

소비자경보

가족·친구 등 지인 사칭 메신저피싱 및 정부지원 대출·채무조정 빙자 보이스피싱 주의하세요

소비자경보 2022-13호

등급 **주의** 경고 위험

대상 금융소비자 일반

최근 가족·친구 등 지인을 사칭하는 메신저피싱을 통한 피해 증가
사기범은 자녀, 친구 등을 사칭하며 문자로 접근하여
개인정보를 작·간접적으로 탈취하고 자금을 편취

아울러, 사기범이 탈취한 개인정보를 이용하여
오픈뱅킹서비스 신청 후 타 금융사 계좌 잔액을 모두 편취하는
사기피해도 발생

한편, **소상공인 저금리 대환대출, 새출발기금** 등
정부지원 대출·채무조정을 빙자하며 악성 URL주소 접속 및
회신 전화를 유도하는 보이스피싱 피해 발생 우려

➡ 금융소비자의 각별한 주의 필요

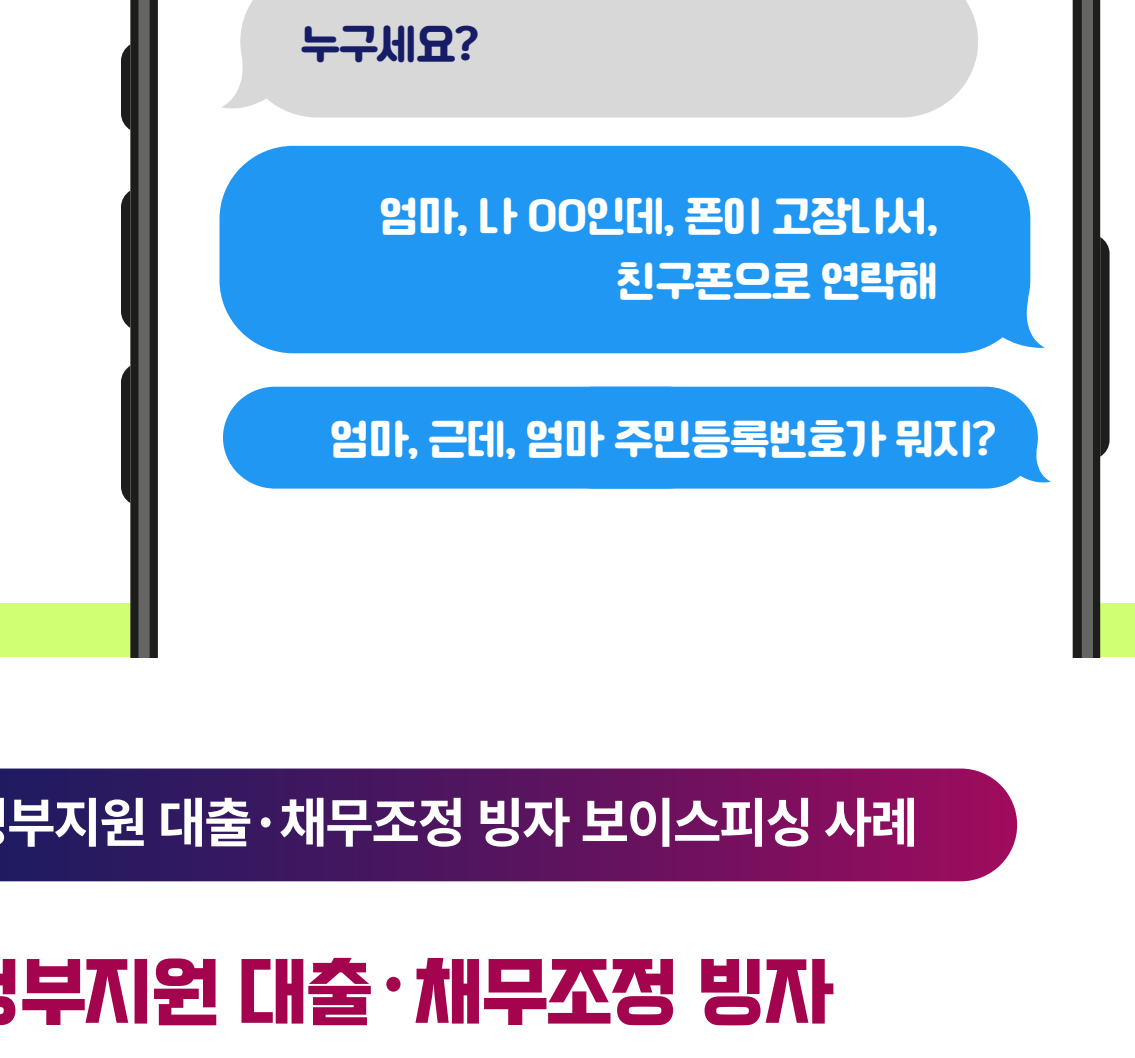
가족·친구 등 지인 사칭 메신저 피싱 사례

가족·친구 등 지인 사칭 메신저피싱이란?

사기범이 문자메시지, SNS 등으로 가족·친구 등을 사칭하며
긴급한 사정을 이유로 피해자에게 개인정보 제공 및 자금 이체를
요구하는 보이스피싱의 일종입니다



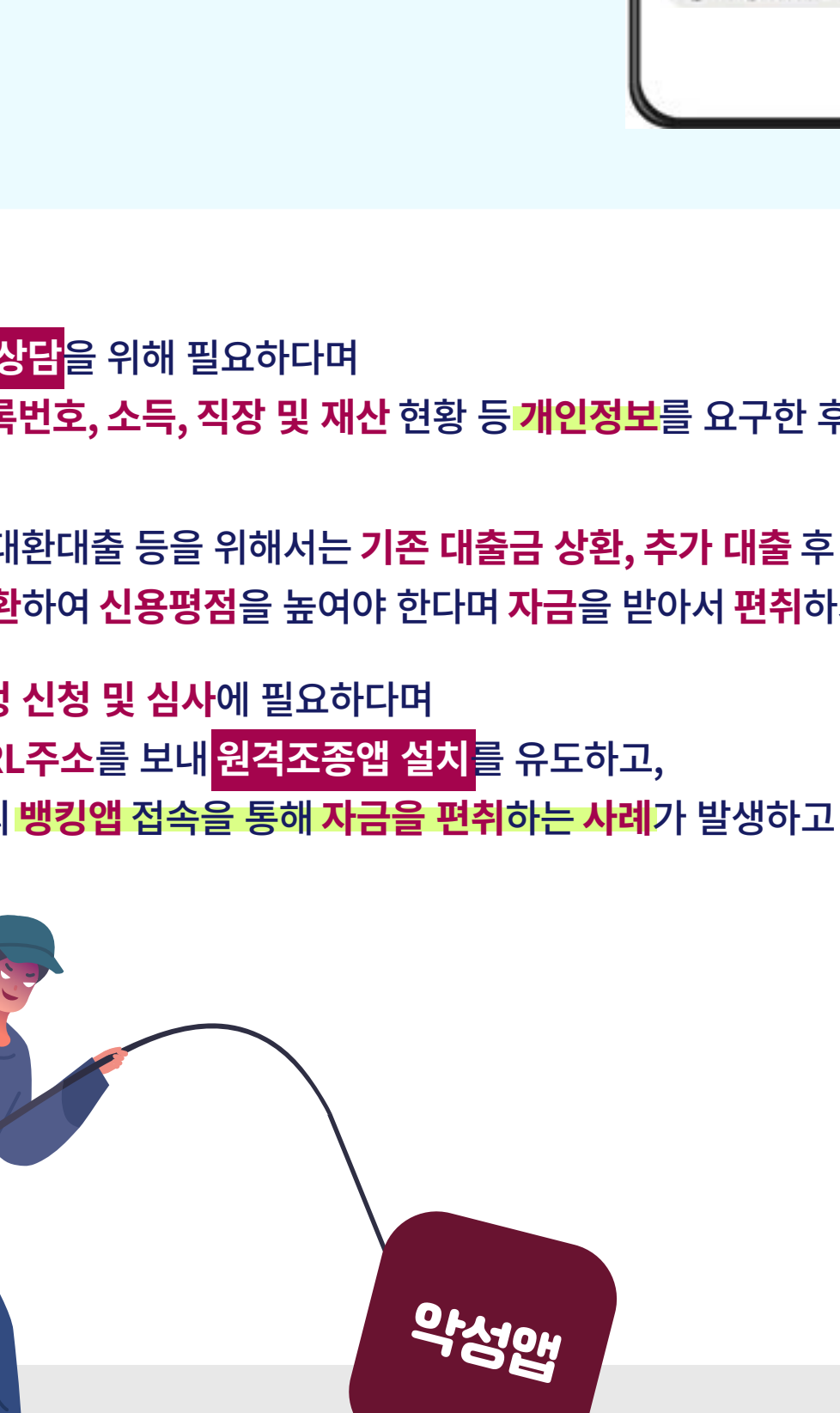
또한, 피해자에게 악성앱을 설치하도록 유도하여
사기범이 휴대폰 원격조종을 통해 직접 개인정보 탈취 및
자금 편취를 하는 사례도 발생하고 있습니다.



사례

사기범은 문자메시지로

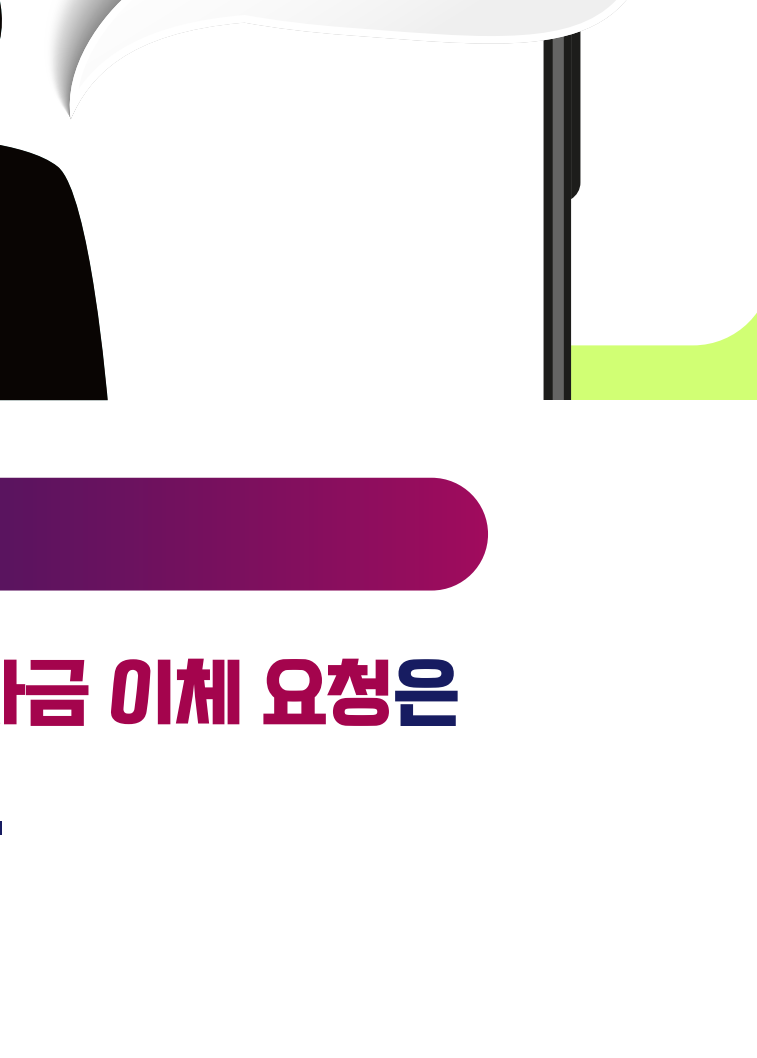
“엄마 나 발인데 폰 고장 나서 친구폰으로 연락해”라며
피해자에게 개인정보를 요구하여 자금을 편취



정부지원 대출·채무조정 빙자 보이스피싱 사례

정부지원 대출·채무조정 빙자 보이스피싱이란?

주로 문자메시지 등을 이용하여
정부지원 대출(소상공인 저금리 대환대출 등),
채무조정(새출발기금 등) 신청 대상이라며
소비자를 유혹하는 보이스피싱의 일종입니다.

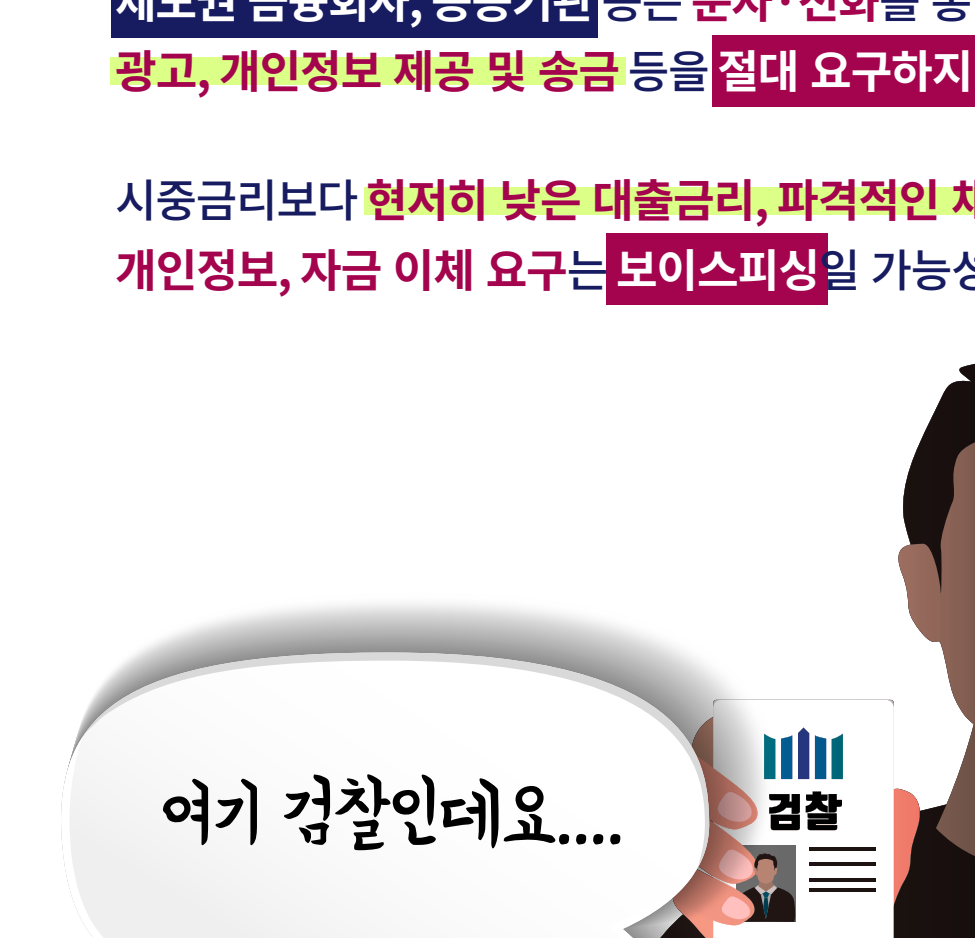


정확한 상담을 위해 필요하며
주민등록번호, 소득, 직장 및 재산 현황 등 개인정보를 요구한 후,

저금리 대환대출 등을 위해서는 기존 대출금 상환, 추가 대출 후
즉시 상환하여 신용평점을 높여야 한다며 자금을 받아서 편취하거나,

채무조정 신청 및 심사에 필요하며
악성 URL주소를 보내 원격조종 앱 설치를 유도하고,

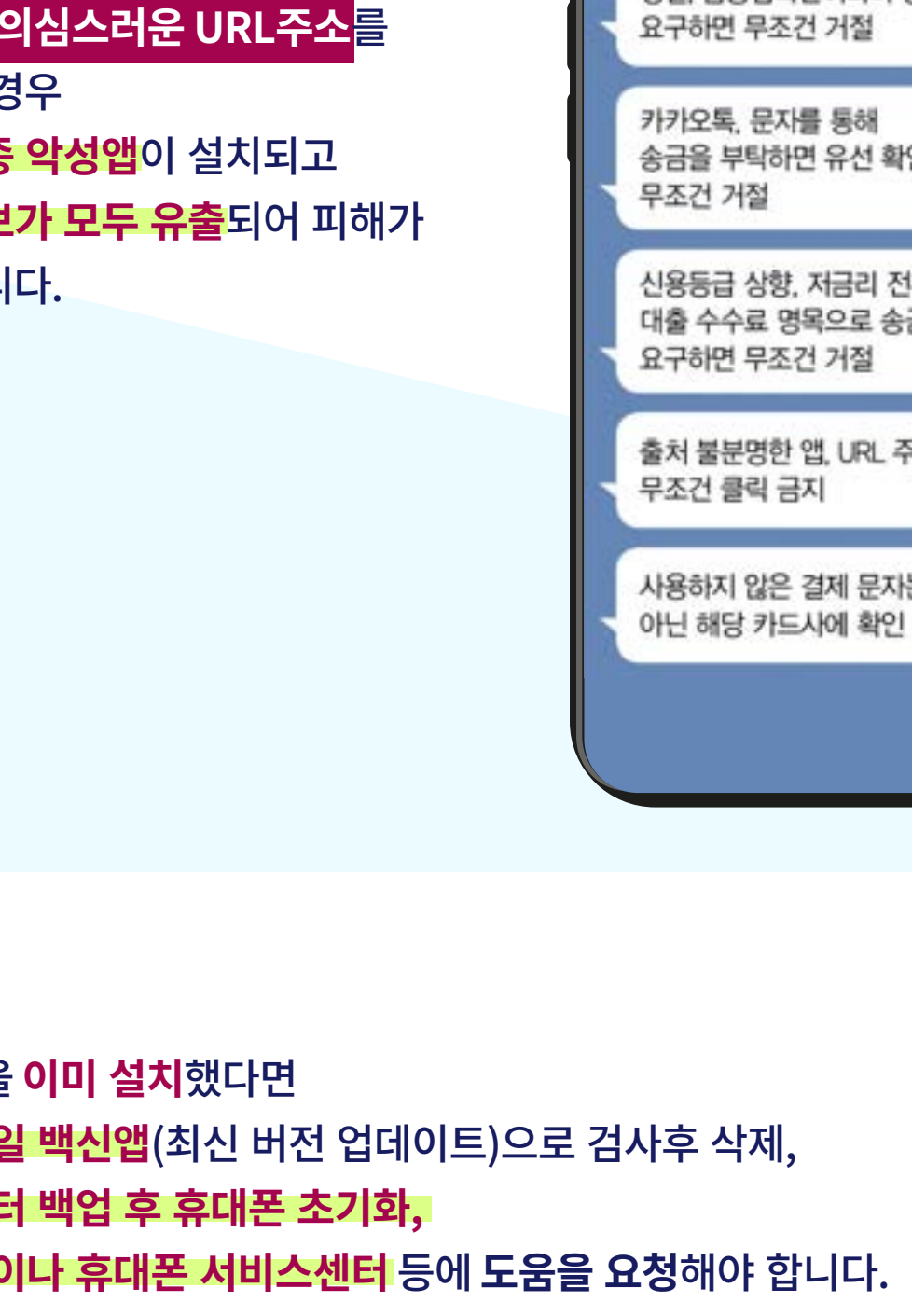
피해자의 뱅킹앱 접속을 통해 자금을 편취하는 사례가 발생하고 있습니다.



사례

사기범은 OO관리공사를 사칭하며

“새출발기금 신청 대상자 안내”라는 문자메시지를 통해
개인정보 및 심사 비용 선납을 요구

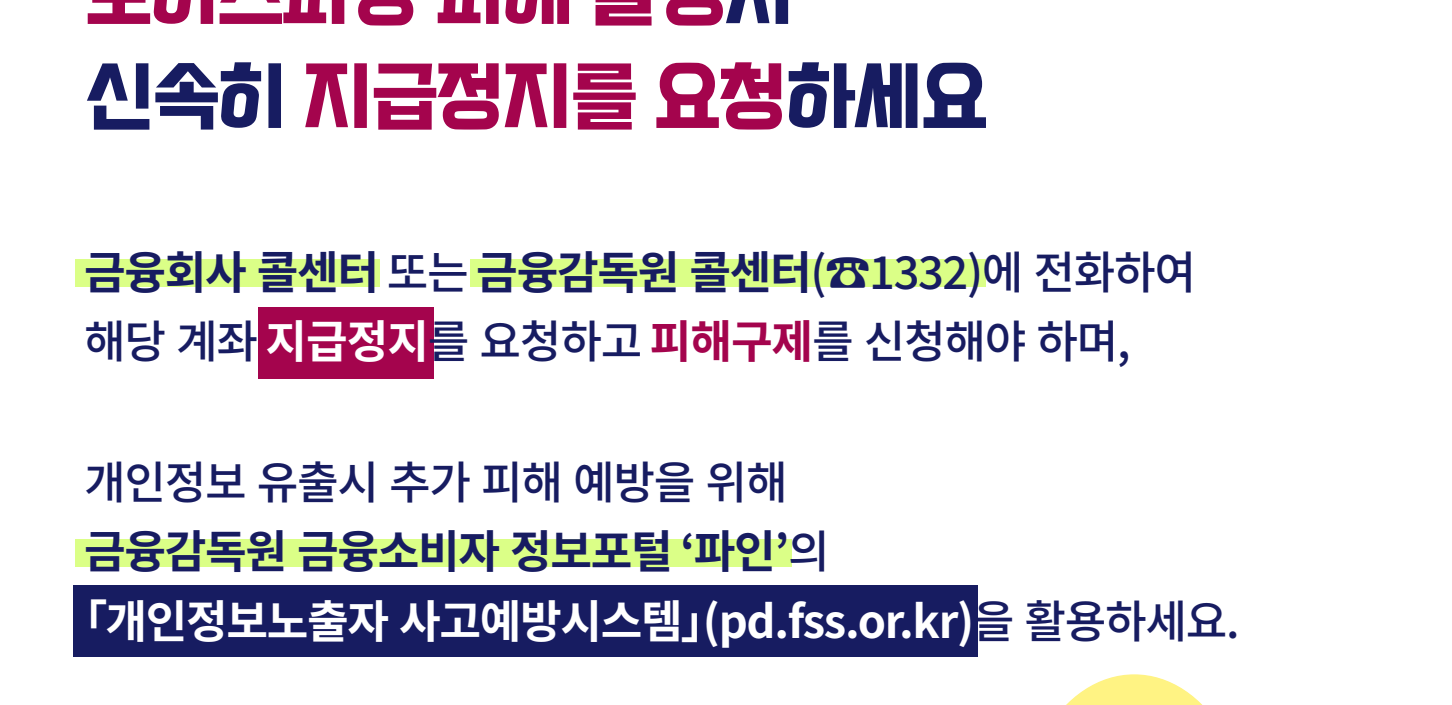


소비자 행동 요령

개인정보 제공 및 자금 이체 요청은 무조건 거절하세요.

메신저피싱

가족·지인이더라도 개인정보, 금전 등을 요구하면 우선 거절하고,
지인 연락처로 직접 전화하여 본인 여부를 확인 후 대응하세요.



정부지원 대출·채무조정 빙자

제도권 금융회사, 공공기관 등은 문자·전화를 통한
광고, 개인정보 제공 및 송금 등을 절대 요구하지 않음을 유념하세요.

시중금리보다 현저히 낮은 대출금리, 파격적인 채무조정 등을 빙자한
개인정보, 자금 이체 요구는 보이스피싱일 가능성이 높습니다.



소비자 행동 요령

출처가 불분명한 URL주소는 절대 클릭하지 마세요.

사기범이 보낸
출처가 의심스러운 URL주소를
클릭할 경우
원격조종 악성앱이 설치되고
개인정보가 모두 유출되어 피해가
발생합니다.



악성앱을 이미 설치했다면

- ① 모바일 백신 앱 (최신 버전 업데이트)으로 검사후 삭제,
- ② 데이터 백업 후 휴대폰 초기화,
- ③ 지인이나 휴대폰 서비스센터 등에 도움을 요청해야 합니다.

악성앱을 설치했다면 꼭 확인하세요!

소비자 행동 요령

보이스피싱 피해 발생시 신속히 지급정지를 요청하세요

금융회사 콜센터 또는 금융감독원 콜센터(☎1332)에 전화하여
해당 계좌 지급정지를 요청하고 피해구제를 신청해야 하며,

개인정보 유출시 추가 피해 예방을 위해
금융감독원 금융소비자 정보포털 '파인'의
「개인정보노출자 사고예방시스템」(pd.fss.or.kr)를 활용하세요.

또한, 「계좌정보 통합관리서비스(www.payinfo.or.kr)」를 활용하여
본인 모르게 개설된 계좌 또는 대출을 한눈에 확인할 수 있고,

본인 모르게 개통된 휴대폰을 조회하거나 추가 개통을 차단하기 위해서는
「명의도용 방지서비스(www.msafar.or.kr)」의
가입사실 현황조회 또는 가입제한 서비스 등을 이용할 수 있습니다.

