Market Talks
교육 센터

암호화폐 · 초급 · 15강 중 14강

사기, 러그풀, 경고 징후

러그풀과 펌프 앤 덤프부터 가짜 투자 플랫폼, 사칭범, 지갑 드레이너까지 가장 흔한 암호화폐 사기의 작동 방식과 이들이 공통으로 보이는 경고 징후

읽는 시간 11분 퀴즈 8문항, 정답 포함

암호화폐 · 초급 · 15강 중 14강

사기, 러그풀, 경고 징후

한 문장 요약

암호화폐 사기는 해마다 수십억 달러를 빼앗아 갑니다. 대부분은 몇 가지 패턴을 따르며, 그 패턴을 알아보게 되면 경고 징후가 훨씬 쉽게 눈에 들어옵니다.

사기가 암호화폐에서 큰 비중을 차지하는 이유

암호화폐 거래는 빠르고, 국경이 없으며, 되돌릴 수 없습니다. 전화해서 환불을 요청할 은행도, 이미 지갑을 떠난 결제를 동결해 줄 중앙 창구도 없습니다. 암호화폐를 유용하게 만드는 바로 이 특징들이 사기꾼에게도 매력적입니다.

규모도 큽니다. 블록체인 분석 기업 Chainalysis는 2025년 암호화폐 사기 피해액이 사상 최대인 **170억 달러 이상**이라고 추정했습니다. 미국에서만 FBI 인터넷 범죄 신고 센터(IC3)에 접수된 암호화폐 관련 신고의 피해액은 2025년 약 **114억 달러**로, 전년보다 22% 늘었습니다. 그중 약 72억 달러는 가짜 투자 사기에서 나왔습니다.

사기는 점점 더 전문화되고 있습니다. Chainalysis에 따르면 2025년 사칭 사기는 1,400% 넘게 늘었고, 결제 한 건당 평균 피해액은 약 782달러에서 약 2,764달러로 커졌습니다. 이제 많은 조직이 AI로 메시지를 쓰고, 대화를 번역하고, 가짜 영상을 만듭니다.



그림 1. 2025년 암호화폐 사기는 사상 최대 규모에 이르렀습니다. 수치는 Chainalysis의 추정치와 FBI에 접수된 신고를 바탕으로 합니다.

러그풀과 허니팟

러그풀(rug pull)은 토큰이나 프로젝트 뒤에 있는 사람들이 갑자기 돈을 챙겨 사라지는 것으로, 매수자들의 발밑에서 "양탄자를 잡아당긴다"는 뜻입니다. 누구나 몇 분 만에 토큰과 거래 풀을 만들 수 있는 탈중앙화 거래소의 신규 토큰에서 가장 흔합니다(7강과 9강).

흔한 형태는 다음과 같습니다.

- **유동성 회수:** 만든 사람들이 거래 풀에서 자금을 빼 갑니다. 맞바꿀 상대가 남지 않으니 토큰 가격은 거의 0으로 무너집니다.
- **팀 물량 투매:** 만든 사람들이 공급량의 큰 몫을 가지고 있다가 한꺼번에 시장에 팝니다.
- **허니팟:** 토큰의 스마트 계약이 살 수는 있지만 팔 수는 없도록 작성되어 있습니다. 만든 사람 외에는 아무도 팔 수 없으므로 가격 차트는 오르기만 합니다.

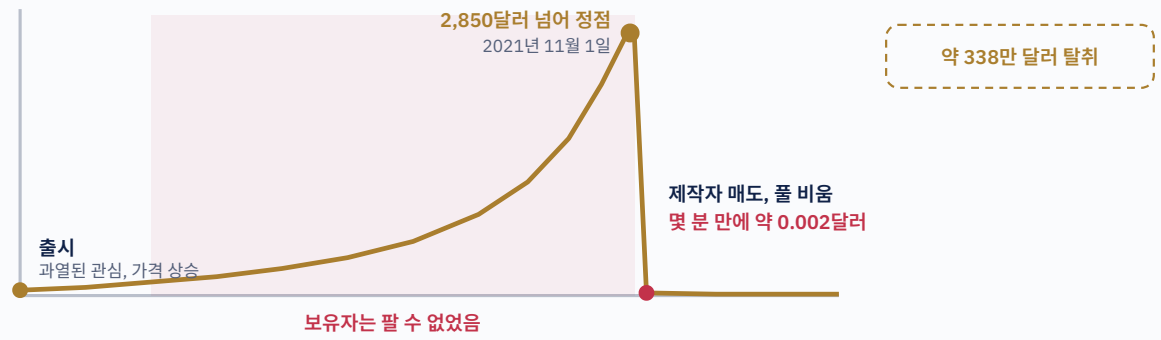


그림 2. 오징어 게임 토큰 러그풀을 단순화한 모습입니다. 가격이 오르는 동안 보유자는 팔 수 없었고, 그 뒤 만든 사람들이 풀을 비웠습니다.

예시: 오징어 게임 토큰, 2021년

2021년 말, 인기 TV 시리즈의 이름을 딴 비공식 토큰이 탈중앙화 거래소 PancakeSwap에 등장했습니다. 가격은 며칠 만에 수만 퍼센트 올라 2021년 11월 1일 **2,850달러**를 넘었습니다. 매수자들은 곧 이 토큰을 팔 수 없다는 사실을 알게 되었습니다. 이어 만든 사람들이 보유 물량을 팔고 풀을 비웠고, 몇 분 만에 가격은 약 **0.002달러**로 떨어졌습니다. 만든 사람들은 약 338만 달러를 챙겨 떠났습니다. 드라마 제작진은 이 토큰과 아무 관련이 없었습니다.

펌프 앤 덤프

펌프 앤 덤프(pump and dump)에서는 한 무리가 거래가 적은 작은 코인을 조용히 사들인 뒤, 소셜 미디어 게시물, 유료 인플루언서, 채팅방을 통해 요란하게 홍보합니다. 새 매수자가 몰려들면 가격이 뛰어오릅니다. 그러면

주도한 사람들이 늦게 들어온 매수자들에게 코인을 팔고("덤프"), 가격은 다시 떨어지며 흔히 출발점보다 낮아집니다.

펌프 앤 덤프가 통하는 것은 작은 코인의 유동성이 매우 적어서(8강) 크지 않은 매수로도 가격이 크게 움직이기 때문입니다. 알려지지 않은 코인에 대해 똑같은 내용의 게시물이 갑자기 쏟아지고, 흔히 카운트다운과 목표 가격이 붙는 것이 전형적인 징후입니다.

가짜 투자 플랫폼과 "돼지 도살" 사기

가장 큰 피해는 가짜 투자 사기에서 나옵니다. 잘 알려진 형태 중 하나가 **돼지 도살**(pig butchering) 사기로, 사기꾼들이 직접 쓰는 중국어 표현을 옮긴 이름입니다. 피해자를 신뢰로 "살찌운" 뒤 "도살"한다는 뜻입니다.

보통은 무해해 보이는 메시지로 시작합니다. "잘못 보낸" 문자, 데이팅 앱 매칭, 소셜 미디어의 새 연락처 같은 것입니다. 몇 주에 걸쳐 사기꾼은 우정이나 연애 관계를 쌓습니다. 그러다 암호화폐 거래로 돈을 잘 번다고 말하고, 방법을 보여 주겠다고 제안합니다.

피해자는 전문적으로 보이지만 가짜인 거래 웹사이트나 앱으로 안내됩니다. 화면 속 잔고는 빠르게 늘고, 처음의 소액 출금은 실제로 되기도 해서 신뢰가 쌓입니다. 입금액은 점점 커집니다. 피해자가 큰 금액을 빼려고 하면 플랫폼은 갑자기 먼저 "세금", "수수료", "해제 보증금"을 내라고 요구합니다. 그 돈을 내고 나면 플랫폼도, 친구도 사라집니다.

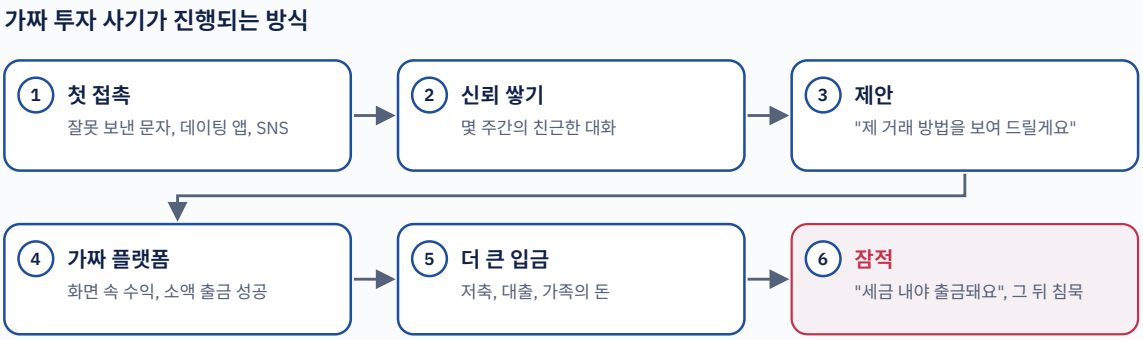


그림 3. 돼지 도살 사기의 일반적인 단계입니다. 신뢰는 천천히 쌓이고, 피해는 마지막에 옵니다.

예시: 안에서 보면 어떤 모습인가

Laura는 Michael에게서 문자를 받습니다. "David, 토요일 골프 약속 그대로죠?" Laura는 번호를 잘못 아신 것 같다고 답합니다. Michael은 사과하고, 두 사람은 대화를 시작합니다. 6주 뒤 Michael은 자신의 거래 수익 스크린샷을 보여 주고, 자신이 쓰는 플랫폼에 Laura가 계정을 여는 것을 도와줍니다. 처음 넣은 1,000달러는 화면에서 1,600달러로 불어나고, 200달러 출금은 실제로 Laura의 지갑에 들어옵니다. Laura는 25,000달러를 입금합니다. 출금을 요청하자 고객 지원은 먼저 수익의 20%를 "세금"으로 내야 한다고 말합니다. 화면 속 숫자는 처음부터 진짜가 아니었습니다.

사칭범, 가짜 고객 지원, 복구 사기

많은 사기는 여러분이 믿는 누군가인 척하는 방식으로 이루어집니다.

- **가짜 고객 지원:** 공개 포럼이나 채팅방에 질문을 올리면, 누군가 거래소나 지갑의 지원팀이라며 개인 메시지를 보냅니다. 실제 지원팀은 먼저 개인 대화를 시작하지 않으며, 시드 문구나 비밀번호를 절대 묻지 않습니다.
- **가짜 거래소 또는 정부 연락:** 전화, 이메일, 문자로 계정이 위험하니 당장 자금을 "안전한" 지갑으로 옮겨야 한다고 말합니다.
- **가짜 유명인과 경품 이벤트:** 영상이나 게시물에서 유명인이 보내는 암호화폐를 두 배로 돌려주겠다고 약속합니다. 이제는 AI로 만든 딥페이크 영상 때문에 그럴듯해 보입니다. 실제 경품 이벤트는 이런 식으로 운영되지 않습니다.
- **복구 사기:** 누군가 돈을 잃은 뒤, "복구 전문가"나 가짜 법률 사무소가 선불 수수료를 받고 돈을 되찾아 주겠다고 제안합니다. 이미 한 번 사기를 당한 사람을 노립니다.

지갑 드레이너, 승인, 가짜 에어드롭

어떤 사기는 여러분이 무언가를 보낼 필요조차 없습니다. 대신 악성 스마트 계약에 토큰을 옮길 권한을 주도록 속입니다.

디파이 앱을 쓸 때 지갑은 흔히 어떤 계약이 대신 특정 토큰을 쓸 수 있도록 **승인**하라고 요청합니다(12강). 무료 **에어드롭**, 민팅, 보상 수령으로 흔히 홍보되는 가짜 웹사이트는 지갑을 연결하고 서명하라고 합니다. 실제로 서명하는 것은 승인이며, 때로는 무제한 금액에 대한 승인이어서 사기꾼의 계약이 토큰을 가져갈 수 있게 됩니다. 이런 도구를 **지갑 드레이너**(wallet drainer)라고 합니다.

그 밖의 흔한 수법으로는 입력하는 시드 문구를 훔치는 가짜 지갑 앱과 브라우저 확장 프로그램, 비슷하게 생긴 웹사이트 주소, 주소 포이즈닝(10강)이 있습니다. 블록체인 과정 9강에서 다뤘듯 **시드 문구**를 가진 사람은 누구

든 지갑을 완전히 통제합니다. 오래된 승인은 제거할 때까지 유효하며, Revoke.cash 같은 도구와 일부 블록 탐색기에서 지갑이 준 승인을 확인할 수 있습니다.



그림 4. 지갑 드레이너는 자금을 보내라고 하지 않습니다. 자금을 가져갈 수 있는 권한에 서명하라고 합니다.

대부분의 사기에 공통된 경고 징후

이야기는 바뀌어도 경고 징후는 되풀이됩니다.

- **보장된 수익이나 매우 높은 수익**, 예를 들어 "하루 2%"나 "위험 없음".
- **재촉과 압박:** 지금 행동하라, 오늘 밤 혜택이 끝난다, 계정이 폐쇄된다.
- **시드 문구나 개인 키 요구**, 이유가 무엇이든.
- **원치 않은 연락**이 서서히 투자 이야기로 넘어가는 것.
- **잘 알려지지 않은 플랫폼**을 새로 사귄 온라인 친구가 추천하는 것, 또는 공식 경로가 아닌 곳에서 받은 앱.
- **먼저 수수료를 내야 하는 출금.**
- **"암호화폐를 보내면 두 배로 돌려준다".**
- **팔 수 없는 토큰**, 공급량 대부분을 가진 익명 팀, 또는 잠기지 않은 유동성.

경고 징후 하나가 사기의 증거는 아니지만, 여러 개가 함께 나타나면 강한 경고입니다.

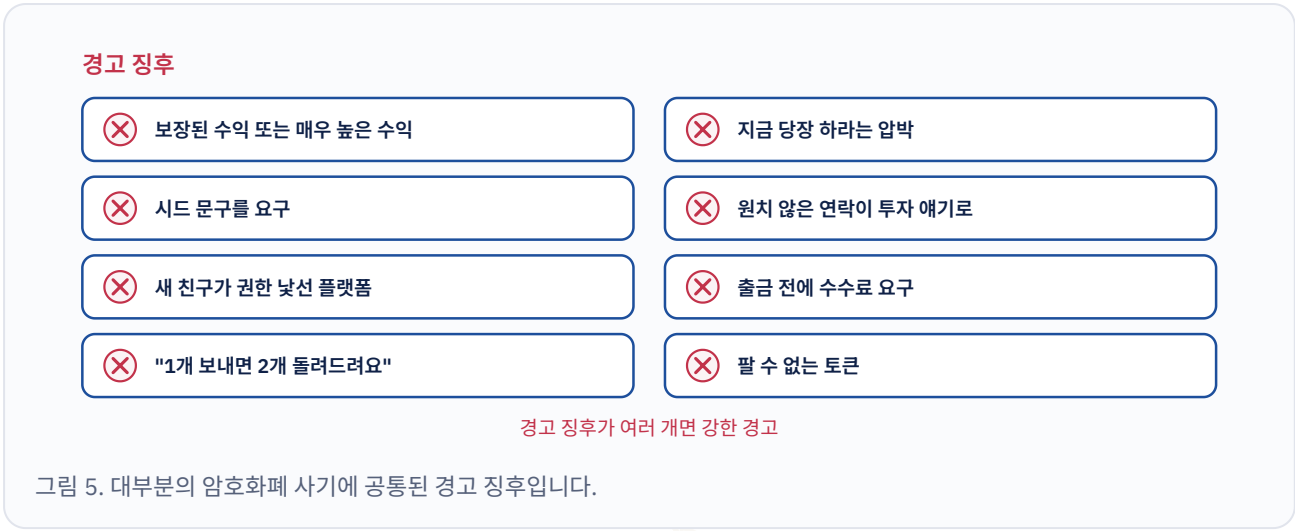


그림 5. 대부분의 암호화폐 사기에 공통된 경고 징후입니다.

사기 이후에 일어나는 일

블록체인 전송은 최종적이므로, 사기꾼에게 보낸 돈이 회수되는 경우는 매우 드뭅니다. 자금이 규제받는 거래소에 빨리 도착하면 그 거래소가 동결할 수 있는 경우가 있고, Tether와 Circle 같은 스테이블코인 발행사가 도난 자금을 동결한 사례도 있습니다.

FBI 같은 당국이 설명하는 절차에는 경찰에 사기를 신고하고 미국에서는 IC3에도 신고하는 것, 이용한 거래소나 플랫폼에 알리는 것, 트랜잭션 해시, 지갑 주소, 메시지, 웹사이트 링크 같은 기록을 남겨 두는 것, 그리고 이미 준 지갑 승인을 제거하는 것이 있습니다. 기존 지갑이 노출되었다고 생각하는 사람들 중 다수는 남은 자금을 새 시드 문구로 만든 새 지갑으로 옮기기도 합니다.

당국은 또한 피해를 신고한 사람에게 나중에 복구 사기꾼이 연락해 오는 경우가 많아, 첫 번째 피해에 두 번째 피해가 이어질 수 있다고 경고합니다.

트레이더에게 왜 중요한가

- **빠른 수익은 사기를 끌어들입니다.** 하루에 엄청나게 오르는 신규 토큰이 바로 러그풀, 허니팟, 펌프 앤 덤프가 일어나는 곳입니다. 토큰을 팔 수 있는지, 공급량을 누가 가지고 있는지, 유동성이 잠겨 있는지 확인하는 것은 많은 트레이더가 하는 기본 조사의 일부입니다.
- **"내 매매를 따라 하세요" 제안.** 입금을 받는 대가로 비공개 매매 정보나 계좌 관리를 약속하는 그룹은 가짜 플랫폼으로 들어가는 흔한 입구입니다.
- **승인은 쌓입니다.** 디파이를 활발히 쓰는 사용자는 시간이 지나면서 오래된 토큰 승인이 많이 쌓일 수 있습니다. 계약이 언젠가 뚫리면 그 하나하나가 위험이 될 수 있습니다.
- **같은 보안 습관이 거래 계정도 지킵니다.** 거래소 계정도 표적입니다. 피싱 이메일, 가짜 로그인 페이지, SIM 스와프는 계정을 탈취해 자금을 출금하려는 수법입니다. 거래소가 제공하는 기본 보호 장치는 15강에서 다룹니다.

핵심 용어

러그풀	프로젝트를 만든 사람들이 유동성을 빼거나 보유 토큰을 투매하는 식으로 갑자기 돈을 챙겨, 토큰을 거의 무가치하게 만드는 것입니다.
허니팟	스마트 계약상 매수는 가능하지만, 만든 사람 외에는 모두 매도가 막혀 있는 토큰입니다.
펌프 앤 덤프	주도 세력이 작은 코인을 사들이고 과장된 홍보로 가격을 끌어올린 뒤, 늦게 들어온 매수자에게 파는 수법입니다.
돼지 도살 사기	사기꾼이 몇 주에 걸쳐 신뢰를 쌓은 뒤, 피해자가 가짜 투자 플랫폼에 큰돈을 입금하도록 유도하는 장기 사기입니다.
피싱	실제 서비스를 흉내 낸 가짜 메시지, 이메일, 웹사이트로 비밀번호, 인증 코드, 시드 문구를 넘겨주도록 속이는 수법입니다.
지갑 드레이너	가짜 웹사이트에 심긴 악성 코드로, 사용자를 속여 토큰을 사기꾼에게 옮기는 승인이나 거래에 서명하게 합니다.
토큰 승인	스마트 계약이 내 지갑의 특정 토큰을 정해진 금액까지 또는 제한 없이 쓸 수 있게 하는, 내가 서명한 권한입니다.
딥페이크	보통 AI로 만든 가짜 영상이나 음성으로, 실제 인물이 하지 않은 말을 하는 것처럼 보여 줍니다.
복구 사기	이미 돈을 잃은 사람을 노려, 선불 수수료를 받고 돈을 되찾아 주겠다고 약속하는 후속 사기입니다.

핵심 정리

1. 암호화폐 결제는 빠르고 최종적이어서 사기꾼에게 매력적입니다. Chainalysis는 2025년 사기 피해액을 170억 달러 이상으로 추정했습니다.
2. 러그풀, 허니팟, 펌프 앤 덤프는 새로 나온 작은 토큰에서 가장 흔합니다. 오징어 게임 토큰은 몇 분 만에 2,850달러 이상에서 거의 0으로 떨어졌습니다.
3. 흔히 긴 온라인 친분을 거쳐 접근하는 가짜 투자 플랫폼이 가장 큰 피해를 냅니다. 가짜 잔고와 초기의 소액 출금이 신뢰를 쌓습니다.
4. 사칭범은 지원팀 직원, 거래소, 공무원, 유명인으로 위장합니다. 실제 지원팀은 시드 문구를 절대 묻지 않습니다.
5. 지갑 드레이너는 자금을 보내라고 하는 대신 서명된 승인을 이용합니다. 오래된 승인은 제거할 때까지 유효합니다.
6. 보장된 수익, 재촉, 시드 문구 요구, 출금 전 수수료가 가장 흔한 경고 징후입니다.

실력 점검

각 문제에 답을 하나씩 표시하세요. 해설이 포함된 정답은 다음 페이지에 있습니다. markettalks.info에서 온라인으로 퀴즈를 풀고 바로 점수를 확인할 수도 있습니다.

1. 암호화폐 결제는 왜 사기꾼에게 매력적인가요?

- A 항상 익명이며 보이지 않는다
- B 빠르고, 국경이 없으며, 되돌릴 수 없다
- C 거래소가 사기꾼의 수익을 보장한다
- D 밤에만 보낼 수 있다

2. 허니팟 토큰이란 무엇인가요?

- A 실제 꿀로 뒷받침되는 토큰
- B 높은 스테이킹 보상을 주는 토큰
- C 계약상 살 수는 있지만 팔 수는 없는 토큰
- D 금에 연동된 스테이블코인

3. 2021년 11월 오징어 게임 토큰에 무슨 일이 있었나요?

A 모든 주요 거래소에 상장되었다
B 만든 사람들이 풀을 비웠고 가격이 2,850달러 이상에서 약 0.002달러로 떨어졌다
C 드라마 제작진이 공급량을 모두 사들였다
D 스테이블코인이 되었다

4. 펌프 앤 덤프에서 보통 누가 돈을 잃나요?

A 먼저 산 주도 세력
B 과장된 홍보를 보고 들어온 늦은 매수자
C 블록체인의 검증자
D 아무도 잃지 않는다, 위험이 없다

5. 돼지 도살 사기에서 초기의 소액 출금은 왜 되는 경우가 많나요?

A 플랫폼이 진짜이기 때문에
B 더 큰 입금 전에 신뢰를 쌓기 위해
C 블록체인 규칙 때문에
D 은행이 강제하기 때문에

6. 누군가 개인 메시지로 지갑 지원팀이라며 문제를 고치려면 시드 문구가 필요하다고 합니다. 이것은 무엇인가요?

A 일반적인 지원 절차
B 필수 보안 점검
C 전형적인 사칭 사기
D 소프트웨어 업데이트

7. 지갑 드레이너는 보통 어떻게 토큰을 가져가나요?

A 비밀번호를 추측해서
B 가짜 사이트에서 승인이나 거래에 서명하게 만들어서
C 블록체인 전체를 해킹해서
D 토큰 가격을 바꿔서

8. 다음 중 흔한 사기 경고 징후는?

A 출금 전에 수수료를 요구하는 플랫폼

B 언제든 토큰을 팔 수 있는 것

C 공개 감사를 받는 잘 알려진 거래소

D 오르기도 하고 내리기도 하는 가격

정답 및 해설

1 B

빠르고, 국경이 없으며, 되돌릴 수 없다

전송이 확정되면 은행이나 결제 회사가 되돌릴 수 없고, 자금은 몇 분 만에 국경을 넘을 수 있습니다.

2 C

계약상 살 수는 있지만 팔 수는 없는 토큰

계약이 일반 보유자의 매도를 막기 때문에, 만든 사람들이 현금화할 때까지 가격이 오르기만 하는 것처럼 보입니다.

3 B

만든 사람들이 풀을 비웠고 가격이 2,850달러 이상에서 약 0.002달러로 떨어졌다

매수자들은 팔 수 없었고, 이어 만든 사람들이 팔고 유동성을 가져가면서 가격이 몇 분 만에 무너졌습니다.

4 B

과장된 홍보를 보고 들어온 늦은 매수자

주도 세력은 일찍 사서 홍보 뒤에 들어온 사람들에게 팔고, 늦은 매수자에게는 떨어지는 코인만 남습니다.

5 B

더 큰 입금 전에 신뢰를 쌓기 위해

소액을 빼 주면 가짜 플랫폼이 진짜처럼 보이고, 피해자는 안심하고 훨씬 많은 돈을 입금합니다.

6 C

전형적인 사칭 사기

시드 문구를 가진 사람은 누구든 지갑을 통제합니다. 실제 지원팀은 시드 문구를 절대 묻지 않습니다.

7 B

가짜 사이트에서 승인이나 거래에 서명하게 만들어서

사용자가 흔히 에어드롭 수령처럼 꾸며진 권한에 서명하면, 사기꾼의 계약이 토큰을 옮길 수 있게 됩니다.

8 A

출금 전에 수수료를 요구하는 플랫폼

출금을 풀어 주기 전에 세금, 수수료, 보증금을 요구하는 것은 가짜 플랫폼의 전형적인 징후입니다.

출처

- Decrypt, AI와 사칭 사기로 2025년 암호화폐 사기 피해액 사상 최대 170억 달러(Chainalysis): https://decrypt.co/354624/ai-impersonation-drove-crypto-scam-losses-record-17-billion-2025-chainalysis
- Yahoo Finance, FBI, 2025년 암호화폐 사기 피해 22% 증가 보고: https://finance.yahoo.com/markets/crypto/articles/fbi-reports-22-rise-crypto-191510401.html
- Cointelegraph, 오징어 게임에서 이름을 딴 암호화폐 사기, 가격이 2,800달러에서 0으로 폭락하며 붕괴: https://cointelegraph.com/news/game-over-squid-game-inspired-crypto-scam-collapses-as-price-crashes-from-2-8k-to-zero
- Cointelegraph, 오징어 게임 토큰을 팔 수 없는 사용자들: https://cointelegraph.com/news/users-not-able-to-sell-squid-game-token-clocking-45-000-gains

Market Talks

계속 학습하기

다음: 15강 실제로 시작하는 법: 거래소, KYC, 지갑

이 강의는 MARKET TALKS 교육 센터의 암호화폐 과정에 속합니다. 초급 강의는 무료이며 강의마다 퀴즈와 다운로드 가능한 PDF가 제공됩니다. 중급과 고급 강의는 회원 전용입니다.

교육 센터
기초 원리부터 고급 주제까지 다루는 강의

시장 분석
주요 시장에 대한 기술적 분석과 기본적 분석

리포트
비트코인, 금, 은, SPX 등

markettalks.info

텔레그램 @MARKET_TALKS

교육 목적으로만 제공됩니다. 이 문서의 어떤 내용도 투자 조언이 아닙니다. © 2026 MARKET TALKS. 이 PDF는 수정 없이 자유롭게 공유하실 수 있습니다.