



금융감독원

# 보도자료



금융은 튼튼하게 소비자 행복하게

보도	배포시	배포	2024. 1. 3. (수)	
담당부서	금융감독원 금융사기전담대응단	책임자	부국장	박정은 (02-3145-8140)
		담당자	선 임	차정은 (02-3145-8137)

## 연초에 많이 발생하는 카드발급, 연말정산, 합격문자 등 보이스피싱 사기 수법, 늘·꼭·또 하세요!

- 늘 의심하고, 꼭 전화끊고, 또 확인하고! -

### □ 소비자경보 2024 - 1호

등급	주의	경고	위험
대상	금융소비자 일반		

### 소비자경보 내용

- ◆ 최근 카드 해외 부정사용 또는 연말정산 등을 이용하여 보이스 피싱을 유도하는 사례가 다수 발생하여 주의할 필요
  - 사기범들은 개인정보를 탈취하여 명의를 도용하거나, 보증금 등의 명목으로 자금을 송금하도록 요구
- ⇒ 개인정보나 자금을 요구하는 경우 한번 더 의심하고 확인할 것

#### <보이스피싱 예방을 위해 다음 사항을 미리 숙지해주세요!>

- ① 개인정보 제공 및 자금 이체 요청은 무조건 거절하세요
- ② 계좌번호나 비밀번호, 신분증 사진들을 휴대전화에 저장하지 마세요
- ③ 제도권 금융회사의 전화번호는 한번 더 확인하세요
- ④ 금융회사의 사전 예방서비스를 활용하여 안전하게 관리하세요
- ⑤ 휴대전화 가입제한 서비스로 명의도용을 사전에 방지하세요

#### <보이스피싱 피해를 당한 경우 다음과 같이 행동해주세요!>

- ① 금융회사 및 112로 본인 및 사기범 **계좌**에 대해 **지급정지** 요청하세요
- ② '**내계좌 통합관리**'에서 명의도용 계좌·대출을 확인하세요
- ③ 금융감독원 홈페이지에서 '**개인정보 노출자**'로 등록하세요
- ④ '**명의도용 방지서비스**'에서 본인 명의의 휴대전화개통 현황을 확인하세요

## 1 사기 수법

※ 구체적인 사기 수법은 (붙임) 보이스피싱 사기 사례 참고

### ① 카드사 사칭 부정사용 의심 문자메세지 발송

- 사기범들은 카드사를 사칭하여 개인정보가 도용되어 카드 신규 발급, 해외 부정 사용이 의심된다는 내용의 문자메세지 발송
  - 문자메세지 내 번호로 문의할 경우 카드번호, 계좌번호 등의 개인정보를 입력하도록 하여 취득한 개인정보를 추가 범죄에 이용
  - 검찰, 경찰 등을 사칭하여 명의도용으로 인한 범죄에 연루되었다며 구속 수사 면제 조건으로 일정 금액을 예치할 것을 요구

### ② 연말정산, 세금환급을 빙자한 개인정보 요구

- 사기범들은 국세청 등을 사칭해 연말정산, 세금환급을 위해 개인정보가 필요하다는 신분증 사진, 계좌번호 등을 요구
  - 피해자의 신분증 사진으로 휴대전화를 신규 개통하고, 개통한 전화로 본인인증을 하여 피해자 명의로 계좌 개설 및 대출 실행
  - 연말정산 등을 위해 필요하다는 URL 접속 또는 애플리케이션 다운로드를 유도하여 악성 프로그램 설치 후 개인정보 탈취

### ③ 대학 입시 및 취업 빙자 사기

- 사기범들은 대학 또는 기업을 사칭하여 입학(취업) 합격 확인 문자메세지를 보내 메신저 피싱으로 이용
  - 합격 확인을 위해 신분증, 주민등록번호 등의 개인정보를 입력하도록 하고 악성 URL 접속을 유도하여 불법 프로그램 설치
  - 허위로 합격 통보를 안내한 후, 입학·입사를 위해서는 일정 금액을 예치할 것을 요구하여 자금을 편취

## 2 보이스피싱 예방을 위한 문단속

**보이스피싱을 당하지 않도록 다음 사항을 숙지하여 사전에 예방하세요**

### 1 개인정보 제공 및 자금 이체 요청은 무조건 거절하세요

- 정부기관 및 제도권 금융회사는 전화·문자를 통한 개인정보 제공, 자금 송금 등을 절대 요구하지 않음

### 2 계좌번호나 비밀번호, 신분증 사진들을 휴대전화에 저장하지 마세요

- 악성앱이 설치된 경우 휴대전화에 저장된 정보가 탈취될 수 있으므로 개인정보를 저장하지 말고 가급적 모두 삭제

### 3 제도권 금융회사의 전화번호를 직접 확인하세요

- 금융소비자 정보포털\*(파인)이나 금융회사 홈페이지에서 금융회사 대표 전화번호를 직접 확인하고, 국외발신 문자메시지의 경우 절대 응하지 말 것

\* 파인(fine.fss.or.kr)>금융회사 정보>제도권 금융회사 조회

### 4 금융회사의 사전 예방 서비스를 활용하여 안전하게 관리하세요

- 개인정보유출에 따른 명의도용으로 발생하는 피해를 방지하기 위한 금융회사의 사전 예방 서비스\*를 적극 활용

\* 지연이체 서비스, 입금계좌 지정 서비스, 단말기 지정 서비스, 해외 IP 차단 서비스, 고령자 지정인 알림서비스 등

### 5 휴대전화 가입제한 서비스로 명의도용을 사전에 방지하세요

- 본인 명의 이동전화의 신규 개설을 차단하는 「가입제한 서비스」를 이용하여 휴대폰 명의 도용에 따른 피해 예방

#### 《가입제한 서비스 신청 방법》

- 명의도용방지서비스 홈페이지(www.msafes.or.kr)내 가입제한서비스
- 모바일 'PASS앱'에서 보안>명의도용방지
- 통신사 명의도용신고접수처(지점, 직영점, 플라자)에 내방(신분증 지참)하여 신청

※ 가입제한 해제시에는 해당 통신사 지점 방문 또는 고객센터에 문의하여 해제 신청 가능

### 3 보이스피싱 피해시 대처요령

신속하게 계좌 지급정지를 요청하고 추가 피해를 예방하세요!

<p><b>계좌 지급정지</b></p>  <p>112 HELP!</p> <p>금융회사 또는 보이스피싱 통합센터에 전화하여 해당 계좌 지급정지를 요청하고 피해구제를 신청</p>	<p><b>개인정보 노출 등록</b></p> <p><a href="https://fine.fss.or.kr">https://fine.fss.or.kr</a> <a href="https://pd.fss.or.kr">https://pd.fss.or.kr</a></p>  <p>금융감독원 금융소비자 정보포털 '파안'의 개인정보 노출자 사고예방 시스템을 활용하여 추가 피해 예방</p> <p><small>신청인이 직접 개인정보 노출 사실을 등록하면 신규 계좌개설, 신용카드 발급 등이 제한됨</small></p>
<p><b>내계좌 통합관리</b></p> <p><a href="http://www.payinfo.or.kr">www.payinfo.or.kr</a></p>  <p>계좌정보 통합관리서비스에서 본인 명의로 개설된 계좌 또는 대출을 확인하고, 필요시 일괄지급정지</p>	<p><b>휴대폰 명의도용 방지</b></p> <p><a href="http://www.msafes.or.kr">www.msafes.or.kr</a></p>  <p>명의도용 방지서비스를 이용하여 본인 모르게 개통된 휴대폰을 조회하거나 추가 개통을 차단</p>

#### 1 계좌 지급정지

- 본인 또는 사기범 계좌의 금융회사\*나 보이스피싱 통합신고·대응센터(☎112)로 지체없이 피해사실을 신고하여 계좌 지급 정지
- \* 빠른 대처를 위해 주거래 금융회사의 콜센터 번호를 알아두면 유사시 도움이 됨
- 가까운 경찰서에 방문하여 피해사실에 대한 '사건사고사실확인원'을 발급받아 3영업일내에 지급정지 신청한 금융회사에 제출

※ 신속한 지급정지로 잔액이 남아있는 경우 금감원의 피해금 환급절차로 피해 구제 가능

## 2 명의도용 계좌·대출 확인(내계좌 통합관리)



- '계좌정보 통합관리서비스(www.payinfo.or.kr)'에서 본인 명의로 개설된 계좌\* 또는 대출\*\*을 확인하여 명의도용 피해 여부 확인  
\* 내계좌 한눈에 또는 내오픈뱅킹 한눈에   \*\*금융정보조회 > 대출정보조회
- 본인 모르게 개설된 계좌가 있을 경우 '내계좌지급정지' 메뉴에서 일괄 지급정지 가능(계좌정보통합관리서비스 > 내계좌지급정지)

## 3 개인정보 노출 등록

- 신분증 사본 등을 제공하였거나, 출처가 불분명한 URL을 클릭하여 개인정보가 노출되었다고 판단한 경우 '개인정보노출자'로 등록\*  
\* 금융소비자포탈 파인 홈페이지 > 신고·상담·자문서비스 > 개인정보 노출 등록·해제 또는 개인정보노출자 사고예방시스템(<https://pd.fss.or.kr>)에서 등록가능
- 개인정보 노출자로 등록되면 신규 계좌개설, 신용카드 발급 등이 제한되어 추가적인 명의도용 피해 예방 가능

## 4 휴대폰 명의도용 방지

- '명의도용 방지서비스(www.msafes.or.kr)'를 이용하여 본인 모르게 개통된 이동전화, 인터넷 전화 등 이동통신사 가입현황 조회
- 가입현황 조회 결과 명의도용으로 인한 개통이 확인되면 해당 통신사 등에 연락하여 회선 해지신청 및 명의도용 신고

	<p>✉ QR 코드로 접속하여 보이스 피싱 피해시 대처요령과 주요 전화번호를 휴대폰에 저장하세요!</p>	
---	--	---

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

## 붙임 보이스피싱 사기 사례

### 카드사 사칭 문자메세지 발송 사례

A씨는 '23.10월 ●●카드가 해외에서 발급되었고 본인이 신청한 사실이 없으면 연락하라는 문자메시지를 수신한 후 메시지에 기재된 전화번호로 연락하였고, 이후 검찰, 경찰, 금융감독원 직원을 사칭한 사기범들로부터 피해자 명의 대포통장이 중고거래 사이트 사기에 연루되었다며 구속 수사를 면하려면 공탁금을 이체해야 한다는 말에 기망당하여 △△은행 계좌로 자금을 이체하여 피해를 입음

#### [카드사 사칭 문자메시지]

[ 카드]  
(5499)카드 신청접수  
고객님 신청이 아니시면  
사고예방접수:1551-

[국외발신]  
[ 카드]  
고객님 (\*\*\*\*2577) 카드 신청접수  
신청사실이 없을경우 빠른신고  
문의: 02-2675-

### 세금환급 빙자 사례

B씨는 ○○○세무서 직원을 사칭한 사기범으로부터 전화를 받아 80만원 상당의 미환급 세금 환급을 위해 신분증 사진, 계좌번호, 비밀번호 등의 정보가 필요하다는 말에 기망당하여 개인정보 및 금융거래정보를 사기범에게 제공하였고, 사기범은 피해자 명의로 ▲▲카드사로부터 대출을 받아 피해자 명의를 도용하여 개설한 □□저축은행 계좌로 입금받아 자금을 편취

### 취업 합격 후 보증금 요구 사례

C씨는 ◇◇여행사 직원으로 사칭한 사기범으로부터 아르바이트에 합격하였다는 통지를 받은 후, 급여 지급을 위해서는 사전에 보증금 및 수수료 납입이 필요하다고 하여 ■■■은행 계좌로 자금을 이체하여 피해를 입음