안전한 금융생활을 위한

사기 예방 백과사전

은행연합회 Banki

안전한 금융생활을 위한

사기 예방 백과사전

이 백과사전에서 다루는 8가지 사기 유형은 모두 금융 거래를 통해 사람들의 재산에 손해를 입힐 수 있다는 공통점을 갖고 있습니다. 이러한 이유로 이 백과사전에서는 본문에 등장하는 사기 유형을 통틀어 '금융사기'라고 표현하였습니다.

안전한 금융생활을 위한

사기 예방 백과사전

발행일 2025년 12월 10일

펴낸 곳 은행연합회 소비자보호부

주소 서울시 중구 명동11길 19

전화 02-3705-5000

홈페이지 www.kfb.or.kr

기획 은행연합회

편집·디자인 소소한소통

자문 김용국(예금보험공사 금융교육팀 팀장)
문호준(경찰청 피싱범죄수사계 경위)

ISBN 978-89-960237-7-7 03060

목차

백과사전을 소개합니다

금융사기에 대해 알고 있나요?

금융사기는 금융 거래에서 사람을 속여 돈이나 물건을 빼앗는 범죄입니다.
보이스피싱이나 로맨스 스캠 등 여러 유형이 있으며,
디지털 기술이 발달하면서 범죄 수법이
점점 더 복잡하고 다양해지고 있습니다.

금융사기는 한 가지 방법으로만 일어나지 않습니다.
여러 범죄 수법이 함께 쓰일 때가 많습니다.
예를 들어, 투자 사기를 저지르면서 보이스피싱 수법을 함께 쓰기도 합니다.

누구나 피해자가 될 수 있어요

문자, 전화, 광고 등 우리의 일상생활 곳곳에 금융사기가 숨어 있습니다.
금융사기는 사기범 혼자서 저지르는 경우도 있지만,
범죄 조직에서 여러 사람이 역할을 나누어 함께 저지르는 경우도 많습니다.
범죄 조직이 저지르는 금융사기는 수법이 훨씬 더 복잡해서
더욱 피해를 해결하기 어렵습니다.

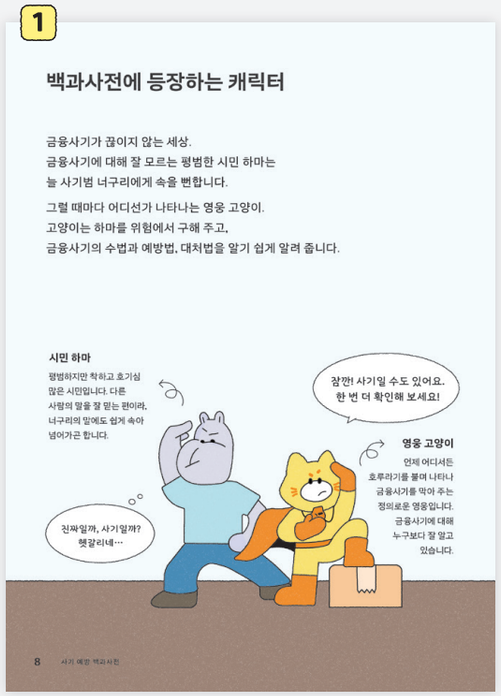
누구나 금융사기의 피해자가 될 수 있습니다.
따라서 평소에 주의 깊게 살피고 미리 예방하는 것이 가장 중요합니다.

이 자료에서는 이런 것을 배울 수 있어요

〈사기 예방 백과사전〉에서는 8가지 주요 금융사기에 대한
예방법, 대처법, 그리고 실제 피해 사례 등을 소개합니다.
귀엽고 든든한 캐릭터와 함께 금융사기에 대해 차근차근 알아보며,
나와 내 소중한 재산을 지키는 방법을 배워 보세요.

백과사전,
이렇게 읽어 보세요

1

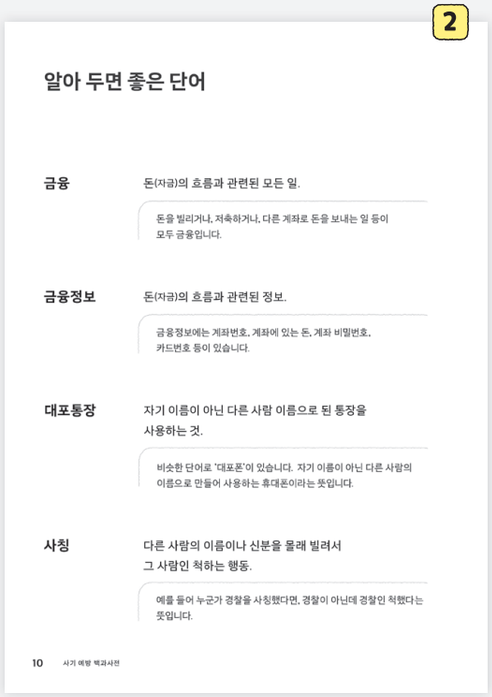


자료에 등장하는 캐릭터들과 친해지기

이 자료에는 금융사기에 대해 알려 주는 3명의 캐릭터가 등장합니다. 각 캐릭터가 어떤 역할을 하는지 먼저 알아보세요. 자료의 내용을 이해하는 데 도움이 됩니다.

→ 8쪽

2



알아 두면 좋은 단어 살펴보기

자료를 읽다 보면 금융사기와 관련된 낯선 단어가 나올 수 있습니다. 자료를 읽기 전에 미리 단어의 뜻을 살펴보면 내용을 훨씬 쉽게 이해할 수 있습니다.

→ 10쪽

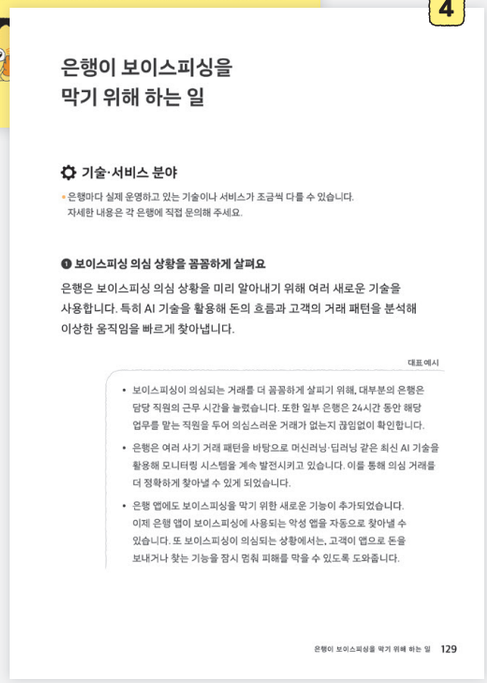
8개의 금융사기에 대해 알아보기

보이스피싱, 스미싱, 투자 사기 등 우리 주변에서 자주 일어나는 8가지 금융사기를 소개합니다. 각 사기의 특징과 예방법, 실제 피해 사례를 함께 살펴보며 금융사기에 대해 배워 보세요.

→ 14쪽부터

3

4



부록으로 마무리하기

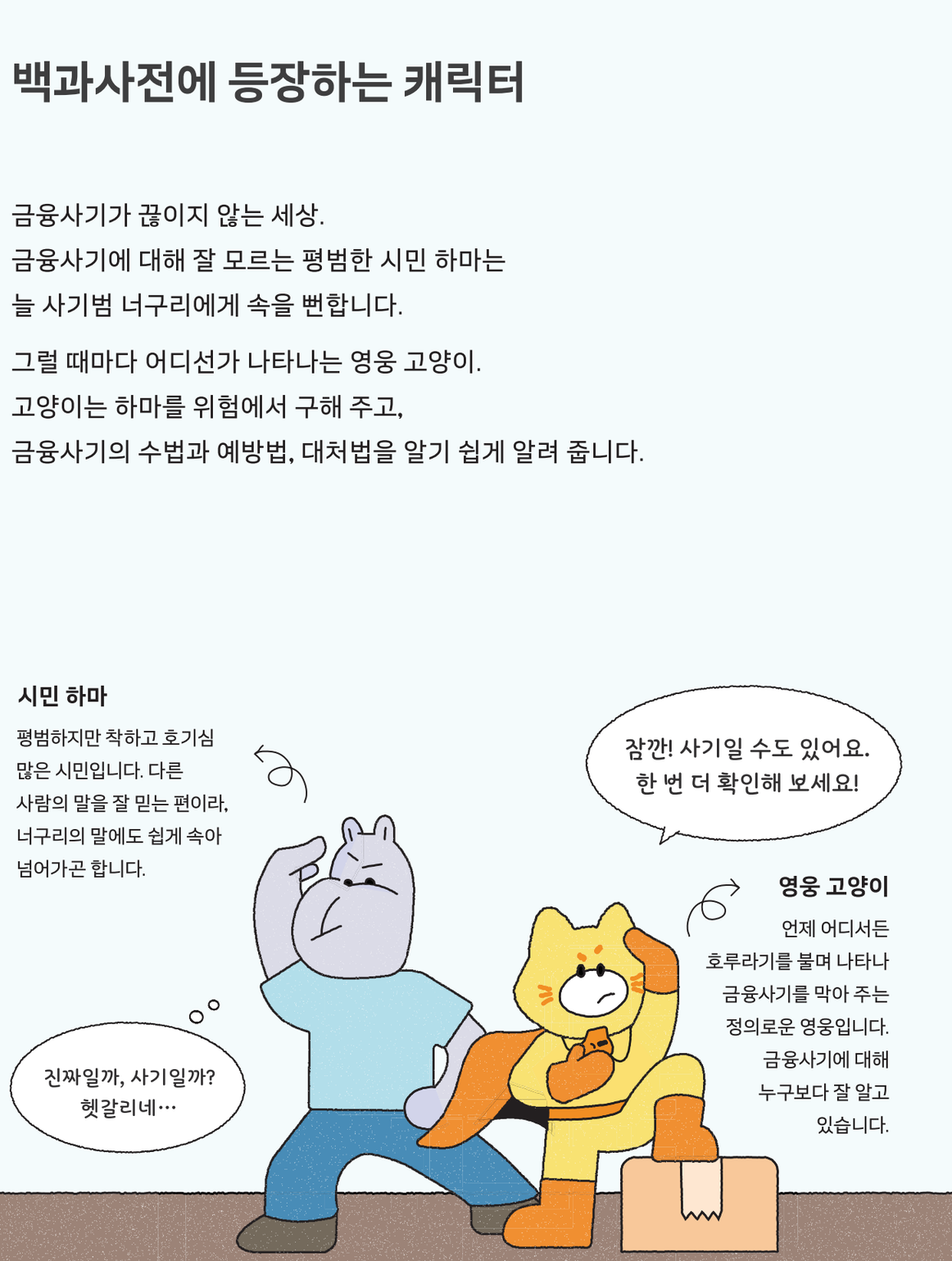
금융사기를 예방하고 피해를 줄이는 데 도움이 되는 정보를 더 알아보세요.

→ 129쪽

백과사전에 등장하는 캐릭터

금융사기가 끊이지 않는 세상.
금융사기에 대해 잘 모르는 평범한 시민 하마는
늘 사기범 너구리에게 속을 뻔합니다.

그럴 때마다 어디선가 나타나는 영웅 고양이.
고양이는 하마를 위험에서 구해 주고,
금융사기의 수법과 예방법, 대처법을 알기 쉽게 알려 줍니다.



시민 하마

평범하지만 착하고 호기심
많은 시민입니다. 다른
사람의 말을 잘 믿는 편이라,
너구리의 말에도 쉽게 속아
넘어가곤 합니다.

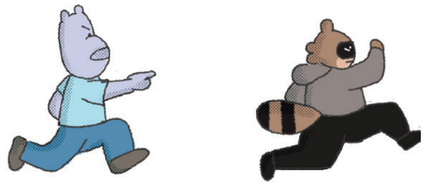
영웅 고양이

언제 어디서든
호루라기를 불며 나타나
금융사기를 막아 주는
정의로운 영웅입니다.
금융사기에 대해
누구보다 잘 알고
있습니다.

사기범 너구리

겉보기엔 친절하지만
실제로는 거짓말로 상대를
속이는 사기범입니다.
달콤한 말로 하마를
속이려 하지만,
항상 고양이에게 들켜
실패하고 맙니다.

알아 두면 좋은 단어



금융 돈(자금)의 흐름과 관련된 모든 일.

돈을 빌리거나, 저축하거나, 다른 계좌로 돈을 보내는 일 등이 모두 금융입니다.

금융정보 돈(자금)의 흐름과 관련된 정보.

금융정보에는 계좌번호, 계좌에 있는 돈, 계좌 비밀번호, 카드번호 등이 있습니다.

대포통장 자기 이름이 아닌 다른 사람 이름으로 된 통장을 사용하는 것.

비슷한 단어로 '대포폰'이 있습니다. 자기 이름이 아닌 다른 사람의 이름으로 만들어 사용하는 휴대폰이라는 뜻입니다.

사칭 다른 사람의 이름이나 신분을 몰래 빌려서 그 사람인 척하는 행동.

예를 들어 누군가 경찰을 사칭했다면, 경찰이 아닌데 경찰인 척했다는 뜻입니다.

수법 어떤 일을 하기 위해 쓰는 방법이나 방식.

예를 들어 '범죄 수법'은 범죄를 저지를 때 사용하는 방법이나 방식을 뜻합니다.

신용등급 돈을 얼마나 잘 갚는 사람인지 보여 주는 평가 체계.

신용등급이 높다면 돈을 제때 잘 갚는 사람이고, 신용등급이 낮다면 돈을 갚지 않고 있거나 늦게 갚은 적이 있는 사람입니다.

유출 밖으로 새어 나가면 안 되는 정보나 물건이 잘못해서 밖으로 새어 나가는 것.

개인정보, 금융정보 등 중요한 정보는 유출되지 않도록 조심해야 합니다.

피싱
Phishing

전화, 문자, 이메일 등 다양한 통신 수단을 활용해 사람들의 돈이나 개인정보, 금융정보를 빼앗는 사기 행위.

개인정보Private data와 낚시Fishing를 합친 말이며, '피싱 사기'라고도 부릅니다.

8가지
금융사기에 대해
알아보아요

“모르는 번호로 전화가 왔어요” — 보이스피싱

“링크 한 번 눌렀을 뿐인데” — 스미싱

“어떤 게 진짜 QR코드일까?” — 큐싱

“사랑하면 돈을 보내 달라고?” — 로맨스 스캠

“싸고 친절해서 믿었는데” — 중고거래 사기

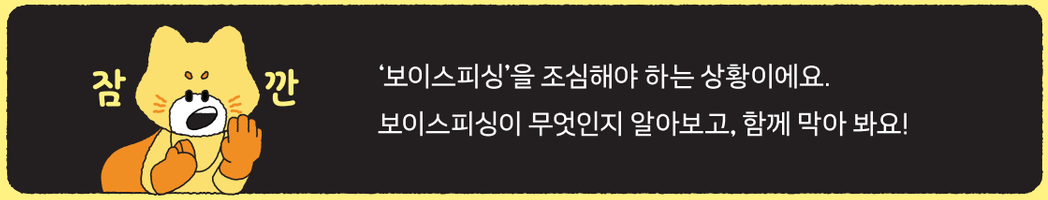
“이자가 끝없이 늘어나요” — 불법사금융

“호기심으로 큰돈을 잃었어요” — 청소년 불법도박

“진짜 좋은 투자 기회라더니” — 투자 사기

"모르는 번호로 전화가 왔어요"

보이스피싱



보이스피싱이란?

보이스피싱은 전화로 다른 사람을 속여서
돈이나 재산을 빼앗는 피싱 사기입니다.

보이스피싱Voice Phishing은 목소리Voice와
피싱Phishing을 합쳐 만든 말입니다.
사기범은 주로 전화로 피해자를 속여 현금을 직접 전달하게 하거나,
계좌이체를 하게 만들어 돈을 빼앗습니다.

보이스피싱 유형으로는 이런 것들이 있어요

보이스피싱 사기범은 주로 불안하게 만드는 말로 사람을 속여
돈을 보내게 합니다. 최근에는 AI(인공지능) 기술이 발전하면서,
딥페이크•로 만든 가짜 음성이나 영상을 이용해
사람들을 속이는 경우도 늘고 있습니다.

• **딥페이크**Deepfake: AI를 이용해 사람의 얼굴이나 목소리를
진짜처럼 바꿔서 만든 가짜 영상이나 음성.

엄마, 난데.
자취방 월세를 내야 하는데 돈이 없어서.
지금 바로 보내 줄 수 있어?

서울중앙지검 ○○○수사관입니다.
당신의 계좌가 범죄에 사용된
사실이 확인되었습니다. 지금 바로 계좌를
옮겨야 하니 안전계좌로 이체해 주세요.

고객님 얼마 전 배송해 드린 택배 배송비를
입금해 주셔야 합니다.
제가 계좌번호 불러 드릴게요.

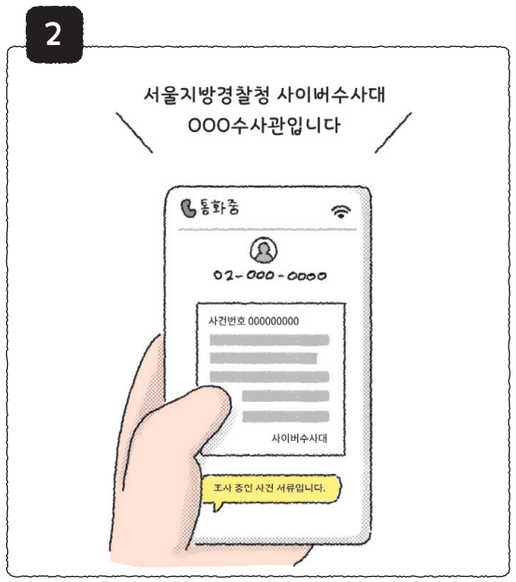
○○은행 고객님,
카드에 오류가 발견되었습니다.
계좌 비밀번호를 알려 주시면 처리해
드리겠습니다.

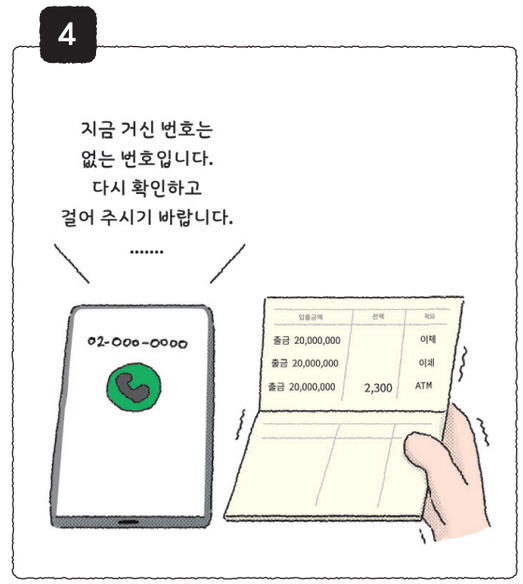
보이스피싱 피해, 현재 이런 상황이에요

보이스피싱 발생 건수(1월~8월 기준)는 2025년 1만 6,765건으로,
2024년 13,443건에 비해 24.7% 늘었습니다.
또한, 같은 기간 피해액은 2025년 8,856억 원으로,
2024년 4,625억 원에 비해 91.5% 늘었습니다.

출처: 경찰청

보이스피싱,
주로 이렇게 일어나요





다른 사람인 척 전화를 걸어요

사기범은 경찰, 은행 직원, 택배 기사처럼 믿을 만한 사람인 척 전화를 겁니다. 가짜 문자를 보내 피해자가 직접 전화를 걸게 만들기도 합니다.

자신의 말을 믿게 해요

사기범은 “서울지방경찰청 사이버수사대 OOO 수사관입니다” 같은 말을 하며 진짜인 것처럼 믿게 만듭니다. 진짜 서류처럼 보이는 가짜 서류를 보여 주며 속이기도 합니다.

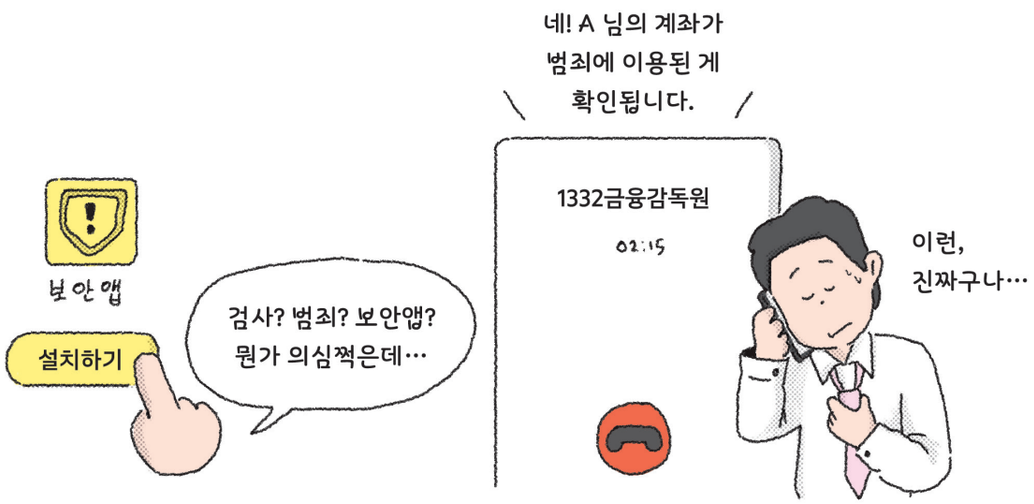
돈이나 개인정보를 요구해요

“정확한 확인을 위해 계좌번호를 알려 주세요”, “안전한 계좌로 돈을 옮겨야 합니다”라고 하며 계좌 비밀번호나 송금을 요구합니다. 개인정보를 빼내가는 악성 앱 링크가 담긴 문자를 보내기도 합니다.

연락을 끊어요

피해자가 돈을 보내는 등 사기범이 원하는 행동을 하면, 사기범은 연락을 끊고 사라집니다.

사례로 알아보는 보이스피싱



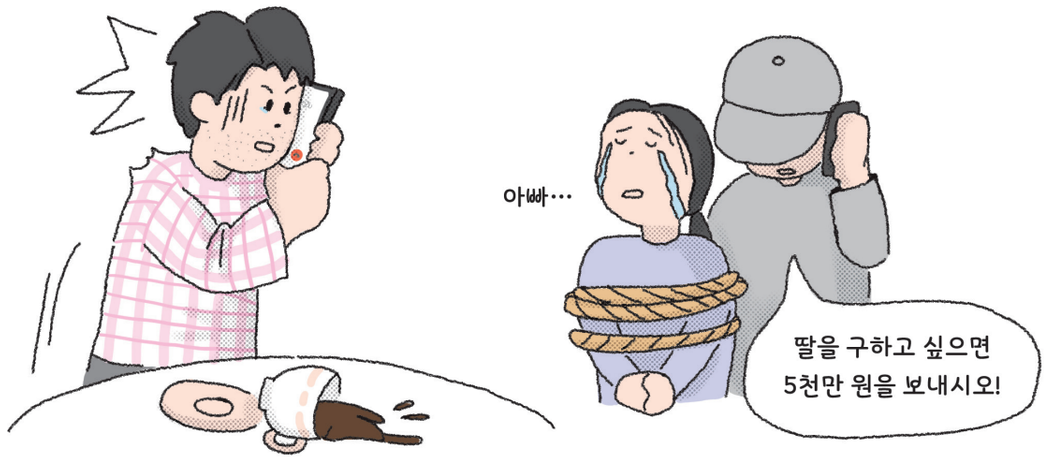
사례 1

“당신의 계좌가 범죄에 이용되었습니다”

직장인 A씨는 어느 날 낯선 전화를 받았습니다. 전화를 건 B씨는 자신을 서울중앙지검 검사라고 소개하며, A씨의 계좌가 범죄에 이용돼서 수사 협조가 필요하다고 말했습니다.

B씨는 보안을 위해 앱을 설치해야 한다며 앱 링크가 담긴 문자를 보냈습니다. 갑작스러운 소식에 놀란 A씨는 B씨의 지시에 따라 앱을 설치했습니다. 이후 불안한 마음에 금융감독원에 직접 전화를 걸어 확인했지만, “계좌가 실제로 범죄에 사용됐다”는 답을 들었습니다. 그러나 그 전화도 가짜였습니다. B씨가 설치하게 만든 앱은 경찰, 검찰, 금융감독원 등 어디로 전화를 걸어도 실제 기관이 아닌 범죄 조직으로 연결되도록 조작된 악성 앱이었던 것입니다.

그렇게 A씨는 한 달 가까이 사기범의 지시에 따라 움직였고, 결국 전 재산은 물론 대출까지 받아 약 40억 원을 범죄 조직에 송금했습니다. 모든 일이 끝난 뒤에야 A씨는 자신이 보이스피싱에 속았다는 사실을 깨달았습니다.



사례 2

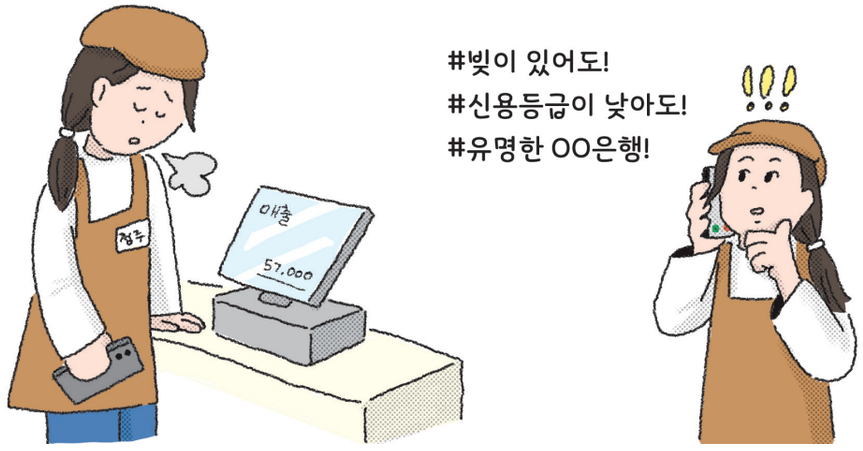
“아빠, 나 지금 납치당했어…”

평화로운 주말을 보내던 C씨는 딸의 번호로 걸려 온 전화를 받았습니다. 반가운 마음도 잠시, 전화 너머로 들리는 딸의 울먹이는 목소리에 가슴이 철렁 내려앉았습니다.

딸은 다급한 목소리로 말했습니다. “아빠, 나 납치당한 것 같아…” 놀란 C씨가 “너 지금 어디야?”라고 묻자, 낯선 목소리가 들려왔습니다. “지금 바로 5천만 원을 보내 주시면 따님을 무사히 집으로 돌려보내 드리겠습니다.”

큰 충격을 받은 C씨는 급히 은행으로 향하려 했습니다. 그런데 평소와 다르게 아주 불안해 보이는 남편의 모습을 이상하게 여긴 아내가 즉시 경찰에 신고했습니다.

곧바로 출동한 경찰은 보이스피싱을 의심하고 C씨의 송금을 막았습니다. 확인 결과, 딸의 목소리는 실제가 아닌 범죄 조직이 AI로 만든 가짜 음성이었습니다. 딸의 목소리와 똑같이 만들어진 그 음성에, C씨는 순식간에 속아 넘어갈 뻔했습니다.



#빚이 있어도!
#신용등급이 낮아도!
#유명한 OO은행!

사례 3

“돈이 필요하신가요? 제가 해결해 드릴게요”

D씨는 생활비 때문에 1천만 원의 빚을 지고 있었습니다. 매달 15%가 넘는 이자를 감당하며 힘든 나날을 보내던 중, **“마이너스 통장**•을 만들어 드립니다”라는 전화를 받았습니다.

전화를 건 사람은 자신을 OO은행 직원 E씨라고 소개했습니다. 그는 “빚이 있는 분들도 신용등급을 조금만 올리면 마이너스 통장을 만들 수 있다”며 D씨를 설득했습니다. 며칠 뒤, E씨는 ‘특별한 방법’이라며 새로운 제안을 했습니다. “알고 있는 대출 업체에서 대출을 받은 뒤 바로 갚으면 신용등급이 오른다”는 것이었습니다.

D씨는 의심스러웠지만, 대출 업체가 유명한 곳이라 안심하고 900만 원을 대출받았습니다. 며칠 후 E씨는 “일주일 뒤 제가 알려 드리는 계좌로 돈을 보내면 신용등급이 오른다”고 말했고, D씨는 그의 지시에 따라 돈을 이체했습니다. 그러나 그 계좌는 대포통장이었고, E씨는 보이스피싱 사기범이었습니다. D씨는 뒤늦게 경찰에 신고했지만, 이미 돈은 사라진 뒤였습니다.

• **마이너스 통장**: 정해진 금액 안에서, 필요할 때마다 돈을 빌려 쓸 수 있는 통장.

사례 4

“세금 납부 확인 부탁드립니다”

F씨는 “해외에서 주문하신 물건이 공항에 도착하여 세금 49만 원이 오늘 오후 6시에 자동이체됩니다”라는 내용의 문자를 받았습니다. 해외에서 물건을 주문한 적이 없던 F씨는 이상하게 생각하고 문자에 적힌 번호로 전화를 걸었습니다.

“해외에서 주문한 적이 없는데 무슨 세금이냐”고 묻자, 상대방은 자신을 세관 직원이라고 소개하며 ‘세금 납부확인증’이라는 서류를 보내 왔습니다. F씨는 그럴듯한 문서를 보고 잠시 안심했지만, 곧 휴대폰 화면에 **‘원격 제어**• 중’이라는 표시가 떠 있는 것을 발견했습니다.

이상하다고 느낀 F씨는 바로 전화를 끊고, 인터넷에서 **세관**•• 전화번호를 찾아 직접 걸었습니다. 확인해 보니, 아까 통화한 세관 직원은 가짜였고, 그때 휴대폰이 해킹될 뻔한 것이었습니다. 다행히 F씨가 빨리 전화를 끊은 덕분에, 개인정보가 새어 나가는 것을 막을 수 있었습니다.

• **원격 제어**: 멀리 떨어진 곳에 있는 사람이 다른 사람의 컴퓨터나 휴대폰에 접속해서 기능을 조종하는 것.

•• **세관**: 해외에서 들어오거나 나가는 물건을 검사하고 세금을 매기는 기관.

이럴 때 보이스피싱을 의심해 보세요

아래 내용 중 1개라도 해당된다면 **보이스피싱**일 수 있습니다.
보이스피싱이 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

모르는 번호로 전화나 문자가 왔어요.

모르는 번호로 연락이 온다면 먼저 의심하세요. 특히 내가 하지도 않은 일에 대한 내용이라면 바로 믿지 마세요. 반드시 공식 기관이나 회사의 대표 번호로 직접 확인해 보세요.

정부, 공공기관, 은행, 금융회사라며 전화가 왔어요.

정부, 공공기관, 은행, 금융회사 같은 곳들은 전화로 수사나 송금 요청을 절대 하지 않습니다. 실제 직원이 맞는지 반드시 확인해 보아야 합니다.

가족이 납치되었다는 전화가 왔어요.

가족의 목소리를 들려주거나, 얼굴이 나온 영상을 보여 줘도 바로 믿지 마세요. 딥페이크로 만든 가짜 음성이나 영상일 수도 있습니다.
먼저 가족에게 직접 전화해 안전을 확인하고, 연락이 닿지 않는다면 즉시 경찰에 신고하세요.

**전화를 끊지 못하게 하거나,
다른 사람에게 알리지 말라고 해요.**

다른 사람에게 들키면 안 되는 일이기 때문입니다. 이런 말을 들으면 바로 통화를 끊고, 가족이나 경찰처럼 믿을 수 있는 사람에게 알리세요.

**영상 통화를 하자고 하거나, 직접 만나자고 하면
계속 이유를 대며 피해요.**

실제 모습을 정직하게 드러낼 수 없기 때문입니다. 또, 실제 얼굴을 보여 줬다고 해도 가짜로 꾸며 낸 것일 수도 있으니 무조건 믿어서는 안 됩니다.

낯선 사이트에 들어가거나 앱을 설치하라고 해요.

낯선 사이트나 앱에는 개인정보나 돈을 빼가는 악성 프로그램이 숨어 있을 수 있습니다. 사이트 이름을 먼저 검색해 보고, 앱은 꼭 공식 앱 스토어(구글 플레이, 앱스토어)에서만 설치하세요.

내 개인정보나 금융정보를 알려 달라고 해요.

정부, 공공기관, 은행 등은 전화로 주민등록번호나 계좌번호, 비밀번호 같은 개인정보나 금융정보를 절대 요구하지 않습니다.

보이스피싱, 이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

보이스피싱 피해를 입었다면, 바로 신고하세요

돈이나 개인정보를 빼앗겼거나, 가족 등 주변 사람이 위험한 것 같다면 바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)
- 금융감독원: 1332 fss.or.kr (금융 피해 구제, 지급 정지 문의)
- 불법스팸대응센터(KISA): 118 spam.kisa.or.kr (스미싱 URL·스팸 차단)

금융정보를 보호하세요

내 금융정보가 새어 나간 것 같다면, 돈이 빠져나가는 것을 막기 위해 계좌를 즉시 정지해야 합니다. 이때 아래 방법을 사용할 수 있습니다.

- 은행 등 해당 금융회사에 연락하여 계좌를 지급정지하고, '오픈뱅킹·여신거래·비대면 계좌개설 안심차단 서비스' 신청하기
- '계좌정보통합관리서비스(payinfo.or.kr)'에 접속해서 직접 지급정지 신청하기
- '개인정보노출자 사고예방시스템(pd.fss.or.kr)'에 접속해서 개인정보가 유출되었는지 확인하고, 추가 계좌 개설을 막기

악성 앱을 즉시 삭제하세요

악성 앱이 설치된 것 같다면, 가장 먼저 휴대폰을 비행기 모드로 전환해 통신을 끊고 악성 앱을 삭제하세요. 이렇게 하면 사기범이 휴대폰에 접근해서 내 정보를 빼앗아 가는 것을 막을 수 있습니다.

낯선 전화를 받았는데, 보이스피싱인지 아닌지 잘 모르겠을 때는 어떻게 해야 되나요?

혼자 판단하기 어렵다면 주변 사람에게 물어보세요. 다른 사람이 함께 들어보면 의심스러운 부분을 더 잘 알아차릴 수 있습니다. 또는 인터넷에 전화 내용이나 번호를 검색해 보세요. 비슷한 보이스피싱 사례가 이미 올라와 있을 수도 있습니다.

검찰수사관이라며 전화가 왔어요. 상대방의 신분이나 관련 서류가 진짜인지 확인하려면 어떻게 해야 하나요?

대검찰청에서 운영하는 '찐센터(보이스피싱 서류 진짜인지 알려줘 콜센터)'에 연락해 보세요. '찐센터'는 보이스피싱 사기범이 검찰을 사칭할 경우, 사기범이 사칭한 사람이나 보내 준 서류가 진짜인지 확인해 주는 콜센터입니다. 1301 010-3570-8242 로 전화하거나, 카카오톡 채널로 채팅을 보내 연락할 수 있습니다.

찐센터 바로가기

- 보이스피싱은 '전화로 사람을 속여 돈이나 개인정보를 빼앗는 피싱 사기'입니다.
- 사기범은 주로 공공기관, 은행, 가족, 지인 등을 사칭해 피해자를 불안하게 하거나 믿게 합니다. 만약 낯선 전화에서 "지금 바로 처리해야 한다", "비밀로 해 달라"는 말이 나온다면, 보이스피싱일 가능성이 매우 높습니다.
- 최근에는 딥페이크로 가짜 음성이나 영상을 만들어 더욱 진짜인 것처럼 속이기도 합니다.
- 보이스피싱에 당해서 돈이나 개인정보를 빼앗긴 것 같다면, 즉시 경찰에 신고해야 합니다. 사기범과의 대화 내용, 사기범의 계좌번호 등은 모두 기록해서 증거로 남겨 놓으세요.

이제 아무 전화나 믿으면 안 되겠어요.
진짜 같아도 꼭 제대로 확인해 보아야겠네요!

"링크 한 번 눌렀을 뿐인데"

스미싱

'스미싱'을 조심해야 하는 상황이에요.
스미싱이 무엇인지 알아보고, 함께 막아 봐요!

스미싱이란?

스미싱은 문자 속 링크를 눌러 가짜 사이트에 접속하게 하거나,
악성 앱을 설치하게 만들어 돈이나 개인정보를 빼앗는 피싱 사기입니다.

스미싱Smishing은 문자메시지SMS와 피싱Phishing을
합쳐서 만든 말입니다. 사기범은 실제 회사나 기관에서 보낸
문자처럼 꾸며 피해자가 링크를 누르게 만듭니다.

스미싱 문자 유형으로는 이런 것들이 있어요

스미싱 문자는 주로 택배 배송, 카드 배송,
이벤트 당첨 같은 내용을 담고 있습니다.

최근에는 청첩장, **부고**•뿐만 아니라 공공기관을 사칭하는
문자까지 등장해 수법이 점점 다양해지고 있습니다.

• **부고**: 사람이 죽었다는 소식을 알리는 것.

[oo마트]
명절 선물로 모바일 상품권이
도착했습니다. 링크를 통해
확인해 보시기 바랍니다.
http://gift.joa

[web 발신] 배송불가. 주소 불일치.
앱 다운 후 배송 주소지 확인 및
변경해 주시기 바랍니다.
http://bit.y/download.aba

[교통민원24]
도로교통법 위반으로 과태료
고지서가 전달되었습니다.
위반 사실 확인
http://car_money

[국세청]
연말정산 내역, 신용카드 소득
공제용 사용 내역, 환급 내역 등
조회 안내
http://yearend1234

[건강보험공단]
25년 건강검진 대상자 안내 지난
검진 내역 보기, 건강검진 병원
조회하기 >> http://abcdef_ab

[web 발신]
새해 희망 정부지원금 지급
신청 선착순 실시.
신청 기간(2025년 1월 ~)
http://come_on_25

스미싱 피해, 현재 이런 상황이에요

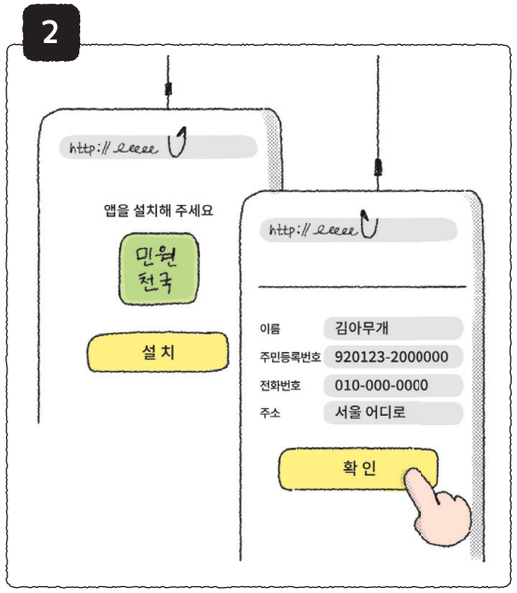
스미싱 발생 건수(1월~12월 기준)는 2024년 4,396건으로,
2020년 822건에 비해 약 5배 늘었습니다.
또한, 같은 기간 피해액은 2024년 546억 원으로,
2020년 11억 원에 비해 약 50배 늘었습니다.

출처: 형사사법정보시스템(KICS)

스미싱,
주로 이렇게 일어나요

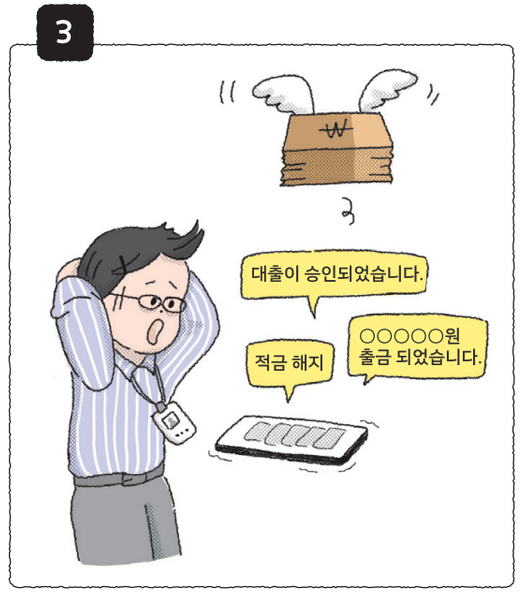
가짜 링크가 담긴 메시지를 보내요

주로 바로 확인해야 할 것 같은 내용을 담아 가짜 링크가 담긴 문자를 보냅니다. 정부, 공공기관, 은행 등인 것처럼 속여서 관심을 끌 때도 있습니다.



링크를 누르면 낯선 사이트나 앱 설치 화면으로 연결돼요

기존 사이트나 앱과 비슷하게 생긴 가짜 사이트나 앱으로 연결되기도 합니다.



돈이나 개인정보를 빼가요

낯선 사이트에 들어가거나 앱을 설치하면 나도 모르게 악성 프로그램이 깔려서 개인정보가 새어 나갈 수 있습니다. 또는 개인정보를 입력하게 만들어 그 정보를 이용해 돈을 빼내기도 합니다.

사례로 알아보는 스미싱

사례 1

“배송 조회는 아래 링크를 눌러 주세요”

온라인 쇼핑을 자주 하던 A씨는 어느 날, ‘물품 배송을 시작했습니다. 확인 부탁드립니다’라는 문자를 받았습니다. 문자 안에는 어떤 링크가 있었고, A씨는 택배 배송 현황을 확인할 수 있는 링크라고 생각했습니다.

기다리던 택배가 어디쯤 왔는지 궁금했던 A씨는 바로 링크를 눌렀습니다. 하지만 그 문자는 가짜였습니다. 링크를 누른 순간 A씨의 휴대폰에는 악성 앱이 자동으로 설치됐고, 사기범은 이 앱을 통해 A씨의 개인정보를 빼내 그의 이름으로 대출을 받았습니다. 결국 A씨는 자신도 모르는 사이 2억 1천만 원을 사기범에게 빼앗기고 말았습니다.

사례 2

“띠링- 모바일 청첩장이 도착했습니다”

B씨는 최근 지인에게서 결혼식 모바일 청첩장을 받았습니다. 평소에도 이런 청첩장을 자주 받아서 별다른 의심 없이 문자 속 링크를 눌렀습니다. 화면에는 예쁜 결혼식 사진과 안내 문구가 보였고, B씨는 자연스럽게 축하 메시지를 남기려 했습니다.

그런데 그 순간, B씨의 스마트폰에 정체를 알 수 없는 앱이 설치되었습니다. 처음에는 아무 일도 일어나지 않아 그냥 넘겼지만, 며칠 뒤 금융기관에서 대출이 완료되었다는 문자가 도착했습니다. 놀란 B씨가 확인해 보니 3곳의 금융기관에서 약 1억 원이 빠져나간 상태였습니다.

알고 보니 청첩장 링크를 눌렀을 때 악성 앱이 설치되면서 B씨의 개인정보와 금융정보가 범죄 조직에 넘어간 것이었습니다. B씨는 사건이 일어난 지 4일 뒤에야 피해 사실을 알고 경찰에 신고했지만, 이미 대부분의 돈은 해외로 송금된 뒤였습니다.

이럴 때 스미싱을 의심해 보세요

아래 내용 중 1개라도 해당된다면 **스미싱**일 수 있습니다.
스미싱이 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

모르는 번호로 문자가 왔어요.

택배 배송이나 이벤트 당첨 같은 문자를 받았는데 보낸 사람을 모른다면, 바로 믿지 마세요. 택배 회사나 이벤트를 진행한 곳의 공식 번호로 직접 전화해 확인해 보세요.

문자 링크가 이상해요.

링크에 이상한 기호나 낯선 글자가 섞여 있다면 클릭하지 마세요. 클릭하기 전에 반드시 문자 속 링크와 공식 기관의 링크가 같은지 확인해 보세요.

문자 링크를 “지금 바로”, “빨리” 클릭하라고 해요.

“지금 눌러야 혜택을 받습니다”, “빨리 확인하세요” 같은 말이 있으면 주의하세요. 마음을 급하게 만들어서 링크를 누르게 하려는 수법일 수 있습니다.

내 개인정보나 금융정보를 알려 달라고 해요.

정부, 공공기관, 은행 등은 문자로 주민등록번호나 계좌번호, 비밀번호 같은 개인정보나 금융정보를 절대 요구하지 않습니다. 이런 문자가 오면 바로 삭제하세요.

낯선 사이트에 들어가거나 앱을 설치하라고 해요.

낯선 사이트나 앱에는 개인정보나 돈을 빼내가는 악성 프로그램이 숨어 있을 수 있습니다. 사이트 이름을 먼저 검색해 보고, 앱은 꼭 공식 앱 스토어(구글 플레이, 앱스토어)에서만 설치하세요.

스미싱이 의심될 때는 보호나라의 스미싱 확인 서비스를 이용해 보세요.

보호나라는 한국인터넷진흥원이 운영하는 정보보호 사이트입니다.
보호나라의 **스미싱 확인 서비스**를 이용하면 스미싱이 의심되는 링크를 검색해 보고 사기 링크인지 아닌지 알 수 있습니다. 아래 방법에 따라 서비스를 이용할 수 있습니다.

1. **카카오톡**에 보호나라 채널 검색 및 추가
2. 채팅창에서 개인 서비스 클릭
3. 스미싱 확인 서비스 클릭
4. 채팅창에 스미싱 의심 링크 입력
5. 결과 확인

보호나라 바로가기

스미싱,
이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

스미싱 피해를 입었다면, 바로 신고하세요

돈이나 개인정보를 빼앗긴 것 같다면 망설이지 말고
바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)
- 금융감독원: 1332 fss.or.kr (금융 피해 구제, 지급 정지 문의)
- 불법스팸대응센터(KISA): 118 spam.kisa.or.kr (스미싱 URL·스팸 차단)

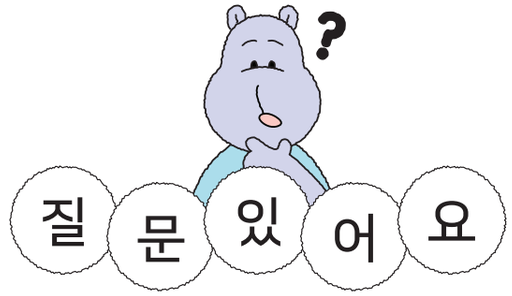
금융정보를 보호하세요

내 금융정보가 새어 나간 것 같다면, 돈이 빠져나가는 것을 막기 위해 계좌를 즉시 정지해야 합니다. 이때 아래 방법을 사용할 수 있습니다.

- 은행 등 해당 금융회사에 연락하여 계좌를 지급정지하고, '오픈뱅킹·여신거래·비대면 계좌개설 안심차단 서비스' 신청하기
- '계좌정보통합관리서비스(payinfo.or.kr)'에 접속해서 직접 지급정지 신청하기
- '개인정보노출자 사고예방시스템(pd.fss.or.kr)'에 접속해서 개인정보가 유출되었는지 확인하고, 추가 계좌 개설을 막기

악성 앱을 즉시 삭제하세요

악성 앱이 설치된 것 같다면, 가장 먼저 휴대폰을 비행기 모드로 전환해 통신을 끊고 악성 앱을 삭제하세요. 이렇게 하면 사기범이 휴대폰에 접근하거나 내 정보를 빼가는 걸 막을 수 있습니다.



스미싱으로 잃은 돈을 되찾을 수 있나요?

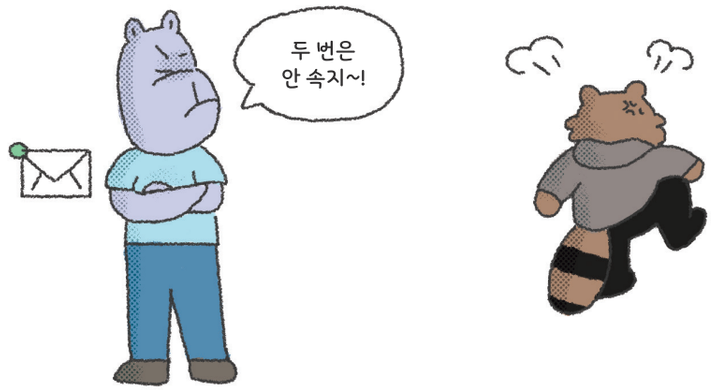
스미싱 같은 피싱 범죄로 잃은 돈을 되찾는 것은 매우 어렵습니다. 범죄 조직 대부분이 해외에 있어 사기범을 잡거나 돈을 빼돌린 곳을 알아 내기 힘들기 때문입니다. 그렇기 때문에 더욱 피해가 심각한 범죄라고 볼 수 있습니다.

스미싱 문자가 오면 삭제만 하면 되나요?

스미싱 문자를 받으면 꼭 신고한 다음, 삭제하세요. 만약 같은 번호에서 계속 스미싱 문자가 온다면 그 번호를 차단해 두는 것이 좋습니다. 가족이나 친구, 이웃에게도 알려 두면 추가 피해를 막는 데 도움이 됩니다.

- 스미싱은 '문자 속 링크를 눌러 가짜 사이트에 접속하게 하거나, 악성 앱을 설치하게 만들어 개인정보를 빼내는 피싱 사기'입니다.
- 문자 속 스미싱 링크는 진짜 링크와 비슷하게 생겼지만, 공식 링크와 글자가 다르거나 이상한 글자가 섞여 있기도 합니다. 이럴 경우에는 클릭하지 마세요.
- 스미싱에 당해서 악성 앱이 설치된 것 같다면, 즉시 삭제하세요. 그리고 금융정보가 새어 나간 것 같다면, 돈이 빠져나가는 것을 막기 위해 계좌를 즉시 정지해야 합니다.
- 스미싱에 당해서 돈이나 개인정보를 빼앗긴 것 같다면, 즉시 경찰에 신고해야 합니다. 사기 문자나 링크 등은 모두 저장해서 증거로 남겨 놓으세요.

평범한 문자처럼 보여도 속에 함정이 숨어 있을 수도 있겠네요. 이제는 문자 속 링크를 누르기 전에 꼭 한 번 더 확인할 거예요.



“어떤 게 진짜 QR코드일까?”

큐싱

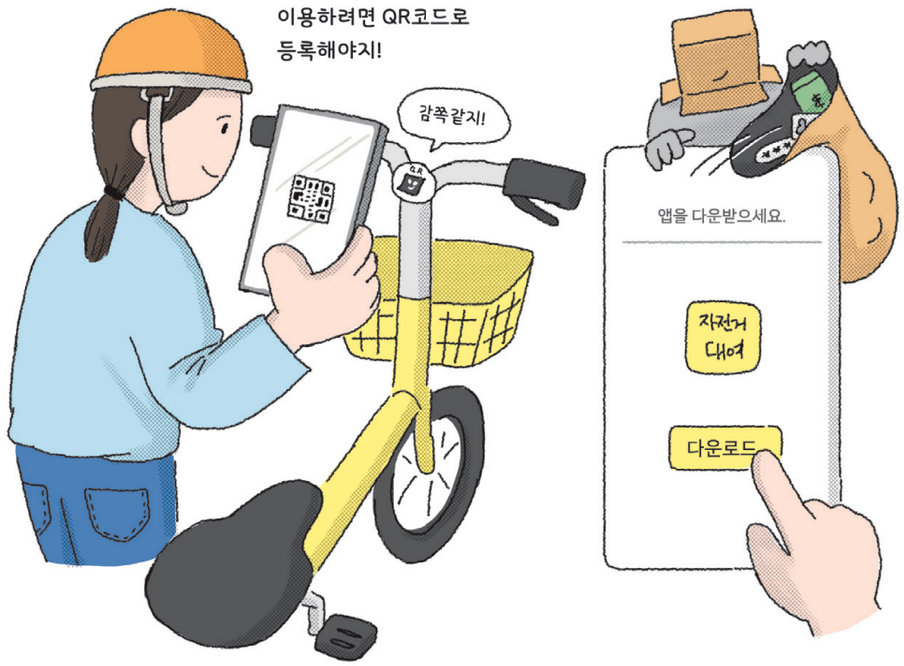
잠깐

‘큐싱’을 조심해야 하는 상황이에요.
큐싱이 무엇인지 알아보고, 함께 막아 봐요!

큐싱이란?

큐싱은 QR코드를 이용해 가짜 사이트로 연결시키거나,
악성 앱을 설치하게 만들어 돈이나 개인정보를 빼앗는 피싱 사기입니다.

큐싱Qshing은 QR코드QR와 피싱Phishing을
합쳐 만든 말입니다. 사기범은 가짜 QR코드를 붙이거나
이미지로 보내 피해자가 QR코드를 스캔하게 만듭니다.



큐싱 유형으로는 이런 것들이 있어요

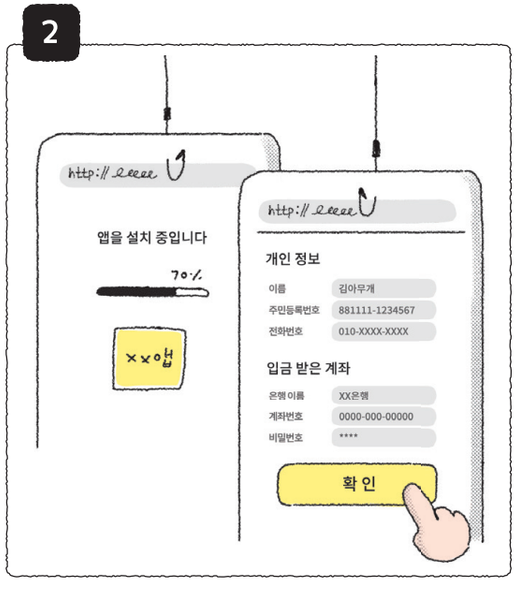
큐싱은 QR코드를 사용하는 곳이라면 어디서든
일어날 수 있습니다. 최근에는 자전거를 빌릴 때,
식당에서 메뉴를 볼 때, 주차 요금을 낼 때 등 일상생활 속
다양한 상황에서 가짜 QR코드로 사람들을 속이는 사례가
늘어나고 있습니다.

일상 속 QR코드 활용 사례

큐싱 피해, 현재 이런 상황이에요

큐싱은 새롭게 등장한 금융사기 수법이라 아직 공식적인
피해 통계는 나오지 않았습니다. 하지만 보이스피싱이나 스미싱 같은
피싱 사기와 함께 계속해서 피해 사례가 늘어나고 있습니다.

큐싱,
주로 이렇게 일어나요



진짜 QR코드를 가짜 QR코드로 바꾸어 놓아요

안내문, 전단지 등 QR코드가 있는 자리에 가짜 QR코드를 붙여 놓습니다. 온라인에 있는 QR코드라면 QR코드 이미지 자체를 가짜 QR코드로 바꾸어 놓기도 합니다.

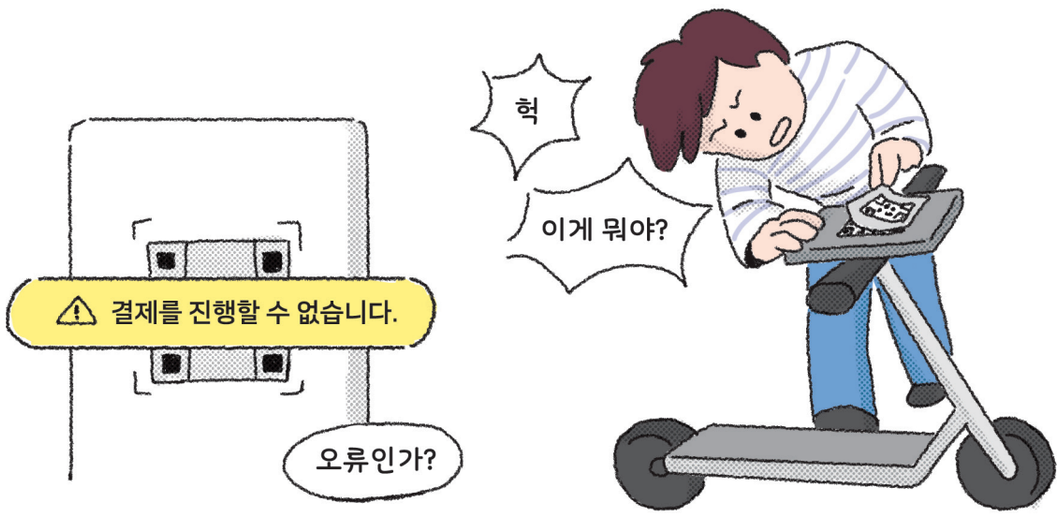
QR코드를 스캔하면 낯선 사이트나 앱 설치 화면으로 연결돼요

기존 사이트나 앱과 비슷하게 생긴 가짜 사이트나 앱으로 연결되기도 합니다.

돈이나 개인정보를 빼가요

낯선 사이트에 들어가거나 앱을 설치하면 나도 모르게 악성 프로그램이 깔려서 개인정보가 새어 나갈 수 있습니다. 또는 개인정보를 입력하게 만들어 그 정보를 이용해 돈을 빼내 가기도 합니다.

사례로 알아보는 큐싱

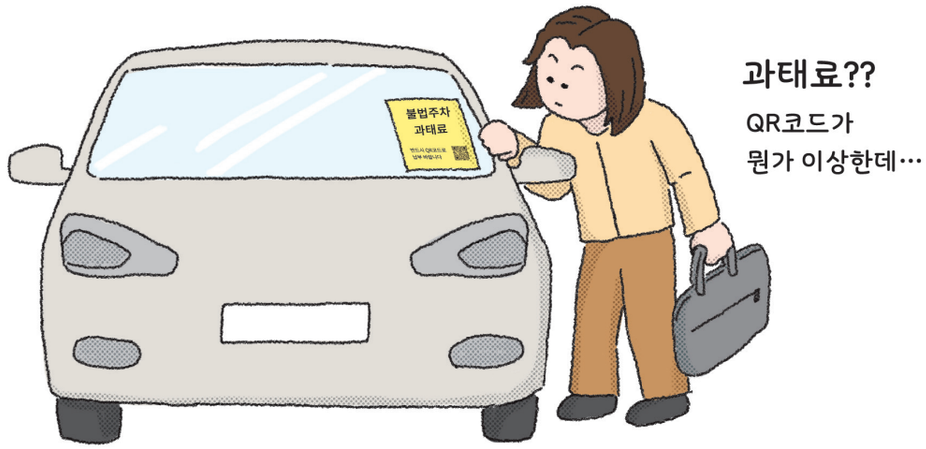


사례 1

“전동킥보드 이용하려면 QR코드를 스캔하세요”

A씨는 지난달 전동킥보드를 이용하기 위해 스마트폰으로 QR코드를 찍었습니다. 결제를 진행하려 했지만 화면에는 “결제를 진행할 수 없습니다”라는 문구가 떴습니다. 단순한 오류라고 생각한 A씨는 다시 QR코드를 살펴보다가 이상한 점을 발견했습니다. QR코드 위에 아주 얇고 비슷한 모양의 스티커가 덧붙여져 있었던 것입니다.

A씨는 결제를 멈추고 스티커를 조심스럽게 떼어 냈습니다. 그 아래에는 진짜 전동킥보드 대여용 QR코드가 있었습니다. 그 QR코드를 스캔하자 이번에는 결제가 제대로 이루어졌습니다.



사례 2

“불법주차하셨습니다. 과태료를 납부해 주세요”

B씨는 아파트 주차장에서 자신의 자동차 유리에 붙은 경고장을 발견했습니다. 종이에 적힌 문구는 평소 단지에서 보던 불법주차 경고장과 거의 똑같았습니다. 그런데 맨 아래에는 ‘관리사무소장’의 이름이 있었고, 옆에는 “반드시 QR코드로 납부 바랍니다”라는 안내 문구가 또렷하게 적혀 있었습니다.

불법주차를 한 기억이 없던 B씨는 잠시 혼란스러웠습니다. ‘혹시 나도 모르게 잘못 주차했나?’ 싶어 휴대폰으로 QR코드를 스캔하려던 순간, 왠지 모르게 이상한 느낌이 들어 손을 멈췄습니다. QR코드 주변의 인쇄 상태가 흐릿하고, 어딘가 어색해 보였던 것입니다.

B씨는 혹시나 하는 마음에 관리사무소에 전화를 걸었습니다. 관리사무소에서는 “B씨는 불법주차를 한 적이 없다”고 말했습니다. 그제야 B씨는 자신이 속을 뻔했다는 사실을 깨달았습니다. 자동차 유리에 붙은 경고장은 진짜처럼 보였지만, 사실은 돈을 빼내기 위한 가짜 경고장이었습니다.

이럴 때 큐싱을 의심해 보세요

아래 내용 중 1개라도 해당된다면 **큐싱**일 수 있습니다.
큐싱이 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

QR코드를 스티커로 붙여 놓은 것 같아요.

누군가 진짜 QR코드 위에 가짜 코드를 붙였을 수도 있습니다. 이럴 땐 바로 스캔하지 말고, 스티커를 떼어내서 아래에 다른 QR코드가 있는지 확인해 보세요. 만약 다른 코드가 있다면 두 코드를 비교해 보고, 수상하면 절대 스캔하지 마세요.

QR코드가 선명하지 않고 모양이 어딘가 어색해 보여요.

글자나 테두리가 흐리거나 잘 보이지 않는다면 가짜 QR코드일 수 있습니다. 조금이라도 이상하면 스캔하지 말고, 올바른 QR코드인지 해당 기관이나 업체에 직접 확인하세요.

QR코드를 스캔했더니 이상한 링크로 연결돼요.

링크에 숫자나 글자가 뒤섞여 있고, 공식 사이트 링크와 다르다면 가짜 사이트일 수 있습니다.

QR코드를 스캔했더니 내 개인정보나 금융정보를 입력하라고 해요.

정부, 공공기관, 은행 등은 주민등록번호나 계좌번호, 비밀번호 같은 개인정보나 금융정보를 절대 요구하지 않습니다. 이런 화면이 뜨면 바로 사이트나 앱을 닫고, 삭제하세요.

QR코드를 스캔했더니 낯선 사이트로 이동하거나 앱을 설치하라고 해요.

낯선 사이트나 앱에는 개인정보나 돈을 빼내가는 악성 프로그램이 숨어 있을 수 있습니다. 사이트 이름을 먼저 검색해 보고, 앱은 꼭 공식 앱 스토어(구글 플레이, 앱스토어)에서만 설치하세요.

여기서 잠깐

큐싱이 의심될 때는 보호나라의 스미싱 확인 서비스를 이용해 보세요.

보호나라는 한국인터넷진흥원이 운영하는 정보보호 사이트입니다.
보호나라의 **큐싱 확인 서비스**를 이용하면 큐싱이 의심되는 QR코드를 검색해 보고 가짜 QR코드인지 아닌지 알 수 있습니다.
아래 방법에 따라 서비스를 이용할 수 있습니다.

1. **카카오톡**에 보호나라 채널 검색 및 추가
2. 채팅창에서 개인 서비스 클릭
3. 큐싱 클릭
4. QR코드 스캔 버튼을 누르고 QR코드 스캔
5. 결과 확인

보호나라 바로가기

큐싱
이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

큐싱 피해를 입었다면, 바로 신고하세요

돈이나 개인정보를 빼앗긴 것 같다면 망설이지 말고
바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)
- 금융감독원: 1332 fss.or.kr (금융 피해 구제, 지급 정지 문의)

금융정보를 보호하세요

내 금융정보가 새어 나간 것 같다면, 돈이 빠져나가는 것을 막기 위해
계좌를 즉시 정지해야 합니다. 이때 아래 방법을 사용할 수 있습니다.

- 은행 등 해당 금융회사에 연락하여 계좌를 지급정지하고,
  '오픈뱅킹·여신거래·비대면 계좌개설 안심차단 서비스' 신청하기
- '계좌정보통합관리서비스(payinfo.or.kr)'에 접속해서
  직접 지급정지 신청하기
- '개인정보노출자 사고예방시스템(pd.fss.or.kr)'에 접속해서
  개인정보가 유출되었는지 확인하고, 추가 계좌 개설을 막기

악성 앱을 즉시 삭제하세요

악성 앱이 설치된 것 같다면, 가장 먼저 휴대폰을 비행기 모드로 전환해
통신을 끊고 악성 앱을 삭제하세요. 이렇게 하면 사기범이 휴대폰에
접근하거나 내 정보를 빼가는 걸 막을 수 있습니다.

공공기관이라며 QR코드를 스캔하라고 하는데 믿어도 되나요?

공공기관은 문자나 채팅으로 QR코드를 보내서 스캔하라고 하지 않습니다. 만약 이런 메시지를 받았다면 대부분 큐싱일 가능성이 높습니다. 이런 경우에는 QR코드를 절대 스캔하지 마시고, 해당 기관의 공식 대표번호로 직접 전화해서 진짜인지 확인해 보세요.

가짜 QR코드를 스캔하면 자동으로 내 개인정보가 빠져나가나요?

그렇지는 않습니다. 하지만 스캔한 뒤에 연결된 화면에서 이름이나 전화번호 같은 개인정보를 입력하라고 하거나, 악성 앱을 설치하라고 하면 매우 위험합니다. 스캔한 후에 이상한 화면이 나오면 바로 그 화면을 닫으세요.

- 큐싱은 ‘QR코드를 이용해 가짜 사이트로 연결시키거나,
  악성 앱을 설치하게 만들어 개인정보를 빼내는 피싱 사기’입니다.
- 진짜 QR코드와 가짜 QR코드는 비슷하게 생겨서 겉보기에
  구별하기 어렵습니다.
- 큐싱에 당해서 악성 앱이 설치된 것 같다면, 즉시 삭제하세요.
  그리고 금융정보가 새어 나간 것 같다면, 돈이 빠져나가는 것을
  막기 위해 계좌를 즉시 정지해야 합니다.
- 큐싱에 당해서 돈이나 개인정보를 빼앗긴 것 같다면,
  즉시 경찰에 신고해야 합니다. 가짜 QR 코드 사진, 사기 링크 등은
  모두 증거로 남겨 놓으세요.

평소 자주 사용하는 QR코드가 가짜일 수도 있다니.
진짜 QR코드와 가짜 QR코드는 구별하기 어려워서
더욱 조심해야 할 것 같아요.

"사랑하면 돈을 보내 달라고?"

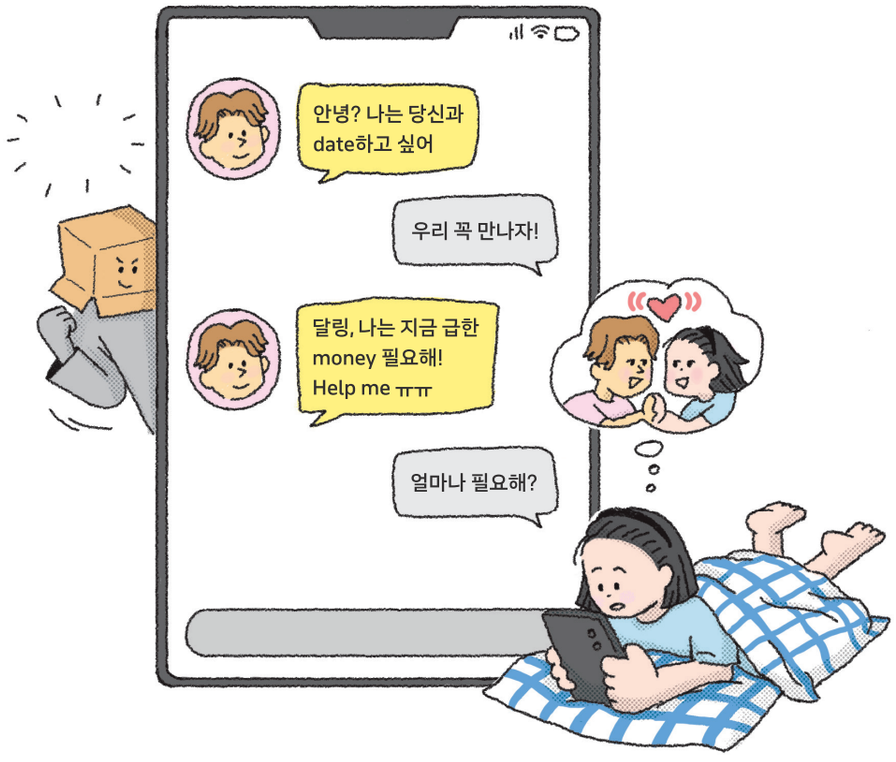
로맨스 스캠

'로맨스 스캠'을 조심해야 하는 상황이에요.
로맨스 스캠이 무엇인지 알아보고, 함께 막아 봐요!

로맨스 스캠이란?

로맨스 스캠은 피해자를 좋아하는 척하면서
돈을 빼앗는 피싱 사기입니다.

로맨스 스캠Romance Scam은 '사랑'을 뜻하는 로맨스Romance와
'사기'를 뜻하는 스캠Scam을 합쳐 만든 말입니다.
사기범은 주로 친근하게 다가와 믿음을 쌓은 뒤,
사랑을 고백하거나 어려운 상황을 이야기하며
돈을 요구합니다.



로맨스 스캠 유형으로는 이런 것들이 있어요

사기범은 주로 외국에 살거나, 전문 직업을 가진 척하면서
여러 이유를 대며 짧은 시간 안에 돈을 보내 달라고 요구합니다.
또한 피해자의 개인정보를 요구하거나, 협박을 통해
피해자에게 다른 사기를 저지르게 하는 경우도 있습니다.

저는 해외에서 일하는 군인이에요.
한국에 가면 꼭 당신을 만나고 싶어요.
그런데 지금 귀국에 필요한 돈이 부족해요.
도와줄 수 있나요?

우리 결혼 준비를 하기로 했으니
이제부터 함께 돈을 모아요.
그래서 특별히 알려 주는 건데,
여기에 투자하면 큰돈을 벌 수 있대요.

당신에게 선물을 보냈는데
공항에서 문제가 생겼대요.
세금만 대신 내주면 바로 받을 수 있어요.

갑자기 사고가 나서 당신을 보러 가기
어려워졌어요. 병원비가 필요해요.
돈을 보내 주면 꼭 갚을게요.

로맨스 스캠 피해, 현재 이런 상황이에요

로맨스 스캠 발생 건수는 2025년(1~9월 기준) 1,565건,
2024년(2월~12월 기준) 1,265건입니다.
또한, 같은 기간 피해액은 2025년 1천억 원으로,
2024년 675억 원에 비해 약 48% 늘었습니다.

출처: 경찰청

로맨스 스캠,
주로 이렇게 일어나요

관심을 표현하며 다가와요

사기범은 주로 SNS, 데이팅 앱, 메신저 등을 통해 관심 있는 척 말을 겁니다. 그리고 실제 사진을 보여 주면서 자신이 믿을 수 있는 사람처럼 보이게 합니다.

좋아한다고 해요

안 지 얼마 되지 않았는데 '좋아한다', '사랑한다' 등 호감을 드러냅니다. 다정하고 친절한 모습을 보이며 마음을 열게 합니다.

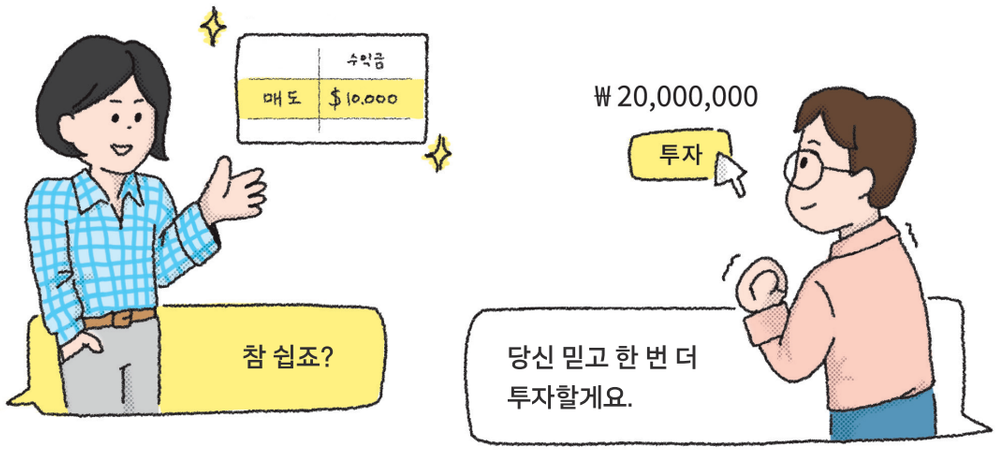
돈을 요구해요

상대가 어느 정도 친해졌다고 느낄 때, 사기범은 돈을 요구하기 시작합니다. 주로 급하게 돈이 필요하다거나, 투자를 해 보라는 이유를 댑니다. 가짜 자료를 보여 주며 속이기도 합니다.

연락을 끊어요

피해자가 돈을 보내는 등 사기범이 원하는 행동을 하면, 사기범은 연락을 끊고 사라집니다.

사례로 알아보는 로맨스 스캠



사례 1

“진짜 좋은 투자 기회예요!”

회사원 A씨는 SNS에서 B씨를 알게 됐습니다. 그녀는 자신을 중국에서 유명한 대학을 졸업하고 싱가포르에서 투자 회사를 운영하는 30세 여성이라고 소개했습니다. 사진 속 모습도 이상형과 비슷해 A씨는 금세 호감을 느꼈습니다.

B씨가 8월에 서울로 휴가를 온다고 하면서 두 사람은 빠르게 가까워졌습니다. 그러던 중 B씨는 자신이 사업에 투자해 큰돈을 벌고 있다며, 30분 만에 1만 달러를 번 거래 화면까지 보여 주었습니다.

A씨가 관심을 보이자 B씨는 “적은 돈으로 시작해 보라”고 말했습니다. A씨는 B씨의 말대로 50만 원을 사업에 투자했고, 이틀 만에 100만 원을 벌게 되었습니다. 돈을 벌자 믿음이 생긴 A씨는 더 큰 돈을 벌기 위해 2천만 원을 더 투자했습니다. 하지만 다음 날 B씨의 계정은 흔적도 없이 사라졌습니다. A씨는 B씨를 찾으려 했지만 그녀가 알려 준 정보는 모두 거짓이었습니다.

사례 2

“지금 응급 수술을 받아야 하는데 도와줄 수 있어요?”

C씨는 평소 SNS에 자신의 고양이 사진을 자주 올렸습니다. 하루는 자신을 미국 군인이라며 소개하는 D씨에게 메시지를 받았습니다. D씨는 “고양이가 귀엽다”며 친근하게 다가왔고, 대화는 빠르게 이어졌습니다.

D씨는 다정하고 유쾌했으며, 시간이 지나면서 “운명 같다”, “한국에 가서 함께 살고 싶다”는 말까지 하며 애정을 드러냈습니다. C씨 역시 마음을 열고 매일 대화를 나눴습니다. 곧 둘은 연인 같은 사이가 되었습니다.

하지만 며칠 뒤, D씨가 일하던 중 쓰러져 병원에 입원했다며 급하게 수술비가 필요하다고 메시지를 보냈습니다. 병원 침대 사진까지 보내자 C씨는 정말 급한 상황이라는 생각에 돈을 보냈습니다. D씨는 고맙다며 곧 회복해 한국으로 가겠다고 약속했습니다.

그러나 그 뒤로 연락이 끊겼습니다. 불안해진 C씨는 D씨가 말한 부대에 직접 확인해 보니, 그런 이름의 군인은 없다는 답변만 돌아왔습니다. 그제야 C씨는 사기를 당했다는 사실을 깨달았습니다.

이럴 때 로맨스 스캠을 의심해 보세요

아래 내용 중 1개라도 해당된다면 **로맨스 스캠**일 수 있습니다.
로맨스 스캠이 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

안 지 얼마 되지 않았는데 “사랑한다”, “운명이다” 같은 애정 표현을 해요.

친절하고 다정한 말에 마음이 끌릴 수 있지만, 얼굴도 보지 못한 사람이 너무 빨리 다가오면 의심해야 합니다.

SNS 계정 속 사진을 보면 멋지고 믿을 만한 사람처럼 보여요.

믿을 수 있는 사람으로 보이기 위해 꾸며 낸 사진일 수 있습니다.

**SNS 계정이 만들어진지 얼마 안 된 것 같아요.
팔로워가 적고, 게시물에 댓글도 거의 없어요.**

가짜 SNS 계정일 수 있습니다. 그 사람이 실제로 어떤 사람들과 교류하고 있는지 꼼꼼히 살펴보아야 합니다.

**음성 통화나 영상 통화를 하자고 하거나,
직접 만나자고 하면 계속 이유를 대며 피해요.**

사진과 실제 모습이 다르기 때문일 수 있습니다. 또, 통화 목소리도 가짜로 꾸며 낼 수 있기 때문에 통화를 했다고 해서 무조건 믿어서는 안 됩니다.

급한 상황이나 좋은 투자 기회가 있다고 돈을 요구해요.

수술비, 여행비, 투자금 등 돈을 요구하는 상황은 다양합니다.
당신을 믿기 때문에 부탁하는 것이라고 안심시키기도 합니다.
하지만 실제로 만나 본 적 없는 사람에게는 아주 적은 돈이라도 보내서는 안 됩니다.

**사진, 서류 등 실제 자료를 보여 주며 자신을 믿고
돈을 보내 달라고 해요.**

가짜 자료는 얼마든지 만들 수 있습니다. 대검찰청 ‘찐센터’에 연락하거나, 은행이나 경찰서에 방문하여 그 자료가 진짜 자료인지 꼭 확인해 보세요.

좋은 정보가 있다며 특정 링크에 접속해 보라고 해요.

그 링크에는 악성 프로그램이 숨어 있을 수 있습니다.
누르는 순간 바로 돈이나 개인정보가 빠져나갈 위험이 있습니다.

로맨스 스캠 이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

로맨스 스캠 피해를 입었다면, 바로 신고하세요

돈이나 개인정보를 빼앗긴 것 같다면 망설이지 말고 바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)

금융정보를 보호하세요

내 금융정보가 새어 나간 것 같다면, 돈이 빠져나가는 것을 막기 위해 계좌를 즉시 정지해야 합니다. 이때 아래 방법을 사용할 수 있습니다

- '계좌정보통합관리서비스(payinfo.or.kr)'에 접속해서 직접 지급정지 신청하기
- '개인정보노출자 사고예방시스템(pd.fss.or.kr)'에 접속해서 개인정보가 유출되었는지 확인하고, 추가 계좌 개설을 막기

증거를 꼼꼼히 모아 두세요

사기범의 흔적이 남아 있는 자료라면 무엇이든 도움이 됩니다. 사기범과의 문자, 채팅, 송금 내역, 계정 정보를 모두 캡처해서 모아 놓으세요. 사기범을 잡을 때 증거 자료로 사용할 수 있습니다.

온라인에서 만난 사람이 추천한 가상자산거래소• 가 가짜 거래소인지는 어떻게 확인할 수 있나요?

해당 거래소가 금융정보분석원에 신고된 가상자산사업자인지 확인해야 합니다. 금융정보분석원 홈페이지(kofiu.go.kr)의 공지사항(가상자산사업자 신고 현황)에서 조회되지 않는 경우 불법 영업일 뿐 아니라 사기 목적으로 만들어진 가짜 거래소일 가능성이 높습니다.

• **가상자산거래소**: 돈이나 돈으로 바꿀 수 있는 재산을 사고팔 수 있도록 만든 온라인 공간.

온라인에서 외국인이 말을 걸어 오면 모두 의심해야 하나요?

모든 외국인이 사기범은 아닙니다. 하지만 만난 지 얼마 안 돼 애정 표현을 과하게 하거나, 돈을 요구하거나, SNS 계정이 어딘가 수상하면 반드시 의심해 봐야 합니다. 조금이라도 수상하다면 바로 대화를 멈추고 주변 사람이나 전문가와 상의해야 합니다.

- 로맨스 스캠은 '피해자를 좋아하는 척하면서 돈을 빼앗는 피싱 사기'입니다.
- 로맨스 스캠은 온라인에서 주로 일어납니다. SNS나 데이팅 앱 등에서 먼저 다가와 친해진 뒤, 여러 이유를 대며 돈을 요구합니다.
- 온라인에서 보이는 모습을 모두 믿지 마세요. 자신의 실제 모습을 드러내지 않고 돈만 요구한다면, 그 사람이 보여 주는 모습은 가짜일 가능성이 큽니다.
- 로맨스 스캠에 당한 것 같다면, 즉시 경찰에 신고해야 합니다. 사기범의 SNS 계정이나 채팅 내역 등은 모두 캡처해서 증거 자료로 남겨 놓으세요.

누군가의 좋아하는 마음과 감정을 이용해
사기를 치다니, 절대 해서는 안 될 일이지요!

"싸고 친절해서 믿었는데"

중고거래 사기

'중고거래 사기'를 조심해야 하는 상황이에요.
중고거래 사기가 무엇인지 알아보고, 함께 막아 봐요!

중고거래 사기란?

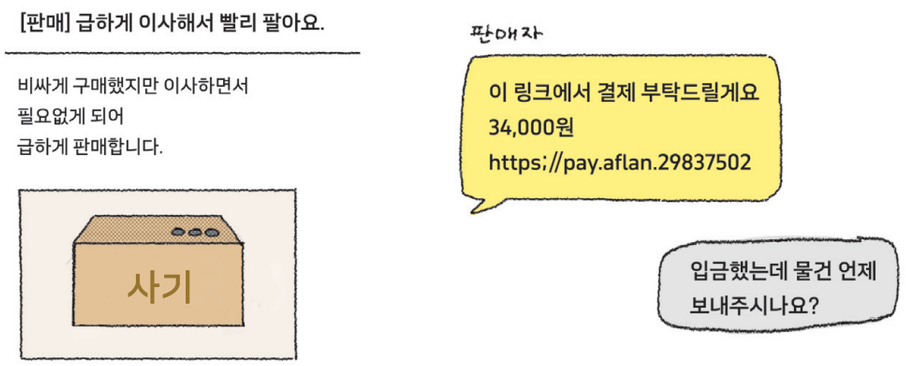
중고거래 사기는 중고 물건을 거래하는 척하면서
돈이나 물건을 빼앗는 범죄입니다.

사기범은 중고거래 사이트에서 판매자인 척 게시물을 올려
상대를 속입니다. 돈만 받고 연락을 끊기도 하고, 물건 대신
빈 상자나 가짜 물건을 넣어 사기를 치기도 합니다.
반대로 구매자인 척 접근해 물건만 가로채는 경우도 있습니다.

중고거래 사기 유형으로는 이런 것들이 있어요

중고거래 사기는 공연 티켓, 상품권, 중고차, 부동산 등
물건을 사고팔 때면 언제든 일어날 수 있습니다.
보통 택배거래에서 피해가 많이 생기지만, **직거래**•도 안전하다고
할 수는 없습니다. 최근에는 **삼자사기**••처럼 더욱 복잡한 방식의
사기도 일어나고 있습니다.

- **직거래**: 직접 만나서 하는 거래.
- **삼자사기**(3자사기): 판매자와 구매자를 모두 속이는 사기. 사기범은 판매자와 구매자 중간에서 서로를 속여서 판매자에게서는 물건을, 구매자에게서는 돈을 빼앗는다.

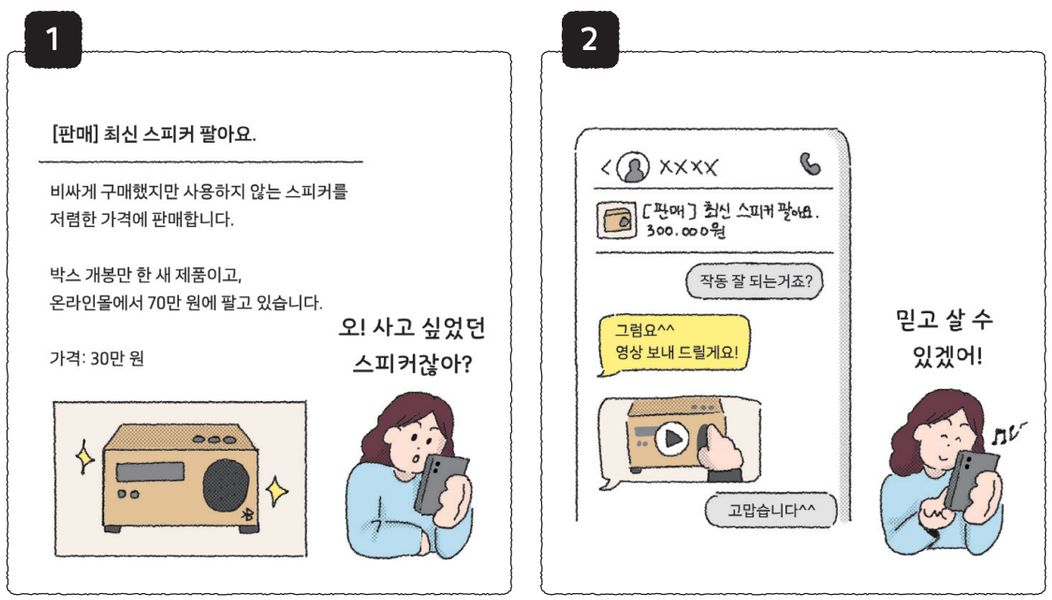


중고거래 사기 피해, 현재 이런 상황이에요

중고거래 사기 신고 건수(1월~12월 기준)는 2025년 10만 539건으로,
2024년 7만 8,320건에 비해 28.4% 늘었습니다.
또한, 같은 기간 피해액은 2025년 3,340억 원으로,
2024년 1,373억 원에 비해 약 2배 늘었습니다.

출처: 경찰청

중고거래 사기,
주로 이렇게 일어나요



가짜 물건을 올려요

사기범은 중고거래 사이트나 앱에 실제로는 팔지 않거나 고장 난 물건을 올립니다. 가격도 다른 사람들보다 더 싸게 올려서 사고 싶은 마음이 들게 만듭니다.

친절하게 대답해서 믿음을 줘요

구매자가 연락하면 답장도 빠르고 말도 친절하게 합니다. 사진과 영상도 원하는 만큼 보내 주며 믿을 수 있게 행동합니다.

입금하게 해요

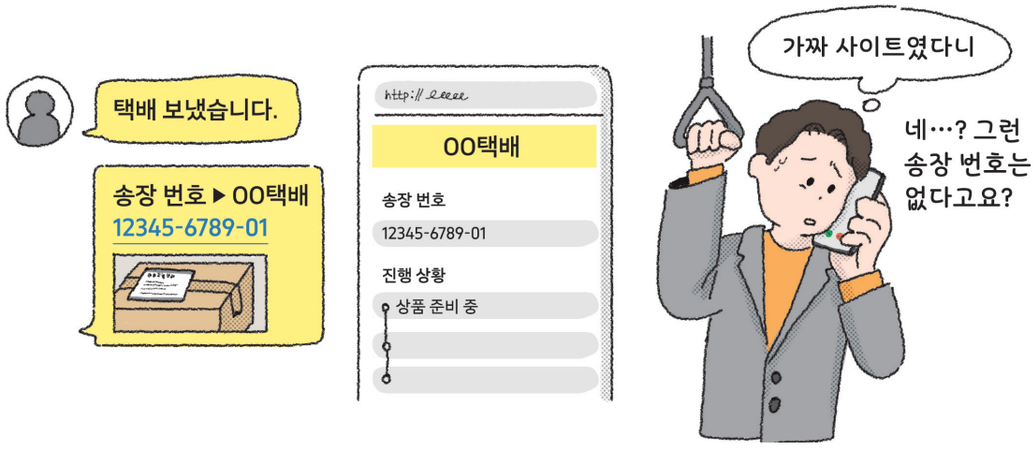
상대가 거래하겠다고 하면 입금을 요구합니다. “지금 입금하면 가격을 깎아 드릴게요”, “오늘 바로 배송해 드릴게요” 같은 말로 빨리 돈을 보내게 만듭니다. 이때 **안전거래**• 링크처럼 보이는 가짜 링크를 보내기도 합니다.

연락을 끊어요

피해자가 돈을 보내면 사기범은 연락을 끊고 사라집니다. 약속했던 물건도 보내지 않습니다.

• **안전거래**(안전결제): 거래할 때 돈을 바로 판매자에게 보내지 않고, 먼저 결제 사이트에 맡겨 두는 방식. 판매자의 계좌로 바로 돈을 보내는 방식보다 더 안전하다.

사례로 알아보는 중고거래 사기



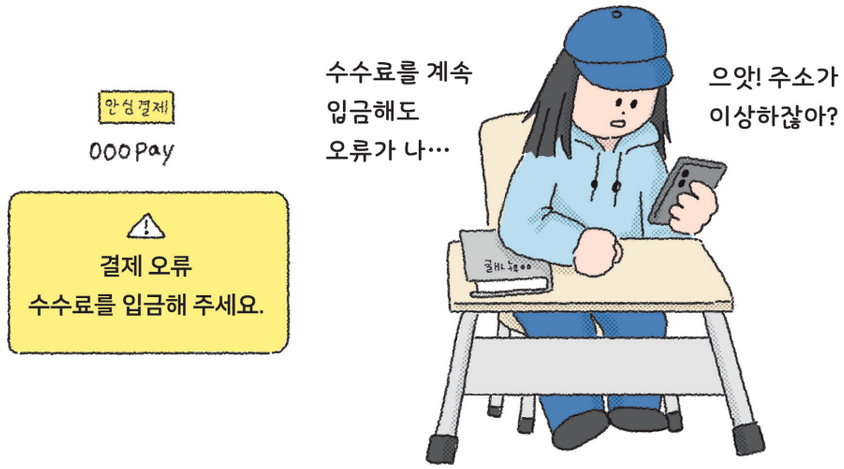
사례 1 “분명 택배를 보냈다는데 못 받았어요.”

A씨는 중고거래 카페에서 가구를 구매하려다 판매자 B씨를 알게 되었습니다. B씨가 올린 글 속의 물건은 상태도 좋고 가격도 저렴했습니다. A씨는 택배로 안전하게 보내 주겠다는 말만 믿고 B씨에게 바로 돈을 보냈습니다.

잠시 후 B씨는 “택배를 보냈다”며 송장 번호와 사진을 보냈습니다. A씨가 번호를 눌러 보니 택배 회사 사이트가 열리고, ‘배송 준비 중’이라는 문구가 떠 있었습니다. A씨는 안심하고 택배를 기다렸습니다.

하지만 며칠이 지나도 물건은 도착하지 않았고, 배송 상태도 ‘배송 중’에서 더 이상 바뀌지 않았습니다. 이상함을 느낀 A씨가 직접 택배 회사에 전화해 보니, 그런 송장 번호는 없다는 답변만 돌아왔습니다.

A씨는 그제야 B씨가 알려 준 택배 회사 사이트가 실제와 비슷하게 만든 가짜 사이트였다는 사실을 알게 되었습니다. B씨는 이미 연락이 끊겼고, 카페에 올렸던 판매 글도 삭제된 후였습니다.



사례 2 “안전거래로 거래하실래요?”

대학생 C씨는 중고거래 앱에서 노트북을 찾고 있었습니다. 그러던 중 가격도 적당하고 조건도 좋은 노트북을 발견해 판매자 D씨에게 메시지를 보냈습니다. D씨는 답장도 빠르고 말투도 친절해 믿음이 갔습니다.

C씨가 “직접 만나서 물건을 보고 사고 싶다”고 하자, D씨는 “요즘은 만나서 거래하기 불안하다”며 ‘안전거래’로 거래하자고 했습니다. D씨가 보낸 링크는 유명한 안전거래 사이트 화면과 똑같아 보여 C씨는 의심하지 않았습니다.

그러나 C씨가 링크에서 결제를 진행하자 ‘결제 오류 — 수수료를 입금해 주세요’라는 문구가 떴습니다. D씨는 “가끔 이런 오류가 나는데, 수수료를 보내면 나중에 환불받을 수 있다”고 말했습니다. C씨는 그 말을 믿고 수수료 10만 원을 입금했지만, 이후에도 같은 문구가 3번이나 나타났고 결국 총 30만 원을 보내게 됐습니다.

이상하다고 느낀 C씨가 링크를 자세히 보니, 공식 사이트 링크와 한 글자가 다른 가짜 사이트 링크였습니다. C씨는 환불해 달라고 메시지를 보냈지만 D씨는 답하지 않았고, 몇 시간 뒤 메신저 화면에는 “탈퇴한 회원입니다”라는 문구만 남았습니다.

이럴 때 중고거래 사기를 의심해 보세요

아래 내용 중 1개라도 해당된다면 **중고거래 사기**일 수 있습니다.
중고거래 사기가 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

택배로만 거래하자고 해요.

돈만 받고 물건을 보내지 않으려는 사기일 수 있습니다. 특히 판매자가 처음엔 직거래가 가능하다고 했다가, 갑자기 바쁘다며 택배로만 거래하자고 바꾸는 경우가 있습니다. 이런 경우 더욱 의심해 봐야 합니다.

지금 안 사면 다른 사람에게 판다고 해요.

판매자가 결정을 서두르게 만들수록 사기일 가능성이 높습니다.
특히 다른 물건보다 훨씬 싸다면 사기일 수 있으니 꼭 의심해 보세요.

판매자 계정에 거래 내역이 거의 없어요.

사기를 치기 위해 새로 만든 가짜 계정일 수 있습니다.
실제로 제대로 거래가 이루어지고 있는 계정인지 거래 후기 등을 꼭 살펴보세요.

입금하면 문 앞에 물건을 걸어 두겠다고 해요.

판매자를 믿고 입금했다가, 문고리에 빈 봉투만 걸려 있을 수 있습니다. 직접 물건을 확인하기 전까지는 절대 입금하지 마세요.

판매자가 보낸 물건 사진이나 영상이 어딘가 이상해요.

물건 사진이나 영상을 보내 달라고 했을 때, 주변 배경이나 손동작이 어색해 보이면 의심해 보세요. 실제 찍은 것이 아니라 가짜로 만든 것일 수도 있습니다.

판매자가 보낸 물건 사진을 인터넷에 검색해 보았더니 비슷한 사진이 떠요.

비슷한 사진이 여러 개 나온다면, 다른 사람의 사진을 가져다 쓴 것일 수 있습니다.

입금했는데 갑자기 택배를 늦게 보낸다고 해요.

“바빠서 늦어요”, “내일 꼭 보낼게요”라며 계속 미루거나 연락을 피한다면 사기일 수 있습니다. 나중에 증거로 사용할 수 있도록 대화 내용을 모두 저장해 두세요.

중고거래 사기, 이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

중고거래 피해를 입었다면, 바로 신고하세요

돈이나 개인정보를 빼앗겼다면 망설이지 말고
바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

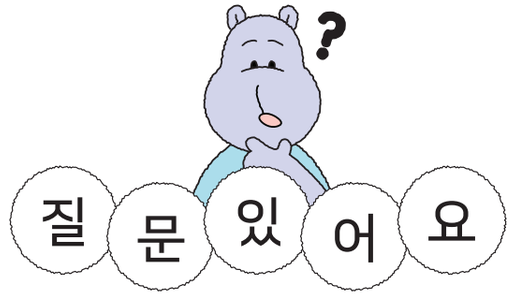
- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)

'더치트'앱에서 사기 피해 정보를 확인하세요

'더치트'는 사기피해 정보를 공유하고 검색할 수 있는 서비스입니다. 사기가 의심되는 계좌번호, 전화번호, 아이디를 검색하면 다른 사람의 신고 이력을 확인할 수 있습니다. 가장 좋은 것은 거래 전에 판매자 정보를 확인해 보는 것입니다.

중고거래 플랫폼에도 꼭 알리세요

대형 중고거래 플랫폼은 자체적으로 사기 대처 시스템을 가지고 있습니다. 사기를 당했을 때 중고거래 플랫폼에 알리면 사기 계정을 차단하고, 다른 사용자에게 알려서 더 큰 피해를 막을 수 있습니다.



인증을 꼼꼼히 받으면 사기를 안 당할 수 있을까요?

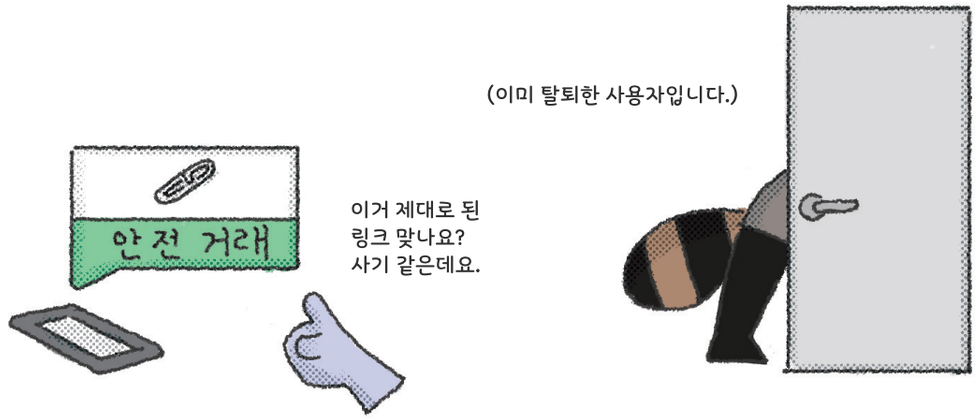
인증을 잘 해 준다고 해서 무조건 믿어서는 안 됩니다. 입금 전에 판매자 정보를 꼼꼼하게 확인하세요. 판매자의 계좌번호나 전화번호를 '더치트'에 꼭 입력해 보세요. 토스 등 일부 금융 앱에서는 송금할 때 사기 의심 계좌인지 알려 주는 기능도 있으니 이런 서비스도 적극적으로 활용해 보세요.

직거래는 다 안심할 수 있나요?

직거래는 직접 만나서 물건을 보고 거래하기 때문에 택배거래보다는 사기 위험이 낮습니다. 하지만 직거래도 사기를 당할 수 있습니다. 가짜 물건을 속여서 팔 수도 있고, 돈을 받고 물건을 주지 않은 채 도망갈 수도 있습니다. 사람이 많고 안전한 공간에서 만나 물건 상태를 꼼꼼히 살펴본 뒤 거래하는 것이 좋습니다.

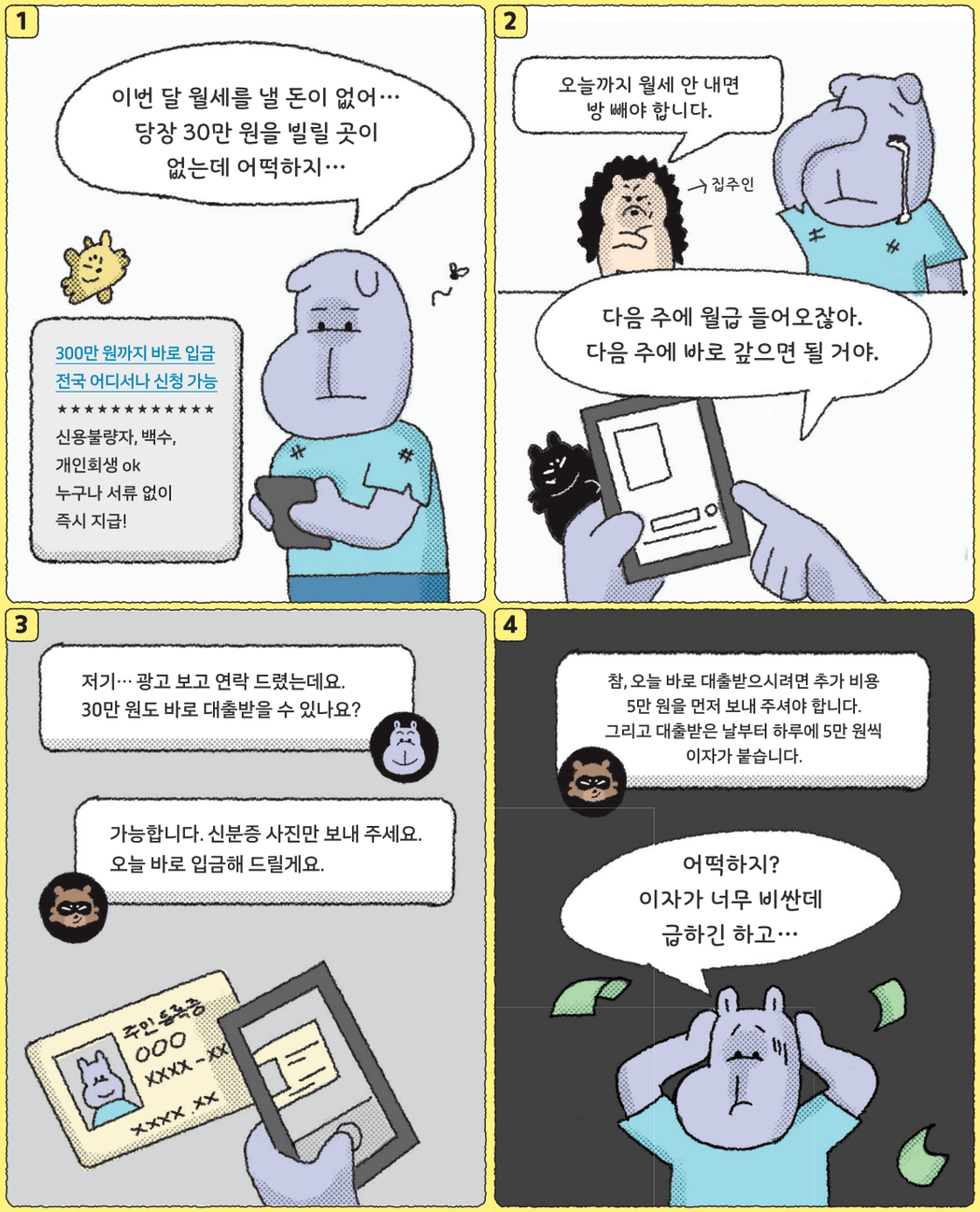
- 중고거래 사기는 '중고 물건을 거래하는 척하면서 돈이나 물건을 가로채는 범죄'입니다.
- 중고거래 사기는 물건을 사고팔 때면 언제든 일어날 수 있습니다. 보통 택배거래에서 피해가 많지만, 직거래도 안전하다고 할 수는 없습니다.
- 판매자가 보낸 물건 사진이나 영상, 링크가 어딘가 이상하다면 사기인지 의심해 보세요. 또한, 빨리 입금해 달라고 하거나 직거래를 피한다면 꼭 의심해 보세요.
- 중고거래 사기에 당해서 피해를 입었다면, 즉시 경찰에 신고해야 합니다. 사기범이 보낸 사진이나 링크 등은 모두 증거로 남겨 놓고, 중고거래 플랫폼의 도움을 받을 수 있는지도 꼭 확인해 보세요.

중고거래할 때 사진이나 영상을 보내 준다고 해서,
안전거래라고 해서, 다 믿어서는 안 되겠어요.



"이자가 끝없이 늘어나요"

불법사금융



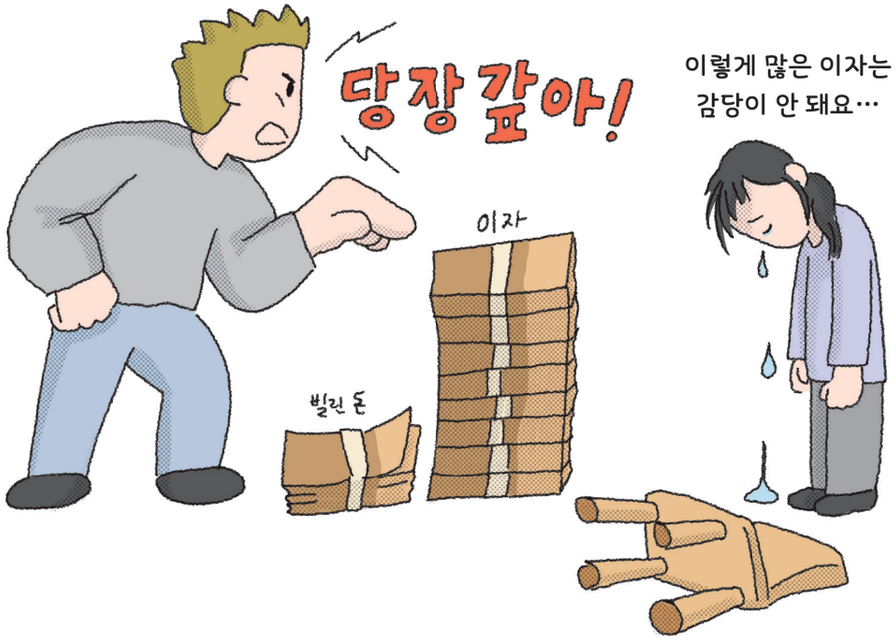
잠깐

'불법사금융'을 조심해야 하는 상황이에요.
불법사금융이 무엇인지 알아보고, 함께 막아 봐요!

불법사금융이란?

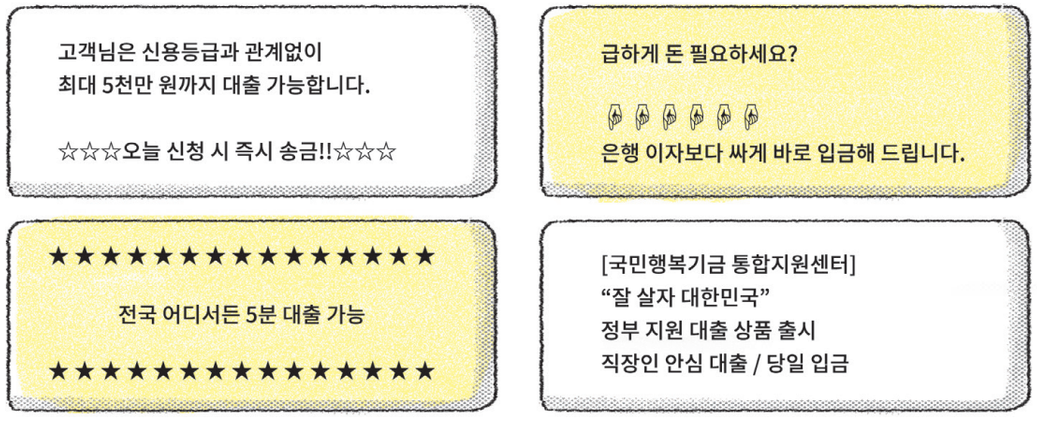
불법사금융은 법을 어기고 다른 사람에게 돈을 빌려주는 일을 말합니다.

불법사금융 대출 업체를 운영하는 사람들은
주로 급하게 돈이 필요한 사람들을 노립니다.
돈을 빌려준 뒤 매우 높은 이자를 요구하거나,
돈을 갚지 못하면 폭력을 저지르거나 협박을 하기도 합니다.



불법사금융 유형으로는 이런 것들이 있어요

불법사금융은 좋은 조건으로 돈을 빌려줄 것처럼 광고하며
사람을 속이는 경우가 많습니다. 특히 급하게 돈이 필요하거나
금융정보에 익숙하지 않은 사람들이 이런 광고에 속아
피해를 입기 쉽습니다.



불법사금융 피해, 현재 이런 상황이에요

불법사금융 피해 상담·신고 건수(1월~10월 기준)는
2024년 1만 2,398건으로, 2023년 1만 1,278건에 비해 9.9% 늘었습니다.

같은 기간 기준 2020년 6,615건, 2021년 8,213건, 2022년 8,947건으로,
피해 상담·신고 건수는 계속해서 늘어나고 있습니다.

출처: 금융감독원 불법사금융 피해신고센터

불법사금융,
주로 이렇게 일어나요

좋은 조건으로 대출해 준다고 해요

문자나 인터넷 배너로 '누구나 가능', '당일 즉시 입금', '서류 없이 바로 대출' 같은 문구가 담긴 광고를 내보냅니다.

하지만 이런 광고는 대부분 거짓이고, 실제로는 다른 안 좋은 조건을 숨긴 경우가 많습니다.

이자를 너무 많이 요구해요

돈을 빌릴 때 법에서 정한 최대 이자율(1년에 20%)보다 훨씬 높은 이자를 요구합니다. 수수료, 심사비 등의 이유로 돈을 먼저 내라고 하거나, 빌려준 돈에서 일부를 빼고 주기도 합니다.

빚이 점점 늘어나게 만들어요

정해진 기간 안에 돈을 갚지 못하면 대출을 더 많이 받으라고 하거나, 추가 수수료를 붙여 빚이 늘어나게 만듭니다. 또는 실제보다 돈을 더 많이 빌린 것처럼 속여서 더 많은 돈을 갚게 만들기도 합니다.

불법적인 방법으로 돈을 갚으라고 해요

돈을 갚지 못하면 밤낮을 가리지 않고 연락하거나, 집이나 직장에 찾아와서 협박하기도 합니다. "가족에게 말하겠다", "사진을 퍼뜨리겠다"라며 겁을 주기도 합니다.

사례로 알아보는 불법사금융

사례 1

“빌린 돈을 다 갚아도 끝난 게 아니래요”

가게 운영이 어려워진 A씨는 급히 생활비가 필요해져 여러 곳에서 대출을 알아봤습니다. 하지만 이미 은행에서 돈을 빌린 상태라 더 이상 대출을 받을 수 없었습니다. 결국 이자가 높은 줄 알면서도 불법사금융을 이용하고 말았습니다.

A씨는 약속된 기간 안에 빌린 돈과 이자를 모두 갚아 이제는 마음 놓아도 되겠다고 생각했습니다. 그런데 며칠 뒤, 낯선 사람이 가게에 찾아와 계속해서 “이자를 더 내라”고 요구했습니다. 알고 보니 그 사람은 A씨가 돈을 빌렸던 불법사금융 대출 업체 직원 B씨였습니다. A씨가 이미 모든 돈을 갚았다고 말해도 B씨는 “아직 남은 돈이 있다”며 계속 괴롭혔습니다.

계속되는 방문과 압박 때문에 A씨는 가게 운영은 물론, 일상생활조차 제대로 하기 어려워졌습니다. 결국 A씨는 혼자 해결하기 어렵다고 판단해 결국 경찰에 도움을 요청했습니다.

사례 2

“지금 당장 돈 안 갚으면 어떻게 될지 몰라요”

취업준비생 C씨는 아르바이트로 생활비를 벌고 있었습니다. 그러던 어느 날, 가족이 갑자기 병원에 입원하면서 당장 치료비가 필요해졌습니다. 급한 마음에 C씨는 SNS에서 본 “누구나 당일 바로 입금!”이라는 광고를 보고 대출을 신청했습니다.

대출 업체 직원 D씨는 “신용등급이 낮아도 괜찮다”며 친절하게 C씨를 안심시켰습니다. 상담을 마치자마자 C씨 통장에는 300만 원이 입금됐고, D씨는 일주일 뒤 이자 30만 원을 더해 330만 원만 갚으면 된다고 했습니다.

일주일 뒤, 정신 없이 가족을 돌보던 C씨는 돈을 갚지 못했습니다. “조금만 기다려 달라”는 말에도, D씨의 태도는 완전히 바뀌었습니다. 밤낮없이 걸려오는 전화로 욕설과 협박이 이어졌고, “지금 당장 돈을 안 갚으면 친구들에게 알리겠다”, “직장에 사진을 퍼뜨리겠다”는 말까지 들었습니다. 게다가 D씨는 돈을 갚을 때까지 매일 이자가 10만 원씩 붙는다고 말했습니다. 당장 돈을 갚기 어려운 C씨는 눈덩이처럼 불어나는 빚 앞에서 어떻게 해야 할지 막막해졌습니다.

이럴 때 불법사금융을 의심해 보세요

아래 내용 중 1개라도 해당된다면 **불법사금융**일 수 있습니다.
불법사금융이 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

정식으로 등록된 대출 업체가 아닌 것 같아요.

모든 대출 업체는 나라에 등록되어 있어야 합니다. 금융감독원이나 한국대부금융협회 홈페이지에서 확인할 수 있습니다. 등록되지 않은 곳은 불법 업체입니다.

이자가 '1년에 20%'보다 높아요.

법에서 정한 최대 이자율은 1년에 20%입니다. 수수료 등을 이유로 실제 이자가 20%를 넘으면 불법 대출입니다.

누구나 쉽게 대출을 받을 수 있다고 강조해요.

"무서류 대출", "누구나 가능" 같은 말은 거짓 광고일 수 있습니다.
정식으로 등록된 업체는 광고에 '심의번호'라는 것을 꼭 표시하니,
그 번호가 있는지 확인하세요.

다른 불법사금융에서 빌린 돈을 해결해 준다며 수수료를 요구해요.

빌린 돈을 갚아 준다면서 돈을 요구하는 것은 불법입니다.
이럴 땐 금융감독원이나 각 지역의 불법사금융 피해신고센터에 연락하세요.

너무 많은 개인정보를 요구해요.

대출과 상관없는 개인정보를 요구한다면 다른 범죄에 사용하려는 목적일 수 있습니다. 계좌 비밀번호나 가족 연락처 같은 중요한 개인정보는 절대 알려 주면 안 됩니다.

밤늦게 돈을 갚으라고 연락이 오거나 대출 사실을 알리겠다고 협박해요.

폭언, 욕설, 협박은 모두 불법입니다. 평일 오전 8시부터 오후 9시가 아닌 시간에 연락하는 것도 불법입니다.

'가입비'나 '수수료'를 요구해요.

대출받기 전에 돈을 내라고 하면 100% 사기입니다.
정상적인 투자라면 먼저 돈을 내라고 하지 않습니다.

불법사금융,
이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

불법사금융 피해를 입었다면, 바로 경찰에 신고하세요

돈이나 개인정보를 빼앗겼다면 망설이지 말고
바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)
- 금융감독원: 1332 fss.or.kr (금융 피해 구제, 지급 정지 문의)

피해 구제를 꼭 신청하세요

법에서 정한 이자율을 지키지 않은 경우는 불법이므로
돈을 돌려 달라고 요구할 수 있습니다. 돈을 갚으라고 협박하거나
폭력을 쓸 때도 도움을 요청할 수 있습니다. 아래 번호로 도움을
요청해 빠르게 피해에서 벗어나세요.

- 법률구조공단: 132
- 한국대부금융협회: 02-6710-0831~4

급하게 대출이 필요하다면 안전한 기관을 이용하세요

돈이 꼭 필요하다면 먼저 정부가 지원하는 안전한 대출 상품을
알아보세요. 서민금융진흥원에서는 버는 돈이 적거나 신용등급이
낮은 사람을 위해 여러 가지 대출 상품을 지원하고 있습니다.

- 서민금융콜센터 불법사금융예방대출: 1397 sloan.kinfa.or.kr
- 신용회복위원회: 1600-5500

대출 계약서를 받지 못했어도 신고할 수 있나요?

계약서가 없더라도 돈을 주고 받은 자료가 있다면 신고할 수
있습니다. 대출 조건을 상담한 문자나 통화 녹음 내용,
돈을 주고받은 입출금 등 거래 내역 등의 자료로 신고하세요.

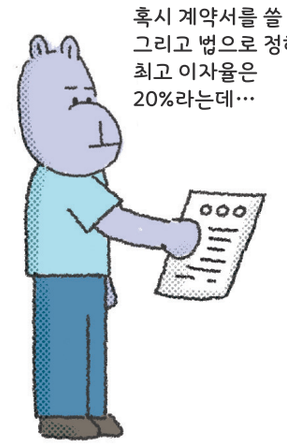
불법사금융 피해를 입었어요. 돈을 갚을 능력이 없는데 어떻게 해야 할까요?

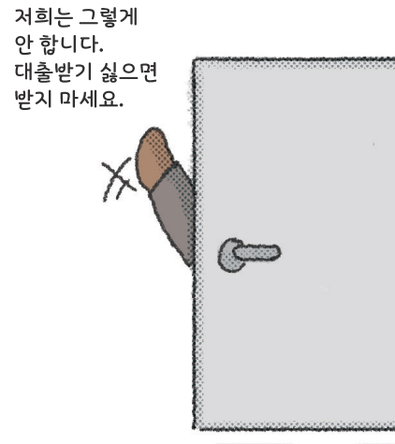
돈을 갚을 수 있는 능력이 없다면 신용회복위원회의 도움을 받을 수
있습니다. 내 상황에 맞는 지원을 받아보세요.

- 신용회복위원회 불법사금융 전담창구: 1600-5500 ccrs.or.kr

- 불법사금융은 '법을 어기고 다른 사람에게 돈을 빌려주는 일'을 말합니다.
- 불법사금융은 조건이 좋은 것처럼 속여 사람들에게 돈을 빌리게 합니다. 하지만 돈을 빌리고 나면 법에서 정한 것보다 훨씬 높은 이자를 요구하며 피해를 입히는 경우가 많습니다.
- 너무 쉽게 돈을 빌려주는 대출 업체는 불법사금융일 수 있습니다. 이런 경우 대출을 받기 전에, 꼭 등록된 업체인지 확인하세요.
- 불법사금융 피해를 당했거나 의심된다면 경찰이나 금융감독원에 즉시 신고해야 합니다. 나라에서는 불법사금융 피해 구제를 위해 다양한 제도를 운영하고 있습니다. 피해를 당했다면 꼭 관련 기관에 도움을 요청하세요.

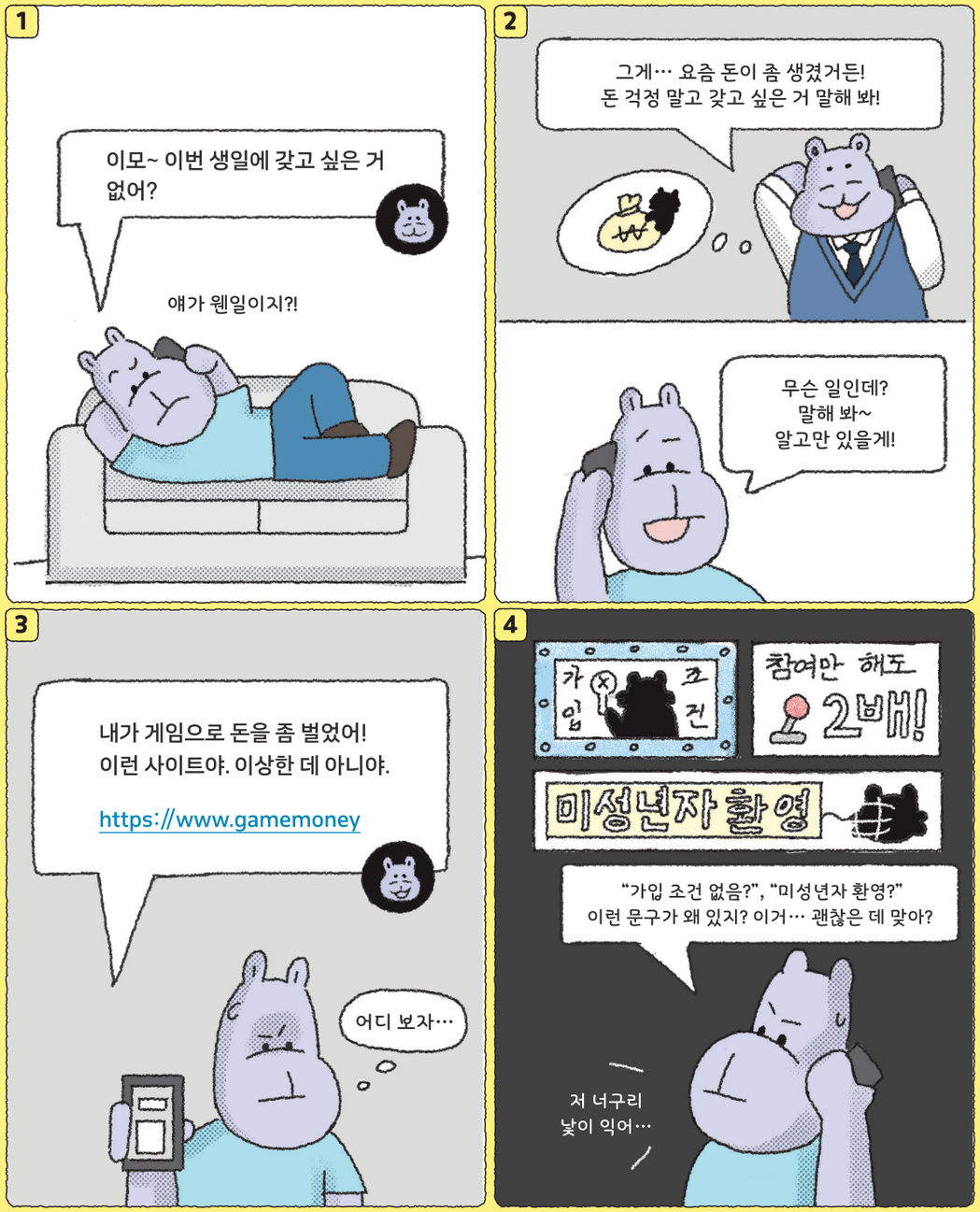
잘못 돈을 빌렸다가 큰 피해를 입을 수도 있겠군요.
급하게 돈이 필요하더라도 잘 알아보고 빌려야겠어요.





"호기심으로 큰돈을 잃었어요"

청소년 불법도박



'청소년 불법도박'을 조심해야 하는 상황이에요.
청소년 불법도박이 무엇인지 알아보고, 함께 막아 봐요!

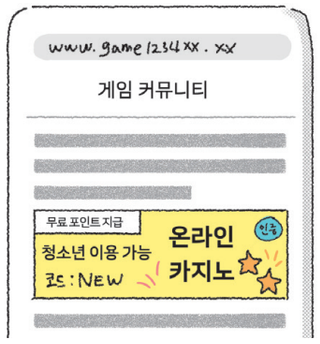
청소년
불법도박이란?

청소년 불법도박은 청소년이 법에서 금지된 도박에
참여하는 것을 말합니다. 도박은 돈이나 물건을 걸고, 결과에 따라
이기면 얻고 지면 잃는 행위입니다.

사기범은 주로 호기심이 많거나 용돈을 벌고 싶은 청소년을 노립니다.
청소년이 관심 가질 만한 내용을 담은 인터넷 광고나 문자를 보내,
가볍게 도박을 시작하게 해서 큰돈을 잃게 만듭니다.

청소년 불법도박 유형으로는 이런 것들이 있어요

청소년을 노리는 불법도박 광고는 청소년들이 자주 보는 SNS, 유튜브,
게임 채널 등에 많이 나타납니다. 이런 광고는 스포츠 경기 결과, 게임 아이템
판매 정보처럼 청소년들이 관심 가질 만한 내용을 담고 있습니다.
최근에는 청소년에게 인기 있는 유명인의 얼굴과 목소리를 딥페이크해서
만든 불법 도박광고 영상까지 생겨나고 있습니다.



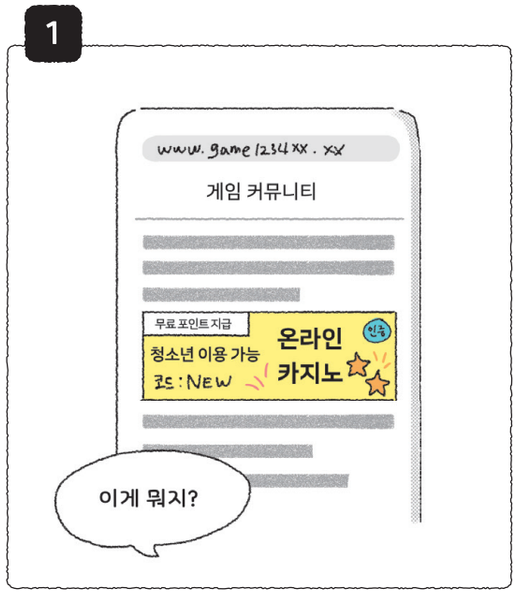
청소년 불법도박 피해, 현재 이런 상황이에요

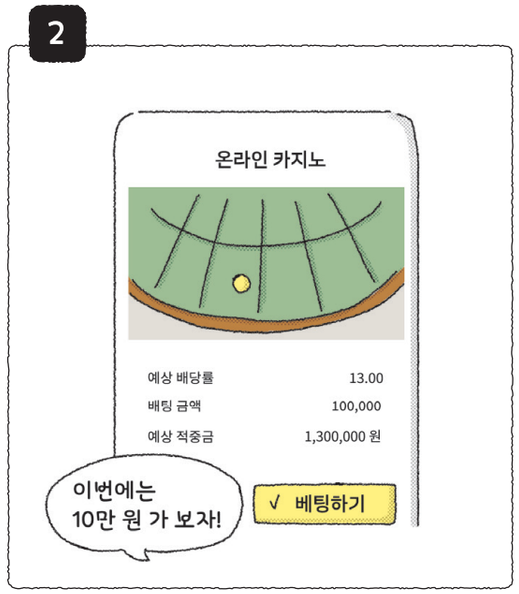
2024년 전국 605개 학교의 청소년 1만 3,368명을 대상으로 한 조사에서,
4.3%가 도박을 해 본 적이 있다고 답했습니다.

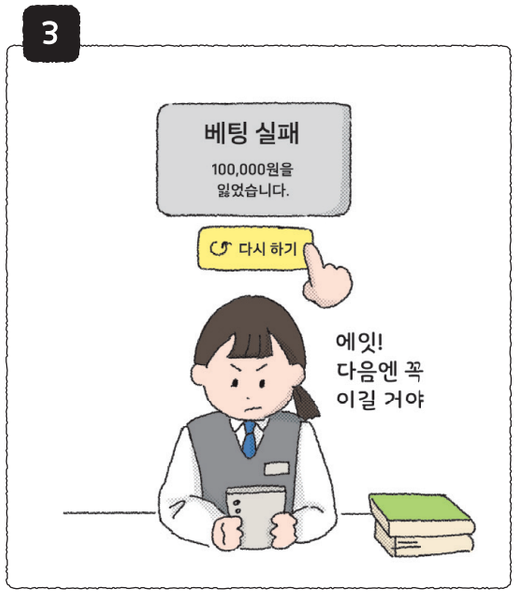
이 중 19.1%는 현재도 도박을 하고 있었고, 그중 48.4%는
다른 사람의 이름이나 계정을 사용했으며, 24.4%는 자신의 계정이나 돈을
다른 사람에게 넘겨 대신 도박에 참여하게 했습니다.

출처: 한국도박문제예방치유원

청소년 불법도박,
주로 이렇게 일어나요







청소년이 관심을 가질 만한 광고를 내보내요

SNS, 유튜브, 온라인 커뮤니티 등에 불법도박 광고를 내보냅니다. 광고에는 '누구나 쉽게 용돈 벌기', '무료 포인트 지급' 같은 문구가 들어 있어 청소년의 호기심을 자극합니다.

적은 돈으로 시작해서 점점 더 큰돈을 걸게 해요

처음에는 가볍게 시작할 수 있도록 지원금을 주기도 합니다. 게임이 진행될수록 적은 돈에서 점차 더 큰돈을 걸게 합니다.

돈을 잃게 만들어요

불법도박은 참여자가 중독되도록 만들어져 있어, 게임을 하다 보면 돈을 잃게 됩니다.

도박에 중독되게 해요

잃은 돈을 메우려 도박을 멈추지 못하게 됩니다. 도박에 중독되거나 주변에서 돈을 훔치는 등 추가 범죄로 이어지기도 합니다. 또한 친구끼리 정보를 공유하며 도박 피해가 늘어나기도 합니다.

사례로 알아보는 청소년 불법도박

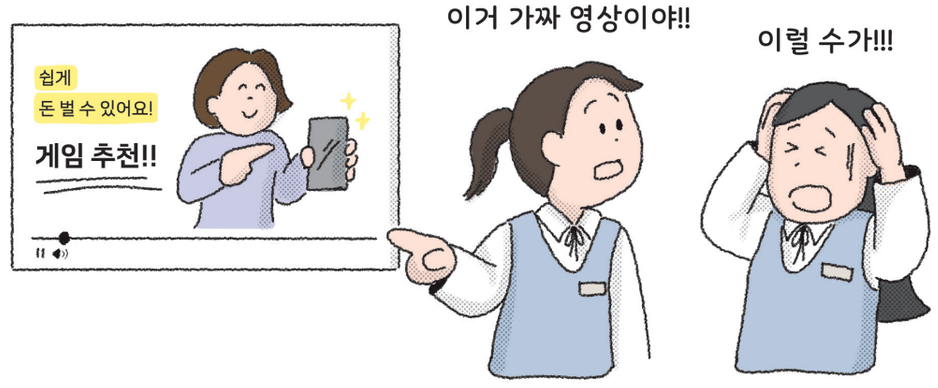
사례 1

“스포츠 결과를 맞히면 돈을 벌 수 있어요!”

야구를 좋아하는 중학생 A씨는 인터넷에서 야구 경기 정보를 찾아보다가, ‘야구 경기 분석 사이트’라는 사이트를 발견했습니다. 궁금한 마음에 사이트에 들어가자 “스포츠 경기 결과를 맞히면 돈을 벌 수 있다”는 팝업이 떴습니다.

A씨는 재미 삼아 5천 원을 걸어 봤습니다. 회원가입이나 본인 인증 없이 바로 사이버 머니로 전환할 수 있었고, 곧 “축하합니다! 2만 원 당첨!”이라는 메시지가 떴습니다. 그렇게 몇 차례 더 돈을 벌자 A씨는 자신감이 붙었고, 설날에 받은 용돈 50만 원을 한꺼번에 걸었습니다.

하지만 이번에는 “꽝”이라는 메시지와 함께 모든 돈이 사라졌습니다. 놀란 A씨는 잃은 돈을 메우려고 친구들에게 돈을 빌리려 했지만, 친구들은 큰돈이라며 거절했습니다. 부모님께 들킬까 두려웠던 A씨는 편의점에서 돈을 훔치려다 경찰에 붙잡혔습니다. 경찰 조사 결과, A씨가 이용한 사이트는 불법도박 사이트로 밝혀졌습니다.



사례 2

“유명 유튜버가 추천하길래 믿고 해 봤어요”

고등학생 B씨는 유튜버 OOO의 오랜 팬이었습니다. 평소처럼 OOO의 영상을 보던 중, OOO이 직접 등장해 “쉽게 돈을 벌 수 있다”며 한 온라인 게임을 광고하는 영상을 보게 되었습니다.

OOO을 좋아하던 B씨는 “좋아하는 유튜버가 하는 거라면 괜찮겠지”라고 생각하며 그 게임 사이트에 가입해 돈을 걸고 게임을 하기 시작했습니다. 처음엔 단순한 호기심이었지만, 곧 푹 빠져들어 점점 더 큰돈을 걸게 되었습니다.

그러던 중 B씨는 친구에게 그 영상을 보여 주었고, 친구는 “이거 이상해. OOO이 만든 영상이 아니라 합성 같아”라고 말했습니다. B씨는 놀라서 영상을 다시 확인하고, 인터넷에 검색해 보았습니다. 알고 보니 그 영상은 OOO의 얼굴과 목소리를 딥페이크해서 만든 온라인 도박 게임 광고였습니다.

이럴 때 청소년 불법도박을 의심해 보세요

아래 내용 중 1개라도 해당된다면 **청소년 불법도박**일 수 있습니다.
청소년 불법도박이 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

광고에 “청소년 전용”, “학생도 이용 가능” 같은 문구가 있어요.

청소년을 노리고 만든 광고입니다. 특히 돈과 관련된 내용이
함께 있다면 불법 광고일 수 있습니다.

실제 돈 대신 사이버 머니와 아이템을 사용해서 안전하다고 해요.

실제로는 사이버 머니를 현금으로 바꾸거나 돈을 걸게 해
결국 금전 피해로 연결됩니다. ‘게임’이라 해도 돈이 오가면 불법으로
여겨질 수 있습니다.

더 많은 정보를 확인하려면 개인정보를 입력하라고 해요.

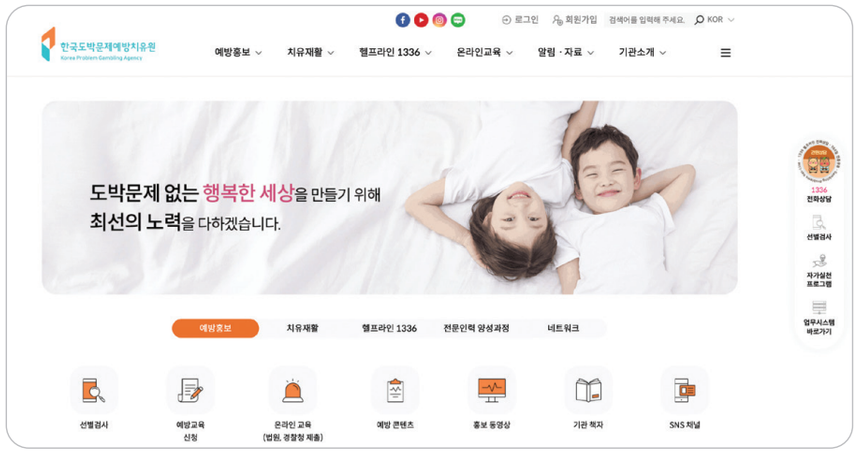
개인정보는 절대 다른 사람에게 함부로 알려 주어서는 안 됩니다.
나의 정보가 범죄에 악용될 수 있기 때문입니다.

사이트에 가입하면 ‘무료 포인트’나 ‘초대 코드’를 보내 준대요.

처음엔 공짜로 가볍게 참여하게 만든 다음,
더 많은 돈을 걸게 만드는 수법입니다.

여기서 잠깐

도박 문제로 어려움을 겪고 있다면
한국도박문제예방치유원에 연락해 보세요.



한국도박문제예방치유원은 도박 중독 위험이 있거나
실제 피해를 겪은 사람들에게 도움을 주는 기관입니다.

이곳에서는 상담 서비스, 예방 교육, 도박 문제 관련 검사 등을 제공합니다.
전화, 채팅, 문자, 게시판 등 다양한 방법으로 상담을 받을 수 있으니,
도움이 필요할 때는 언제든 상담을 신청해 보세요.

청소년 불법도박, 이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

청소년 불법도박 피해를 입었다면, 바로 신고하세요

돈이나 개인정보를 빼앗겼다면 망설이지 말고
바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)

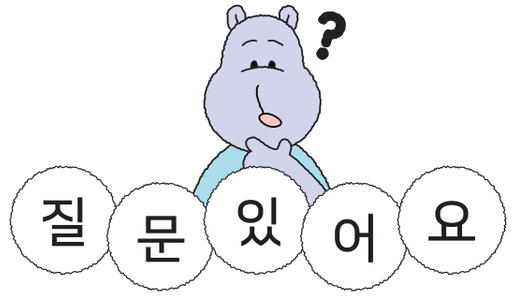
가족이나 믿을 수 있는 어른에게 꼭 알려요

혼자 해결하려 하지 마세요. 부모님, 선생님, 보호자 등
믿을 수 있는 사람에게 바로 말해 도움을 받으세요.
숨기면 상황이 더 나빠질 수 있습니다.

자꾸 접속하게 되면 상담을 받으세요

옳지 않다는 것을 알면서도 불법도박을 끊기 어렵다면
전문 기관에서 상담을 받으세요.

- 한국도박문제예방치유원: 1336 kcgp.or.kr



청소년 불법도박을 하면 어떤 처벌을 받게 되나요?

나이에 따라 처벌 방식이 다릅니다.

- 만 14세 이상: 「형법」에 따라 도박죄로 처벌받을 수 있습니다.
- 만 14세 미만: 형사처벌 대신 소년보호처분을 받게 됩니다.

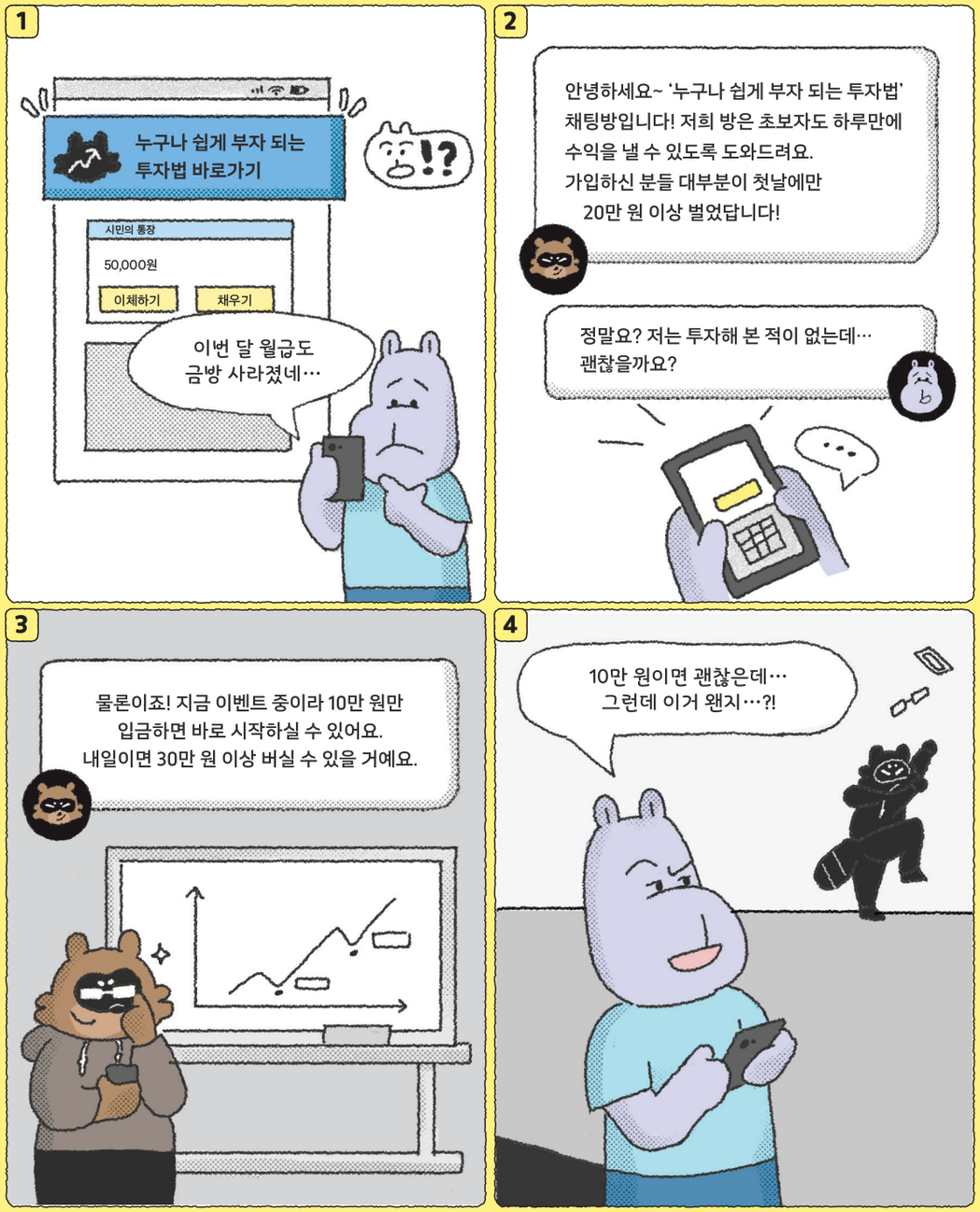
또한 불법 스포츠 도박 사이트를 이용하면 처벌이 더 무거워질 수 있습니다. 「국민체육진흥법」에 따라 5년 이하 징역 또는 5천만 원 이하 벌금을 받을 수 있어, 일반 도박죄(1천만 원 이하 벌금)보다 훨씬 더 처벌이 무겁습니다.

- 청소년 불법도박은 '청소년이 법에서 허락하지 않은 도박에 참여하는 것'을 말합니다.
- 청소년들은 불법도박인지 알지 못한 채 호기심이나 용돈 벌이로 가볍게 시작했다가, 결국 큰돈을 잃거나 중독으로 이어지는 피해를 겪기도 합니다.
- 실제 현금이 아닌, 현금을 사이버 머니로 바꾸어 하는 게임이라도 실제 돈이 오가는 것과 같습니다. 이 또한 불법도박의 한 종류가 될 수 있습니다.
- 청소년 불법도박 피해를 입은 것 같다면, 즉시 믿을 수 있는 어른에게 알리고 경찰에 신고해야 합니다. 불법도박 사이트 화면 등은 모두 캡처해서 증거 자료로 남겨 놓으세요.

청소년의 호기심을 돈벌이 수단으로 이용해서는 안 돼요. 게임처럼 꾸며져 있는 사이트라도 조심해야겠어요.

"진짜 좋은 투자 기회라더니"

투자 사기

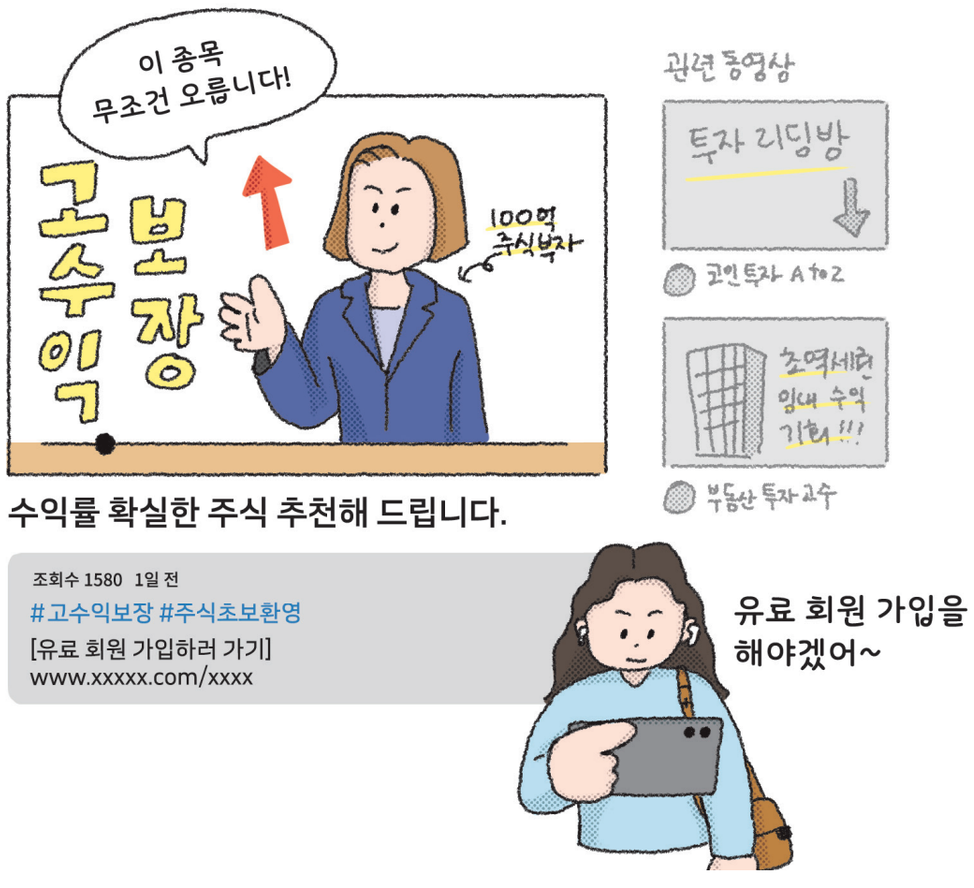


'투자 사기'를 조심해야 하는 상황이에요.
투자 사기가 무엇인지 알아보고, 함께 막아 봐요!

투자 사기란?

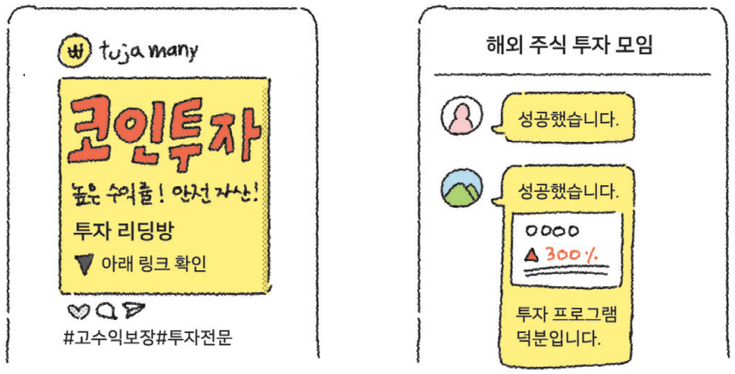
투자 사기는 돈을 불리게 해 주겠다고 속여서
돈이나 개인정보를 빼앗는 범죄입니다.

사기범은 큰돈을 벌 수 있다며 주식, 부동산, 미술품 등
그럴듯한 상품 또는 사업에 돈을 투자하게 해서 돈을 가로챕니다.



투자 사기 유형으로는 이런 것들이 있어요

투자 사기는 '쉽게 돈을 벌 수 있다'는 말로
사람의 욕심과 불안을 이용합니다. 최근에는 SNS, 유튜브, 메신저 등
일상 속 채널을 통해 접근한 다음, 실제 금융상품을 파는 것처럼 꾸며
속이는 수법이 늘고 있습니다.



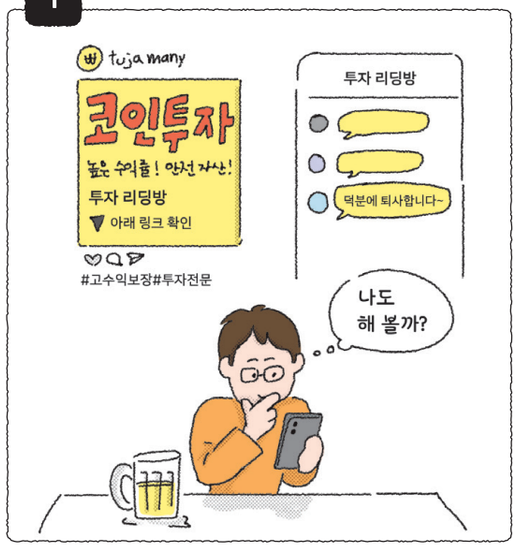
투자 사기 피해, 현재 이런 상황이에요

2024년부터 2025년까지 투자 사기를 경험해 본 비율은
전체 2,573명 중 평균 9.29%, 실제 피해를 본 비율은 평균 2.43%였습니다.
또한, 투자 사기는 '소셜미디어 플랫폼'(27.8%), '온라인 커뮤니티'(27.0%),
'메신저'(25.0%) 등 주로 온라인 공간을 중심으로 발생했습니다.

출처: 한국금융소비자보호재단

투자 사기,
주로 이렇게 일어나요

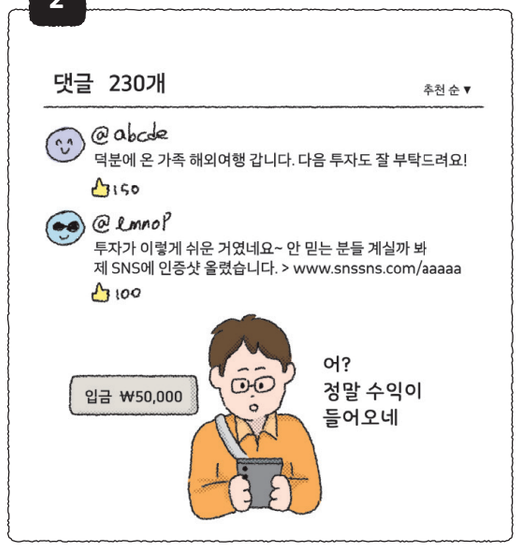
1



좋은 조건의 제안을 해요

사기범은 SNS, 유튜브, 문자, 오픈채팅방 등을 통해 접근합니다. “누구나 쉽게 돈 벌 수 있어요”, “무조건 돈을 벌 수 있습니다” 같은 말로 관심을 끕니다.

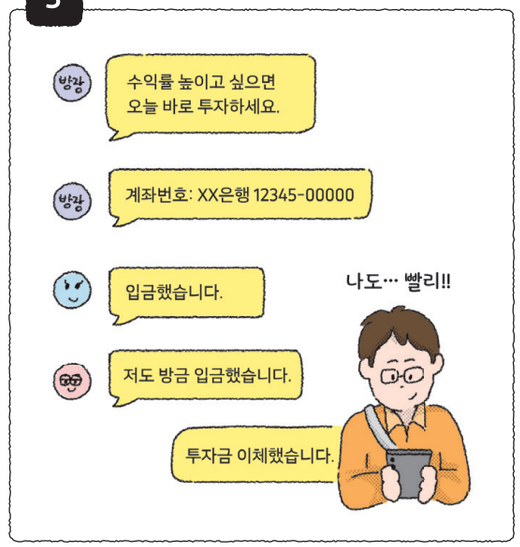
2



믿음을 줘요

돈을 벌었다는 가짜 후기나 인증 사진을 보여 주며 신뢰를 쌓습니다. 처음에는 실제로 돈을 보내 주며, 피해자가 진짜 돈을 벌었다고 생각하게 만들기도 합니다.

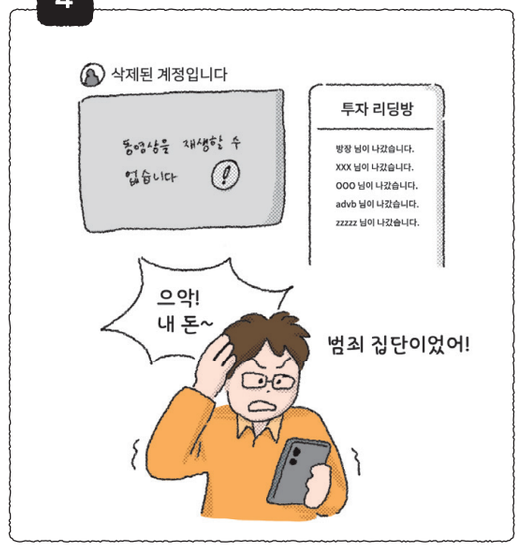
3



투자금을 보내게 해요

“가입비만 내면 시작할 수 있다”, “지금 투자하면 수익이 더 커진다”는 말로 투자금을 늘리게 합니다. 은행 보증서나 계약서 같은 가짜 서류를 보여 주며 진짜처럼 속이기도 합니다.

4



연락을 끊어요

피해자가 돈을 보내는 등 사기범이 원하는 행동을 하면, 사기범은 연락을 끊고 사라집니다. 사이트나 채팅방도 흔적 없이 없어집니다.

사례로 알아보는 투자 사기

사례 1

“이 채팅방에 들어오면 누구나 수익을 낼 수 있어요”

A씨는 평소 경제 정보를 얻기 위해 자주 들어가던 온라인 카페에서 “해외 주식 투자로 고수익을 올릴 수 있다”는 문구와 함께 투자 정보를 공유하는 단체 채팅방을 발견했습니다.

채팅방에는 ‘성공했다’는 사람들의 글과 수익 인증 사진이 계속 올라왔습니다. “저도 처음엔 진짜 될까 의심했는데, 지금은 하루에 30만 원씩 벌어요!”, “이 프로그램만 따라 하면 누구나 수익 낼 수 있어요.” 이런 메시지들에 마음이 흔들린 A씨는 결국 채팅방에서 추천하는 투자 프로그램에 가입하고 돈을 입금했습니다.

하지만 시간이 지나도 수익금은 들어오지 않았고, 채팅방도 갑자기 사라졌습니다. 뒤늦게 확인해 보니, 투자 프로그램은 가짜였고, 채팅방 속 ‘참여자들’ 역시 A씨 같은 피해자를 믿게 만들기 위한 범죄 조직의 사기범들이었습니다.

사례 2

“신재생에너지에 투자해 보실래요?”

공무원으로 일하다 퇴직한 B씨는 은퇴 후 모은 돈을 어떻게 불릴지 고민하던 중, 유튜브에서 ‘신재생에너지 투자로 고수익을 얻는 법’이라는 영상을 보게 됐습니다.

영상에서는 “하루 0.1%~0.3% 수익 보장”, “안정적인 투자”라는 말이 계속 나오고, “진짜 수익 들어왔어요!”, “믿을 만한 투자처예요!” 같은 댓글이 달렸습니다. 처음엔 시험 삼아 적은 금액만 투자했지만, 며칠 뒤 이자가 입금되는 것처럼 보이자 B씨는 안심했고, ‘이 정도면 안전하겠지’ 하는 생각에 아내 몰래 더 큰돈을 투자했습니다.

그러나 다음 날, 투자 사이트에 접속하자 “서버 점검 중”이라는 문구만 뜨고 이후엔 사이트가 완전히 사라졌습니다. 알고 보니 그곳은 유튜브 채널과 홈페이지를 진짜처럼 꾸며 만든 가짜 업체였고, B씨가 본 이자 입금 내역도 모두 가짜 화면이었습니다.

이럴 때 투자 사기를 의심해 보세요

아래 내용 중 1개라도 해당된다면 **투자 사기**일 수 있습니다.
투자 사기가 의심된다면 주변 사람이나 전문가와 꼭 이야기 나눠 보세요.
함께 확인하는 것만으로도 큰 피해를 막을 수 있습니다.

확실한 수익을 약속해요.

투자에 확실한 수익은 없습니다. 확실한 수익을 내게 해 준다는 말을 하면 반드시 사기를 의심해 봐야 합니다.

‘지금 바로 투자해야 한다’며 서둘러요.

시간을 재촉하며 결정을 서두르게 하는 건 사기의 흔한 수법입니다.

‘가입비’나 ‘수수료’를 요구해요.

투자하기 전에 돈을 내라고 하면 100% 사기입니다.
정상적인 투자라면 먼저 돈을 내라고 하지 않습니다.

처음에는 이익을 줘서 신뢰를 쌓아요.

일부 이익을 입금해서 정말 돈을 벌 수 있다고 믿게 만듭니다.
그리고 이후에 더 큰돈을 보내게 합니다.

회사나 담당자를 직접 확인할 수 없어요.

전화, 영상 통화, 만남을 요청해도 계속 피하거나 연락이 끊깁니다.
회사 주소를 물어도 제대로 대답해 주지 않습니다.

유명인이나 금융기관 이름을 내세워요.

잘 알려진 은행이 보증했다거나, 유명 전문가가 추천했다는 말은 거짓일 가능성이 높습니다. 반드시 금융감독원의 ‘파인(fine.fss.or.kr)’ 사이트에 접속하여 실제 존재하는 회사 혹은 기관인지 확인해 보세요.

투자 내용을 ‘비밀로 해 달라’고 해요.

비밀을 강조하면 다른 사람에게 들키면 안 되는 일이라는 뜻입니다.
사기를 의심해 보아야 합니다.

투자 사기,
이렇게 대처해 보세요

금융사기 피해 신고 시 도움이 되는 연락처와 서비스가 더 궁금하다면, 134~136쪽을 확인해 보세요.

투자 사기 피해를 입었다면, 바로 신고하세요

돈이나 개인정보를 빼앗겼다면 망설이지 말고
바로 경찰과 관련 기관에 신고해서 도움을 요청하세요.

- 경찰청: 112 ecrm.police.go.kr (금융사기 통합 피해 신고)

금융정보를 보호하세요

내 금융정보가 새어나간 것 같다면, 돈이 빠져나가는 것을 막기 위해 계좌를 즉시 정지해야 합니다. 이때 아래 방법을 사용할 수 있습니다

- '계좌정보통합관리서비스(payinfo.or.kr)'에 접속해서 직접 지급정지 신청하기
- '개인정보노출자 사고예방시스템(pd.fss.or.kr)'에 접속해서 개인정보가 유출되었는지 확인하고, 추가 계좌 개설을 막기

증거를 꼼꼼히 모아요

사기범의 흔적이 남아 있는 자료라면 무엇이든 도움이 됩니다.
불법 채팅방 화면, 채팅 내역, 불법 사이트 링크 등을 모두 캡처해서 모아 놓으세요. 사기범을 잡을 때 증거 자료로 사용할 수 있습니다.

지인이 추천하는 투자도 사기일 수 있나요?

네, 지인이 추천한다고 해서 무조건 안전하다고 생각하면 안 됩니다. 지인도 이미 사기에 속아 투자하고 있을 수 있습니다. 투자를 하기 전에 그 내용이 진짜인지 스스로 확인해보고, 금융감독원 같은 믿을 수 있는 곳에 물어보는 것이 좋습니다.

오픈채팅방에서 추천해 준 투자 사이트에 들어갔더니 회사 정보가 제대로 나와 있는 것 같아요. 믿어도 될까요?

주소, 전화번호, 사업자등록번호 등 모든 정보가 다 나와 있어도 가짜로 등록한 정보일 수도 있습니다. 특히 "바로 수익을 내게 해 준다" 같은 문구가 있거나, 가입비나 수수료를 요구하면 사기일 가능성이 높습니다.

- 투자 사기는 '돈을 불리게 해 주겠다고 속여서 돈이나 개인정보를 빼앗는 범죄'입니다.
- 투자 사기는 주로 SNS, 메신저 같은 일상 속 채널을 통해 일어납니다. 조건이 좋아 보이는 가짜 금융상품, 투자 프로그램 등을 만들어서 사람들을 속입니다.
- '확실한 수익'을 약속한다는 말은 절대 믿지 마세요. 투자를 제안하는 사람이 정말 믿을 만한지, 또는 관련 기관이 실제로 운영되는 곳인지 꼭 확인해야 합니다. 가족이나 주변 사람에게 한 번 더 물어보거나, 직접 전화해 사실인지 확인해 보세요.
- 투자 사기에 당한 것 같다면, 즉시 경찰에 신고해야 합니다. 불법 채팅방, 채팅 내역, 계좌번호 등은 모두 캡처해서 증거 자료로 남겨 놓으세요.

이제부턴 '수익을 많이 낼 수 있다'는 말에 흔들리지 않겠어요.
아무리 좋은 투자 기회라도 먼저 믿을 수 있는 곳인지
확인해 봐야겠어요.

더 알아보기

- 은행이 보이스피싱을 막기 위해 하는 일
- 금융사기 피해를 신고할 때 도움이 되는 연락처
- 금융사기 피해를 막는 데 도움이 되는 서비스

출처: 「안전한 금융생활을 위한 보이스피싱 대처 방법」(은행연합회 소비자보호부)

은행이 보이스피싱을 막기 위해 하는 일

⚙ 기술·서비스 분야

- 은행마다 실제 운영하고 있는 기술이나 서비스가 조금씩 다를 수 있습니다. 자세한 내용은 각 은행에 직접 문의해 주세요.

❶ 보이스피싱 의심 상황을 꼼꼼하게 살펴요

은행은 보이스피싱 의심 상황을 미리 알아내기 위해 여러 새로운 기술을 사용합니다. 특히 AI 기술을 활용해 돈의 흐름과 고객의 거래 패턴을 분석해 이상한 움직임을 빠르게 찾아냅니다.

대표 예시

- 보이스피싱이 의심되는 거래를 더 꼼꼼하게 살피기 위해, 대부분의 은행은 담당 직원의 근무 시간을 늘렸습니다. 또한 일부 은행은 24시간 동안 해당 업무를 맡는 직원을 두어 의심스러운 거래가 없는지 끊임없이 확인합니다.
- 은행은 여러 사기 거래 패턴을 바탕으로 머신러닝·딥러닝 같은 최신 AI 기술을 활용해 모니터링 시스템을 계속 발전시키고 있습니다. 이를 통해 의심 거래를 더 정확하게 찾아낼 수 있게 되었습니다.
- 은행 앱에도 보이스피싱을 막기 위한 새로운 기능이 추가되었습니다. 이제 은행 앱이 보이스피싱에 사용되는 악성 앱을 자동으로 찾아낼 수 있습니다. 또 보이스피싱이 의심되는 상황에서는, 고객이 앱으로 돈을 보내거나 찾는 기능을 잠시 멈춰 피해를 막을 수 있도록 도와줍니다.

❷ 직원들이 보이스피싱 예방 역량을 키울 수 있도록 지원해요

은행에서는 직원들이 스스로 보이스피싱을 막는 방법을 배우고
역량을 키울 수 있도록 여러 노력을 하고 있습니다.

대표 예시

- 직원을 평가할 때, 보이스피싱 피해를 막는 교육을 받았는지,
  실제로 보이스피싱을 막은 적이 있는지를 중요하게 살펴봅니다.
- 영업 현장에서 보이스피싱 사고를 막은 직원에게는 상을 주는 등 직원들이
  보이스피싱을 막는 일에 적극적으로 참여할 수 있도록 격려합니다.
- 명절처럼 보이스피싱이 많이 일어날 수 있는 기간에는 직원들이 실제
  상황과 똑같이 연습하는 훈련을 하며 보이스피싱에 대처하는 능력을 키웁니다.

❸ 보이스피싱 의심 상황을 고객에게 알려요

은행은 꼭 알아야 할 금융사기 정보가 생기면 문자, 앱 알림, 알림톡 등을 통해
고객에게 빠르게 알립니다. 그 외 다양한 방법으로 고객이 보이스피싱에
관심을 가지고 스스로 조심할 수 있도록 돕습니다.

대표 예시

- 일부 은행은 고객의 휴대폰 번호가 알뜰폰 통신사 번호로 바뀌면,
  이전 번호로 대포폰을 조심하라고 알려 주는 메시지를 보냅니다.
- 일부 은행은 금융 앱에서 금융사기로 의심되는 거래가 발생하면 자동으로
  경고 배너를 띄우고, 보이스피싱을 막는 데 도움이 되는 예방 정보를 함께
  제공합니다.

❹ 통신사와 힘을 합쳐 보이스피싱을 막아요

은행은 통신사와 협력해 보이스피싱 피해가 생기기 전에 미리 막을 수 있도록
노력하고 있습니다.

대표 예시

- 은행과 통신사는 일반 전화번호 목록(화이트리스트)과 사기 문자를
  보낸 적이 있는 전화번호 목록(블랙리스트)을 서로 공유합니다.
  이렇게 해서 고객이 사기 문자를 받지 않도록 미리 차단합니다.

❺ 보이스피싱 피해 예방 서비스를 개발해요

은행은 고객이 스스로 보이스피싱을 더 잘 막을 수 있도록, 원하는 사람이
선택해서 가입할 수 있는 다양한 예방 서비스를 만들고 있습니다.

대표 예시

오픈뱅킹 지킴이 서비스

- 신청한 사람이 오픈뱅킹에 가입하거나 계좌를 새로 만드는 것을 막아 줍니다.

안심케어 서비스

- 고객이 직접 거래할 수 있는 장소, 시간, 계좌를 정해서 안전하게 은행
  서비스를 이용할 수 있게 도와줍니다.

금융사기 피해 보상 서비스

- 사기 피해를 당했을 때, 정해진 조건을 만족하면 보험회사나 은행에서 돈을
  돌려받을 수 있습니다.

가족보안 알리미

- 계좌에서 보이스피싱이 의심되는 거래가 일어나면, 고객의 가족에게 즉시
  알림이 전송됩니다.

📖 교육·홍보 분야

❶ 보이스피싱 예방법을 교육해요

은행은 사람들을 직접 찾아가거나 온라인 강의를 여는 등 다양한 방식으로 보이스피싱 예방 교육을 합니다. 특히 어르신, 외국인 유학생, 보호가 필요한 아동처럼 사기에 당할 위험이 높은 사람들을 위한 교육을 더욱 늘려 보이스피싱 피해를 막고 있습니다.

대표 예시

- 어르신들을 위해서는 보이스피싱 사기가 어떤 것인지, 어떻게 막을 수 있는지를 연극으로 보여 줍니다.
- 초등학생부터 고등학생, 성인들에게 보이스피싱을 막는 방법을 알려 주는 교재를 만들어서 가르칩니다.

❷ 보이스피싱 예방법을 홍보해요

은행은 여러 방법을 통해 사람들이 보이스피싱을 잘 알고 스스로 조심할 수 있도록 돕습니다. 영업점(은행 창구)에서 직접 안내하기도 하고, 알림톡이나 SNS 같은 온라인 채널로 정보를 전달하기도 합니다. 또한 보이스피싱 예방 캠페인을 열거나 TV 광고를 제작해, 많은 사람이 보이스피싱에 대해 쉽게 이해할 수 있도록 합니다.

대표 예시

영업점

- 사람들의 눈에 잘 띄는 곳에 최신 보이스피싱 피해 주의 안내문 등을 둡니다.
- 사은품을 줄 때 보이스피싱 예방 문구를 함께 넣어 안내합니다.
- 영업점 TV에서 보이스피싱 예방 영상을 상영해 자연스럽게 정보를 전달합니다.

공공장소

- 편의점, 지하철역 같은 사람들이 많이 지나는 곳에 보이스피싱 예방 안내문을 붙여 더 많은 사람이 자연스럽게 볼 수 있도록 합니다.

알림톡, 문자 메시지

- 은행은 고객에게 새로운 금융사기 유형과 대처 방법을 알림톡이나 문자를 통해 수시로 안내합니다.

SNS

- 은행은 유튜브, 인스타그램, 페이스북 등 다양한 SNS에 누구나 이해하기 쉬운 보이스피싱 예방 콘텐츠를 올려 많은 사람들이 쉽게 정보를 접하도록 돕습니다.

그 외(캠페인, 영상광고 등)

- 보이스피싱의 위험성을 알리기 위해 캠페인을 진행합니다.
- 신문, TV 등 여러 매체에 보이스피싱 예방 광고를 내보냅니다.

금융사기 피해를 신고할 때 도움이 되는 연락처

정부 기관

경찰청	112 (금융사기 피해신고)
금융감독원	1332 (금융사기 관련 문의 및 상담)
대검찰청	1301 (찐센터, 서류진위 확인)

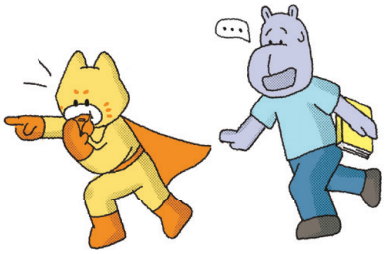
은행

KDB산업은행	1588-1500	**Sh수협은행**	1588-1515, 1644-1515
NH농협은행	1661-3000, 1522-3000	**DGB대구은행**	1566-5050, 1588-5050
신한은행	1577-8000, 1599-8000, 1544-8000	**BNK부산은행**	1544-6200, 1588-6200
우리은행	1588-5000, 1599-5000	**광주은행**	1588-3388, 1600-4000
SC제일은행	1588-1599	**제주은행**	1588-0079
하나은행	1588-1111, 1599-1111	**전북은행**	1588-4477
IBK기업은행	1566-2566, 1588-2588	**BNK경남은행**	1600-8585, 1588-8585
KB국민은행	1588-9999, 1599-9999, 1644-9999	**케이뱅크**	1522-1000
한국씨티은행	1588-7000	**카카오뱅크**	1599-3333
		토스뱅크	1661-7654

금융사기 피해를 막는 데 도움이 되는 서비스

1	금융감독원 **파인 - 제도권 금융회사 조회**	실제로 존재하는 금융회사인지 확인할 수 있는 서비스입니다.	
2	은행연합회 **은행전화번호 진위확인 서비스**	은행을 사칭한 전화나 문자가 의심될 때, 진짜인지 확인할 수 있는 서비스입니다. 은행연합회 소비자포털(portal.kfb.or.kr)에 접속해서 이용할 수 있습니다.	
3	금융결제원 **본인계좌 일괄지급정지 서비스**	내가 가진 모든 계좌를 막아서 더 이상 돈이 나가지 못하게 하는 서비스입니다. 거래 중인 은행의 영업점 방문하거나 전화하여 문의할 수 있습니다. 또한 금융결제원의 계좌정보 통합관리서비스(payinfo.or.kr) 에 접속하여 이용할 수 있습니다. PC와 모바일 앱에서도 이용 가능	
4	금융감독원 **개인정보 노출자 사고예방시스템**	개인정보가 노출된 사람이 등록되면, 다른 사람이 그 사람의 이름으로 계좌, 신용카드, 오픈뱅킹 등을 만들지 못하도록 막아 주는 서비스입니다.	
5	한국정보통신진흥협회 **명의도용된 휴대전화 개설 여부 조회** (Msafer)	누군가 내 이름으로 휴대폰을 새로 만들거나, 내 이름을 다른 사람 이름으로 바꾸려고 하면, 그 사실을 문자로 알려 주는 서비스입니다.	

6	개인정보보호위원회· 한국인터넷진흥원 **털린 내 정보 찾기 서비스**	내 개인정보가 악성 사이트에 올라와 있는지 확인하여 추가 피해를 막도록 도와주는 서비스입니다.	
7	개인정보보호위원회 **정보주체 권리행사 서비스**	내 이름으로 인증된 기록을 한번에 확인할 수 있고, 다른 사람이 내 이름을 사용한 것으로 의심되는 웹사이트는 바로 탈퇴 신청할 수 있는 서비스입니다.	
8	경찰청 **스마트폰 악성앱 탐지 서비스** (시티즌코난)	내 휴대폰에 악성 앱이 설치되어 있는지 검사해 주는 앱입니다. 경찰청과 ㈜인피니그루가 함께 만들었습니다.	
9	**오픈뱅킹·여신거래·비대면 계좌개설 안심차단 서비스**	다른 사람이 몰래 내 이름으로 오픈뱅킹을 연결하거나, 여신거래(대출 신청)를 하거나, 비대면으로 계좌를 만들려고 한다면 이를 차단해 피해를 막아 주는 서비스입니다.	



안전한 금융생활을 위한

사기 예방 백과사전

ISBN 978-89-960237-7-7 03060
비매품/무료