

최근 금융권 개인정보 유출사고에 따른 보이스피싱·스미싱 등 피해에 **주의**하세요.

- ✓ 최근 일부 금융권 개인정보 유출로 인한 피싱·스미싱 등 2차 피해 우려 확산
 - 비밀번호·OTP 정보 등은 유출되지 않았으나 유출된 개인정보를 결합한 맞춤형 대출빙자 사기에 각별히 유의
- ✓ 대출을 이유로 선입금·기존 대출 상환·앱 설치 등을 요구하면 사기이며, 「금융거래 안심차단서비스」 가입 및 「개인정보노출자 사고예방시스템」 등록 등을 통해서도 명의도용 대출 등 금융사기 피해를 사전 예방 가능
- ✓ 금융당국은 10.6. 금융회사를 긴급 소집하여 개인정보 유출 2차 피해 특별대응기간(1개월 연장 가능) 및 피해고객 전담 창구 운영, 유출 개인정보를 결합한 이상거래탐지시스템(FDS) 강화, 보이스피싱 정보공유·분석 AI 플랫폼(ASAP)을 통한 대응 등 2차 피해 방지에 총력을 다하도록 지도

■ 소비자경보 2026 - 26 호

등급	주의	경고	위험
대상	금융소비자 일반		

■ 개인정보 유출을 틈탄 맞춤형 '대출 빙자 사기'에 주의

최근 금융회사에서 개인정보 유출사고가 잇따라 발생하면서 보이스피싱·스미싱 등 금융사기 피해로 이어질 수 있다는 소비자 불안이 커지고 있어, 금융당국은 소비자 피해 예방을 위해 소비자경보(주의*)를 발령하였다.

* 피해 발생 확인시 즉시 소비자경보 격상 예정

특히 연휴 이후 금융거래가 본격 재개되는 시점을 틈타 사기범들은 성명, 주소지 등 유출된 개인정보를 바탕으로 금융회사 직원 등을 사칭하여

저금리 대출, 대환대출 등 정상적인 대출 상담을 가장하거나, 개인정보 유출 피해보상 등을 미끼로 피해자에게 접근할 우려가 있다.

사기범은 소득, 대출한도 등 본인의 금융정보를 정확히 언급하며 실제 금융회사의 대출 안내인 것처럼 접근할 수 있어, 내 정보를 알고 있다는 이유만으로 정상적인 연락이라고 믿어서는 안 된다.

※ 개인정보 유출을 빙자한 주요 금융사기 수법

- ① **(유출보상 빙자)** '유출 피해고객 대상 금리우대·특별대출', '유출 피해고객 대상 피해보상 안내' 등의 문자를 발송하여 인터넷 주소(URL) 클릭 및 상담 유도
- ② **(대환대출 빙자)** 저금리 대환대출이 가능하다는 기존 대출을 먼저 상환해야 한다고 속여 사기범 계좌로 이체 유도
- ③ **(선입금 요구)** 신용점수 향상, 거래실적 확보, 보증료 등을 명목으로 대출 실행 전 금전 입금 요구
- ④ **(악성앱 설치)** 대출신청서 작성, 보안점검 등을 명목으로 원격제어앱·악성앱 설치를 유도하여 휴대폰 장악

이 밖에도 사기범이 금융회사나 금융감독원 직원 등을 사칭하여 '유출 피해로부터 자산을 보호해야 한다'며 특정 계좌로 자금 이체를 요구할 수도 있다. 그러나 금융당국과 금융회사는 전화·문자로 비밀번호나 인증번호를 요구하거나, 피해보상·계좌보호를 이유로 자금 이체를 요구하지 않는다. 또한, 대출 과정에서 어떠한 명목으로도 선입금이나 앱 설치를 요구하지 않는다. 따라서 기존 대출 상환을 이유로 개인 명의 계좌로 이체를 요구하면 사기이므로 즉시 거절해야 한다.

아울러 금융회사나 금융당국은 개인정보 유출 안내나 피해보상 등 어떠한 이유로도 인터넷 주소(URL)를 보내지 않으니 불분명한 문자메시지의 인터넷 주소(URL)는 절대 클릭하지 말고 바로 삭제해야 한다. 본인의 개인정보 유출 여부는 해당 금융회사의 공식 홈페이지·앱 또는 고객센터 대표번호를 통해 직접 확인해야 하며, 혹시 모를 개인정보 추가 유출에 대비하여 본인 인증에 필요한 정보*를 휴대폰에 저장하지 말아야 한다.

* 주민등록번호, 금융계좌 비밀번호, 신분증 사본 등

■ 「금융거래 안심차단서비스」 가입 및 「개인정보노출자 사고예방 시스템」 등록으로 명의도용 대출 피해를 사전 예방

한편, 사기범이 악성앱 등을 통해 확보한 정보로 피해자 명의의 대출을 무단 실행하는 피해도 우려된다. 금융권에서는 이러한 명의도용 피해로부터 소비자들이 안심하고 금융거래를 할 수 있도록 여신거래·비대면 계좌개설·오픈뱅킹 등 「금융거래 안심차단서비스(3종)」를 시행하고 있다. 안심차단 서비스에 가입하면 대출, 비대면 예금계좌 개설, 오픈뱅킹이 무단으로 실행되어 피해가 발생하는 것을 사전에 차단할 수 있다.

지난 '25년 SKT 해킹사고 및 쿠팡 개인정보 유출 사고 등 발생 당시 금융사기 위험으로부터 스스로를 보호하고자 하는 소비자들이 급격히 늘어나면서 안심차단서비스 가입 신청이 크게 증가*한 바 있다.

* '26.8월말 기준 약 700만명 가입(중복 가입 가능)

※ **안심차단서비스 개요** ☞ 안심차단서비스 가입방법은 (붙임2)~(붙임4) 참고

- ① **(여신거래 안심차단)** 신용대출, 카드로, 신용카드 발급, 할부금융, 예·적금 담보대출 등 개인 명의의 여신거래를 차단('24.8.23. 시행)
- ② **(비대면 계좌개설 안심차단)** 범죄조직의 수익의 통로로 사용될 수 있는 대포통장 개설로 인한 피해 방지를 위해 비대면 계좌개설을 차단('25.3.12. 시행)
- ③ **(오픈뱅킹 안심차단)** 오픈뱅킹을 통한 계좌정보 무단조회 및 이체 등을 방지할 수 있도록 오픈뱅킹 서비스를 차단('25.11.14. 시행)

「안심차단서비스」는 거래 중인 금융회사* 영업점을 방문하거나 '내계좌한눈에'(payinfo.or.kr) 또는 은행앱을 통해 간편하게 신청할 수 있다. 서비스 신청 이후에도 필요한 경우에는 언제든지 금융회사 영업점을 방문하여 서비스를 해제할 수 있다. 서비스를 해제하면 곧바로 해당 금융거래가 가능하고, 다시 서비스에 재가입하는 것도 가능하다.

* 은행, 저축은행, 농협, 수협, 신협, 새마을금고, 산림조합, 우체국

아울러 금융감독원 금융소비자정보포털 '파인'(fine.fss.or.kr)의 「개인정보노출자 사고예방시스템」에 본인 정보를 등록할 수 있다. 등록된 정보는 금융회사에 실시간으로 공유되며, 이후 본인 명의의 신규 계좌개설, 신용카드 발급 등이 제한되어 명의도용 피해를 예방할 수 있다.

■ 피해 의심 또는 실제 금전 피해 발생 시 즉시 신고하고 지급정지 요청

만약 보이스피싱 등 금융사기 피해가 의심될 경우 경찰청 전기통신금융사기 통합대응단(1394)를 통해 피해 상담을 받을 수 있다. 또한 사기범에게 속아 돈을 이체하는 등 실제 금전적인 피해가 발생한 경우 즉시 경찰(112)이나 금융회사 콜센터에 연락하여 지급정지를 요청해야 한다.

■ 개인정보 유출사고 관련 금융당국의 대응

금융당국은 10.6.부터 1개월간 「**개인정보 유출 2차피해 특별대응기간**」(필요시 연장)으로 지정하고 금융권과 함께 개인정보 유출 등에 따른 2차 피해 예방을 위하여 **총력 대응**하고 있다.

10.6. 금융회사를 대상으로 **피해예방점검회의***를 **긴급 소집**하고 유출된 정보가 금융사기에 악용될 가능성에 대비하여 아래와 같은 사항을 지도하였다.

* (일시·장소) 10.6.(화) 14:00 금융감독원 9층 회의실

(참석기관) 은행·금융투자·상호금융·여신업권 금융회사, DAXA, 금융보안원 등

① (**피해고객 전담창구 설치·운영**) 특별대응기간동안 관련 금융회사가 개인정보 유출 전담 상담창구를 운영하고, 정보유출 고객에 대해서는 안심 차단서비스 가입 등을 개별적으로 적극 안내하도록 하였다. 또한 피해 신고가 접수되거나 의심될 경우 **금융당국**에 **즉시 보고** 및 타 금융회사와 공유하여 피해 확산 방지 조치가 신속히 이루어지도록 하였다.

② (**FDS 모니터링 강화**) 금융회사에 대해서는 유출된 개인정보를 결합한 이상거래에 대해 밀착 모니터링하고 임시조치를 실시하는 등 FDS 운영 강화를 지도하였다. 이에 따라 해당 고객 명의의 비대면 대출 및 계좌개설, 고액 이체 등 고위험 거래에 대한 모니터링과 추가 본인확인이 강화된다.

③ (**ASAP 활용 공동 대응**) 금융회사·통신사·수사기관이 참여하는 보이스피싱 정보공유·분석 AI 플랫폼(ASAP*)으로 유출사고 관련 의심정보를 신속히 공유** 하여 의심계좌 지급정지 등 피해 차단에 적극 활용할 수 있도록 지도하였다.

* AI-based anti-phishing Sharing & Analysis Platform

** '25.10월 출범 이후 '26.8월까지 의심정보 50만건 공유, 의심계좌 7,666개 지급정지 및 약 699.4억원의 피해를 예방

④ (**피해구제 관리·감독**) 사고 관련 금융회사가 피해 발생 여부를 지속 모니터링하고 실제 피해 확인시 피해구제 및 보상 절차가 신속하게 이루어질 수 있도록 지도하였다.

아울러, 금융당국은 개인정보 유출을 이용한 실제 피해가 확인되는 경우 소비자정보 등급을 격상(주의→경고)하고 추가 조치를 마련할 계획이다.

■ 대국민 당부사항

현재까지 금번 금융회사의 개인정보 유출 사고와 관련하여 보이스피싱 등 피해로 고객 자금이 유출된 사례는 확인되지 않았습니다. 따라서 소비자는 예금 등 금융자산의 안전에 대해 불필요한 오해를 지양해 주시기 바랍니다.

※ 개인정보 유출여부 및 유출 내용 등은 금융회사 공식 홈페이지·앱 또는 고객센터 대표번호 등 공식 채널로 직접 확인

다만, 피해 발생 가능성을 완전히 배제할 수는 없으므로, 금융당국과 금융회사가 안내하는 「개인정보 유출 관련 소비자 행동요령*」 등에 따라 필요한 조치를 취하고 금융사기 등 2차 피해에 각별히 주의해 주시기 바랍니다.

* 「개인정보 유출 관련 소비자 행동요령」은 (붙임1) 참고

담당 부서	금융위원회 금융안전과	책임자	과 장	김태훈	(02-2100-2970)
		담당자	사무관	이다행	(02-2100-2975)
	금융감독원 금융사기대응단	책임자	팀 장	정윤미	(02-3145-8130)
		담당자	선 임	이다영	(02-3145-8124)
	과학기술정보통신부 사이버침해조사팀	책임자	과 장	김우철	(044-202-6490)
		담당자	사무관	김성환	(044-202-6491)
			사무관	김재남	(044-202-6493)
	개인정보보호위원회 사전실태점검과	책임자	과 장	김해숙	(02-2100-3060)
		담당자	사무관	정진아	(02-2100-2424)
	은행연합회 소비자보호부	책임자	팀 장	모경원	(02-3705-5043)
		담당자	차 장	김찬수	(02-3705-5042)
	금융투자협회 투자자보호부	책임자	부 장	김효실	(02-2003-9420)
		담당자	과 장	이다솜	(02-2003-9427)
	저축은행중앙회 소비자보호부	책임자	부 장	윤호병	(02-397-8680)
		담당자	과 장	김정중	(02-397-8692)
	여신금융협회 소비자금융부	책임자	부 장	이경원	(02-2011-0742)
		담당자	팀 장	조숙희	(02-2011-0717)
	농협중앙회 금융소비자보호부	책임자	팀 장	박혜순	(02-2080-2221)
		담당자	차 장	노혜연	(02-2080-2225)
	신협중앙회 금융소비자보호팀	책임자	팀 장	박미연	(042-720-1462)
		담당자	차 장	민영숙	(042-720-1465)

수협중앙회 소비자보호단	책임자	차 장	국대근	(02-2240-2221)
	담당자	직 원	송예린	(02-2240-5990)
새마을금고중앙회 금융사기대응부	책임자	부 장	장봉중	(02-2145-9541)
	담당자	차 장	구혜주	(02-2149-9549)
디지털자산거래소 공동협의체	책임자	본부장	홍 균	(02-6959-8084)
	담당자	차 장	김광연	(02-6959-8087)
금융보안원 ASAP실	책임자	실 장	유영록	(02-3495-9950)
	담당자	팀 장	이득기	(02-3495-9970)
온라인투자연계 금융협회	책임자	사무국장	한성택	(02-761-2781)
	담당자	과장	김서준	(02-761-2782)

사전에 미리 해두기	
① 안심차단서비스 가입	「금융거래 안심차단서비스」에 가입*하여 명의도용 대출·계좌개설·오픈뱅킹 등을 사전 차단 * 금융회사 영업점 방문 또는 '내계좌한눈에'(payinfo.or.kr) 및 은행앱 통해 신청
② 개인정보노출자 등록	「개인정보노출자 사고예방시스템*」에 본인 정보를 등록하여 본인 명의의 신규 계좌개설 및 카드 발급 등 제한 * 금융감독원 금융소비자정보포털 '파인'(fine.fss.or.kr) 접속
③ 내 계좌 및 대출 점검	'내 계좌 한눈에'(payinfo.or.kr)에서 본인 모르게 개설된 계좌나 실행된 대출이 있는지 확인
④ 개인정보 저장 금지	신분증 사본, 계좌 비밀번호 등 개인정보를 휴대폰에 저장하지 않기

의심스러운 연락을 받았을 때	
① URL 클릭 금지	'개인정보 유출 확인', '피해보상', '저금리 대출' 등을 안내하는 문자의 URL은 누르지 말고 삭제
② 내 정보를 알아도 의심	상대방이 이름·소득·대출정보 등을 정확히 알고 있더라도 정상적인 연락으로 믿지 않기
③ 공식 채널로 직접 확인	개인정보 유출 여부와 대출 안내는 해당 금융회사 공식 홈페이지·앱 또는 고객센터 대표번호로 직접 확인
④ 요구에 응하지 않기	'선입금', '기존대출 상환', '앱 설치', '인증번호·신분증 사진 요구'는 모두 사기이므로 거절

피해가 의심될 때	
① 즉시 지급정지 요청	경찰(1394 또는 112) 또는 금융회사 콜센터에 즉시 지급정지 요청
② 피해구제 신청	지급정지 요청 후 최대 14일 이내(가급적 3영업일 이내 권장) 해당 금융회사에 피해구제 신청서 제출
③ 악성앱 조치	악성앱 설치가 의심되면 다른 전화로 신고하고, 휴대폰을 백신앱으로 점검하거나 초기화
④ 추가 피해 차단	개인정보노출자 등록, 금융거래 비밀번호 변경 등

① 홈 화면-"메뉴" 클릭	② 인증/보안 클릭	③ 안심차단서비스 클릭
		
④ 여신거래 차단 선택	⑤ 약관 동의	⑥ 신청 완료
		

① 홈 화면-"전체메뉴" 클릭



② 비대면 계좌개설 안심차단 클릭



③ 안심차단 신청



④ 오픈뱅킹 이용정보 확인



⑤ 동의서 작성



⑥ 결과 확인



붙임4

오픈뱅킹 안심차단서비스 신청방법(어카운트인포 앱)

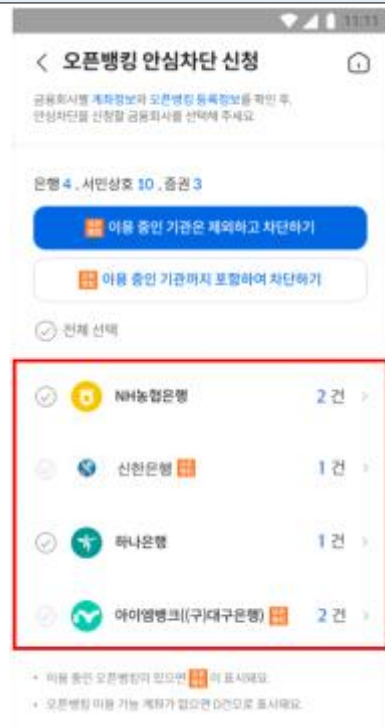
① “내 금융 안심차단” 클릭



② 안심차단 신청 화면



③ 신청 가능 금융회사 확인



④ 오픈뱅킹 이용정보 확인



⑤ 가입 신청



⑥ 결과 확인





여신거래 안심차단 시스템이란?
소비자의 선택으로 개인의 신규 여신거래를 사전차단 할 수 있는 시스템입니다.

적용대상 신용카드 발급, 신용대출, 담보대출, 할부·리스, 서민금융

기존에 거래중인 금융회사 영업점을 방문하여
안심 차단 신청하세요.

※ '24.10월부터 거래중인 인터넷 전문은행을 통해 비대면으로도 신청가능

자세한 내용은 QR코드로 접속하여 보이스피싱자킴이 사이트에서 확인하세요.



나도 모르게 개설된 계좌가 보이스피싱 범죄에? 비대면 계좌개설 안심차단 서비스 신청으로 예방하세요.



| 서비스 신청방법



금융회사 방문
거래중인 금융회사 영업점에
방문하여 신청



비대면 신청
금융결제원의 어카운트 인포
(모바일 앱 및 홈페이지) 또는 거래중인
은행의 모바일·인터넷뱅킹을 통해 신청

| 서비스 해제방법



보이스피싱, 명의도용 사기범 등의
무단 해제를 방지하기 위하여
금융회사의 영업점 방문을
동해서만 해제 신청이 가능합니다.

비대면 계좌개설 안심차단 서비스에
가입하시면 전 금융권의 수시입출식 계좌의
비대면 개설을 사전에 일괄 차단할 수 있습니다.



금감원 보이스피싱저지QR

금융위원회

금융감독원

은행연합회

금융투자협회

저축은행중앙회

농협중앙회

신협중앙회

MG새마을금고중앙회

수협중앙회

우정사업본부

오픈뱅킹을 통한 무단 출금 · 이체

오픈뱅킹안심차단

서비스 신청으로 예방하세요.



오픈뱅킹 안심차단 서비스는 소비자가 원하지 않는 오픈뱅킹 거래를 사전 차단하는 서비스로, 차단 희망 금융회사를 직접 선택하여 안심차단을 신청할 수 있습니다.

**적용
대상**

은행, 저축은행, 농협, 수협, 신협, 새마을금고,
산림조합, 우체국, 증권사에서 **개설한 모든 계좌**



신분증 분실, 악성앱 설치 등으로
개인정보가 노출되어 오픈뱅킹을 통한
무단 계좌 출금 및 조회를 방지하고자
하는 분들에게 유용합니다.



거래중인 금융회사의 영업점에 방문
하거나, 금융결제원의 어카운트인포
(모바일) 및 은행의 모바일 앱을 통해
안심차단 서비스를 신청할 수 있습니다.



서비스 해제 신청은 보이스피싱, 명의
도용 사기범의 무단해제를 방지하기
위해 거래 중인 금융회사의 영업점
방문을 통해서만 가능합니다.

