

 금융감독원	보도자료	금융은 투명하게 소비자는 행복하게
---	------	--------------------

보도	배포시	배포	2024. 8. 22. (목)
담당부서	금융사기대응단 금융사기대응1팀	책임자	팀장 장종현 (02-3145-8140)
		담당자	선임조사역 김대희 (02-3145-8149)
		조사역 조준원	(02-3145-8139)

보이스피싱 피해예방을 위해 꼭 알아두세요!!! - 안전한 금융거래를 위한 6가지 레시피 -

<input checked="" type="checkbox"/> 소비자경보 2024 - 29호
등급
주의 경고 위험

대상 금융소비자 일반

- 최근 高금리·高물가 상황에서 서민층의 자금 사정이 어려워지고 있는 가운데, 서민들의 궁박한 사정을 악용한 보이스피싱 피해 사례가 다수 발생하는 등 보이스피싱 피해 우려가 커지고 있습니다.

※ 경찰청에 따르면 올해 1~5월 총 8,434건·2,563억원 상당 피해 발생('24.7.9. 보도자료)

- 특히 최근에는 미끼문자·악성앱 등을 이용하여 접근한 사기범들이 금융회사·금감원·경찰·검찰 등 여러 기관을 조직적으로 사칭하며 피해자를 혼란에 빠뜨린 뒤, 피해자가 비대면 대출까지 받도록 요구하여 편취하는 수법이 성행하고 있습니다. (☞<붙임1>)
- 이에 금융감독원은 금융소비자의 이해를 돋고 안전한 금융거래 환경을 조성하기 위하여 최근 발생한 보이스피싱 피해사례를 바탕으로 금융소비자가 반드시 알아야 할 유의사항을 안내해 드립니다.

안전한 금융거래를 위한 6가지 레시피

- 수상한 문자메시지는 삭제하고, 전화는 바로 끊으세요!
- 알 수 없는 출처의 앱 설치를 차단하세요!
- 대부광고에 개인 연락처를 함부로 남기지 마세요!
- 금융회사는 대환대출시 기존 대출을 먼저 상환하라고 요구하지 않습니다.
- 단기간에 신용점수를 올려주겠다는 것은 사기입니다!
- M-safer의 휴대폰 가입제한서비스를 활용하세요.

소비자 대응요령 및 유의사항

레시피 ① 수상한 문자메시지는 삭제하고, 전화는 바로 끊으세요!

- **(미끼문자)** 미끼문자란 사기범이 문자메시지 수신자를 속여 수신자의 개인정보·금전을 빼앗기 위해 불특정 다수에게 보내는 문자*입니다.

* 주로 신용카드 발급, 과태료·범칙금 납부안내, 택배배송, 지인의 경조사 알림 등을 사칭

- 사기범은 미끼문자를 통해 수신자가 문자 속 전화번호로 전화를 걸도록 유도한 이후 금융회사·금감원·경찰·검찰을 사칭하며 피해자를 속여 금전을 빼앗습니다.

관련 피해 사례

- ◆ 사기범1은 피해자에게 우편집배원, 택배 기사 등을 사칭해 "신청하신 OO신용카드를 배송할 예정이다"라고 전화하여, 피해자가 신용카드 신청 사실이 없다고 답하자 명의도용 피해를 우려하며 허위 고객센터의 전화번호를 알려주며 문의하라고 기망
- 피해자가 위 전화번호로 전화하자 카드사 직원을 사칭하는 사기범2는 피해자 모르게 계좌가 개설된 것 같으니 금감원·검찰에 연결시켜주겠다고 기망
- 이후 금감원·검찰을 사칭하는 사기범3, 4는 피해자 명의로 사기계좌가 개설되어 큰 피해가 발생하였다며, 불법자산 유출 금지조치를 위해 피해자가 보유한 모든 예금을 국가 안전계좌로 이체할 것을 압박하여 편취

미끼문자 예시

[Web 발신]
[1533-4015]
(**2778) 카드 정상 발급
되었습니다.
본인의 신청 아니면 즉시
확인 바랍니다.

[Web 발신]
쓰레기 무단투기로
단속되어 과태료가
부과되었습니다.
과태료확인
<http://co.lys.to.net>

[OO택배]
송장번호 4604****
주소 불일치로 물품 보
관중입니다.
확인하기
<http://t.me/afad0>

[소비자 유의사항]

- ① 문자메시지 속 수상한 링크, 첨부파일 등은 열지 말고 즉시 삭제해야 합니다.
- ② 금융사·금감원·경찰·검찰이라며 전화가 오면 일단 전화를 끊으세요.
- ③ 의심스러운 문자메세지를 받은 경우 곧바로 문자메시지 화면 최상단에 위치한 "스팸으로 신고" 버튼을 클릭하세요.

레시피 ② 알 수 없는 출처의 앱 설치를 차단하세요!

- **(악성앱)** 사기범은 대출에 필요하다거나, 범죄에 연루되었는지 확인해주겠다며 피해자의 휴대폰에 악성앱을 설치하도록 유도합니다.(☞ 붙임2)

악성앱의 주요 기능

- ◆ **발신번호 조작** : 피해자 휴대폰에 표시되는 발신 전화번호를 112 등 임의의 번호로 조작
- ◆ **전화 가로채기** : 피해자 휴대폰의 통화 기능을 제어(강제수신·강제발신)
- ◆ **개인정보 탈취** : 휴대폰에 저장된 신분증, SMS, 연락처 등 모든 개인정보를 탈취
- ◆ **원격제어** : 사기범이 피해자 휴대폰의 모든 기능을 통제

[소비자 유의사항]

- ① 평소 휴대폰의 알 수 없는 출처의 앱 설치를 제한하면 악성앱 설치를 막는 데 도움이 될 수 있습니다. (☞붙임3)
- ② V3, 시티즌코난 등 모바일 백신앱을 설치하면 악성앱 상시 탐지를 통해 악성앱 설치를 막을 수 있습니다.
- ③ 악성앱이 설치되었다면 ①모바일 백신앱(최신 버전)으로 검사 후 삭제하고, ②데이터 백업 후 휴대폰을 초기화하고, ③휴대폰 서비스센터 AS를 요청하세요.

레시피 ③ 대부광고에 개인 연락처를 함부로 남기지 마세요!

- **(불법대부광고)** 이는 사기범이 급전이 필요한 피해자에게 접근하기 위해 유튜브·인터넷포털 등에 게재하는 가짜 대부광고*입니다.

* 일반적인 대부광고는 대출업체의 연락처를 남기며, 소비자에게 연락처를 남길 것을 요구하지 않음

- 피해자가 대부광고 댓글에 연락처를 남기면, 금융회사 상담원으로 위장한 사기범이 대환대출 등 대출이 가능하다며 피해자를 속입니다.

관련 피해 사례

- ◆ 피해자가 유튜브에서 <서민안심전환대출> 광고를 보고 대출상담을 위해 댓글에 연락처를 남기자, OO캐피탈 직원을 사칭하는 사기범이 전화하여 "신용점수가 낮아 당장 대출 진행은 어렵지만, 신용보증금을 입금하면 저리대환대출이 가능하다"고 기망하여 편취

[소비자 유의사항]

- 제도권 금융회사는 고객에게 유튜브·인터넷포털에 게재된 광고 댓글에 고객 연락처를 남기라고 요구하지 않습니다.

레시피 ④

금융회사는 대환대출 시 기존 대출을 먼저 상환하라고 요구하지 않습니다.

- **(대환대출)** 대환 대출이란 기존 대출을 상환하기 위해 새롭게 받는 대출^{*}이므로, 제도권 금융회사는 대환대출을 받기 위해 기존 대출을 먼저 상환하라고 요구하지 않습니다.

* 대환대출 승인·실행 → 기존 대출 상환 순으로 이루어짐

관련 피해 사례

- ◆ 피해자는 금융회사 상담원을 사칭한 사기범1에게 속아 대출신청앱을 가장한 악성앱을 설치한 후 해당 앱을 통해 대환대출을 신청
- 이후 피해자는 기존 대출 금융회사 직원을 사칭한 사기범2로부터 "기존 대출 상품은 대환대출이 안되는 상품인데 **대환대출을 진행한 것은 계약 및 금융법 위반이며, 대출 지급이 정지되는데 지급정지를 해제하고 대출을 받으려면 기존 대출금을 전부 상환하라**"는 요구를 받고 송금하여 피해를 입음

[소비자 유의사항]

- ① "대환대출은 계약·법 위반"이라며 대환대출을 받으려면 "기존 대출 먼저 상환하라"는 요구는 모두 보이스피싱입니다.
- ② 대출을 받기 위해 SNS 메신저 등으로 보낸 앱을 설치하도록 하는 경우 보이스피싱입니다.

레시피 ⑤

단기간에 신용점수를 올려주겠다는 것은 사기입니다!

- **(신용점수)** 신용점수는 단기간에 올릴 수 없으며, 금융회사가 신용 점수를 올려주겠다며 선입금을 요구하는 경우는 없습니다.

관련 피해 사례

- ◆ 사기범은 피해자에게 OO저축은행 직원을 사칭하며 "신용점수가 낮아 당장 대출 진행은 어렵지만, 대출신청액의 20%를 송금하여 45일 정도 예치하여 거래실적을 쌓으면 신용등급이 올라 대출이 가능하다"고 기망하여 금전을 편취

[소비자 유의사항]

- ① 신용점수를 단기간에 올려주겠다는 것은 무조건 사기입니다.
- ② 거래실적을 쌓아야 한다며 금전 입금을 요구할 경우 보이스피싱입니다.
- ③ 제도권 금융회사는 공탁금, 저금리 전환 예치금, 보증보험료, 선이자 등의 명목으로 대출과 관련한 선입금을 요구하지 않습니다.

레시피 ⑥ M-safer의 휴대폰 가입제한서비스를 활용하세요.

- (휴대전화 명의도용)** 사기범이 악성앱을 이용하여 탈취한 피해자의 개인정보로 피해자가 모르게 피해자 명의 알뜰폰을 개통한 후
 - 새 휴대폰에 금융앱을 재설치하고 오픈뱅킹을 통해 예·적금을 중도해지하고 비대면 대출을 받아 편취

관련 피해 사례

- ◆ 피해자는 속도위반 과태료 부과 문자를 받고 문자 안의 URL을 클릭하여 핸드폰에 악성앱이 설치됨
 - 사기범은 악성앱을 통해 피해자의 핸드폰에 저장되어 있던 개인정보·신분증 사진 등을 탈취하여 피해자 명의 알뜰폰을 개통하였고, 이를 이용하여 캐피탈·카드사 등으로부터 피해자 명의로 각종 비대면 대출을 받아 편취

[소비자 유의사항]

- M-safer(www.msafer.or.kr)의 휴대폰 가입제한서비스를 통해 본인도 모르게 다른 이동통신사에 휴대폰이 개통되어 입을 수 있는 피해를 예방할 수 있습니다. (☞ 불임4)

향후 계획

- 금융감독원은 보이스피싱 피해 예방·구제대책을 대폭 확대하는 개정 「통신사기피해환급법」(8.28. 시행)이 현장에 안착될 수 있도록 다방면으로 지원할 것이며,
 - '보이스피싱은 반드시 근절된다'는 믿음을 가지고 전금융권과 협력하여 보이스피싱 근절을 위한 노력을 계속해나가겠습니다.

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

① 기관사칭형 수법

- ① **(미끼문자)** 금융회사·공공기관을 사칭하는 미끼문자^{*}를 통해 피해자가 가짜 상담번호로 전화하도록 유인

* 신규카드 발급, 카드결제 승인, 금융범죄 연루 등 허위내용을 담은 문자메시지(SMS)를 전송

- ② **(시나리오)** 가짜 상담사는 피해자의 개인정보가 유출된 것 같다며 금감원·검찰 등으로 연결시켜주겠다고 허위 안내

- 금감원·검찰 등에 전화하면 또다른 사기범이 피해자 명의로 불법계좌가 개설되는 등 범죄에 연루되었다고 기망

- ③ **(악성앱)** 기망 과정에서 악성앱 설치를 유도하여 금융회사·금감원·검찰 등 대표번호로 전화해도 사기범에게 연결되도록 조치

- ④ **(비대면대출)** 불법자산 유출 금지 등 명목으로 예·적금 뿐만 아니라 각종 비대면 대출을 최대한도까지 받게 하여 안전계좌로 이체할 것을 지시

② 대출빙자형 수법

- ① **(불법광고)** 사기범은 유튜브·인터넷포털 등에 불법금융광고를 게시하고, 이를 보고 연락처를 남긴 피해자에게 전화

- ② **(제2금융권 사칭)** 캐피탈사, 저축은행 등 제2금융권을 주로 사칭하며 저리대환대출 등이 가능하다고 기망

- ③ **(시나리오)** 신용점수가 낮아 당장 대출 진행은 어렵지만, 거래실적 등을 쌓아 신용등급을 높이면 대출이 가능하다며 입금을 유도

- 이후 다른 사기범이 전화하여 ‘대환대출 진행은 법 위반이므로 기존 대출을 먼저 전부 상환하라’며 추가 입금을 압박

불임2

악성앱 실행화면 예시

- 사기범에 정책자금 신청에 필요하다며 피해자에게 설치를 요구한 악성앱
 - 악성앱이 설치되면, 강제수신·발신과 같은 휴대전화 통화 제어 기능과 SMS, 연락처, 사진 등 정보를 탈취하는 기능 등 여러 가지 악의적인 행위가 가능해짐

궁금한 내 정책자금
빠르게 확인하자!

빠르고 간편한
원클릭 조회 서비스!

정책자금 확인 Click!

소상공인 대출·대출중개
등록번호: 2022-경기고문-680-등록
소상공인 경영자금신청센터
2021 중앙일보
올해의 우수브랜드 대상1위

소상공인 경영자금 신청센터

신청대상: 소상공인, 자영업, 중소기업, 법인회사
신청자금: 소상공인 베일자금, 개인사업자대출, 정부창업자원금, 자영업정책자금, 중소기업 정책자금, 기타 정책자금 및 대출

승인가능여부 바로조회
은행간 연계시스템 구축으로 승인가능
여부 최단시간 조회

최저이율·최대한도
전국에서 이율이 가장 낮고 한도가
제일 많은 은행 바로조회

최단기간 자금수령
당일신청후 1~3일 이내로 수령가능

금리·한도·승인가능 여부 조회

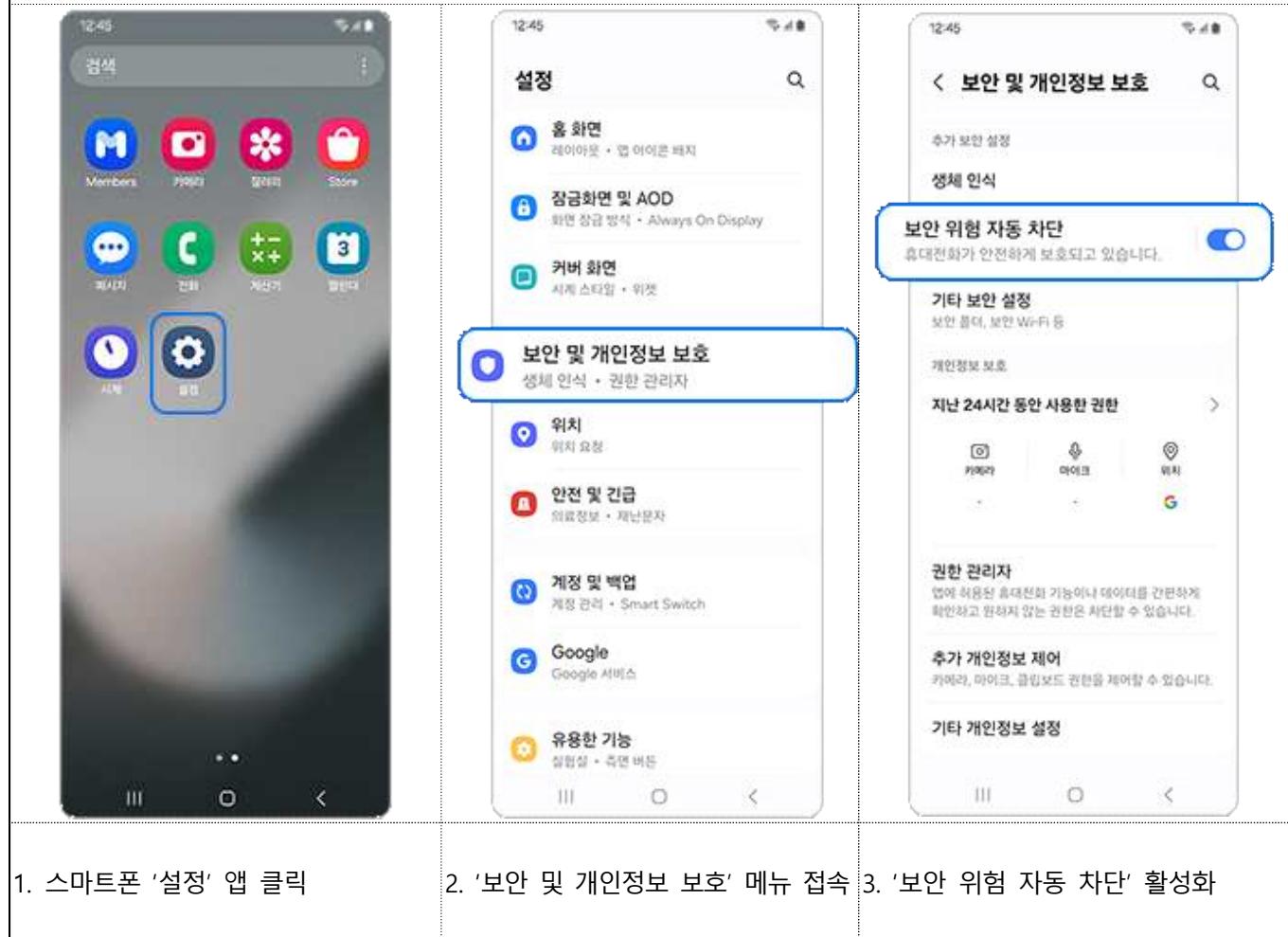
성함
연락처
주민등록번호
거주지 주소
필요금액

상담신청

불임3

알수 없는 출처의 앱 설치 차단 방법

< 차단 기능 설정 방법(안드로이드) >



※ 차단 방법은 스마트폰에 탑재된 안드로이드 OS 버전에 따라 다를 수 있음

불임4

휴대폰 가입현황 조회 및 가입제한 방법

< 명의도용방지 서비스(Msafer) >

<p>가입사실현황조회 서비스 이동전화, 무선인터넷, 인터넷전화의 가입현황을 실시간으로 조회합니다.</p> <p>가입제한 서비스 통신사 지정 범위없이 온라인으로 이동전화 신규가입 사전 차단</p> <p>이메일안내 서비스 내 명의로 등록된 우편집 등신사, 인터넷, 인터넷방송의 개통사실을 이메일로 알립니다.</p>	<h3>로그인</h3> <p>명의도용방지서비스 이용을 위한 약관에 동의해 주시기 바랍니다.</p> <p>서비스 이용에 대한 약관 동의</p> <p><input type="checkbox"/> (총8) 서비스 이용약관 (필수) [자세히보기] <input type="checkbox"/> (총8) 개인정보처리방침 (필수) [자세히보기] <input type="checkbox"/> (총8) 계약 체결용약관 (필수) [자세히보기] <input type="checkbox"/> (총8) 고유식별정보 처리방침 (필수) [자세히보기]</p> <p>동의하시기 전에 아래의 이용약관 안내문을 반드시 읽어주세요. 최종의 신상정보는 [가인정보보호법]에 의해 놀라하게 보호됩니다.</p>															
1. www.msafer.or.kr에서 '가입사실현황조회서비스' 클릭	2. 공동인증서를 통하여 로그인															
<p>가입사실현황조회서비스</p> <p>나의 가입현황조회 전체 가입현황조회</p> <p>KT1건 SK텔링크(SKT) 1건</p> <p>조회 결과</p> <table border="1"> <thead> <tr> <th>서비스 구분</th> <th>사업자</th> <th>가입(건)</th> <th>상세</th> <th>고객센터</th> </tr> </thead> <tbody> <tr> <td>이동통신</td> <td>KT</td> <td>1</td> <td>1588-0010</td> <td></td> </tr> <tr> <td>인터넷</td> <td>SK텔링크(SKT) (인터넷)</td> <td>1</td> <td>1599-0999</td> <td></td> </tr> </tbody> </table>	서비스 구분	사업자	가입(건)	상세	고객센터	이동통신	KT	1	1588-0010		인터넷	SK텔링크(SKT) (인터넷)	1	1599-0999		<p>가입제한서비스</p> <p>이동전화 신규거래 및 번호이동 - 명의이전 기기변경(LGU+만 해당)를 나중의 없이 할 수 있도록 사건에 차단하는 서비스로 통신사 대리점과 직접 방문하지 않고 온라인으로서 신청할 수 있는 편리한 서비스입니다. 본 서비스는 이용자가 신发展格局에 맞춰 통신사별 업무를 통신사별 업무로, 기밀화된 것 해제 처리는 통신사에서 진행하나, 조류 발생시 해당 통신사 고객센터에 확인하시기 바랍니다.</p> <p>가입 제한 이동통신사</p> <ul style="list-style-type: none"> ● 전체 ● SKT ● KT (알뜰폰 포함) ● LG U+ (알뜰폰 포함) ● KCT ● 세콤 넷워콤 ● LG헬로비전 (KT) ● SKT 알뜰폰 <p>가입제한을 해제한 이동통신사</p> <p>* 가입제한을 하게하고자 할 경우 원하는 이동통신사를 선택 후 [제한해제] 버튼을 클릭하세요.</p>
서비스 구분	사업자	가입(건)	상세	고객센터												
이동통신	KT	1	1588-0010													
인터넷	SK텔링크(SKT) (인터넷)	1	1599-0999													
3. 조회 결과 명의도용으로 인한 개통이 확인되면 해당 통신사에 연락하여 회신 해지신청 및 명의도용 신고	4. '가입제한서비스'를 통하여 통신사별로 휴대폰 신규 가입을 사전 차단 가능															

※ 명의방지도용 서비스는 휴대폰 PASS앱 및 카카오뱅크 앱에서도 신청 가능

< PASS·카카오뱅크앱을 통한 신청 방법 >

<p>PASS</p> <p>알파스탁</p> <p>부동산지키미</p> <p>보안</p> <p>세이프가드</p> <p>더치트 프리미엄</p> <p>명의도용방지</p>	<p>상품, 서비스, 증명서 검색</p> <p>금융보안</p> <p>명의도용방지 서비스</p> <p>최근 금융사기 유형 신규</p>
(PASS앱) '보안' 메뉴에서 '명의도용방지' 접속	(카카오뱅크앱) '금융보안' 메뉴에서 '명의도용방지 서비스' 접속