

예방 수칙

여섯가지만,
기억해주세요!

① 투자정보를 준사람과 내용을 확인하세요

- 금융감독원 금융소비자 정보포털 [파인\(fine.fss.or.kr\)](#)에서 정보 제공자가 제도권 금융회사인지, 신고된 유사투자 자문업자인지를 반드시 확인
- 금융감독원 전자공시시스템([dart.fss.or.kr](#)) 및 [한국거래소\(krx.co.kr\)](#) 홈페이지를 통해 추천받는 기업의 재무상태 등을 반드시 확인

② 공공기관이나 유명인 사칭에 유의하세요

- 주식 리딩방 관련 분쟁해결, 손실복구 명목으로 공공기관의 문서를 제시하는 경우 해당 기관에 연락하여 진위여부를 직접 확인

③ 개인정보를 요구하는 경우 대부분 사기입니다

- 방송 플랫폼, 공개 채팅방 및 주식 종목 게시판 등을 통해 개인정보를 요청 받더라도 절대 응하지 않도록 유의 / 업자간 DB거래로 2차 3차 피해 우려

④ 불법 영업 리딩방은 이용하지 마세요

- 리딩방에서 1:1 투자자문 및 자동매매 프로그램을 판매/대여하는 행위는 불법
- 사설 HTS(홈트레이딩시스템), 선물거래계좌 대여 명목의 입금/송금 요청에 주의

⑤ 자칫 주가조작범죄에 연루될 수도 있습니다

- (시세조종에 연루) 리딩방 운영자가 인위적인 주가상승을 목적으로 대량의 시세조종성 주문을 제출하여 회원들에게 동참을 요구
- (선행매매에 노출) 리딩방 운영자 등이 특정 종목의 주식을 매매하기 전 미리 알고 있는 내부정보를 이용, 대량 매수 후 리딩방에 추천하고 주가상승 유도

⑥ 피해구제 및 제보방법을 기억해주세요

- (불법영업/투자사기) 경찰청 182, 금융감독원 1332
- (불공정 거래행위) 금융위원회 2100-2500, 금융감독원 1332, 한국거래소 1577-0088
- (피해구제) 한국소비자원 1372

투자리딩방 불법행위

"모르는 타인을 통해
큰 돈을 벌 수 있는
방법은 없습니다."

피하는 것이
가장 현명한
투자입니다.

신종 범죄

이렇게 예방하세요

- 투자리딩방 불법행위 편 -

책임을 다하는
국민의 경찰



강원경찰청
지치경찰위원회



강원경찰청
지치경찰위원회

투자 전문가? 당신의 돈을 노립니다

투자리딩방 불법행위?!

문자, 전화, SNS 등을 이용해 고수익을 보장한다며 투자 종목을 추천하거나
매매시점을 안내하는 방법으로 투자를 이끌어 피해금을 편취하는 **범죄**입니다.
(리딩 : leading)

| 이런 수법! 투자리딩방 불법행위입니다!!

No.1 접근 단계

투자광고

페이스북, 유튜브, 블로그 등을
이용해 투자광고

"투자전문가, 연예인 운동
선수, 은행, 증권사들을 사칭
하는 경우가 많습니다"

문자/단체채팅방

문자(미시지) 수신자가 링크를
눌러 오픈채팅방 참여 유도

"무료 투자정보 제공, 고수
익 보장 손실보상 문구로 관
심을 유도합니다"

No.2 속임 단계

앱/홈페이지

범죄자가 만든 기afa 홈페이지,
앱 접속 유도

"앱 설치를 유도, 실재와 우사한
앱 홈페이지를 실행해 조직한
수익률/기각을 보여줍니다"

바람잡이

범죄자가 수백개의 가짜 ID
이용 단체채팅방에 수반방이
있는 것처럼 조작

"당신 회사원을 속이기 위해
사실은 1명이 매크로를 이용, 복
사를 넣기하고 있습니다"

No.3 편취 단계

출금 거부

피해자는 안심시키기 위해
소액의 수익은 출금이 가능
하도록 하나,

"피해자가 안심하고 거액을 입금
하는 순간 출금 거부됩니다"

회수 불능

범죄자는 대포통장, 가상자산
지갑으로 편취

"피해금은 자금세탁되어
회수 불능인 경우가
많습니다"

“
미리 알고 예방하세요
”

투자리딩방 불법행위

이런 경우 피해가
발생할 수 있습니다

01

허위정보 제공 후
투자금을 가로채는 행위

거래소 상장 빙자(비상장주식/가상자산)

상장 계획이 없는 비상장 주식 또는 허위 가상자산으로 속여 투자금 편취
이주시 상장되면 최소 350% 이상 수익을 보실 수 있습니다! 지금 참여하세요!

투자 손실을 보장해 주겠다며 접근

투자손실자를 투자리딩방에 초대 투자회사 직원을 사칭해 손실보상 빌미로 편취

**손실보상입니다(금육당국 기자문서 제시) **만원 입금하시면 복구해드려요!!

대신 투자해 고수익을 보장해주겠다며 접근

투자에 미숙한 고령층 등 공략, 투자리딩방 초대 후 대리투자 유도하여 편취

노후걱정 없는 대리 투자 무료방 초대합니다: http://open*****.com

허위 거래소/사이트/HTS 개설

기afa 사이트, 호가창 등 제작 리딩방에서 허위의 수익률을 보여주며 유인/편취

10만원에서 단 5일만에 200만원으로! 여러분도 이렇게 수익이 나옵니다!

가상자산을 빌미로 한 각종 기망행위

가상자산을 위탁채굴 / AI매매 / 예치 후 이자 지급하겠다고 속여 편취

인공지능 프로그램으로 시세를 예측합니다. 100% 수익 보장합니다!

알면 피할 수 있습니다

02

투자금 횡령

투자업체 직원 또는 대리투자 중 횡령

정상 업체 직원이 회사 DB 이용, 리딩방으로 개별 투자 유치 후 투자금
횡령하거나, 인가 없는 매매중개업체에서 고객 투자금을 사적 용도로 유용

**투자 직원입니다. 투자리딩방 개설했습니다. 이쪽에서 진행해 드릴게요

여기 리딩방에 계신 분들에게만 기회 드립니다. 투자금 예치하시면 2배로!!

03

불공정 거래행위

시세조종 / 선행매매

리딩방 회원들에게 동참할 것을 요구, 시세 조종하여 부당이득 취득(시세조종)

회원 여러분 구매 동참 부탁드립니다. *** 종목 주가 상승 시켜야죠!!

내부 정보 이용해 산값에 주식을 선매수 후 회원을 '물량받이'로 삼아 시세를
올리고 매도하여 차익 실현(선행매매)

오늘의 추천 종목은 ****입니다. 수익률 100% 보장합니다!!

허위사실 유포

허위사실을 리딩방에 유포, 해당 주식을 매수하도록 하여 부당이득 취득

'해외 현지 관공서와 업무 독점 계약 체결' 바로 매수하세요!!!

3 피해시 대응 방법

STOP 즉시 '지급정지' 신청

범죄자에게 계좌이체를 했거나 개인·금융정보를 알려준 경우 경찰청(112) 또는 은행 콜센터로 전화하여 즉시 지급정지 신청

※ 이후 경찰에 신고 및 피해사실확인서(사건사고사실확인원)·신분증·구체신청서를 3영업일 이내 은행에 제출해야 지급정지 유지

경찰에 신고

112신고

112상황실에서 접수 후 「전기통신금융사기 통합 신고센터」로 이관 → 대응방안 안내 구제 지원
* 경찰청·금융감독원·한국인터넷진흥원 합동 근무

온라인(PC)신고

경찰청 '사이버범죄신고시스템' 내 신고하기 (ecrm.police.go.kr) → 범죄유형 선택 → 본인인증 → 신고내용·진술서 작성
※ 신속한 처리가 필요한 경우 직접 경찰서로 방문하여 신고

방문신고

진정서·신분증·증거자료(이체확인서·메신저 대화내용 등)를 지참하여 인근 경찰관서 방문

명의도용 피해 예방 추가 조치

조치	내용
명의도용 확인	통신사 지점 방문·엠세이퍼(msafer.or.kr)를 통해 본인 명의로 개통된 이동전화·무선인터넷 등 확인
휴대전화 신규 가입 등 차단	통신사 지점 방문·엠세이퍼(msafer.or.kr)·애플리케이션(PASS)를 통한 신규가입·번호이동 등 차단
신분증 재발급	(주민등록증) 정부 24 홈페이지(gov.kr) 또는 주민센터 방문 ※ 6개월 이내 활동한 증명사진 및 기존 주민등록증 지참 (운전면허증) 도로교통공단 홈페이지·면허시험장·경찰서 방문
인증서 재발급	은행 홈페이지 또는 애플리케이션에서 재발급
개인정보 도용 유출여부 확인	개인정보포털(privacy.go.kr)에서 명의도용 의심 사이트 탈퇴 탈린 내 정보 찾기 서비스(kidc.eprivacy.go.kr)에서 유출 확인
명의도용 계좌·카드 조회	계좌정보통합관리서비스(payinfo.or.kr)에서 계좌·대출 조회 개인정보노출자 사고예방시스템(pd.fss.or.kr)에 정보 노출 등록

피싱범죄 관련 주요 Q&A

Q 피싱범죄를 당했을 때는 가장 먼저 무엇을 해야 하나요?

A 즉시 지급정지를 신청하고, 경찰에 신고(112·온라인·방문)해야 합니다.

Q 피싱 링크를 클릭했을 때 가장 먼저 무엇을 해야 하나요?

A 휴대폰을 비행기모드로 변경하고 보안 프로그램(V3M, 시티즌코난 등)을 통해 악성 앱을 삭제해야 합니다.

Q 금융·공공기관에서 전화·문자등으로 개인정보를 요구하면 응답해도 되나요?

A 절대로 전화·문자 등으로 금융정보나 개인정보를 요구하지 않습니다. 기관 대표번호로 전화해서 상대방 등을 직접 확인하거나 112로 신고해 주세요

Q 피싱범죄는 주로 어떤 사람들을 대상으로 하나요?

A 연령과 관계없이 누구나 범죄의 표적이 될 수 있으며, 최근에는 의사·연구원 등의 고학력자나 검사·은행원 등 직업적 관련성이 있는 피해자도 발생하고 있습니다.

Q 내 계좌로 작은 금액이 입금된 후 전화가 왔어요. 왜 그럴까요?

A 이는 '시험송금'이라는 수법으로 여러분의 계좌가 유효한지 확인하고 이를 피싱계좌로 이용하고자 전화를 걸었을 가능성이 높습니다. (예시 : 착오송금 반환요구)

Q 피싱 사이트를 어떻게 구분할 수 있나요?

A 인터넷 주소에 오타가 있거나 'https://'가 아닌 'http://'로 시작하는 경우 의심해봐야 하며, 주소창에 보안 인증 마크가 없는 사이트도 주의가 필요합니다.

※ △ https : 모든 데이터를 암호화된 형태로 전송 △ http : 일반 텍스트 형태로 전송

피해 구제 절차

피해금 환급은 지급정지 이후 금융감독원에서 진행

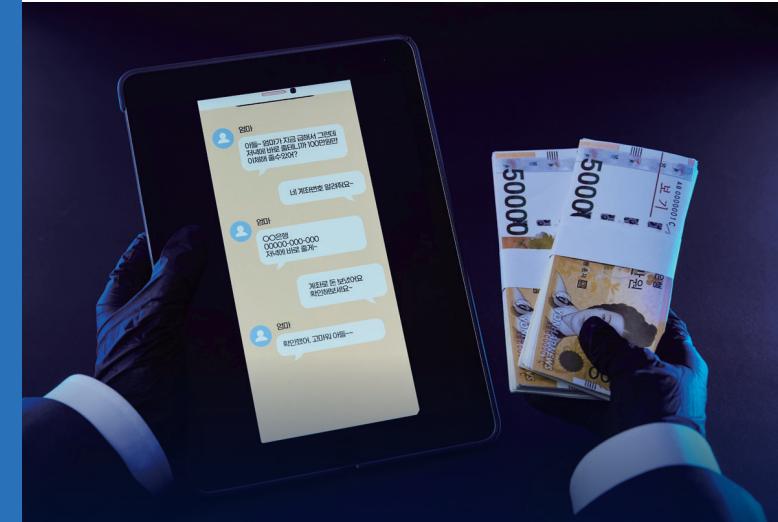


※ 대면편취형 범죄는 입금계좌 특정 시 지급정지 및 피해금 환급

신종 범죄

이렇게 예방하세요

- 피싱범죄 편 -



강원 경찰청 지방경찰위원회
경인 특별자치도

1 피싱범죄란?

전화·문자 등을 이용해 공공기관이나 금융기관 등을 사칭하여 개인정보나 금융거래정보를 불법적으로 알아내어 금전적 손실을 발생시키는 범죄입니다.

이런 전화 무조건 피싱사기입니다!



<금융기관 사칭> "00 저축은행 상담원
김ㅁㅁ입니다. 고객님에게 저금리 대출을
해드립니다. 대출금 상환을 위해 계좌
이체를 하거나 현금을 저희 직원에게
전달해주셔야 합니다"



<수사기관 사칭> "서울중앙지검 강00
검사입니다. 본인 명의로 개설된 통장이
범죄에 사용되어 조사차 연락드렸습니다."

이런 문자 무조건 피싱사기입니다!

[국제발신]
[해외승인] XYZ를
676,320원 결제완료
본인 아님
상담센터 070-1234-5678

상품결제 사칭

[국제발신]
[00카드] 고객님의 카드가
신규 발급되었습니다.
본인 아님 신고바랍니다
신고센터 070-1600-1234

카드발급 사칭

[국제발신]
[ㅁㅁ은행]
주식이 다가왔습니다. 다음
링크를 클릭해서 선물을
받아가세요 <http://abank...>

명절선물 사칭

[국제발신]
[00지방법원] 사건번호
2024-12345 관련 법원
출석서가 발부되었습니다
내용확인 <http://court.abc...>

법원 사칭

[국제발신]
[00구청] 주차위반 벌칙금
고지서가 발부되었습니다.
고지서 확인 <http://....go.kr>

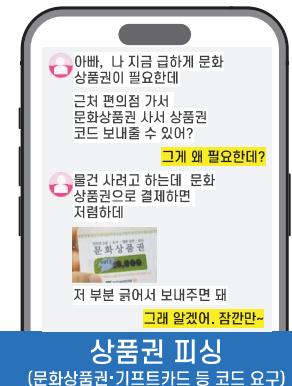
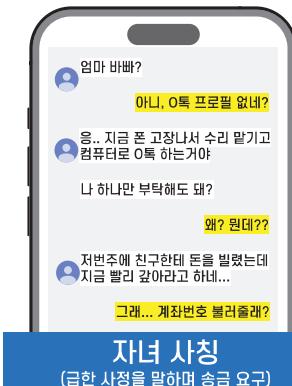
벌칙금 사칭

[WEB발신]
[AA택배]
택배가 도착하였으나 부재중
으로 위탁 장소에 보관
문의전화 070-1600-0000

택배 사칭

주변인과 상의하지 못하도록 홀로있는 공간으로
이동을 요구하는 전화·문자는 무조건 의심해야 합니다

이런 메신저 무조건 피싱사기입니다!



악성 애플리케이션은 **피해자 휴대폰의 전화 가로채기**
개인정보 탈취 등 모든 기능을 조작할 수 있습니다.

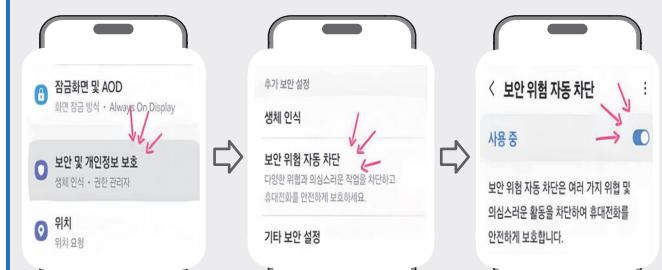
2 평상시 예방 방법

예방 수칙 네 가지만 기억!

- ✓ 출처 불명 인터넷 주소 클릭 금지
- ✓ 송금 상대방은 반드시 확인
- ✓ 모르는 전화를 받은 후 계좌이체·
현금 인출·전달 무조건 금지
- ✓ 스마트폰에 신분증 사진·계좌번호·
비밀번호 등 저장하지 않기

보안 관리는 필수!

'보안 위험 자동 차단' 설정(안드로이드)
⇒ 출처를 알 수 없는 애플리케이션 설치 방지



* 필요시 서비스센터·대리점 등에 방문해서 핸드폰 초기화 진행

보안 애플리케이션 설치!



V3 Mobile



알약M



싹다잡아



예방 서비스 가입 권장!

여신거래
안심차단

신용대출·신용카드 발급 등 개인의 신규 여신
거래를 사전에 차단하는 서비스
※ 현재 거래중인 은행을 직접 방문하여 신청

지연 이체

계좌 이체 시 수취인 계좌에 일정 시간 경과
이후 입금되도록 하는 서비스
※ 최소 3시간 이상 선택 가능 / 창구거래는 미적용

입금계좌
지정

본인이 사전에 지정한 계좌 이외의 계좌는
소액 송금만 가능한 서비스
※ 1일 1백만원 이내 이체한도 선정 / 창구거래는 미적용

해외IP차단

국내 IP대역이 아닌 곳에서 접속한 경우 이체
거래를 할 수 없도록 사전에 차단하는 서비스

영상물 삭제, 차단

경찰 이외 본인도 직접 신청 가능

- 경찰(112, 방문, 온라인)



• 디지털성범죄피해자지원센터

디지털성범죄피해자 상담센터(d4u.stop.or.kr, 02-735-8994, 24시간 운영) 홈페이지 '상담하기 메뉴'에서 신청

1 본인 확인

본인 명의 휴대폰
또는 아이핀

2 상담 신청

상담하기 메뉴 클릭 후
피해내용 기재

3 초기 상담

상담사가 피해자에게
연락

4 피해확인 및 서류접수

- 피해영상을 유포개시물 URL 확보
- 삭제지원 신청서류 안내/접수

• 방송통신심의위원회

방송통신심의위원회(www.kocsc.or.kr, 국번없이 1377, 24시간 운영) 홈페이지 '전자민원' - '디지털성범죄 신고 메뉴'에서 신청

1 본인 확인

본인 명의 휴대폰
또는 아이핀

2 신청인 정보입력

본인 및 대리인 신분증
사본, 위임장 등

3 심의대상 정보 입력

해당 정보의 고유주소(URL) 입증자료

접수 완료(필요시 추가자료 요구)

※ 제3자는 방송통신심의위원회로 삭제요청 가능

피해자 보호 지원

- 경찰 (피해자안전조치) 112신고 시스템 등록, 맞춤형 순찰, 스마트 위치 지급 등
(수사사) 기명조서, 조사사 피해자 예비 지급, 국선변호인 참여 등

• 상담 / 치료 기관(단체)

푸른나무재단 구원의 팔 상담전화 : 학교, 사이버폭력 상담 1588-9128

한국여성안전진흥원 지원센터 : 02-735-8994(24시간), 여성긴급전화 : 1366(24시간)

시도교육청 학교 Wee 클래스, 교육청 Wee 센터 : www.wee.go.kr

한국청소년 상담복지개발원 청소년 상담 1388 (전화, 문자, 온라인 24시간)

딥페이크 디지털 성범죄

어떻게 대처해야 할까요?

딥페이크 사진이나 동영상을 받았을 때
클릭하거나 시청하지 마세요!

1. 알 수 없는 인터넷 링크 / 파일 클릭, 시청 금지!

2. 악성앱 설치 여부 확인!

설정앱 Click! → 애플리케이션 → 내파일 → 하단열기

APK설치 파일 (*.apk) 삭제

3. 불법영상을 확인 시 즉시 112신고!

책임을 다하는
국민의 경찰

딥페이크 허위영상물!!
놀이가 아니라 범죄입니다.
당신의 가족, 아이들이 피해자
또는加害者가 될 수도 있습니다.



강원 경찰청
Gyeonggi Provincial Police
지지경찰위원회

신종 범죄

이렇게 예방하세요

- 딥페이크 편-



강원 경찰청
Gyeonggi Provincial Police
지지경찰위원회

딥페이크란(Deepfake)?

특정인의 얼굴을 인공지능(AI) 기술을 활용해 기존의 영상, 사진에 있는 인물의 얼굴이나 특정 부위에 합성하는 기술

딥러닝(Deep learning)+페이크(Fake)의 혼성어

NEWS 00대 딥페이크 성범죄, 여학생 얼굴에 신체 합성해

NEWS 딥페이크 피의자 96%가 청소년

NEWS 딥페이크 '지인능욕방' 운영한 20대 대학생

내가 저기에 **왜?**
도와주세요...

신고하고 싶은데,
어떻게 하지?

허위영상이
유포되고 있는데, **어떻게** 막지?

딥페이크, 이런 경우 **처벌**됩니다.

딥페이크 유형과 적용 법률



성적 허위영상물
제작, 판매, 배포, 구입, **소지, 저장, 시청** 행위 모두 처벌

아동청소년의 영상, 사진 등을 이용하여 제작/영리목적 판매·대여·배포/소지·시청 등의 경우 가중처벌됩니다.



성적 내용이 아닌 허위영상물
→ **스토킹, 명예훼손, 개인정보 유출로 처벌**

허위영상물 등과 함께 대상자의 동의 없이 이름, 연락처, 학교 등 개인정보를 유출한 경우 처벌 됩니다.

“실수? 큰 책임으로 돌아옵니다!”

성폭력처벌법

성적 허위영상물 편집, 합성, 가공 등(7년 이하 징역)
영리 목적 반포(3년 이상 징역) 소지·시청(3년 이하 징역)

청소년성보호법

아동청소년 영상/사진 제작(무기징역),
영리 목적 반포(5년 이상 징역), 구입, 소지, 시청(1년 이상 징역)

스토킹처벌법

스토킹 범죄(3년 이하 징역)

정보통신망법

온라인 상 명예훼손(3년 이하 징역)

개인정보보호법

타인 개인정보 이용 등(5년 이하 징역)

스토킹처벌법 제2조(정의) 1호 바. 상대방 등의 정보(개인정보보호법 제2조 제1호의 개인정보 등)를 정보통신망을 이용하여 제3자에게 제공하거나 배포 또는 게시하는 행위

딥페이크 영상을 발견한다면?
어떻게 해야 할까요?

즉시 경찰에 112 긴급신고! 증거 확보!



피해영상물이 유포된 사이트의 URL 확인하고, 텔레그램/카카오톡 등으로 유포된 경우 파일 다운로드 후 대화방 내용 캡처, 녹화



범행에 사용된 기기 확보 시, 증거 확보를 위해 '비행기 모드'로 전환하여 외부접속 차단(임의로 초기화, 삭제 금지)

공통

사진 영상 댓글 채팅 저장 또는 캡처
피의자를 특정할 수 있는 게시글,
계정, ID, 닉네임 등 저장

텔레그램

대화방, 메시지 삭제 시 복구 추적이
불가능. 내용 전체 캡처/촬영해 백업
대화 참여자의 프로필화면 촬영

페이스북

URL: 'facebook.com' 이후
영문으로 사용자 아이디 특정

인스타그램

http://www.instagram.com/
000?igsh=...으로 사용자 구분
(000부분으로 사용자 아이디 특정)

증거수집 방법

카카오톡

'대화내용 내보내기' 기능, 캡처를
통해 대화내용 저장
ID, 전화번호, 프로필 등 캡처

기타 SNS

SNS 계정, URL, ID, 일자 등 가능한
많은 정보 촬영/캡처/영상물 저장

“그 밖에 신고하는 방법 꼭 기억하세요!!!”

① 경찰관서 방문신고

② 경찰청 사이버범죄신고시스템
(<https://ecrm.police.go.kr>, 24시간)

③ 디지털 성 범죄
피해자지원센터
(02-735-8994, 24시간)

