

국민 금융생활 안전 교육자료 · EDU-01

금융사기·명의도용·디지털 안전

송금·앱 설치·인증정보 요구 앞에서 멈추고, 피해가 생기면 바로 행동합니다.

큰글자 학습본

본문 10.5pt 이상 · 내용 기준 2026-08-24 · NEXUS FMI 국민 금융생활 안전 교육

큰글자 핵심학습본

이 자료는 교육 목적의 일반 정보입니다. 긴급한 피해가 생겼다면 자료를 읽는 것보다 112와 금융회사에 먼저 연락하세요. 기관의 서비스와 절차는 바뀔 수 있으므로 이용 직전에 공식 안내를 다시 확인하세요.

왜 배우나요?

사기는 금융지식의 많고 적음보다 판단할 시간을 빼앗는 문제입니다

이 과제를 네 문장으로 먼저 이해하기

- 금융사기는 믿게 만든 뒤 서두르게 하여 돈이나 금융거래 권한을 빼앗는 범죄입니다.
- 전화번호·기관 이름·화면이 진짜처럼 보여도 통화를 끊고 공식 대표번호로 다시 확인합니다.
- 비밀번호·인증번호·원격제어앱·안전계좌 송금 요구는 즉시 멈춰야 할 위험 신호입니다.
- 돈이나 정보가 넘어갔다면 혼자 해결하려 하지 말고 금융회사·112 등 공식 창구에 즉시 알립니다.

생활 변화와 새 위험

AI 음성·영상도 본인 확인을 대신하지 못합니다

가족이나 기관의 목소리·얼굴처럼 보여도 합성되거나 계정이 탈취되었을 수 있습니다.

- 하지 않을 것: 영상통화가 연결됐다는 이유만으로 송금하거나 인증번호를 알려 주지 않습니다.
- 확인할 것: 통화를 끊고 내가 저장해 둔 번호로 다시 걸어 사실을 확인하며, 가족과 미리 정한 질문이나 암호어를 사용합니다.
- 지금 할 일: 송금했다면 즉시 금융회사와 112에 지급정지를 요청하고, 악성 앱·스미싱은 안전한 다른 기기로 118에 상담합니다.

속았다는 자책보다 신고 속도가 중요합니다

사기범은 두려움·신뢰·시간압박을 이용합니다. 피해 사실을 숨기면 지급정지와 증거보존이 늦어질 수 있습니다.

- 하지 않을 것: 혼자 만회하려고 추가 송금하거나 사기범과 협상하지 않습니다.
- 확인할 것: 송금시각·계좌·전화번호·대화 원본을 그대로 남기고, 이미 한 조치와 남은 위험을 구분합니다.
- 지금 할 일: 안전한 기기에서 금융회사·112·1394·118의 공식 경로로 바로 알립니다.

먼저 알아둘 필수개념

사칭

다른 사람이나 기관인 것처럼 꾸미는 행동입니다.

- 생활 예: 경찰·금융회사 이름과 로고를 보여 주며 안전계좌로 송금하라고 합니다.
- 확인: 발신번호가 공식 번호와 같으면 믿어도 되나요? 아닙니다. 번호는 조작될 수 있으므로 전화를 끊고 공식 번호로 다시 연락합니다.

인증정보

비밀번호·인증번호·보안카드처럼 거래 권한을 확인하는 정보입니다.

- 생활 예: 인증번호를 입력하면 송금이나 계정 변경이 승인될 수 있습니다.
- 확인: 금융회사 직원이 전화로 인증번호를 요구하면 알려 줘도 되나요? 아닙니다. 통화를 끊고 공식 금융회사에 직접 확인합니다.

원격제어

다른 사람이 내 기기 화면을 보고 조작할 수 있게 하는 기능입니다.

- 생활 예: 상담을 이유로 앱을 설치하면 상대가 문자와 금융앱 화면을 볼 수 있습니다.

- 확인: 원격제어 앱을 설치한 기기로 계속 금융거래해도 되나요? 안 됩니다. 다른 안전한 기기로 금융회사와 118에 연락합니다.

지급정지

피해금이 더 이동하지 않도록 거래를 긴급히 멈춰 달라고 요청하는 조치입니다.

- 생활 예: 송금 피해를 알게 되면 112나 금융회사에 즉시 연락합니다.
- 확인: 신고서를 모두 작성한 뒤 지급정지를 요청해야 하나요? 아닙니다. 송금 피해를 알게 되면 우선 긴급 연락부터 합니다.

명의도용

다른 사람이 내 신분정보로 계좌·휴대전화·대출 등을 만드는 행위입니다.

- 생활 예: 유출된 신분증 사진으로 비대면 계정 개설을 시도합니다.
- 확인: 돈이 빠지지 않았으면 명의도용 확인은 필요 없나요? 필요합니다. 신규 계좌·대출·통신 개통 여부를 확인해야 합니다.

기초학습 1 · 금융사기는 어떻게 판단을 흔드는가

왜 알고도 속을 수 있을까요?

금융사기는 지식이 없는 사람만 당하는 일이 아닙니다. 범인은 기관이나 가족을 사칭하고, 손실·처벌·기회를 강조해 생각할 시간을 줄입니다.

따라서 말의 그럴듯함보다 '지금 즉시 행동하라', '다른 사람에게 말하지 말라', '새 앱을 설치하라' 같은 압박 방식을 먼저 살펴야 합니다.

- 상대가 누구라고 주장하는지 적습니다.
- 지금 요구하는 돈·정보·설치를 구분합니다.
- 통화를 끊고 내가 직접 찾은 공식 경로로 다시 확인합니다.
- 생활 예: 검찰을 사칭한 사람이 '계좌가 범죄에 연루됐으니 안전계좌로 옮기라'고 합니다. 진짜 수사기관인지 논쟁하지 않고 송금을 멈춘 뒤 112에 확인하는 것이 먼저입니다.

- 흔한 오해: 전화번호나 기관 로고가 같으면 진짜라는 생각은 위험합니다. 발신번호와 화면은 조작될 수 있습니다.

확인: 상대가 내 이름과 일부 개인정보를 알고 있으면 믿어도 될까요? 아닙니다. 유출된 정보일 수 있으므로 대화를 끝내고 공식 대표번호로 다시 확인해야 합니다.

기초학습 2 · 인증정보는 왜 돈과 같은가

인증번호 하나가 왜 위험할까요?

비밀번호·인증번호·보안카드·신분증 사본은 단순한 정보가 아니라 거래 권한을 확인하는 수단입니다.

범인이 이 정보를 얻으면 송금뿐 아니라 계정 변경, 비대면 대출, 새 계좌 개설 등 여러 행동을 시도할 수 있습니다.

- 비밀번호와 인증번호는 누구에게도 전달하지 않습니다.
- 신분증 사본에는 용도와 제출처를 표시합니다.
- 의심 시 다른 안전한 기기로 금융회사에 연락해 계정과 거래를 점검합니다.
- 생활 예: 택배 환급을 받으려면 인증번호가 필요하다는 문자를 받았습니다. 환급을 위해 금융거래 인증번호를 요구하는 것 자체를 위험 신호로 봅니다.
- 흔한 오해: 적은 금액이나 잠깐의 인증이라 괜찮다는 생각은 틀립니다. 권한이 넘어가면 피해 범위가 커질 수 있습니다.

확인: 은행 직원이라고 밝힌 사람이 전화로 인증번호를 묻는다면 어떻게 하나요? 말해 주지 않고 통화를 끝낸 뒤 은행 앱이나 공식 대표번호로 직접 확인합니다.

기초학습 3 · 원격제어와 악성앱의 위험

앱 하나를 설치하면 무엇이 달라질까요?

원격제어앱은 다른 사람이 내 화면을 보고 조작하게 할 수 있습니다. 악성앱은 전화 연결을 가로채거나 문자와 금융정보를 훔칠 수 있습니다.

설치 뒤에는 같은 휴대전화로 기관에 전화해도 범인에게 연결될 가능성이 있으므로 다른 안전한 기기를 사용해야 합니다.

- 출처가 불분명한 링크와 앱 설치를 멈춥니다.
- 이미 설치했다면 네트워크와 금융거래를 차단합니다.
- 다른 기기로 금융회사·112·118에 연락하고 안내에 따라 점검합니다.
- 생활 예: 대출상담원이 신용점수 확인 앱을 설치하라고 합니다. 앱을 설치하지 않고 해당 금융회사의 공식 앱과 대표번호에서 상품과 직원을 확인합니다.
- 흔한 오해: 앱을 삭제하면 모든 위험이 사라진다고 단정하면 안 됩니다. 계정·거래·기기 점검이 함께 필요합니다.

확인: 의심 앱을 설치한 휴대전화로 계속 인터넷뱅킹을 해도 될까요? 안 됩니다. 금융거래를 멈추고 다른 안전한 기기로 금융회사와 전문기관에 연락해야 합니다.

기초학습 4 · 피해 직후의 우선순위

피해가 생기면 무엇부터 해야 할까요?

피해 직후에는 범인을 설득하거나 돈을 더 보내 회수하려 하지 않습니다. 추가 손실을 막는 조치가 가장 먼저입니다.

지급정지는 회수를 보장하는 절차가 아니지만 피해금이 더 이동하는 것을 막을 가능성을 지킴으로 즉시 요청해야 합니다.

- 금융회사와 112에 즉시 알립니다.
- 계정·카드·기기의 추가 사용을 차단합니다.
- 문자·전화번호·계좌·송금시각 등 원본 기록을 보존합니다.
- 생활 예: 이미 50만 원을 보낸 뒤 추가 수수료를 요구받았습니다. 추가 송금을 멈추고 금융회사에 지급정지 가능성을 묻고 112에 신고합니다.
- 흔한 오해: 증거를 완벽히 정리한 뒤 신고하겠다는 생각 때문에 시간을 보내면 안 됩니다. 먼저 긴급 연락하고 기록은 이어서 보완합니다.

확인: 신고서 작성을 끝내야 지급정지를 요청할 수 있나요? 아닙니다. 피해 송금 사실을 알게 된 즉시 금융회사와 112에 먼저 연락합니다.

PART 1 · EDU-01

학습 목표

- 사칭·피싱·스미싱·투자유인·명의도용의 공통 신호를 구별합니다.
- 송금·앱 설치·화면공유·인증정보 요구 앞에서 4단계 행동 절차를 적용합니다.
- 피해 직후 지급정지·신고·계정차단·증거보존 순서를 실행합니다.
- 본인과 가족 계정의 예방 설정과 공식 연락경로를 점검합니다.

PART 2 · EDU-01

금융사기 공통 흐름

- 접촉: 전화·문자·SNS·광고·지인 계정으로 접근합니다.
- 신뢰: 기관명·로고·가족 사진·전문가 수익 인증을 보여 줍니다.
- 고립: 통화를 유지하고 가족·직원·금융회사에 말하지 말라고 합니다.
- 압박: 체포·손실·마감·기회를 내세워 시간을 줄입니다.
- 이전: 돈·정보·통장·카드·기기 권한을 넘기게 합니다.

PART 3 · EDU-01

금융사기 4단계 행동

- 멈춤: 송금·링크·앱 설치·화면공유·인증정보 제공을 중단합니다.
- 따로 확인: 상대가 준 번호와 링크를 버리고 저장된 번호·공식 누리집·직접 방문으로 다시 시작합니다.
- 경로 차단: 통화·채팅·원격 연결을 끊고 계정과 번호를 차단·신고합니다.

- 즉시 신고: 송금 피해는 112·금융회사, 피싱 상담은 1394, 악성 앱·스미싱은 118에 연락합니다.

PART 4 · EDU-01

피해 직후 행동

- 지금-10분: 돈과 연결을 먼저 멈춥니다
- 10-30분: 안전한 기기에서 계정과 신원을 보호합니다
- 오늘 안에: 연결된 피해와 증거를 확인합니다
- 1-7일: 후속 절차와 재발 방지를 이어갑니다
- 30일 안에: 생활 속 안전장치를 다시 설계합니다

PART 5 · EDU-01

공식 근거로 확인한 사실

확정 사실 · 보이스피싱 의심 상담·신고·제보 통합번호 1394는 2026년부터 365일 24시간 운영된다.

확인할 조건: 범죄가 진행 중이거나 돈을 보냈다면 112와 금융회사 지급정지를 함께 우선한다.

출처: 경찰청 · https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1007&q_bbscttSn=20260209152732394

조건 확인 · 지급정지는 추가 인출을 막기 위한 긴급조치이며 전액 환급을 자동으로 보장하지 않는다.

확인할 조건: 지급정지·피해구제 대상과 회수 결과는 송금수단·잔액·신고시점 등에 따라 달라진다.

출처: 금융위원회·금융감독원 · <https://www.fsc.go.kr/po010101/86250>

안전 원칙 · 악성 앱이 의심되면 같은 휴대전화로 금융거래와 신고를 계속하지 않고 안전한 다른 기기를 이용한다.

확인할 조건: 기기 초기화나 앱 삭제 전에 신고기관의 안내에 따라 증거 보존과 계정 보호를 함께 진행한다.

출처: 한국인터넷진흥원 보호나라 · <https://www.boho.or.kr>

오늘 할 일

- ☐ 돈이나 개인정보를 요구하는 연락은 누구의 목소리·얼굴이어도 일단 끊습니다.
- ☐ 가족의 저장된 번호와 두 번째 연락대상을 정해 두 경로로 확인합니다.
- ☐ 확인 질문이나 암호호는 보조 수단으로만 쓰고 메신저에 남기지 않습니다.
- ☐ 피해가 의심되면 혼내거나 숨기게 하지 않고 지급정지와 신고를 먼저 돕습니다.
- ☐ 한 사람이 연락을 받으면 다른 사람이 금융회사·112·1394·118 중 필요한 곳에 연락합니다.