

보도	2025.2.13.(목) 14:00	배포	2025.2.13.(목)
-----------	----------------------------	-----------	---------------

담당부서	금융사기대응단	책임자	국 장	정재승	(02-3145-8150)
	금융사기대응1팀	담당자	팀 장	김호빈	(02-3145-8140)

카드배송 사칭 보이스피싱 증가, 소비자경보 상행! (주의 → 경고)

- 신청한 적 없는 카드배송으로 고령층에 접근하여, 사고접수 도움을 주는 척 원격제어앱 설치
- 검찰, 금감원 사칭 직원이 자산보호 등 명목으로 자금이체를 유도...이체 요구시 무조건 사기

■ 소비자경보 2025 - 1호

등급	주의 경고 위험
대상	금융소비자 일반

I 경보발령 배경

- 금융감독원은 '24년 하반기 관계부처의 노력에도 불구하고 **보이스 피싱**이 **증가***함에 따라 보이스피싱 피해사례의 **주요특징** 및 **수법**을 분석하였습니다.

* [보이스피싱 피해액 추이] 249억원(9월) → 453억원(10월) → 614억원(11월) → 610억원(12월)

※ 「통신사기피해환급법」에 따라 '24년중 금융감독원에 접수된 보이스피싱 피해구제 신청 건 기준(추가 피해 접수시 변동가능)으로 수사당국의 범죄사건통계와 차이가 있을 수 있습니다.

- 분석 결과, 수법이 더욱 **교묘**해진 **가짜 카드배송**으로 시작된 **기관 사칭형 수법**에 속은 **고령층**의 **고액피해 사례 증가**가 주요원인인 것으로 나타났으며,
 - '24.12월중 **소비자경보 발령** (주의)*에도 불구하고 해당 범죄가 지속 발생함에 따라 **소비자경보 등급**을 주의에서 **경고**로 **상향**하고, 금융소비자들의 **각별한 주의**를 **당부**하였습니다.

* (24.12.10.) 「고령층을 대상으로 범죄에 연루되었다며 거액 주택담보대출을 유도하는 보이스피싱에 주의하세요!!!」

II 최근 보이스피싱 주요 특징 및 수법

□ 카드배송을 사칭한 보이스피싱 사기의 주요 특징 및 단계별 수법은 아래와 같습니다.

1 [고령층 여성을 타겟] 고액 피해자의 2명중 1명은 60대 여성

※ '24년 하반기 보이스피싱 고액피해(2억원 이상) 관련 금융감독원 자체분석 결과

- 고액 피해자의 약 80%가 여성이었으며, 특히 60대 여성이 과반수를 차지하였고, 서울의 경우 강남3구의 피해액이 서울 전체 피해액의 약 30%를 차지하는 것으로 나타났습니다.

2 [카드배송 사칭] 카드배송원으로 위장하여 가짜 콜센터로 전화를 유도

- 종전에는 카드배송 미끼문자를 발송하였으나 문자차단 대책 등이 시행됨에 따라 배송원을 사칭하여 전화하거나 위조된 실물카드를 직접 배송하러 방문하는 등 적극적인 범행을 시도하고 있습니다.
- 사기범들은 신청하지 않은 카드가 발급되었다고 피해자가 오인하게 만들어 카드사 고객센터로 위장한 사기범들의 연락처로 전화하게 유도합니다.

카드배송 사칭 보이스피싱 수법(실제사례)

- ▶ [카드배송 사칭법] “안녕하세요. ○○년생 △△△씨 맞으시죠? 카드 배송차 연락드렸는데요. ... 카드 신청하신 적 없다고요? 그럼 반송처리 하셔야하는데 ◇◇카드 대표번호 1788-0XXX로 전화해보세요” → 생년월일, 성명을 언급하며 의심을 최소화하고 사기범의 연락처 전달
- ▶ [카드사 상담원 사칭법] “카드내역 조회하니 고객님의 신용카드랑 연동된 계좌가 있는데요, 계좌번호 837번으로 시작하고 61번으로 끝나는 번호요. 금일 배송 중인 ◇◇카드와 연동된 ○○계좌가 정상개설 되신 것으로 확인되거든요?” → 명의도용 카드발급 사고로 기망

3 [피해자 휴대폰 통제] 공식 등록 원격제어앱 설치를 유도해 피해자의 휴대폰 장악

- 피해자가 가짜 고객센터로 전화시 개인정보 유출로 명의를 도용되었다며 보안점검, 악성앱 검사, 사고접수 등을 명목으로 앱 설치를 유도하면서 실제로는 원격제어앱을 설치합니다.

- 종전 문자에 URL을 포함하여 출처가 불분명한 악성앱을 설치토록 유도하는 방식이 어려워지자*, 사기범들은 공식 앱스토어에 등록된 원격제어앱을 다운받게 유도하여 앱 설치에 대한 경각심을 최소화합니다.

* '24년 보이스피싱 범정부 대책이 시행됨에 따라 휴대폰 금융앱 등의 강화된 보안기능을 무력화 하기 위해 공식 앱스토어에 등록된 정상앱(원격제어앱)을 악용

- 원격제어앱 설치후 악성앱까지 설치되면 금감원(1332)·검찰청(1301) 공식번호로 전화해도 사기범들에게 연결되므로 의심하기 더욱 어렵고, 사기범들은 위치추적, 녹음 등까지 가능하게 됩니다.

※ (참고) 원격제어앱 : any**, OS**, Air** 등 다수

- ▶ 휴대폰, 컴퓨터 등을 원격으로 '제어'할 수 있도록 만든 공식 어플리케이션. 주로 원격근무나 가족(고령, 어린이 등)의 휴대폰 관리 등에 활용되는 유용한 프로그램이나, 사기범들이 설치시 피해자 휴대폰을 통제하여 악성앱을 설치하는 등 악용가능

4 [심리지배] 검찰 금감원을 사칭한 정교한 시나리오로 피해자를 완전히 '가스라이팅'

- 검찰 사칭 사기범이 피해자가 연루된 사기범죄로 다수 피해자가 발생하여 구속수사한다고 협박하면, 금감원 직원 등을 사칭한 다른 사기범은 약식수사 등을 할 수 있도록 도와준다고 하면서 피해자와의 강한 신뢰관계(rapport)를 형성시켜 피해자의 심리를 지배합니다.
- 아울러, 가족에게 알리면 가족도 수사대상이 된다고 위협하는 등 피해자를 철저히 고립시킵니다.

사기범들의 '가스라이팅' 시나리오(실제사례)

- ▶ [검찰 사칭범] "□□은행에서 당신 명의로 계좌가 만들어져서 불법자금세탁 사건에 이용됐고, 피해자 70여명이 집단 고소장을 접수한 상황... 72시간 동안 조사 후에 구속할 예정... 만약에 연락을 회피하거나 주변 사람들에게 수사내용을 발설하면 바로 체포하고, 가족까지 소환장 발부해서 구속합니다." → 피해자를 협박하는 역할
- ▶ [금감원 사칭범] "최근 명의도용 사건이 많이 접수되는데 선생님도 피해를 입으신 거 같네요. ... 제가 약식조사 받을 수 있도록 얘기해 둘테니 검찰청 대표번호 1301로 전화해보세요." → 피해자를 도와주는 역할

⑤ [피해자 직접이체] 피해자를 조종하여 직접 자금이체를 유도

- 최근 금융앱 보안강화 등에 따라 악성앱, 대포폰 등을 통해 사기범이 이체하는 방식이 어려워지자, 사기범들은 **자산보호, 약식기소 공탁금** 등의 명목으로 피해자를 속여 **피해자 스스로** 사기범에게 자금을 이체하도록 **수법을 변경**하였습니다.
- 사기범들은 금융회사의 **본인확인, 거래목적확인** 등 **문진**에 대비하여 자금 사용처 등 답변을 **사전에 교육**하고, **금융회사·통신사·경찰까지 범죄**에 **연루**되어 있다고 **속여** 주변의 도움을 무력화시킵니다.
- **최근**에는 완전히 **가스라이팅** 당한 피해자가 **직접 이체**함에 따라 금융회사가 이상거래로 탐지하여 **문진**을 하더라도 본인 거래로 주장하면서 **도움**을 **거절**하는 사례도 확인되고 있습니다.

▶ [사례] 은행이 이상거래로 탐지하여 본인확인을 하였으나, **피해자는 아들의 사업투자 목적 거래이므로 관여말라**고 답변(70대 여성, 피해금 21억원)

Ⅲ 소비자 주의사항 및 대응 요령

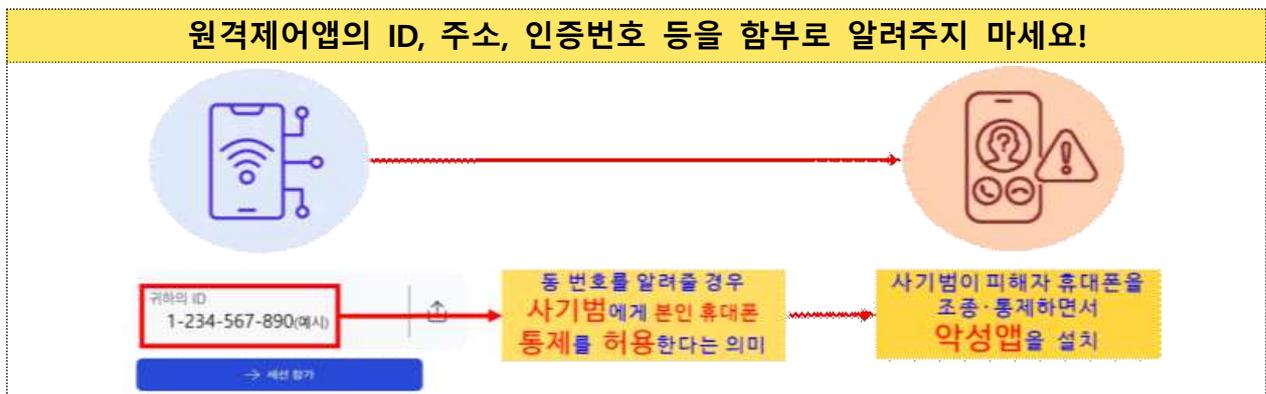
① 본인이 신청하지 않은 카드배송 연락을 받은 경우 카드사에 직접 확인하세요.

- 본인이 카드를 신청하지 않은 경우 배송직원이 알려준 번호가 아닌 **카드사 홈페이지·앱·콜센터 전화번호**를 통해 경위를 **확인**하세요.
- 확인 결과, 카드배송 사칭을 통한 **보이스피싱**이 의심되는 경우에는 ☎112(경찰청 통합신고대응센터)로 **상담·신고**합니다.

② 카드사 등 금융회사와 공공기관은 앱 설치를 요구하지 않습니다.

- URL 링크를 통한 출처가 불분명한 앱뿐만 아니라 공식 앱스토어의 앱 다운로드를 요구하더라도 거절하세요. 카드사 등 금융회사와 금감원 등 공공기관은 앱설치를 요구하지 않습니다.
- 공식 앱스토어에 등록된 원격제어앱*이라도 ID·주소·인증번호 등을 타인에게 알려주는 것은 상대방에게 내 휴대폰을 맡기는 것과 같습니다.

* Any**, Air** 등이 대표적이나 어플명만으로는 원격제어앱 여부를 알기 어렵다는 사실 인지필요



- 원격제어앱이나 악성앱 설치가 의심되는 등 조금이라도 꺼림칙하다면 본인의 휴대폰이 아닌 가족 등 지인의 전화를 이용하여 경찰(통합신고대응센터 ☎112) 또는 금감원(☎1332)으로 전화하여 상담하십시오.

③ 금감원, 검찰 등 국가기관은 절대 직접 자금이체를 요구하지 않습니다.

- 금감원, 검찰 등 국가기관이 자산검수, 안전계좌 송금, 약식기소 공탁금 등의 이유로 자금이체를 요구할 경우 100% 사기이므로 거절하고 경찰에 신고하세요.

④ 통신사의 AI 보이스피싱 탐지 서비스를 적극 활용하세요.

- 최근 보이스피싱 수법은 주소, 계좌번호 등 개인정보가 이미 노출된 피해자에게 전화를 걸어 실제 금융회사 상담센터와 유사한 내용 및 방식으로 접근하는 등 교묘한 방식으로 진화하여 피해자 스스로 알아차리기가 어렵습니다.

- 통신사에서 제공중인 **AI 보이스피싱 탐지 서비스***를 이용하면 보이스피싱 여부를 휴대폰 알람으로 전달받을 수 있어 피해예방에 도움이 됩니다.

※ AI 보이스피싱 탐지 서비스

- ▶ 금감원의 '그놈 목소리' 등 실제사례를 활용하여 AI가 통화내용을 실시간으로 분석하고 보이스피싱 의심 통화에 해당할 경우 이용자에게 **경고메시지** 및 **알람** 송출
- (LG유플러스) '익시오'앱(유플러스 아이폰 用), (KT) '후후'앱(모든 통신사 안드로이드폰 用)
→ 공식 앱스토어에서 다운가능

5] 사기범에게 속아 금전을 이체한 경우에는 최대한 신속히 경찰(112) 또는 금융회사 콜센터로 연락하여 지급정지를 요청하십시오.

IV 향후 계획

- 향후 금융감독원은 금융권뿐 아니라 범정부 TF 등을 통해 관계 부처와도 긴밀히 공조하여 보이스피싱의 근원적 차단을 위한 노력을 지속해 나가겠습니다.
- 「비대면 계좌개설 사전차단 서비스*」 등 구축·시행, 「이상거래 탐지시스템(FDS)」 기능 고도화 및 통신사-금융사간 정보공유 체계 마련 등을 통해 보이스피싱에 대한 금융회사의 현장대응 능력을 지속적으로 강화해 나갈 계획입니다.

* 소비자가 원하지 않는 비대면 계좌개설, 오픈뱅킹 사전 차단

보이스피싱 피해시 대응요령



01 피해신고 및 지급정지 요청



경찰(112), 금감원(1332), 금융회사에 피해신고 및 지급정지 요청

02 개인정보 노출등록



개인정보 노출자 사고예방시스템 [<http://pd.fss.or.kr>] 사고등록

03 계좌 일괄 지급정지 신청



계좌정보통합관리서비스[www.payinfo.or.kr] 및 금융회사 영업점에서 일괄지급정지

04 명의도용 신고



명의도용방지서비스[www.msafar.or.kr]에 명의도용 신고로 휴대전화 개설 방지

05 악성앱 삭제 및 휴대전화 초기화



악성코드 감염시 바로 삭제 및 휴대전화 초기화

06 피해사례 공유



보이스피싱지킴이 사이트에 접속하여 피해사례 공유

