

보도시점 2023. 7. 14.(금) 배포 2023. 7. 13.(목) 9:00

## 금융당국과 전 금융권이 합심하여 신종 보이스피싱 사기수법에 적극 대처해 나가겠습니다.

- “보이스피싱, 의심하고 · 끊고 · 확인하세요”
- 휴가철 예상되는 사기수법을 신속대응체계를 통해 선제적으로 대응

금융당국은 카드사 사칭 비밀번호 요구, 해외결제 빙자 스미싱, 가족 납치 명목 금전요구 등 여름 휴가철을 앞두고 예상되는 보이스피싱 사례 및 대처요령을 민관합동 대응체계\*를 통해 전 금융권에 전파하여 금융 소비자가 휴가철에도 보이스피싱에 대한 경각심을 유지하여 피해를 예방할 수 있도록 조치하였다.

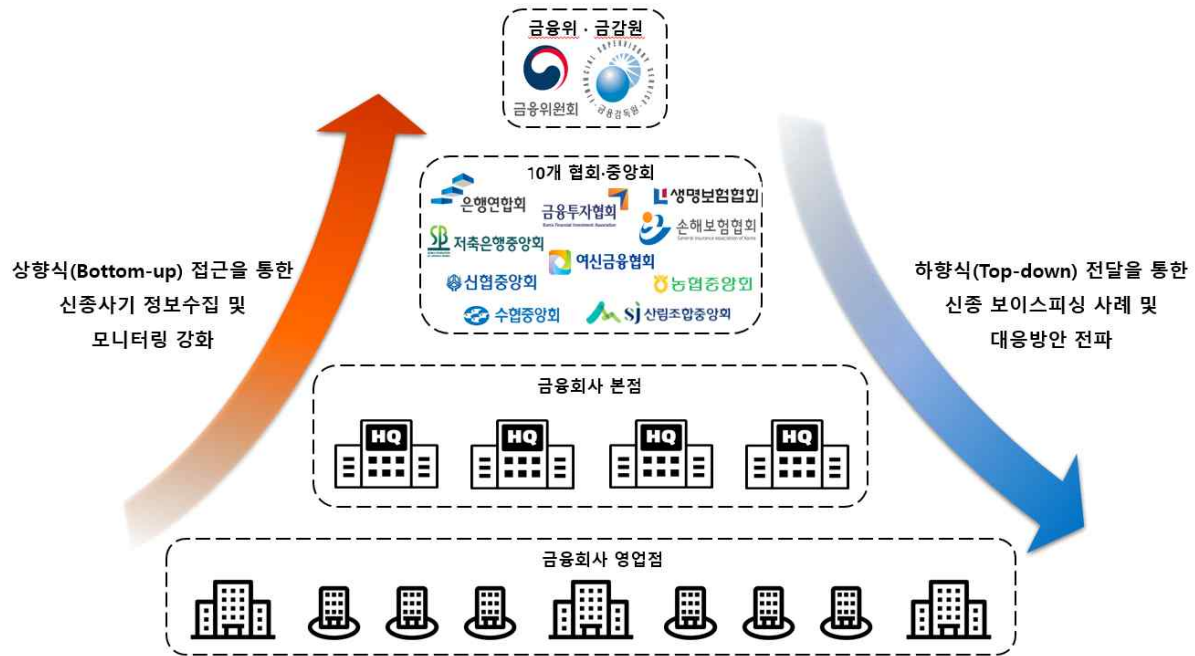
\* 10개 금융업권 소속 금융회사 본점 352개, 영업점 17,934개와 신종 사기수법을 신속히 수집하고 전파하여 적극 대응할 수 있는 체계를 구축('23.5월말 기준)

또한, 금융당국은 협회·중앙회 사이 원활한 양방향 소통이 가능하도록 전담 창구를 지정하는 등 실시간 소통 채널을 가동하여 전 금융권이 신종사기에 합심하여 신속히 대처할 수 있는 기틀을 마련하였다.

특히, 금융당국은 최근 유행 중인 청첩장·돌잔치 가장 보이스피싱을 비롯하여 금융회사 유튜브 및 카카오톡 채널 사칭, 택배회사 혹은 정부 정책을 빙자한 보이스피싱 등 신종 사례에 대하여 꾸준히 소비자정보 발령 등 신속한 대국민 홍보 및 영업점 전파로 소비자 피해 예방에 최선을 다하고 있으며, 앞으로도 신속대응체계를 통해 신종사기 정보수집을 강화하고 사기수법의 내용, 사안의 시급성 및 피해규모 등을 종합적으로 고려하여 유형별로 ①신속전파, ②금융권 공동 대처, ③종합대책 수립으로 신종사기에 대응하여 보이스피싱 근절에 앞장설 예정이다.



< 신속대응체계를 활용한 신종사기 수집·전파 체계도 >



< 신종사기 유형별 대응방안 >

유형	<b>유형 1 : 신속전파</b> ◆ <u>신속한 대국민 홍보</u>	<b>유형 2 : 공동 대처</b> ◆ <u>금융권 공동 대처방안 마련</u>	<b>유형 3 : 종합대책 수립</b> ◆ <u>금융서비스 이용 행태 변화</u>
사안	▶ 피해 건수 아직 미미하고, 기존 수법과 유사	▶ 피해 건수 급증하거나, 기존 방안으로는 대처 곤란	▶ 피해 건수 급증하고, 제도개선 및 금융소비자 행태 변화가 필요
대응방안	▶ 사기수법 및 피해예방 요령 등을 신속히 전파하여 피해 예방에 주력	▶ 공동 대응계획 수립 및 대처방안 금융권 전파하여 피해 확산 방지에 주력	▶ 종합대책을 마련하여 제도개선 및 금융서비스 변화 내용의 충분한 안내로 피해 근절에 주력

◆ 보이스피싱 피해가 발생했거나 발생이 우려되는 경우, 여름 휴가철에도 '본인계좌 일괄지급정지' 서비스를 이용하여 본인 명의로 개설된 모든 계좌를 신속하게 지급정지하여 출금거래를 정지시킬 수 있음을 알려드립니다.

- **(온라인)** 금융결제원 어카운트인포 홈페이지(accountinfo.or.kr) 및 모바일 앱 또는 금융감독원 금융소비자 포털 파인(fine.fss.or.kr)
- **(영업점·고객센터)** 거래 금융회사 영업점 방문 및 고객센터 전화로 모든 계좌 지급정지가 가능하고, 지급정지 해제는 거래 금융회사 영업점 방문을 통해서만 가능



담당 부서	금융위원회 전자금융과	책임자	과 장	김수호 (02-2100-2970)
		담당자	사무관	남명호 (02-2100-2974)
	금융감독원 금융사기전담대응단	책임자	국 장	임정환 (02-3145-8150)
		담당자	팀 장	서강훈 (02-3145-8521)
	은행연합회 소비자보호부	책임자	본부장	지순구 (02-3705-5150)
		담당자	부 장	박혜정 (02-3705-5040)
	금융투자협회 소비자보호부	책임자	상 무	이봉헌 (02-2003-9014)
		담당자	부 장	김동오 (02-2003-9420)
	생명보험협회 소비자보호부	책임자	본부장	최종윤 (02-2262-6614)
		담당자	부 장	김윤창 (02-2262-6643)
	손해보험협회 소비자보호부	책임자	본부장	최종수 (02-3702-8526)
		담당자	부 장	최정수 (02-3702-8670)
	여신금융협회 소비자보호부	책임자	상 무	김민기 (02-2011-0711)
		담당자	부 장	김태훈 (02-2011-0784)
	저축은행중앙회 소비자보호부	책임자	본부장	이경연 (02-397-8617)
		담당자	부 장	양희경 (02-397-8680)
	신협중앙회 금융소비자보호본부	책임자	부문장	추창호 (042-720-1461)
		담당자	본부장	박용남 (042-720-1462)
	농협중앙회 상호금융소비자보호부	책임자	상 무	서국동 (02-2080-4603)
		담당자	부 장	김동석 (02-2080-2200)
	수협중앙회 상호금융본부	책임자	부대표	문진호 (02-2240-2034)
		담당자	본부장	이옥진 (02-2240-2200)
	산림조합중앙회 상호금융수신부	책임자	상 무	김용배 (02-3434-7123)
		담당자	부 장	임성훈 (02-3434-7220)



## 참고1

## 휴가철을 앞두고 예상되는 보이스피싱 사례 및 대처요령

### 1 카드사 콜센터 ARS를 가장한 피싱

- 사기범은 카드사 콜센터 ARS를 가장하여 본인인증 등 명목으로 카드 비밀번호 앞 두 자리 입력을 요구
- 사기범은 탈취한 카드 비밀번호 등을 이용하여 핸드폰을 개통한 후 핸드폰 본인인증을 통한 계좌이체 등의 방법으로 자금을 편취

#### 카드사 콜센터 ARS를 가장한 피싱 사례

- ◆ 사기범은 전화로 OO카드 콜센터 직원을 사칭하면서 본인인증을 위해 필요하다며 ARS 음성 안내멘트를 통해 비밀번호 앞 두 자리 입력을 요구하였고, 피해자가 이를 입력하자 얼마 후 피해자 명의로 핸드폰이 개통되었다는 SMS 문자메시지를 수신, 그 뒤 피해자 명의 은행계좌에서 피해금이 인출

☞ 휴대폰에 개인정보(신분증, 신용카드, 운전면허증, 기타 계약서 등)를 저장하지 마세요!

- 사진첩, 파일폴더, SNS 전송 내역 등에 보관된 개인정보는 원격조정 악성앱을 통해 사기범에게 탈취될 우려가 있습니다.

☞ 또한, 본인이 요청하지 않은 본인인증에는 절대 응하지 마시고,

- 카드 비밀번호 등 민감한 금융정보 요구에는 특별히 신중을 기할 필요가 있습니다!

### 2 해외결제 문자메시지를 빙자한 피싱

- 사기범은 해외결제 승인 문자메시지로 통화를 유도한 후 해외 구매내역 확인을 위해 필요하다며 악성 앱 설치를 유도
- 이후 핸드폰에 설치된 원격조정 앱을 통해 피해자의 개인정보를 탈취한 후 비대면 대출, 계좌이체 등으로 피해금을 편취



### 해외결제 문자메시지를 빙자한 피싱 사례

- ◆ 평소 해외직구를 사용하여 물품을 구매하던 피해자는 사기범이 전송한 해외 구매 승인내역 문자메시지에 기재된 구매내역 확인 링크를 클릭하였고, 이에 피해자 핸드폰에 악성 앱이 설치, 핸드폰에 저장된 신분증 등 개인정보가 유출되어 비대면 대출승인, 계좌이체 등을 통해 재산상 피해를 입음
- ◆ 사기범은 피해자에게 '해외결제 승인 완료'라는 문구가 기재된 문자메시지를 발송하여 전화 통화를 유도하였고 피해자와 통화 시 쇼핑몰 직원을 사칭하여 구매내역 확인 및 명의도용 여부를 확인하기 위해서는 어플리케이션 설치가 필요하다는 핸드폰 원격조정 악성 앱을 피해자 핸드폰에 설치하게 유도한 후 원격조정 앱을 통해 피해자의 계좌에서 자금을 이체

- ☞ 문자메시지에 기재된 콜센터 번호가 정상적인 금융회사 혹은 쇼핑몰 번호인지 인터넷 공식 홈페이지 등을 통해 확인하고,
  - 상담원이 출처가 불분명한 앱 설치 또는 URL 주소 클릭을 유도하는 경우 절대 응하지 마세요!

### 3 가족 납치, 상해 등을 빙자한 금전 요구

- 사기범은 자녀 또는 부모를 납치했다며 가족의 안전을 빌미로 금전을 요구하고 당황한 피해자로부터 피해금을 편취

### 가족납치, 상해 등을 빙자한 금전 요구 사례

- ◆ 사기범은 피해자에게 전화하여 '아들이 지하철에서 칼을 맞고 지하실에 감금되어 있으니 시키는대로 하면 병원에 보내서 치료해주겠다'라며 피해자를 협박하였고, 사기범에게 기망당한 피해자로부터 기프트카드 핀번호 교부 및 계좌이체를 통해 자금을 편취

- ☞ 납치 전화를 받은 경우, 조용히 가족 본인 혹은 지인(친구, 학교, 학원, 경로당 등)에게 연락하여 안전을 확인하고
  - 자금을 송금한 경우, 금융회사 또는 금융감독원 콜센터로 즉시 전화하여 해당 계좌 지급정지를 요청하고 피해구제를 신청하세요!



## 참고2

## 그간 신속대응체계를 통해 수집·전파한 사기수법 사례

### 1 유튜브를 악용한 은행 사칭 피싱

- 유튜브에서 은행직원을 사칭해 금융상품을 홍보하는 것처럼 가장한 후 은행을 사칭한 피싱사이트로 연결시켜 자금을 편취
- 피싱사이트에 예·적금 가입시 필요하다며 연락처, 은행 계좌정보 등 개인정보를 입력하도록 하고 예치금을 가상계좌에 입금토록 유도

#### 유튜브 동영상 썸네일



(실제 사연) 은행원이 폭로합니다.  
남다른 저축으로 더 많은 이자 받...

조회수 7.4만회

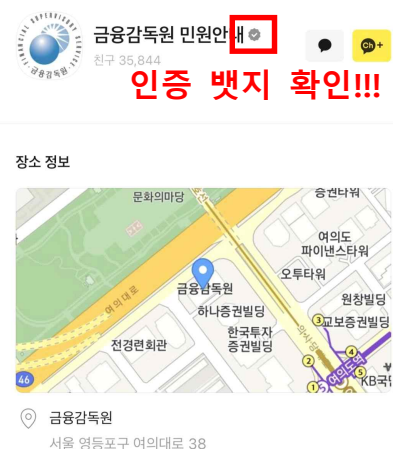
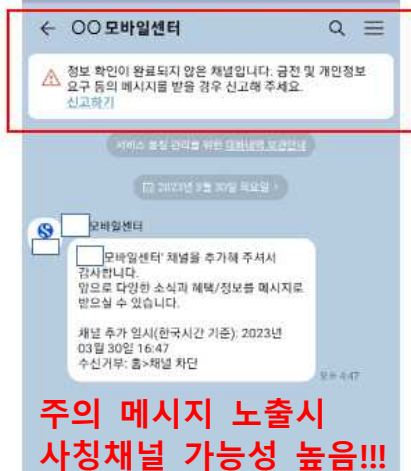
여러분에게 사연을 전달해드리고자 합니다. 실제 은행원이 저축하는 방법에 대한 내용을 폭로하는 영상입니다. 좋은 영상 잘 봐주세요. 중...

### 2 카카오톡 채널을 이용한 은행 사칭 피싱

- 사기범들은 인터넷에서 대출 정보를 검색하는 피해자에게 접근하여 은행 직원임을 사칭하며 카카오톡 상담채널로 유도
- 은행 상담채널을 사칭한 카카오톡 채널\*에서 대출 상담 진행을 위해 필요하다며 피해자의 개인정보를 요구

\* 금융회사로 인증된 채널인 경우 채널명 우측에 인증 뱃지(📌) 여부 확인

#### 카카오톡 인증채널 구분방법





### ③ 택배회사 혹은 정부정책을 사칭한 피싱

- 택배회사를 사칭하여 주소 또는 송장번호 불일치 등의 내용으로 문자메세지를 발송하고,
  - 문자 내 인터넷 주소(URL)를 클릭할 경우, 피싱사이트 연결 또는 악성앱 설치로 개인정보를 탈취한 후 자금을 편취
- 질병관리청 직원을 사칭하여 방역지원금 등을 사유로 개인정보를 요구하고 자금을 편취
  - 정부기관을 사칭하며 일반 국민에게 생활안정자금, 근로장려금 등의 지원을 핑계로 개인정보를 요구

### ④ 청첩장 또는 돌잔치를 빙자한 피싱

- 사기범은 결혼식(혹은 돌잔치)에 초대한다며 모바일 청첩장 링크가 포함된 가짜 문자메시지를 피해자에게 발송
  - 피해자가 해당 문자메시지에 기재된 URL주소를 클릭하자 휴대폰에 악성앱이 설치되었고, 사기범은 악성앱을 통해 탈취한 개인정보를 이용하여 피해자 명의로 비대면 대출을 받는 등 자금을 편취

