내용의 전화나 문자는 **늘 의심**하고 전화는 **꼭 끊고** 문자 내 URL 주소는 **또 확인**하여 클릭하지 마세요

### 은행권 민생금융 이자환급에는 별도 신청절차가 없습니다!!!

- 민생금융지원방안에 따른 이자 환급(캐시백)은 은행이 자체적으로 지원대상 선정 후 환급액을 지원하는 것으로 **별도의 신청절차가 불요**
    - 자영업자·소상공인 등이 캐시백을 받기 위해 ①**일정 기간 내에 신청**을 해야 하거나, ②**추가로 대출**을 받을 필요는 **없으므로** 보이스피싱에 유의
  - 중소기업권 이자환급은 **별도 신청**(3월중순 예정)이 **필요하나** 현재 관계기관의 전산시스템 개발 중으로 이를 빙자한 **스미싱** 등에 주의(신청절차 3월초 별도 보도예정)
- ※ 관련 문자, 카톡 수신시 금융회사 대표번호를 확인하고 금융회사 대표번호로 직접 문의

## 1 소비자경보 발령 배경

- '24.2.5. 은행권이 자영업자·소상공인 등 취약계층에 대한 이자환급 등을 개시\*하면서

\* '24.2.1. 보도자료 (「은행권, 자영업자·소상공인 이자환급을 시작으로 "2.1조원+α" 규모의 민생금융지원 본격 시행」) 참조

- 사기범이 은행 직원 등을 사칭하여 이자환급(캐시백) 대상여부 확인, 지원금 신청절차 등을 명목으로 개인정보를 요구하거나
- 지원대상이 되기 위한 조건으로 기존대출 상환후 추가대출이 필요하다고 속여 자금을 편취하는 등 보이스피싱에 악용될 우려

## 2 사기 수법

### 이런 순간엔 꼭 의심해야 합니다!

- (스미싱) 사기범들이 특정 은행으로 가장하여 불특정다수에게 민생금융 관련 이자환급 신청 또는 조회를 빙자하여 문자발송
  - 문자메시지내 '민생금융지원방안 안내' 등으로 명시하고 제도권 은행의 상호를 기재하여 실제 은행에서 발송한 문자로 오인유도
  - '선착순 지급', '한도소진 임박' 등의 자극적인 표현으로 웹주소(URL)를 클릭하거나 상담번호로 전화하도록 유인
- ⇒ 웹주소 클릭시 악성코드에 감염되어 연락처, 사진 등 개인정보가 유출되거나 전화시 피해자를 기망하여 계좌이체 등 요구
- (대환대출) 사기범들은 이자환급, 대환대출을 위해 기존 대출을 우선 상환하고 추가대출을 받아야 한다거나 신용등급 상향을 위한 예치금 입금 등이 필요하다고 속여 자금 편취
- (수수료) 사기범들은 대출, 정책지원금 등을 받기 위해서는 신용보증금 등 수수료를 내야 한다고 속여 자금을 편취

< 과거 대출·정책자금지원 빙자 보이스포싱 유사사례 >

- ◆ ◎◎은행 직원을 사칭한 사기범은 저금리 대출을 받으라며 피해자를 속이고 금융감독원 직원을 사칭한 공범이 대출금의 30%를 신용보증금으로 내야 한다며 자금 편취
- ◆ ○○은행 직원을 사칭한 사기범 A가 피해자에게 전화를 걸어 정책자금 지원을 통해 낮은 이율로 대환대출이 가능하다고 속여 대출을 신청하자
  - 기존 대출은행인 △△은행 직원을 사칭한 공범 B가 전화해 대환대출은 계약위반으로 추심절차가 개시될 수 있으니 기존 대출금을 상환해야 한다면서 4,690만원을 편취

### 3 소비자 행동 요령

#### 보이스피싱을 당하지 않도록 다음 사항을 숙지하세요!

- **은행권 이자환급은 별도 신청절차가 없습니다**
  - 은행이 대상 차주 및 환급액을 자체 선정·계산한 후 입출금계좌(대출계좌와 동일은행)로 입금할 예정으로 개인이 별도 신청하지 않음
  - ※ 중소기업권\* 이자환급은 3월 중순경 차주의 '신청'을 받을 예정이나, 현재 전산시스템을 구축 중이므로 이를 빙자한 스미싱 등에 주의
  - \* 저축은행·단위조합·새마을금고·카드·캐피탈
- **중소금융권 이자환급은 대환대출이나 수수료를 요구하지 않습니다**
  - 중소기업권 이자환급(24.3월말 예정)시 기존 대출 상환 또는 수수료 先입금을 요구하지 않으므로 관련 문자나 전화에 주의
- **제도권 금융회사의 전화번호를 직접 확인하세요**
  - 금융소비자 정보포털\*(파인)이나 금융회사 홈페이지에서 금융회사 대표 전화번호를 직접 확인하고, 국외발신 문자메시지의 경우 절대 응하지 말 것
  - \* 파인(fine.fss.or.kr)>금융회사 정보>제도권 금융회사 조회

☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다.(<http://www.fss.or.kr>)

※ 해당 보이스포싱 소비자경보 동영상은 금융감독원 공식 SNS 유튜브 채널에서 보실 수 있습니다.

- 동영상 바로가기  
<https://m.site.naver.com/1iWa7>

보이스피싱 소비자경보 동영상



- 스마트폰에 출처를 알 수 없는 앱이 설치되지 않도록 보안 설정을 강화하고, 앱은 받은 문자의 링크가 아닌 공인된 마켓 (플레이스토어·앱스토어)을 통해 다운로드 받을 것
- 최신 백신 프로그램을 설치하고 업데이트 및 실시간 감시 상태를 유지할 것
- 제도권 금융회사 및 정부기관은 어떠한 경우에도 전화·문자를 통한 개인정보 제공, 자금 송금을 요구하지 않으니 주의할 것
- 전화, 문자, 메신저 등의 상대방이 금전, 개인정보·금융정보를 요구하거나 앱 설치를 요구하는 경우 반드시 영상통화 등으로 상대방을 확인할 것
- 택배 배송조회, 부고장·청첩장, 모바일 상품권·승차권·공연예매권 증정 등의 문자에 포함된 출처가 불명확한 인터넷 웹 주소(URL) 또는 전화번호를 클릭하지 않을 것
- 신분증이 유출되지 않도록 스마트폰 내에 저장된 주민등록증, 운전면허증, 여권 사진을 바로 삭제할 것
- 본인 모르게 본인 명의의 휴대전화를 개통하여 보이스피싱에 이용하지 않도록 명의도용방지서비스(www.msafes.or.kr)를 활용하여 실시간 명의도용 여부를 확인할 것(무료 서비스)

<h3 style="text-align: center;">계좌 지급정지</h3>  <p style="text-align: center;">112 HELP!</p> <p style="text-align: center;">금융회사 또는 보이스피싱 통합센터에 전화하여 해당 계좌 지급정지를 요청하고 피해구제를 신청</p>	<h3 style="text-align: center;">개인정보 노출 등록</h3> <p style="text-align: center;"> <a href="https://fine.fss.or.kr">https://fine.fss.or.kr</a>  <a href="https://pd.fss.or.kr">https://pd.fss.or.kr</a> </p>  <p style="text-align: center;">금융감독원 금융소비자 정보포털 '파인'의 개인정보 노출자 사고예방 시스템을 활용하여 추가 피해 예방</p> <p style="text-align: center;"><small>신용등급, 취급 개인정보 노출 사실로 통학하면 신규 계좌개설, 신용카드 발급 등이 제한됨</small></p>
<h3 style="text-align: center;">내계좌 통합관리</h3> <p style="text-align: center;"><a href="http://www.payinfo.or.kr">www.payinfo.or.kr</a></p>  <p style="text-align: center;">계좌정보 통합관리서비스에서 본인 명의로 개설된 계좌 또는 대출을 확인하고, 필요시 일괄지급정지</p>	<h3 style="text-align: center;">휴대폰 명의도용 방지</h3> <p style="text-align: center;"><a href="http://www.msafar.or.kr">www.msafar.or.kr</a></p>  <p style="text-align: center;">명의도용 방지서비스를 이용하여 본인 모르게 개통된 휴대폰을 조화하거나 추가 개통을 차단</p>

- (지급정지) 계좌이체 등 금전피해 발생시 보이스피싱 통합신고·대응센터(☎112) 또는 금융회사 콜센터로 지체없이 신고하여 계좌 지급정지
  - (내계좌 통합관리) 「계좌정보 통합관리서비스([www.payinfo.or.kr](http://www.payinfo.or.kr))」에서 본인 모르게 개설된 계좌 또는 대출을 확인하여 명의도용 여부 확인
  - (개인정보 노출등록) 개인정보가 노출된 경우 「파인」에서 '개인정보 노출자\*'로 등록하여 신규계좌 개설, 신용카드 발급 등 제한
- \* 금융소비자정보포털 「파인([fine.fss.or.kr](http://fine.fss.or.kr))」 > 신고·상담·자문서비스 > 개인정보 노출 등록·해제 또는 개인정보노출자 사고예방시스템([pd.fss.or.kr](http://pd.fss.or.kr))에서 등록 가능

- **(휴대폰 명의도용 방지)** 「명의도용 방지서비스([www.msafes.or.kr](http://www.msafes.or.kr))」를 통해 본인 모르게 개통된 휴대폰을 조회하거나 추가개통 차단
- **(악성앱 삭제)** 문자 내 웹 주소를 클릭하여 악성 앱이 설치되었다면 즉시 관련 앱을 삭제하고 모바일 백신 프로그램을(V3, 알약 등) 통해 상태 검사
- **(휴대전화 초기화)** 휴대전화를 초기화하여 악성 프로그램을 완벽하게 삭제(초기화 전까지 휴대전화 전원을 끄거나 비행기모드로 전환\*)
  - \* 이에 따라 피해 발생 후 대응은 다른 휴대전화나 PC 사용을 권장
- **(폐기 및 해지)** 휴대전화에 신용카드, 신분증 사진, 공인인증서 등이 저장되어 있었다면 공인인증서 폐기, 신용카드 해지, 계좌 비밀번호 변경 등을 실시하고 경찰서에 신분증 분실 신고
- **(소액결제 확인)** 통신사 고객센터를 통해 모바일 소액결제 내역을 확인하고 추가피해 예방을 위해 소액결제를 차단
- **(경찰신고)** 개인정보 유출, 금전 피해 등 발생시 경찰서에서 사건사고사실 확인원을 발급받고 지급정지를 신청한 금융회사 영업점에 피해구제 신청