금융감독원	**보 도 자 료**	금융은 튼튼하게 소비자는 행복하게

보도	2026.11.13.(금) 조간	배포	2026.11.12.(목)	
담당부서	금융사기대응단 금융사기대응2팀	책임자	팀 장	강 인 (02-3145-8521)
		담당자	선 임	이인성 (02-3145-8536)

"누가 내 신분증과 위임장을 들고 주민센터에 왔다고요?" 100% 보이스피싱 사기입니다!

▣ 소비자경보 2026 - 28호			
등급	주의	경고	위험
대상	금융소비자 일반		

소비자경보 내용

◈ 최근 주민센터 직원을 사칭하여 "누군가 선생님의 신분증과 위임장을 들고 서류를 떼러 왔다"며 접근하는 신종 보이스피싱이 확인되고 있습니다.

◈ 사기범들은 명의도용을 걱정하는 피해자에게 가짜 전화번호를 불러주어 피해자가 직접 신용정보원·금융감독원에 전화를 걸게한 뒤,

○ 금감원 직원, 검사 등을 차례로 사칭하며 자금을 편취합니다.

⇒ 불러 준 번호로 전화를 거는 순간부터 통화 상대는 모두 사기범이며, 금감원·공소청·중수청·경찰은 어떤 명목으로도 돈을 보내라고 요구하지 않습니다.

< 소비자 유의사항 및 대응요령 >

① **상대가 불러 주는 번호 대신 직접 찾은 대표번호로 확인하거나 가까운 주민센터를 직접 방문하시기 바랍니다.**

② **한국신용정보원은 명의도용 신고를 접수하지 않습니다. 명의도용이 걱정되면 어카운트인포 등에서 직접 조회하십시오.**

③ **"누구에게도 알리지 말라"는 말은 절대 듣지 마시고 즉시 가족과 경찰 등에게 신속하게 알리시기 바랍니다.**

※ 이미 돈을 보내셨다면 즉시 **☎112 또는 송금한 금융회사 콜센터**로 지급정지를 요청하세요.
의심 전화는 **전기통신금융사기 통합대응단(☎1394), 금융감독원(☎1332)**에서 상담하실 수 있습니다.

Ⅰ. 소비자경보 발령 배경

"○○동 주민센터입니다. 어떤 사람이 선생님 신분증과 위임장을 가지고 등본을 떼러 왔는데, 신분을 확인하려니 황급히 나갔습니다. 혹시 주민등록증을 잃어버리신 적 있으십니까?"

□ 지난 **10월 실제 피해자**가 받은 전화입니다. 그런 일이 없다고 답하자 이번에는 **한국신용정보원 직원, 금융감독원 팀장, 공소청 검사**를 사칭한 사람들이 차례로 나타나 **"명의도용으로 범죄에 연루되었으니 자산검수를 진행해야 한다"**고 말했습니다.

○ 이 피해자는 첫 전화를 받은지 **사흘 만에 1억원**을 넘게 사기범에게 보냈습니다.

○ 이처럼 **주민센터 직원**을 **사칭**하는 **신종 보이스피싱 수법**이 확인되고 있습니다.

○ 그동안 **기관사칭형 보이스피싱**은 **검찰·금감원·경찰**을 내세워 겁을 주는 경우가 많았습니다. 그러나 이번 수법은 **주민센터 직원**이 **명의도용**을 막아주려는 듯한 모습으로 시작합니다. 소비자는 의심받는 사람이 아니라 **보호받는 사람의 입장**에서 전화를 받게 되므로 **경계심**을 갖기 어렵습니다.

□ 더욱이, **사기범**은 **피해자**가 **직접 전화**를 걸게 만듭니다. 한 사례에서 **주민센터 직원을 사칭한 사기범**은 **"금융감독원에 전화해 보이스피싱 신고를 하라"**며 전화번호를 알려 주었고, 그 번호로 연결된 **가짜 금감원** 팀장은 **"보이스피싱 피해를 당한 것"**이라고 말했습니다.

○ **보이스피싱을 신고**하려고 건 전화가 **바로 보이스피싱**이었던 것입니다.

□ 이에, **금융감독원**은 **소비자경보**를 **발령**하여 **주민센터 사칭 보이스피싱 수법**을 상세히 알려 드리고, **법원 등기 반송, 택배·카드 배송 등을 미끼로 삼는 변종 수법**도 함께 안내해 드리니 금융소비자 여러분의 **각별한 주의**를 당부드립니다.

Ⅱ. 주민센터 사칭 보이스피싱 주요 수법

□ **피해 사례**를 분석해 보면 이번 수법은 **미끼, 릴레이 기관 사칭, 공포·고립, 자금 편취**의 **4단계**로 진행됩니다. 전화 속 기관의 이름은 계속 바뀌지만 통화 상대는 **처음부터 끝까지 같은 범죄조직**입니다.

< 주민센터 사칭 보이스피싱 '릴레이 기관 사칭' 구조 >



* 본 이미지는 실제 피해사례의 수법을 토대로 생성형AI를 활용하여 제작한 예시임

1 (미끼 : 주민센터 사칭) "누가 선생님 신분증과 위임장을 들고 왔습니다"

□ **사기범**은 **주민센터 직원**을 **사칭**하여 **"어떤 사람이 선생님의 위조 신분증과 위임장을 가지고 왔다"**거나 **"누군가 선생님 명의로 주민등록등본과 인감증명서를 발급받으려 한다"**고 말합니다.

○ 피해자가 모르는 일이라고 답하면 **"신분을 확인하려 하니 황급히 떠났다", "도망을 갔다"**고 둘러대며 주민등록증을 잃어버린 적이 있는지 묻기도 합니다.

○ **공공기관 신뢰**를 **악용**한 **주민센터 공무원 사칭범**이 **서류를 발급하러 왔다는 사람**의 이름까지 구체적으로 거론하면서 기망하면, 당황한 피해자는 본인 모르게 **명의가 도용**되었다고 강하게 믿게 됩니다.

2 (릴레이 기관 사칭) "명의가 도용된 것 같으니 알려드리는 번호로 전화해 보세요"

□ **주민센터 공무원**을 사칭한 사기범은 **"명의가 도용된 것 같으니 신용정보원에 전화해 보라", "금융감독원에 전화해 보이스피싱 신고를 하라"**며 전화번호를 불러 줍니다.

○ 이 번호가 **이번 수법의 핵심**입니다. 내가 **직접 전화**를 걸었으니 진짜 기관일 것이라고 믿기 쉽지만, **그 번호로 연결되는 사람은 모두 사기범**입니다.

○ **신용정보원 직원**을 사칭한 사기범은 다시 **금감원**에 전화하여 **보이스피싱을 신고**하도록 유도하고, **금감원 직원**을 사칭한 사기범은 **담당 검사**에게 전화하라고 합니다.

3 (피해자 공포 · 고립 유도) "구속되기 싫으면 시키시는 대로 하세요"

□ **금감원 직원·검사**를 사칭한 사기범은 **"본인 명의로 작년 11월 ○○ 은행에서 계좌가 개설되었고, 이 통장이 범행에 사용되어 다수의 피해자가 발생했다"**고 말합니다.

○ **"구속을 당하기 싫으면 시키는 대로 하라"**고 협박하고, **"일급 비밀이니 누구에게도 피해 사실을 알리지 말라"**고 하며 피해자를 **고립**시킵니다.

4 (자금 편취) "피해재산은 수사가 끝나면 돌려드립니다"

□ **마지막 단계**에서 사기범은 **돈을 보내야 하는 이유**를 만들어 냅니다. **"명의도용으로 범죄에 연루되었으니 자산검수를 진행해야 한다", "자산은 국가에서 관리하고 수사가 마무리되면 피해 없이 반환한다"**는 말이 대표적입니다.

○ 피해자가 망설이지 않도록 **"정기예금 해약에 따른 피해도 보상해 주겠다"**고 안심시키고, **은행 지점장을 사칭**한 **사기범**까지 등장시켜 **"재산을 국가에서 관리해 줄 것"**이라고 안심 시킵니다.



* 본 이미지는 실제 피해사례의 수법을 토대로 생성형AI를 활용하여 제작한 예시임

Ⅲ. 소비자 주의사항 및 대응요령

□ **주민센터 사칭** 전화에 대응하는 **핵심**은 **금융감독원**이 **금융권**과 함께 알리고 있는 **행동요령**, **"의심하고, 끊고, 확인하고!"**입니다.



* 본 이미지는 실제 피해사례의 수법을 토대로 생성형AI를 활용하여 제작한 예시임

1 "위임장," "명의도용" 전화를 받으면 일단 끊으세요!

□ **주민센터, 신용정보원, 금융감독원** 등 어떤 기관을 내세우더라도 **명의도용**을 해결해야 한다며 **특정 번호**로 전화하라고 하면 **일단 끊으세요!**

○ **서류 발급 시도**가 있었는지 확인하고 싶다면 **정부민원안내콜센터**(☎110) 등을 통해 **주민센터 번호**를 **직접 확인**하거나 **가까운 주민센터**를 **방문**하시기 바랍니다.

2 명의도용 여부는 전화가 아니라 직접 조회하세요!

□ **한국신용정보원**은 **명의도용 신고**를 **접수하지 않습니다.**

○ **"본인 명의로 계좌가 개설되었다"**는 말을 믿지 마시고 **어카운트인포**(www.payinfo.or.kr)에서 및 **명의도용방지서비스**(www.msafer.or.kr)에서 직접 **명의도용 및 휴대전화 부정 개통 여부**를 확인할 수 있습니다.

3 금감원·공소청·중수청·경찰은 어떤 명목으로도 돈을 보내라고 요구하지 않습니다.

□ **"자산검수", "국가 관리", "수사 후 반환"** 등 명목이 무엇이든 돈을 보내거나 **현금·수표·골드바**를 전달하라는 요구는 **모두 사기**입니다.

○ **금융감독원**은 전화로 사건을 접수해 **담당 검사**를 연결해 주지 않으며, 수사를 이유로 예금을 보내면 **국가가 대신 관리**해 주는 **제도도 존재하지 않습니다.**

4 "누구에게도 알리지 말라"는 말은 사기의 신호입니다.

□ **수사기관**은 수사 중이라는 이유로 **전화를 끊지 못하게** 하지 않습니다.

○ **비밀을 지키라는 말**을 듣는 순간이 **바로 가족**에게 **전화**해야 할 때입니다. **은행 창구**에서 **예금 해지나 이체 사유**를 물으면 **사실대로 말씀**해 주세요.

5 앱 설치와 링크 접속은 거절하고, 의심되면 다른 사람의 전화로 신고하세요!

□ **주민센터 사칭 수법**에서도 **링크 클릭**이나 **악성앱·원격제어앱 설치**를 요구한 사례가 확인되고 있습니다.

○ **악성앱**이 **설치**되면 **경찰**(☎112) 또는 **금융감독원**(☎1332)으로 전화를 걸어도 **사기범에게 연결**될 수 있으므로, **앱을 설치**했거나 의심된다면 **가족 등 다른 사람의 전화**로 **신고**하시기 바랍니다.

6 신속히 지급정지를 요청하세요!

□ **범죄 피해 사실**을 **인지**하셨다면 **즉시 경찰**(☎112) **또는 금융회사 콜센터**에 **지급정지를 요청**하시기 바랍니다.

○ 아울러, 「안심차단 서비스 3종 세트」(여신거래·비대면 계좌개설·오픈뱅킹)에 **미리 가입**해 두시면 본인도 모르게 이루어지는 **대출**과 **계좌 개설**을 **사전**에 **차단**할 수 있습니다.

Ⅳ. 향후 계획

□ **금융감독원**은 **주민센터 사칭 보이스피싱**이 확산되지 않도록 다음과 같이 대응해 나가겠습니다.

① 이번 수법을 **全 금융권**에 **신속히 전파**하겠습니다.

- **보이스피싱 피해예방점검회의** 등을 통해 사례를 공유하고, 금융회사가 **영업점 창구**와 **이상거래탐지시스템**(FDS)에서 **고액 예금 중도해지, 여러 계좌로의 분할 이체** 등 **이상 징후**를 세심하게 살피도록 지도하겠습니다.

② **전기통신금융사기 통합대응단** 등 **관계기관**과 **긴밀히 공조**하겠습니다.

- 범행에 이용된 **전화번호**와 **계좌 정보**가 **신속히 공유**되도록 하고, **보이스피싱 정보공유·분석 AI 플랫폼**(ASAP*)을 활용하여 금융권의 **선제적 대응**을 지원하겠습니다.

  * **A**I-based anti-phishing **S**haring & **A**nalysis **P**latform

③ **변종 수법**을 **지속적으로 모니터링**하여 **새로운 수법**이 확인되는 즉시 **소비자경보** 등을 통해 알려 드리겠습니다.

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

붙임1 주민센터 사칭 외 주요 변종 수법

□ 사기범들은 주민센터 외에도 **법원 등기, 택배, 카드 배송**처럼 일상에서 흔히 접하는 연락을 미끼로 삼고 있습니다.

○ **첫 접촉 방식**은 달라도 사기범이 알려 준 **번호**나 **링크**로 끌어들인 뒤 **기관을 사칭해 돈을 요구**하는 구조는 같습니다.

< 기타 변종 보이스피싱 수법 >

유형	주요 수법	대응 요령
 **법원 등기 반송 사칭**	- **"법원 등기가 반송되었습니다"**, "등기를 받을 수 있습니까?"라며 연락한 뒤 악성앱 설치 링크나 가짜 공문서를 보냄 - 가짜 사이트에서 사건을 조회하게 하거나, 송달 안내문을 현관문에 붙여 연락을 유도하기도 함	- 법원 등기는 **우체국을 통해 배송**되며, 인터넷으로 영장을 제시·확인하는 것은 불가능 - 전화를 끊고 법원에 직접 확인
 **택배·카드 배송 사칭**	- 택배기사나 집배원을 사칭해 **"신청하신 카드를 배송하려 한다"**고 연락 - 신청한 적 없다고 하면 가짜 고객센터 번호를 알려 주고, 원격제어 앱 설치 후 금감원·검사 사칭으로 이어짐	- 전화를 끊고 '내 카드 한눈에' 서비스로 카드 발급 여부를 직접 확인
 **택배 반송 문자(스미싱)**	- **"송장번호 미확인입니다. 반송처리합니다"** 같은 문자로 링크 접속을 유도 링크를 누르면 악성앱이 설치되거나 개인정보가 유출될 수 있음	- 문자 속 링크는 누르지 말 것 - 배송 여부는 택배사 공식 앱 또는 홈페이지에서 직접 조회

⇒ **유형은 달라도 공통점은 같습니다.** ①일상적인 연락으로 시작하고, ②사기범이 알려 준 번호나 링크로 이동시키며, ③비밀 유지를 요구해 고립시킨 뒤, ④돈을 요구합니다. 이 중 하나라도 해당하면 **일단 끊고 직접 확인**하십시오.

붙임2 보이스피싱 피해 예방을 위한 안심차단 서비스3종 세트

□ 「**안심차단 서비스 3종 세트**」에 가입하시면 본인도 모르게 **대출, 비대면 계좌개설, 오픈뱅킹**이 실행되어 피해가 발생하는 것을 **사전**에 **차단**할 수 있습니다.

○ **은행, 저축은행, 농협, 수협, 신협, 새마을금고, 산림조합, 우체국** 등 한 곳에만 신청하여도 **전 금융권**에 **자동으로 전파**되며,

○ **금융회사 영업점**이나 **은행 애플리케이션, 어카운트인포**를 통해 간편하게 신청하실 수 있습니다.

❶ 여신거래 안심차단	신용대출, 카드론, 신용카드 발급, 할부금융, 예·적금 담보대출 등 개인 명의의 여신거래를 차단('24.8.23. 시행)
❷ 비대면 계좌개설 안심차단	범죄조직의 수익 통로로 사용될 수 있는 대포통장 개설을 막기 위해 비대면 계좌개설을 차단('25.3.12. 시행)
❸ 오픈뱅킹 안심차단	오픈뱅킹을 통한 계좌정보 무단조회 및 이체 등을 방지할 수 있도록 오픈뱅킹 서비스를 차단('25.11.14. 시행)

붙임3 보이스피싱 피해 발생시 대응요령

① 피해신고 및 지급정지	경찰(☎112), 전기통신금융사기 피해신고 통합센터(☎1394), 또는 금융회사에 즉시 피해신고 및 계좌 지급정지 요청
② 개인정보 노출등록	개인정보노출자 사고예방시스템(pd.fss.or.kr)에 노출 사실을 등록하여 신규 계좌개설·카드발급 제한
③ 계좌 일괄 지급정지	계좌정보통합관리서비스(www.payinfo.or.kr) 또는 금융회사 영업점에서 본인 명의 계좌 일괄 지급정지
④ 명의도용 신고	명의도용방지서비스(www.msafer.or.kr)에서 본인 모르게 개통된 휴대전화 조회 및 추가 개통 차단
⑤ 악성앱 삭제 및 초기화	악성코드 감염이 의심되는 경우 관련 앱을 즉시 삭제하고 휴대전화를 초기화
⑥ 피해사례 공유	보이스피싱지킴이 사이트*에 접속하여 피해사례를 공유하고 최신 수법을 확인 * 금융감독원 홈페이지(www.fss.or.kr) → 민원·신고 → "보이스피싱지킴이"

붙임4 여신거래 안심차단서비스 신청방법(은행 앱)

① 홈 화면-"메뉴" 클릭



② 인증/보안 클릭



③ 안심차단서비스 클릭



④ 여신거래 차단 선택



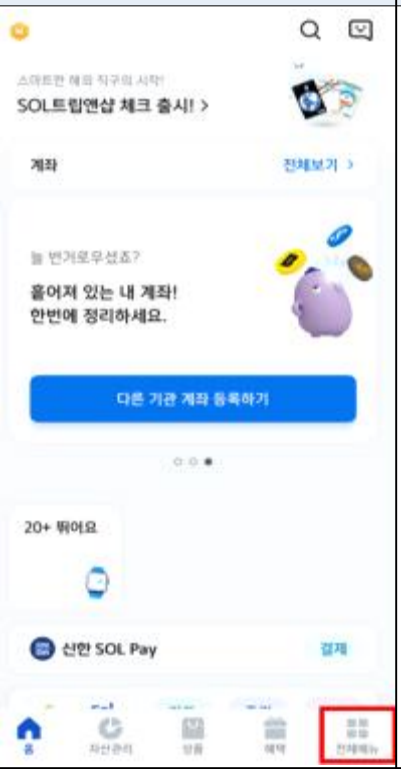
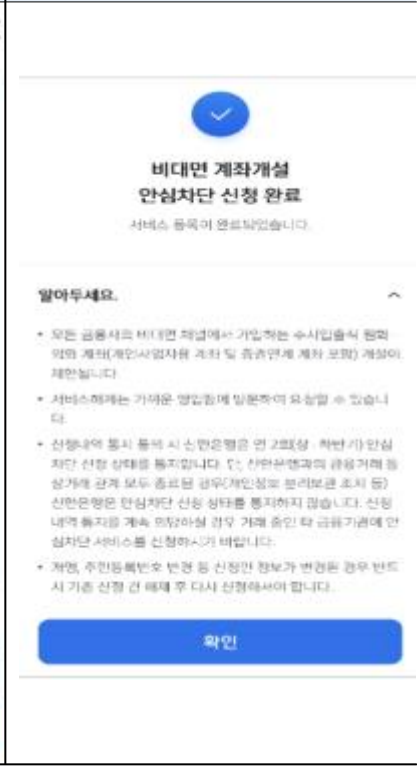
⑤ 약관 동의



⑥ 신청 완료



붙임5 비대면 계좌개설 안심차단서비스 신청방법(은행 앱)

① 홈 화면-"전체메뉴" 클릭	② 비대면 계좌개설 안심차단 클릭	③ 안심차단 신청
		
④ 오픈뱅킹 이용정보 확인	⑤ 동의서 작성	⑥ 결과 확인
		

붙임6 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**
		