

개인정보 유출 2차 피해

최근 금융권 개인정보 유출사고에 따른 보이스피싱 등 피해에 주의하세요!

유출된 개인정보를 결합한
맞춤형 대출빙자 사기에 특히 유의하세요.



OO님, 기존 대출 있으시죠?



저금리 대환대출 가능합니다



주요 사기 수법 4가지

내 정보를 알고 있더라도 금융회사라고 **무조건 믿지 마세요!**

수법
1

개인정보 유출 피해보상 빙자

"유출 피해고객 대상 금리우대·특별대출입니다"

→ 문자로 인터넷 주소(URL) 클릭 또는 상담 유도

수법
2

저금리 대환대출 빙자

"대환대출 전에 기존 대출부터 갚으세요"

→ 기존 대출 상환을 요구한 뒤 사기범 계좌로 이체 유도

수법
3

선입금 요구

"신용점수 상향, 거래실적 확보를 위해 불러드리는 계좌로
먼저 입금하세요"

→ 대출 실행 전 금전 입금 요구

수법
4

악성앱 설치 요구

"대출 신청 또는 보안점검 등을 위해 앱을 설치해주세요"

→ 원격제어앱·악성앱 등 앱 설치 유도



금융감독원

이것만 기억하세요

정부기관과 금융회사는 절대 이런 요구를 하지 않습니다.



전화 또는 문자로 **비밀번호·인증번호** 요구



피해보상·계좌보호 명목의 **자금이체** 요구



대출 과정에서 **선입금·앱 설치** 요구

의심되면 대응하지 마시고,
공식 홈페이지·앱·고객센터 대표번호로
직접 확인하세요.

소비자 행동요령 01

사전에 미리 해두기



1 안심차단서비스 가입

→ 명의도용 대출·계좌개설·오픈뱅킹 등을 **사전 차단**

신청 | 금융회사 영업점 방문, 내계좌한눈에(payinfo.or.kr), 은행앱

2 개인정보노출자 등록

→ 본인 명의의 신규 계좌개설·카드 발급 등 **제한**

등록 | 금융감독원 개인정보노출자 사고예방시스템(pd.fss.or.kr)

3 내 계좌 및 대출 점검

→ 나도 모르게 개설된 계좌·실행된 대출이 있는지 **확인**

확인 | 내 계좌 한눈에(payinfo.or.kr)

4 개인정보 저장 금지

→ 신분증 사본·계좌 비밀번호 등을 **휴대폰에 저장하지 않기**

소비자 행동요령 02

의심스러운 연락을 받았을 때

1



URL 클릭 금지

'개인정보 유출 확인',
'피해보상', '저금리 대출'
문자 URL은 누르지 말고 삭제

2



내 정보를 알아도 의심

이름·소득·대출정보를
정확히 알고있더라도
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 요구는
모두 사기이므로 거절

소비자 행동요령 03

피해가 의심될 때



1 즉시 지급정지 요청

경찰(112), 전기통신금융사기 통합대응단(1394)
또는 금융회사 콜센터에 즉시 지급정지를 요청



2 피해구제 신청

지급정지 요청 후 최대 **14일 이내**(가급적 3영업일 이내 권장)
해당 금융회사에 피해구제 신청서 제출



3 악성앱 조치

다른 전화로 신고 후, 휴대폰 **백신앱 점검 또는 초기화**



4 추가 피해 차단

개인정보노출자 등록, 금융거래 **비밀번호 변경** 등



개인정보 유출 2차 피해 차단을 위해 총력 대응하고 있습니다.

'개인정보 유출 2차피해 특별대응기간' 운영(10.6.~)



피해고객
전담창구 설치·운영

FDS
모니터링 강화

ASAP을 통한
보이스피싱 의심정보 공유·대응

금융회사 피해구제
관리·감독

2차 피해 가능성에 대비해
가족·지인에게도 공유해 주세요.