

국민 금융생활 안전 교육자료 · EDU-01

금융사기·명의도용·디지털 안전

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

학습자용 교재

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

이 교재를 사용하는 법

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.

내 상황에 맞는 읽기 순서

1. 급한 피해가 있으면 7부부터 봅니다

돈을 보냈거나 앱을 설치했거나 인증정보를 알려주었다면 처음부터 읽지 않아도 됩니다. 7부의 상황별 연락처와 6부의 피해 직후 행동을 먼저 실행합니다.

2. 평소 대비라면 1부부터 차례로 읽습니다

자가진단으로 시작해 공통 구조와 4단계 행동을 익힌 뒤 다섯 사례에서 판단을 연습합니다. 읽으면서 활동지에 우리 집의 확인 규칙과 연락처를 적습니다.

3. 모르는 말은 뜻을 확인하고 행동으로 바꿉니다

용어를 외우는 것이 목적이 아닙니다. 그 말이 나왔을 때 무엇을 멈추고 어디에서 다시 확인할지를 함께 기억합니다.

4. 인쇄본은 기준일을 확인합니다

전화번호와 서비스 범위는 바뀔 수 있습니다. 인쇄본의 내용 기준일을 확인하고 실제 신청·신고 직전에는 HTML 원문과 공식기관 안내를 다시 확인합니다.

배운 뒤 할 수 있는 일

- ☐ 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.

학습 전 필수 기초

왜 이것을 배워야 하나요?

사기는 금융지식의 많고 적음보다 판단할 시간을 빼앗는 문제입니다

사기범은 기관·가족·직원을 흉내 내고 지금 행동하지 않으면 큰일 난다고 재촉합니다. 이때 송금, 앱 설치, 화면 공유, 인증정보 제공 중 하나만 해도 돈과 명의가 함께 위험해질 수 있습니다.

먼저 ‘상대가 누구인지 확인하는 법’과 ‘내가 넘기면 안 되는 권한’을 이해해야 사례 속 위험신호와 피해 직후 행동이 왜 필요한지 알 수 있습니다.

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.

이 학습이 지키는 것

- 계좌 잔액
- 휴대전화와 계정
- 내 이름으로 생기는 대출·통신
- 가족과 지인의 정보
- 신고와 지급정지에 쓸 시간

생활안전으로 이어지는 네 단계

순서	무엇을 하는가
1	사칭 연락이 신뢰와 두려움을 만듭니다.
2	송금·앱·화면공유·인증정보를 요구합니다.
3	돈 또는 기기·계정 통제권이 넘어갑니다.
4	멈추고 따로 확인한 뒤 경로를 차단하고 즉시 신고합니다.

먼저 알아둘 필수개념

뜻만 외우지 않고 생활 예와 반대 예를 대조한 뒤 다른 개념과의 관계를 확인합니다.

기초개념 1 · 사칭

다른 사람이나 기관인 것처럼 꾸미는 행동입니다.

생활 예	해당하지 않는 예
경찰·금융회사 이름과 로고를 보여 주며 안전계좌로 송금하라고 합니다.	공식 기관이 대표번호로 일반 안내를 하는 모든 경우를 사기라고 단정하는 것입니다.

개념 연결: 사칭 여부는 이름·번호가 아니라 내가 직접 찾은 공식 경로로 다시 확인합니다.

확인해 봅니다

발신번호가 공식 번호와 같으면 믿어도 되나요?

답과 이유: 아닙니다. 번호는 조작될 수 있으므로 전화를 끊고 공식 번호로 다시 연락합니다.

기초개념 2 · 인증정보

비밀번호·인증번호·보안카드처럼 거래 권한을 확인하는 정보입니다.

생활 예	해당하지 않는 예
인증번호를 입력하면 송금이나 계정 변경이 승인될 수 있습니다.	돈이 아니므로 인증번호는 알려 줘도 된다고 생각하는 것입니다.

개념 연결: 인증정보는 명의와 거래 권한을 연결하므로 현금처럼 보호합니다.

확인해 봅니다

금융회사 직원이 전화로 인증번호를 요구하면 알려 줘도 되나요?

답과 이유: 안 됩니다. 통화를 끊고 공식 금융회사에 직접 확인합니다.

기초개념 3 · 원격제어

다른 사람이 내 기기 화면을 보고 조작할 수 있게 하는 기능입니다.

생활 예	해당하지 않는 예
상담을 이유로 앱을 설치하면 상대가 문자와 금융 앱 화면을 볼 수 있습니다.	통화만 연결된 상태도 모두 원격제어라고 부르는 것입니다.

개념 연결: 원격제어와 화면공유는 인증정보·메시지·금융거래를 한꺼번에 노출할 수 있습니다.

확인해 봅니다

원격제어 앱을 설치한 기기로 계속 금융거래해도 되나요?

답과 이유: 안 됩니다. 다른 안전한 기기로 금융회사와 118에 연락합니다.

기초개념 4 · 지급정지

피해금이 더 이동하지 않도록 거래를 긴급히 멈춰 달라고 요청하는 조치입니다.

생활 예	해당하지 않는 예
송금 피해를 알게 되면 112나 금융회사에 즉시 연락합니다.	지급정지를 요청하면 전액이 반드시 돌아온다고 생각하는 것입니다.

개념 연결: 지급정지는 피해 회복을 보장하지 않지만 남은 피해금을 막기 위한 시간 싸움입니다.

확인해 봅니다

신고서를 모두 작성한 뒤 지급정지를 요청해야 하나요?

답과 이유: 아닙니다. 송금 피해를 알게 되면 우선 긴급 연락부터 합니다.

기초개념 5 · 명의도용

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

생활 예	해당하지 않는 예
유출된 신분증 사진으로 비대면 계정 개설을 시도합니다.	내 계좌에서 돈이 빠져나간 경우만 명의도용이라고 보는 것입니다.

개념 연결: 명의도용은 금융거래뿐 아니라 통신·계정·신분증 재발급 점검이 필요합니다.

확인해 봅니다

돈이 빠지지 않았으면 명의도용 확인은 필요 없나요?

답과 이유: 필요합니다. 신규 계좌·대출·통신 개통 여부를 확인해야 합니다.

개념이 실제로 작동하는 과정을 배웁니다

용어를 외우는 데서 멈추지 않고, 왜 필요한지와 실제 판단 순서를 생활 사례로 익힙니다.

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.

이 순서로 생각합니다

- 1. 상대가 누구라고 주장하는지 적습니다.
- 2. 지금 요구하는 돈·정보·설치를 구분합니다.
- 3. 통화를 끊고 내가 직접 찾은 공식 경로로 다시 확인합니다.

생활 속에서 보면: 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.

다음으로 넘어가기 전 확인

상대가 내 이름과 일부 개인정보를 알고 있으면 믿어도 될까요?

답과 이유: 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.

이 순서로 생각합니다

- 1. 비밀번호와 인증번호는 누구에게도 전달하지 않습니다.
- 2. 신분증 사본에는 용도와 제출처를 표시합니다.
- 3. 의심 시 다른 안전한 기기로 금융회사에 연락해 계정과 거래를 점검합니다.

생활 속에서 보면: 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.

다음으로 넘어가기 전 확인

은행 직원이라고 밝힌 사람이 전화로 인증번호를 묻는다면 어떻게 하나요?

답과 이유: 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.

이 순서로 생각합니다

- 1. 출처가 불분명한 링크와 앱 설치를 멈춥니다.
- 2. 이미 설치했다면 네트워크와 금융거래를 차단합니다.
- 3. 다른 기기로 금융회사·112·118에 연락하고 안내에 따라 점검합니다.

생활 속에서 보면: 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.

다음으로 넘어가기 전 확인

의심 앱을 설치한 휴대전화로 계속 인터넷뱅킹을 해도 될까요?

답과 이유: 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 지키므로 즉시 요청해야 합니다.

이 순서로 생각합니다

- 1. 금융회사와 112에 즉시 알립니다.
- 2. 계정·카드·기기의 추가 사용을 차단합니다.
- 3. 문자·전화번호·계좌·송금시각 등 원본 기록을 보존합니다.

생활 속에서 보면: 이미 50만원을 보낸 뒤 추가 수수료를 요구받았습니다. 추가 송금을 멈추고 금융 회사에 지급정지 가능성을 묻고 112에 신고합니다.

흔한 오해: 증거를 완벽히 정리한 뒤 신고하겠다는 생각 때문에 시간을 보내면 안 됩니다. 먼저 긴급 연락하고 기록은 이어서 보완합니다.

다음으로 넘어가기 전 확인

신고서 작성을 끝내야 지급정지를 요청할 수 있나요?

답과 이유: 아닙니다. 피해 송금 사실을 알게 된 즉시 금융회사와 112에 먼저 연락합니다.

교재가 먼저 보여 주는 시범풀이

검찰을 사칭한 전화

수사에 연루됐다며 통화를 끊지 말고 안전계좌로 돈을 옮기라고 합니다.

1. 결정: 송금하지 않고 통화를 끝냅니다.
2. 정보: 발신번호가 아니라 검찰·경찰의 공식 대표경로를 찾습니다.
3. 위험: 비밀 유지와 즉시 송금 요구는 별도 확인을 막습니다.
4. 행동: 다른 안전한 전화로 112 또는 공식 기관에 확인합니다.
5. 기록: 번호·시간·메시지를 보존하되 링크와 파일은 열지 않습니다.

권위를 믿는 것이 아니라 연락을 끊고 내가 찾은 경로에서 다시 시작하는 것이 핵심입니다.

기초 이해확인

1. 발신번호가 공식 번호와 같으면 믿어도 되나요?

확인: 아닙니다. 번호는 조작될 수 있으므로 전화를 끊고 공식 번호로 다시 연락합니다.

2. 금융회사 직원이 전화로 인증번호를 요구하면 알려 줘도 되나요?

확인: 안 됩니다. 통화를 끊고 공식 금융회사에 직접 확인합니다.

3. 원격제어 앱을 설치한 기기로 계속 금융거래해도 되나요?

확인: 안 됩니다. 다른 안전한 기기로 금융회사와 118에 연락합니다.

4. 신고서를 모두 작성한 뒤 지급정지를 요청해야 하나요?

확인: 아닙니다. 송금 피해를 알게 되면 우선 긴급 연락부터 합니다.

5. 돈이 빠지지 않았으면 명의도용 확인은 필요 없나요?

확인: 필요합니다. 신규 계좌·대출·통신 개통 여부를 확인해야 합니다.

6. 상대가 내 이름과 일부 개인정보를 알고 있으면 믿어도 될까요?

확인: 아닙니다. 유출된 정보일 수 있으므로 대화를 끝내고 공식 대표번호로 다시 확인해야 합니다.

7. 은행 직원이라고 밝힌 사람이 전화로 인증번호를 묻는다면 어떻게 하나요?

확인: 말해 주지 않고 통화를 끝낸 뒤 은행 앱이나 공식 대표번호로 직접 확인합니다.

8. 의심 앱을 설치한 휴대전화로 계속 인터넷뱅킹을 해도 될까요?

확인: 안 됩니다. 금융거래를 멈추고 다른 안전한 기기로 금융회사와 전문기관에 연락해야 합니다.

9. 신고서 작성을 끝내야 지급정지를 요청할 수 있나요?

확인: 아닙니다. 피해 송금 사실을 알게 된 즉시 금융회사와 112에 먼저 연락합니다.

9개 질문의 뜻과 이유를 설명할 수 있으면 본 학습으로 이동합니다. 어렵다면 해당 기초개념을 다시 읽거나 EDU-00 공통 기초과정을 먼저 학습합니다.

생활 변화와 새 위험

AI 합성과 피해 뒤의 수치심까지 실제 대응 과정에 포함합니다.

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, 악성앱·스미싱은 안전한 다른 기기로 118에 상담합니다.

공식 근거: 한국인터넷진흥원 · 118 상담 · 검토 2026-08-24
<https://www.kisa.or.kr/118/>

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.

공식 근거: 경찰청 · 보이스피싱 통합신고대응센터 1394 · 검토 2026-08-24
https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1007&q_bbscttSn=20260209152732394

기초개념 다음에 확인할 생활용어

용어	뜻	행동으로 기억하기
피싱	기관·회사·지인을 사칭해 돈이나 개인정보를 빼내는 속임수입니다.	이름이나 발신번호를 믿지 말고 통화를 끊은 뒤 공식 번호로 다시 확인합니다.
스미싱	문자메시지와 피싱을 합친 말로, 링크를 눌러 정보 입력이나 악성 앱 설치를 유도합니다.	문자 속 링크와 번호를 쓰지 말고 공식 앱이나 누리집을 직접 엽니다.
큐싱	QR코드로 가짜 누리집이나 악성 앱 설치 화면에 연결하는 수법입니다.	출처가 분명하지 않은 QR은 읽지 않고, 읽더라도 주소와 요청 권한을 확인합니다.
악성 앱	문자·통화·화면·금융정보를 보거나 휴대전화를 조작하도록 만든 프로그램입니다.	설치가 의심되면 그 기기로 금융거래를 계속하지 말고 안전한 다른 기기로 118과 금융회사에 연락합니다.
원격제어	다른 사람이 내 기기 화면을 보거나 조작하는 기능입니다. 정상 상담에도 쓰이지만 사기에 악용될 수 있습니다.	금융·수사·환급을 이유로 설치나 화면공유를 요구하면 통화를 끊습니다.
지급정지	피해금이 든 계좌에서 돈이 더 빠져나가지 않도록 거래를 멈추는 긴급 조치입니다.	송금 피해를 알았다면 112 또는 금융회사에 즉시 요청합니다. 지급정지가 전액 환급을 보장하지는 않습니다.
명의도용	다른 사람이 내 신분정보로 휴대전화·계좌·카드·대출 등을 만드는 행위입니다.	통신, 계좌, 대출, 신규 금융거래를 각각 공식 경로에서 확인합니다.
안심차단	원하지 않는 여신거래·비대면 계좌개설·오픈뱅킹 이용을 미리 막는 서비스입니다.	생활에 필요한 거래도 제한될 수 있으므로 범위와 해제 방법을 확인한 뒤 신청합니다.

사전 자기진단

각 문장을 읽고 지금 할 수 있는 행동에 표시합니다. 점수보다 오늘 바꿀 한 가지를 찾습니다.

- ☐ 문자나 메신저에 온 링크를 누르기 전에 보낸 사람과 주소를 따로 확인합니다.
- ☐ 기관이나 금융회사가 앱 설치·화면공유·원격제어를 요구하면 통화를 끊습니다.
- ☐ 가족이나 지인이 급하게 돈을 요구하면 저장된 번호로 직접 다시 연락합니다.
- ☐ 검찰·경찰·금융감독원이라는 말만 믿지 않고 공식 대표번호를 직접 찾아 확인합니다.
- ☐ 비밀번호·인증번호·보안카드·신분증 사진을 통화나 메신저로 보내지 않습니다.

- ☐ 투자 수익 인증, 단체대화방의 칭찬, 출금 전 추가 입금을 경계합니다.
- ☐ 계좌 출금 알림과 통신서비스 개통 알림을 켜 두었습니다.
- ☐ 피해가 생겼을 때 연락할 112, 1394, 금융회사, 118의 역할을 알고 있습니다.

PART 1 · EDU-01

나도 속을 수 있습니다

사기는 지식이 부족한 사람만 노리지 않습니다. 놀람, 두려움, 기대, 책임감을 한꺼번에 자극해 확인 할 시간을 빼앗습니다.

진단의 목적은 점수가 아니라 다음 행동을 찾는 것입니다

위 문항에서 '아니요'가 나왔다면 잘못된 것이 아닙니다. 아직 준비하지 않은 안전장치를 찾은 것입니다. 오늘 한 가지부터 바꾸면 됩니다.

사기범은 실제 기관명, 가족 사진, 익숙한 말투, 정상적인 앱 화면을 섞어 씁니다. 전화번호나 목소리가 익숙하다는 이유만으로 상대방을 확인했다고 볼 수 없습니다.

- 0-2개 확인: 긴급 대응 순서부터 읽습니다.
- 3-5개 확인: 금융사기 4단계 행동을 연습합니다.
- 6-8개 확인: 가족이나 동료와 확인 규칙을 공유합니다.

피해자를 타하면 다음 피해를 막기 어렵습니다

'왜 속았나요?'라고 묻기보다 어떤 압박과 조작이 있었는지 확인합니다. 피해 사실을 숨기면 지급정지와 증거 확보가 늦어질 수 있습니다.

돈을 보냈거나 정보를 알려주었다면 부끄럽다는 생각 때문에 신고를 늦추지 마세요. 안전한 사람에게 도움을 청하고 먼저 행동합니다.

진단 결과를 행동으로 바꿉니다

확인한 문항	먼저 할 일	완료 표시
0-2개	7부의 긴급 대응 경로를 읽고 112·1394·118·금융회사 역할을 구분합니다.	☐
3-5개	4부의 4단계 행동을 소리 내어 읽고 사례 1개에 적용합니다.	☐
6-8개	가족·동료와 별도 확인 경로와 비상 연락 담당자를 정합니다.	☐

기억해야 할 태도: 피해 사실을 말한 사람에게 '왜 속았나요?'라고 묻지 않습니다. 어떤 압박이 있었는지 듣고 지급정지·신고·계정 보호를 먼저 돕습니다.

PART 2 · EDU-01

사기는 판단을 서두르게 만듭니다

사기 수법은 달라도 판단을 흐리는 방식은 비슷합니다. 급하게 만들고, 혼자 두고, 확인 경로를 장악합니다.

다섯 가지 조작 신호를 찾습니다

첫째, '지금 안 하면 체포된다'거나 '오늘만 수익이 난다'며 시간을 줄입니다. 둘째, 가족이나 직원에게 말하지 말라고 고립시킵니다. 셋째, 보안을 이유로 앱 설치나 화면공유를 요구합니다.

넷째, 안전계좌·보호계좌·검수계좌 같은 그럴듯한 이름으로 송금을 시킵니다. 다섯째, 이미 보낸 돈을 돌려주겠다며 세금·보증금·인증비를 더 요구합니다.

- 긴급성: 지금, 즉시, 마지막 기회
- 권위: 검찰·경찰·금융회사·정부기관 사칭
- 고립: 가족과 상의 금지, 통화 유지 요구
- 기기 장악: 앱 설치, 화면공유, 원격제어
- 반복 입금: 출금·환급·수사 협조를 빌미로 추가 송금

정상 기관도 연락할 수 있지만 확인 방법은 내가 정합니다

기관 이름과 전화번호 표시만으로 진위를 판단하지 않습니다. 통화를 끊고, 문자나 상대방이 준 링크를 쓰지 말고, 공식 누리집이나 문서에서 대표번호를 직접 찾습니다.

상대방이 통화를 끊지 못하게 하거나 별도 확인을 방해하면 위험 신호가 더 커집니다. 확인을 미루는 동안 생기는 불편보다 잘못 송금했을 때의 손실이 훨씬 큼니다.

AI로 만든 목소리와 영상도 확인을 대신하지 못합니다

짧은 음성이나 공개된 영상만으로도 가족이나 유명인처럼 들리는 합성물이 만들어질 수 있습니다. 목소리와 얼굴이 자연스럽더라도 송금 요구가 나오면 별도 경로로 다시 확인합니다.

가족끼리만 아는 질문이나 암호는 보조 수단입니다. 암호가 맞더라도 저장된 번호로 직접 전화하고, 가능하면 다른 가족에게도 확인합니다.

판단을 되찾는 세 문장

- 지금 결정하지 않겠습니다.
- 통화를 끊고 제가 직접 확인하겠습니다.
- 가족이나 담당자와 함께 확인한 뒤 답하겠습니다.

상대가 화를 내거나 불이익을 말해도 확인을 늦추지 않습니다. 정상 기관이라면 독립된 공식 확인을 막지 않습니다.

PART 3 · EDU-01

공통 구조와 아홉 가지 수법을 봅니다

수법의 이름은 달라도 접촉→신뢰→고립→압박→이전의 흐름은 반복됩니다. 돈·정보·통장·카드·기기 권한을 넘기라는 요구를 먼저 봅니다.

접촉→신뢰→고립→압박→이전의 흐름을 끊습니다

사기범은 전화·문자·SNS·광고·지인 계정으로 접촉한 뒤 기관·전문가·가족·거래처의 신뢰를 빌립니다. 이어서 비밀 유지와 통화 지속을 요구해 주변 사람과의 확인을 막습니다.

처벌·손실·마감으로 시간을 줄인 다음 돈·정보·통장·카드·기기 권한을 넘기게 합니다. 어느 단계에서든 대화를 멈추고 상대가 주지 않은 경로로 확인하면 흐름을 끊을 수 있습니다.

사칭은 신뢰를 빌리고 확인 경로를 가로칩니다

가족·지인 사칭은 급한 병원비나 휴대전화 고장을 내세웁니다. 기관 사칭은 범죄 연루, 안전계좌, 수사 협조 같은 말을 씁니다. 금융회사 사칭은 저금리 대환대출이나 카드 배송 확인을 빌미로 접근합니다.

발신번호는 조작될 수 있고, 악성 앱은 전화를 다른 곳으로 돌릴 수 있습니다. 의심되는 휴대전화가 아니라 다른 전화나 직접 방문으로 확인하는 편이 안전합니다.

스미싱은 링크 뒤에서 앱·정보·결제를 노립니다

택배, 범칙금, 부고, 청첩장, 지원금 문자는 평소 관심을 끄는 소재를 씁니다. 링크를 누른 것만으로 항상 피해가 생기는 것은 아니지만, 앱을 설치하거나 인증정보를 입력했다면 위험이 커집니다.

문자의 번호로 전화하지 말고 해당 기관의 공식 앱이나 누리집을 직접 엽니다. 앱은 문자 링크가 아니라 공식 앱 장터에서 이름과 개발자를 확인한 뒤 설치합니다.

원격제어 앱은 화면을 함께 보는 수준을 넘어설 수 있습니다

상담이나 보안 점검을 핑계로 원격제어 앱을 설치시키면 사기범이 화면을 보거나 조작할 수 있습니다. 통화 가로채기, 문자 확인, 금융앱 조작으로 이어질 수 있습니다.

설치했다면 그 기기로 금융회사나 경찰에 전화하지 않는 편이 안전합니다. 가능한 경우 다른 전화나 직접 방문을 이용하고, 118의 안내에 따라 검사·삭제·초기화를 진행합니다.

투자방은 작은 성공 뒤에 큰 입금을 요구합니다

단체대화방의 수익 인증과 칭찬이 실제 투자 결과라는 보장은 없습니다. 처음에는 소액 출금을 허용해 믿게 한 뒤 더 큰 금액이나 대출을 요구할 수 있습니다.

출금을 위해 세금·보증금·등급 상향비를 먼저 내라고 하면 추가 입금을 멈춥니다. 상품 구조와 사업자 상태를 판단하는 내용은 EDU-13에서 더 자세히 다룹니다.

명의도용은 휴대전화·계좌·대출을 연결합니다

신분증 사진, 얼굴 영상, 인증번호가 유출되면 본인도 모르는 휴대전화나 계좌, 대출이 만들어질 수 있습니다. 한 곳만 확인해서는 연결된 피해를 놓칠 수 있습니다.

통신 가입은 Msafer, 계좌와 대출은 어카운트인포 등 공식 조회 경로를 확인합니다. 개인정보 노출자 등록과 금융거래 안심차단은 추가 거래를 막는 데 도움을 줄 수 있지만 이용 제한도 있으므로 설명을 읽고 신청합니다.

아홉 가지 수법을 요구 행동으로 비교합니다

기관·금융회사 사칭, 가족·지인·딤페이크, 스미싱·큐싱·악성 앱, 투자리딩방·가상자산, 로맨스·친분형, 대출·불법사금융, 쇼핑·중고거래, 취업·부업·통장 대여, 거래처·대표 사칭을 함께 살핍니다.

이야기가 달라도 먼저 돈을 보내라거나 인증정보·앱·통장·카드·비밀 유지를 요구하면 멈춥니다. 쇼핑은 플랫폼 내부 결제, 회사는 기존 번호 콜백과 2인 승인, 가족은 저장된 번호와 다른 가족 확인을 사용합니다.

- 되돌리기 어려운 결제: 개인계좌·상품권·가상자산·현금
- 기기와 계정 장악: 앱 설치·화면공유·인증번호·비밀번호
- 확인 차단: 통화 유지·비밀 요구·플랫폼 밖 이동
- 반복 입금: 세금·보증금·수수료·등급 상향비

공통 흐름 5단계

단계	사기범이 하는 일	내가 던질 질문
접촉	전화·문자·SNS·광고·지인 계정으로 접근합니다.	나는 이 연락을 요청한 적이 있나요?
신뢰	기관명·로고·가족 사진·전문가 수익 인증을 보여 줍니다.	상대가 보여 준 정보 말고 독립된 확인 근거가 있나요?
고립	통화를 유지하고 가족·직원·금융회사에 말하지 말라고 합니다.	왜 다른 사람과 확인하지 못하게 하나요?
압박	체포·손실·마감·기회를 내세워 시간을 줄입니다.	지금 행동하지 않아도 공식 확인을 할 시간이 있나요?
이전	돈·정보·통장·카드·기기 권한을 넘기게 합니다.	한 번 넘기면 되돌리기 어려운 것은 무엇인가요?

아홉 가지 수법 비교

기관·가족·문자·투자에서 먼저 볼 것

유형	대표 위험 신호	별도 확인 경로
기관·금융회사 사칭	범죄 연루·안전계좌·수사 협조·대환대출을 말합니다.	통화를 끊고 공식 대표번호나 공식 앱에서 직접 확인합니다.
가족·지인·딥페이크	사고·납치·휴대전화 고장을 이유로 비밀 송금을 요구합니다.	저장된 번호와 다른 가족·지인을 통해 두 번 확인합니다.
스미싱·큐싱·악성 앱	택배·부고·범칙금·지원금을 미끼로 링크·QR·앱 설치를 요구합니다.	공식 앱을 직접 열고 의심되면 118에 문의합니다.
투자리딩방·가상자산	수익 화면을 보여 주고 출금 전에 세금·보증금·등급비를 요구합니다.	추가 입금을 멈추고 대화·입금 기록을 보존합니다.

친분·대출·거래·취업·기업에서 먼저 볼 것

유형	대표 위험 신호	별도 확인 경로
로맨스·친분형	오랜 대화로 신뢰를 만든 뒤 치료비·통관비·투자를 부탁드립니다.	영상·신분증보다 실제 만남과 별도 사실 확인을 우선합니다.
대출·불법사금융	저금리 전환을 약속하며 선입금·수수료·개인계좌 상환을 요구합니다.	제도권 금융회사 공식 채널에서 상품과 담당자를 확인합니다.
쇼핑·중고거래	플랫폼 밖 채팅·개인계좌·가짜 안전결제 링크로 이동시킵니다.	플랫폼 내부 결제와 분쟁 절차를 사용합니다.
취업·부업·통장 대여	업무용이라며 통장·카드·OTP를 빌리거나 먼저 돈을 내라고 합니다.	통장과 접근매체를 넘기지 말고 사업자·채용 공고를 별도로 확인합니다.
거래처·대표 사칭	계좌가 바뀌었다거나 대표 지시라며 긴급 이체를 요구합니다.	기존 번호 콜백과 2인 승인으로 계좌변경을 확인합니다.

통장·카드·OTP·인증정보를 빌려주거나 넘기지 않습니다. 단순 심부름이라고 생각해도 범죄 자금 이동에 이용될 수 있습니다.

PART 4 · EDU-01

멈춤-따로 확인-경로 차단-즉시 신고로 결정합니다

상대방의 말을 완벽하게 판별하려 애쓰기보다, 돈과 정보가 넘어가기 전에 확인 절차를 실행합니다.

1단계 멈춤: 송금·설치·공유를 하지 않습니다

통화를 끊거나 답장을 멈춥니다. 돈을 보내지 않고, 링크를 누르지 않고, 앱을 설치하지 않습니다. 화면 공유와 원격제어를 종료하고 인증번호·비밀번호·보안카드·신분증 사진을 보내지 않습니다.

‘잠시 확인하겠습니다’라고 말할 필요도 없습니다. 상대방이 화를 내거나 불이익을 말해도 확인이 끝날 때까지 행동하지 않습니다.

2단계 별도경로 확인: 상대방이 준 길을 벗어납니다

가족이라면 저장된 번호로 직접 전화합니다. 기관이라면 공식 누리집이나 종이 고지서에서 대표번호를 찾습니다. 악성 앱이 의심되면 다른 전화나 직접 방문을 이용합니다.

송금 계좌의 예금주, 요구 이유, 금액, 되돌려 받을 조건을 소리 내어 다시 확인합니다. 한 가지라도 설명이 바뀌면 거래를 중단합니다.

- 누가 요구했나요? 이름보다 공식 소속과 대표번호를 확인합니다.
- 왜 지금 해야 하나요? 시간을 줄이는 이유가 타당한지 묻습니다.
- 무엇을 넘기게 되나요? 돈·계정·기기·신분 중 하나라도 넘어가면 멈춥니다.

3단계 경로 차단: 연결을 끊고 기록을 남깁니다

전화와 대화를 차단하고 플랫폼에 신고합니다. 문자, 계정, 전화번호, 송금 계좌, 대화 시간, 요구 내용은 삭제하지 말고 화면을 보존합니다.

이미 돈이나 정보가 넘어갔다면 혼자 추가 협상을 하지 않습니다. 역할에 맞는 공식 기관으로 바로 이동합니다.

4단계 즉시 신고: 상황에 맞는 첫 연락처를 고릅니다

범죄가 진행 중이거나 돈을 보냈다면 112와 송금 금융회사에 연락합니다. 피싱인지 의심되거나 신고·제보가 필요하면 1394를 이용합니다. 악성 앱·스미싱·사이버 보안 상담은 안전한 다른 기기로 118에 연락합니다.

112와 1394는 서로 대신하는 번호가 아닙니다. 상황이 겹치면 두 번호와 금융회사를 함께 이용하고, 지급정지와 긴급 신고를 온라인 신고서 작성보다 먼저 합니다.

금융사기 4단계 행동을 말과 행동으로 연습합니다

1단계 · 멈춤

송금·링크·앱 설치·화면공유·인증정보 제공을 중단합니다.

- 말할 문장: '지금 처리하지 않겠습니다. 제가 직접 확인하겠습니다.'

이미 보냈거나 설치했다면 상대와 협상하지 말고 4단계로 이동합니다.

2단계 · 따로 확인

상대가 준 번호와 링크를 버리고 저장된 번호·공식 누리집·직접 방문으로 다시 시작합니다.

- 말할 문장: '대표번호로 다시 전화하겠습니다.'

악성 앱이 의심되면 같은 휴대전화가 아닌 다른 안전한 기기를 씁니다.

3단계 · 경로 차단

통화·채팅·원격 연결을 끊고 계정과 번호를 차단·신고합니다.

- 말할 문장: 더 답하지 않고 대화·계좌·링크·시간을 캡처합니다.

증거를 남기기 전 앱과 대화를 성급히 지우지 않습니다.

4단계 · 즉시 신고

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

- 말할 문장: 송금 시각·금액·상대 계좌·앱 설치 여부를 짧게 설명합니다.

긴급 지급정지를 온라인 신고서 작성보다 먼저 진행합니다.

송금 직전 30초 확인

- ☐ 누가 요구했나요? 이름이 아니라 공식 소속과 대표번호를 확인합니다.
- ☐ 왜 지금 해야 하나요? 시간을 줄이는 이유가 타당한지 묻습니다.
- ☐ 무엇이 넘어가나요? 돈·계정·기기·신분 중 하나라도 넘어가면 멈춥니다.
- ☐ 어떻게 되돌리나요? 환급·출금에 추가 입금이 필요하다면 중단합니다.

PART 5 · EDU-01

생활 속 다섯 장면에서 선택을 연습합니다

정답을 외우기보다 선택 뒤에 어떤 일이 생기는지 확인합니다. 사례의 이름과 금액은 모두 가상입니다.

사례 1 · 가족 목소리로 들리는 급한 송금 요청

민서 씨에게 울먹이는 아들의 목소리로 전화가 왔습니다. 사고가 났고 합의금 800만 원을 지금 보내야 한다고 합니다. 전화를 끊으면 일이 커진다고 말합니다.

눈에 보이는 위험 신호

- 목소리를 믿게 만듦
- 통화를 끊지 못하게 함
- 즉시 송금 요구
- 다른 가족 확인 차단

내 선택과 예상 결과

- ☐ A. 통화를 유지한 채 100만 원만 먼저 보낸다
- △ 소액 송금도 계좌와 대응 가능성을 확인하는 신호가 될 수 있습니다. 먼저 보내지 않습니다.
- ☐ B. 통화를 끊고 저장된 아들 번호와 다른 가족에게 확인한다

- 상대방이 통제하는 통화에서 빠져나와 별도 경로로 확인했습니다.
- C. 목소리가 비슷하므로 가족 암호호만 묻는다
- △ 암호호는 보조 수단입니다. 별도 번호로 직접 확인해야 합니다.

판단의 갈림길: 송금 금액을 흥정하는 순간이 아니라, 통화를 끊고 별도 경로로 가족의 안전을 확인하는 순간이 피해를 가릅니다.

뒤늦게 드러난 정보: 실제 아들은 안전했고, 공개 영상에서 가져온 음성으로 만든 합성 목소리였습니다.

이어서 할 행동

- 저장된 가족 번호로 직접 전화합니다.
- 연결되지 않으면 학교·직장·다른 가족에게 확인합니다.
- 납치·협박이 이어지면 주변에 도움을 청하고 112에 신고합니다.

사례 2 · 택배 문자 링크와 원격제어 앱

현우 씨는 배송 주소가 틀렸다는 문자의 링크를 눌렀습니다. 상담원이 오류를 고치려면 보안 앱을 설치하고 화면공유를 켜야 한다고 합니다.

눈에 보이는 위험 신호

- 문자 링크
- 공식 장터 밖 앱 설치
- 화면공유·원격제어 요구
- 상담원 지시대로만 확인

내 선택과 예상 결과

- A. 공식 택배 앱을 직접 열어 배송 내역을 확인한다
- 문자 링크를 벗어나 공식 앱이라는 별도 경로를 사용했습니다.
- B. 상담원이 알려준 앱을 설치하되 금융앱만 열지 않는다
- △ 원격제어와 악성 앱은 문자·통화·화면까지 장악할 수 있습니다.
- C. 문자에 적힌 번호로 전화해 진짜인지 묻는다
- △ 문자 속 번호도 사기범이 마련한 경로일 수 있습니다.

판단의 갈림길: 링크를 눌렀다는 사실보다 앱 설치·권한 허용·정보 입력을 더 진행하지 않는 것이 중요합니다.

뒤늦게 드러난 정보: 설치 파일은 금융앱과 문자를 보려는 악성 앱이었고, 전화도 사기범 쪽으로 돌릴 수 있었습니다.

이어서 할 행동

- 공식 택배 앱이나 누리집을 직접 열어 배송을 확인합니다.
- 설치했다면 같은 휴대전화로 금융거래·신고를 계속하지 않습니다.

☐ 안전한 다른 기기로 118과 금융회사에 연락합니다.

사례 3 · 지인 메신저의 급전 요청

동료 계정에서 회의 중이라 전화는 못 받는다며 상품권 50만 원어치를 대신 사 달라는 메시지가 왔습니다. 곧 갚겠다고 합니다.

눈에 보이는 위험 신호

- 전화 확인 거부
- 상품권 번호 요구
- 평소 계정을 그대로 사용
- 빠른 처리 압박

내 선택과 예상 결과

- ☐ A. 평소 말투와 같으므로 상품권 번호를 보낸다
△ 말투와 프로필 사진은 탈취된 계정에서도 그대로 보입니다.
- ☐ B. 금액을 절반으로 줄여 돕는다
△ 금액을 줄여도 확인 없는 지급이라는 위험은 같습니다.
- ☐ C. 저장된 전화번호로 연락하고 회사의 다른 동료에게도 확인한다
○ 두 개의 별도 경로로 신원을 확인했습니다.

판단의 갈림길: 말투와 프로필을 확인하는 데서 멈추지 않고, 저장된 번호와 다른 동료라는 별도 경로를 쓰는지가 핵심입니다.

뒤늦게 드러난 정보: 동료의 메신저 계정이 탈취되었고 같은 메시지가 여러 사람에게 보내졌습니다.

이어서 할 행동

- ☐ 저장된 번호로 직접 연락합니다.
- ☐ 다른 동료에게 계정 탈취 가능성을 알립니다.
- ☐ 메신저 플랫폼에 계정을 신고하고 이미 보냈다면 112·금융회사에 연락합니다.

사례 4 · 수익 인증 투자방과 추가 입금

유진 씨는 전문가가 종목을 알려주는 투자방에 들어갔습니다. 처음 10만 원은 출금됐지만, 2천만 원의 수익을 받으려면 세금 300만 원을 먼저 내라고 합니다.

눈에 보이는 위험 신호

- 조작 가능한 수익 화면
- 단체방의 사회적 증거
- 소액 출금으로 신뢰 형성
- 출금 전 추가 입금

내 선택과 예상 결과

- ☐ A. 이미 수익이 보이므로 세금을 낸다
- △ 앱 화면의 숫자는 실제 자산을 증명하지 않습니다. 출금 전 추가 입금 요구를 멈춥니다.
- ☐ B. 추가 입금을 중단하고 대화·계좌·입금기록을 보존한다
- 손실을 더 키우지 않고 신고에 필요한 기록을 남겼습니다.
- ☐ C. 다른 참여자에게 출금 여부를 묻고 다수가 된다고 하면 낸다
- △ 대화방 참여자도 사기 조직이거나 조작된 계정일 수 있습니다.

판단의 갈림길: 이미 넣은 돈을 되찾으려는 마음 때문에 더 보내지 않는 것이 가장 어려우면서도 중요한 결정입니다.

뒤늦게 드러난 정보: 화면의 수익과 다른 참여자의 칭찬은 조작된 것이었고, 추가 입금 뒤에도 출금은 되지 않았습니다.

이어서 할 행동

- ☐ 세금·보증금·등급비라는 이름의 추가 입금을 멈춥니다.
- ☐ 대화방·사이트·입금계좌·거래내역을 보존합니다.
- ☐ 112-1394와 금융회사에 연락하고 상품 구조 판단은 EDU-13에서 이어서 확인합니다.

사례 5 · 휴대전화 개통 뒤 이어진 대출 명의도용

정호 씨는 신청하지 않은 휴대전화 개통 알림을 받았습니다. 며칠 전 신분증 사진과 얼굴 영상을 대출 상담자에게 보냈습니다.

눈에 보이는 위험 신호

- 신청하지 않은 개통 알림
- 신분증 사진·얼굴 영상 제공
- 비공식 대출 상담
- 통신과 금융 피해 연결

내 선택과 예상 결과

- ☐ A. 통신사에 회선만 해지하고 끝낸다
- △ 통신 회선 외에 계좌·대출·개인정보 노출도 함께 확인해야 합니다.
- ☐ B. Msafer, 어카운트인포, 개인정보 노출 등록과 금융회사 확인을 이어간다
- 연결된 명의도용 경로를 나누어 확인했습니다.
- ☐ C. 대출 상담자에게 자료 삭제를 요청하고 기다린다
- △ 사기범과의 추가 대화보다 공식 기관을 통한 차단과 확인이 먼저입니다.

판단의 갈림길: 휴대전화 회선 하나만 해지하고 끝내지 않고 계좌·대출·신규 거래까지 연결해 확인해야 합니다.

뒤늦게 드러난 정보: 도용된 휴대전화가 본인인증에 쓰였고 비대면 계좌와 대출 시도가 이어졌습니다.

이어서 할 행동

- ☐ 통신사와 Msafer에서 가입 현황·가입 제한을 확인합니다.
- ☐ 어카운트인포와 금융회사에서 조회 대상 계좌·대출을 확인합니다.
- ☐ 개인정보 노출 등록과 금융거래 안심차단을 검토하고 신고 기록을 남깁니다.

PART 6 · EDU-01

평시·의심 중·피해 후 행동을 나눕니다

사기가 시작된 뒤 모든 안전 설정을 하기는 어렵습니다. 평소 준비와 피해 직후 행동을 따로 정합니다.

평소에는 알림과 차단 장치를 준비합니다

계좌 출금, 카드 사용, 통신서비스 개통 알림을 켭니다. 신분증 사진을 휴대전화에 오래 보관하지 않고, 계정마다 다른 비밀번호와 추가 인증을 사용합니다.

여신거래·비대면 계좌개설·오픈뱅킹 안심차단은 필요하지 않은 거래를 미리 막는 선택입니다. 신청은 금융회사 영업점, 어카운트인포 앱이나 참여 금융회사 앱 등 공식 경로를 이용하고, 해제는 영업점에서 대면 본인확인 뒤 할 수 있습니다. 정상적인 금융거래가 제한될 수 있으므로 이용 범위를 확인한 뒤 신청합니다.

- 가족 확인 규칙과 비상 연락 담당자를 정합니다.
- 금융회사 공식 고객센터 번호를 종이나 안전한 주소록에 보관합니다.
- 앱 설치 권한과 화면공유·접근성 권한을 정기적으로 확인합니다.
- 고액 이체 한도는 실제 생활에 필요한 수준인지 점검합니다.

의심 중에는 기기와 대화에서 빠져나옵니다

상대방과 통화를 끝내고 송금과 인증을 멈춥니다. 의심 문자는 보호나라 스미싱 확인서비스나 118을 통해 확인할 수 있습니다.

악성 앱이 의심되면 그 휴대전화에서 비밀번호를 바꾸거나 금융거래를 계속하지 않습니다. 다른 안전한 기기에서 금융회사와 공식 기관에 연락합니다.

피해 뒤에는 돈-기기-신원-증거 순으로 막습니다

돈을 보냈다면 112 또는 금융회사에 지급정지를 요청합니다. 악성 앱과 계정 탈취가 의심되면 118의 안내를 받고, 안전한 기기에서 주요 계정의 비밀번호와 인증수단을 바꿉니다.

신분증과 개인정보가 유출되었다면 개인정보 노출 등록, 계좌·대출 조회, 통신 가입 조회와 가입 제한을 검토합니다. 마지막으로 대화·문자·송금내역·상대 계좌·전화번호·앱 이름과 시간 순서를 보존합니다.

피해 직후 시간대별 행동표

지금-10분 · 돈과 연결을 먼저 멈춥니다

- ☐ 송금 피해는 112 또는 금융회사에 전화해 지급정지를 요청합니다.
- ☐ 상대와 통화·채팅·원격제어를 끊고 추가 송금과 정보 제공을 멈춥니다.
- ☐ 악성 앱이 의심되면 그 휴대전화를 금융거래와 신고 전화에 계속 쓰지 않습니다.

10-30분 · 안전한 기기에서 계정과 신원을 보호합니다

- ☐ 다른 안전한 전화로 1394 또는 118에 상황에 맞는 상담을 요청합니다.
- ☐ 주요 이메일·메신저·금융 계정의 비밀번호와 인증수단을 안전한 기기에서 바꿉니다.
- ☐ 신분증·얼굴 영상·인증정보가 유출되었다면 개인정보 노출 등록과 안심차단을 검토합니다.

오늘 안에 · 연결된 피해와 증거를 확인합니다

- ☐ 어카운트인포에서 조회 대상 계좌·대출을, Msafer에서 통신 가입 현황을 확인합니다.
- ☐ 문자·대화·전화번호·상대 계좌·송금내역·앱 이름·설치 시각을 시간순으로 보존합니다.
- ☐ 신고기관·금융회사·담당자·접수번호·안내받은 다음 절차를 기록합니다.

1-7일 · 후속 절차와 재발 방지를 이어갑니다

- ☐ 금융회사에 피해구제 신청의 서류·기한·진행 상태를 확인합니다.
- ☐ 휴대전화 점검·초기화가 필요하면 118 또는 제조사·통신사의 공식 안내에 따릅니다.
- ☐ 가족에게 사실을 알리고 추가 사칭 연락, 계좌·카드·통신 알림을 함께 확인합니다.

30일 안에 · 생활 속 안전장치를 다시 설계합니다

- ☐ 통신 가입·계좌·대출·앱 권한·연결서비스를 다시 점검합니다.
- ☐ 이체 한도와 여신거래·비대면 계좌개설·오픈뱅킹 안심차단 필요성을 검토합니다.
- ☐ 가족 확인 규칙과 비상 연락 담당자가 실제로 작동하는지 연습합니다.

가족 디지털 안전 약속

- ☐ 돈이나 개인정보를 요구하는 연락은 누구의 목소리·얼굴이어도 일단 끊습니다.
- ☐ 가족의 저장된 번호와 두 번째 연락대상을 정해 두 경로로 확인합니다.
- ☐ 확인 질문이나 암호는 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.

본인계좌 일괄지급정지를 신청하면 자동이체·오픈뱅킹 등 출금거래와 연결된 체크카드 이용이 제한될 수 있습니다. 조회에서 빠지는 계좌가 있을 수 있고 해제는 금융회사 절차가 필요하므로 공식 안내를 확인합니다.

PART 7 · EDU-01

기관마다 맡은 일이 다릅니다

긴급 신고, 금융 지급정지, 기기 보안, 명의도용 확인을 한 곳에서 모두 처리한다고 생각하지 않습니다.

긴급 상황은 112와 금융회사, 피싱 상담은 1394로 연결합니다

자금을 송금했거나 범죄가 진행 중이면 112에 신고하고 지급정지를 요청합니다. 돈이 나간 금융회사나 돈이 들어간 금융회사 고객센터에도 직접 요청할 수 있습니다.

지급정지가 곧 전액 환급을 뜻하지는 않습니다. 남아 있는 피해금, 피해 유형, 확인 절차에 따라 결과가 달라질 수 있습니다. 필요한 서류와 신청기한은 금융회사에 바로 확인합니다.

보이스피싱인지 의심되거나 상담·신고·제보가 필요하면 전기통신금융사기 통합 신고 대표번호 1394를 이용합니다. 365일 24시간 상담하며, 송금 직후에는 112와 금융회사 지급정지를 함께 진행합니다.

기기와 문자는 118, 온라인 범죄 신고는 ECRM을 이용합니다

한국인터넷진흥원 118은 해킹·스팸·개인정보침해 상담과 악성 앱 대응 안내를 제공합니다. 경찰청 사이버범죄 신고시스템(ECRM)은 온라인으로 사이버범죄 피해를 신고하는 경로입니다.

긴급한 송금 피해는 온라인 신고서를 먼저 작성하느라 지급정지를 늦추지 않습니다. 112와 금융회사에 먼저 연락한 뒤 필요한 온라인 신고와 서류 절차를 이어갑니다.

추가 명의도용을 여러 경로에서 확인합니다

금융감독원 개인정보 노출자 사고예방시스템에 등록하면 신규 계좌개설이나 카드 발급 등 일부 거래가 제한될 수 있습니다. 어카운트인포에서는 조회 대상 계좌와 대출을 확인하고 본인계좌 일괄지급정지를 신청할 수 있습니다.

Msafer에서는 본인 명의 통신서비스 가입 현황을 조회하고 이동전화 가입을 제한할 수 있습니다. 각 서비스는 대상과 제외 범위가 있으므로 한 경로만 확인하고 끝내지 않습니다.

상황별 첫 연락처

기관·서비스	언제	무엇을 요청할지
경찰청 112	돈을 보냈거나 범죄가 진행 중일 때	진행 중인 피싱·송금 피해 신고, 지급정지 연계
통합 신고 1394	피싱인지 의심되거나 추가 피해가 걱정될 때	피싱 의심 상담·신고·제보와 관계기관 연계
거래 금융회사	송금·계좌·카드 피해가 있을 때	본인·사기이용계좌 지급정지, 피해구제 서류와 기한 안내
KISA 118	의심 링크·앱·기기 감염이 있을 때	악성 앱·스미싱·해킹·개인정보침해 상담
금융감독원 1332	금융 절차와 분쟁 상담이 필요할 때	금융피해 상담과 제도 안내
어카운트인포	계좌·대출 명의도용이나 추가 출금이 걱정될 때	조회 대상 계좌·대출 확인, 본인계좌 일괄지급정지와 안심차단
개인정보 노출자 사고예방시스템	신분증·인증정보가 유출되었을 때	개인정보 노출 등록으로 신규 금융거래 일부 제한
Msafer	휴대전화 명의도용이 걱정될 때	통신 가입 현황 조회와 이동전화 가입 제한
경찰청 ECRM	긴급 대응 뒤 온라인 신고를 이어갈 때	사이버범죄 온라인 신고

연락 전에 준비하면 좋은 기록

- ☐ 송금 시각·금액·상대 계좌와 예금주
- ☐ 연락받은 번호·계정·링크·앱 이름
- ☐ 앱 설치·화면공유·인증정보 제공 여부와 시각
- ☐ 신고·상담 기관, 담당자, 접수번호, 다음 안내

증거는 확인 가능한 사실과 시간 순서로 남깁니다. 비밀번호·인증번호·신분증번호 전체를 활동지나 공유 문서에 적지 않습니다.

PART 8 · EDU-01

오늘 한 가지를 바꾸고 다시 확인합니다

안전은 모든 수법을 외우는 일이 아니라 확인할 시간을 되찾는 습관입니다.

다섯 문장만 기억합니다

급하게 만들면 멈춥니다. 상대방이 준 링크와 번호를 쓰지 않습니다. 앱 설치·화면공유·인증정보 요구를 거절합니다. 돈을 보냈다면 112와 금융회사에 바로 연락하고 피싱 상담·신고는 1394를 이용합니다. 피해 사실을 숨기지 않고 증거를 남깁니다.

7일과 30일 뒤에 행동을 확인합니다

7일 안에 가족 확인 규칙을 정하고 계좌·카드 알림을 점검합니다. 30일 안에 통신 가입과 계좌·대출 현황, 앱 권한, 사용하지 않는 연결서비스를 확인합니다.

이 자료의 사후평가는 지식을 얼마나 외웠는지보다 위험한 순간에 어떤 순서로 움직이는지를 확인합니다. 틀린 문항은 해당 장으로 돌아가 행동을 다시 연습합니다.

행동 수행 점검

- ☐ 의심 연락에서 위험 신호 두 가지 이상을 말할 수 있습니다.
- ☐ 상대가 준 경로를 버리고 별도 확인 경로를 고를 수 있습니다.
- ☐ 송금·악성 앱·명의도용 상황의 첫 연락처를 구분할 수 있습니다.
- ☐ 우리 집의 확인 규칙과 비상 연락 담당자를 정했습니다.

이어서 할 학습

별도 평가세트의 10문항을 풀고 틀린 문항은 해당 Part로 돌아가 다시 연습합니다. 신종 투자상품의 구조·보호범위 판단은 EDU-13, 분쟁과 피해구제 기록은 EDU-15에서 이어집니다.

마지막 확인

돈을 보냈다면 112와 송금 금융회사에 즉시 지급정지를 요청합니다. 피싱 의심 상담·신고·제보는 1394, 악성 앱·스미싱 상담은 안전한 다른 기기로 118에 연락합니다.

오늘 바로 할 일

- ☐ 가족과 별도 확인 질문 또는 암호 정하기
- ☐ 계좌·카드·통신 알림 상태와 안심차단 3중 확인하기
- ☐ 112·1394·118·1332와 거래 금융회사 번호 저장하기

공식 근거와 최신본 확인

최신 HTML 자료: 넥서스 금융 브리핑 '국민 금융생활 안전교육'

금융위원회·경찰청·한국인터넷진흥원·금융결제원·Msafes 등 공식 자료를 기준으로 작성했습니다. 실제 신청·신고 전에는 HTML 기준본의 검토일과 공식기관 안내를 확인합니다.