# AI와 함께 해외송금·환전 사칭 "입금 후 출금 차단" 사기 사이트의 증거를 보존하고 각 기관에 신고한 사례

전국민 AI활용 사례 공모전 시즌 3 | 분야: 생활 속 AI 활용(금융·소비) | 응모자: 박성상 | 사용 AI: Claude(Anthropic), Claude Code 환경

## 1. 사례 개요

- 대상: 해외송금·환전 서비스를 사칭해 입금을 유도하고 출금을 막는 사기 의심 사이트 1건(주소는 qtorm****.shop 으로 마스킹).
- 기간: 2026년 10월 11일~12일 조사·증거 수집, 12일 08:45~15:15 신고 집중 발송.
- 핵심: 일반 시민이 가입·로그인·입금 없이 공개 정보만으로 사기 구조를 확인하고, 증거를 해시(SHA-256)로 고정한 뒤, 서버·CDN·도메인·메일·채팅 사업자와 수사·침해대응기관 10여 곳에 신고했다.
- 역할: 응모자는 범위(공개 정보만)·신고처 결정·결과 검토를 맡았고, Claude는 분석·수집 스크립트·보고서·신고 메일 작성과 회신 정리를 수행했다.

## 2. 진행 절차와 AI의 역할

| 단계 | 응모자의 지시 | Claude가 한 일 |
|---|---|---|
| 1 분석 | 공개 정보만 볼 것. 가입·로그인·입금 금지 | 공개 설정 파일(JSON)과 메인 JS 분석, 구조 요약 |
| 2 보존 | 원본을 그대로 보관 | 수집 스크립트 작성, 수집 시각·출처·방법과 SHA-256 해시 목록 기록(65건), 메일 원본 35통 보관 |
| 3 추적 | 운영 정황 확인 | 도메인·IP 등록정보, 라우팅 기록, 과거 서버 주소 조회. 확인된 것과 추정을 구분 표기 |
| 4 문서 | 수사기관·해외 업체 제출용 | 한국어 신고서, 영어·중국어 증거 보고서, 해외 수사기관 신고 입력 내용 작성 |
| 5 신고 | 신고처 결정, 결과 검토 | 기관별 양식·언어로 메일 작성·발송, 접수 확인·거절 회신을 시각순으로 정리, 거절에는 반박 자료와 기한을 정리해 재발송 |

## 3. AI 분석으로 드러난 사기 수법(일반화)

| 수법 | 확인 근거(공개 정보) |
|---|---|
| 단계별 출금 차단 문구 | 사이트 설정에 1단계 "인증된 계좌 필요", 2단계 "수수료 미납", 3단계 "외환거래법상 신분확인 필요"가 모두 "고객센터 문의"와 함께 미리 저장됨 -> 출금 시 핑계를 대며 추가 입금 유도 |
| 경고 무력화 | 접속 즉시 "사기피해·피해복구 글은 허위사실, 법적 대응" 팝업을 띄워 피해자가 경고를 믿지 못하게 함(첨부2) |
| 도메인 교체 장기 운영 | 설정 생성일은 2022년, 도메인 등록은 2026년 10월 -> 도메인만 바꿔 4년 넘게 운영한 정황 |
| 서버 은닉 | Cloudflare 프록시 뒤에 실제 서버를 숨김. 다만 JS 파일에 과거 서버 주소가 남아 있어 소유 기관과 라우팅 기록까지 추적 가능 |
| 신원 위장 | 하단 사업자 표기는 무관한 업체의 정보를 도용한 것으로 추정 -> 운영자 신원으로 취급하지 않음 |
| 유사 범행 단서 | 같은 IP를 2022~2023년에 쓴 일본어 유사 사이트가 공개 DNS 기록·웹 아카이브에 있음. 다른 고객이 쓴 시기도 있어 "참고 단서"로만 분류 |

## 4. 결과와 한계

- 증거(원본 + 수집 기록 + 해시 + 설명서)를 수사기관에 낼 수 있는 형태로 정리했고, 피해자 입금 내역이 확보되면 그대로 붙여 제출할 수 있다.
- 신고 대상을 서버·CDN·도메인·메일·채팅·결제 계좌 층으로 나눠, 한 곳이 거절해도 다음 층으로 이어갈 수 있었다. 호스팅 업체는 정형 거절을 반복해 반박 자료와 기한을 정리해 재신고했다.
- 한계: 신고 후 사이트 차단·운영자 확인 여부는 확인하지 못했다. 피해자 정보는 보유하지 않아 신고서에 적지 않았다. 범인 특정과 판단은 수사기관의 몫이다.

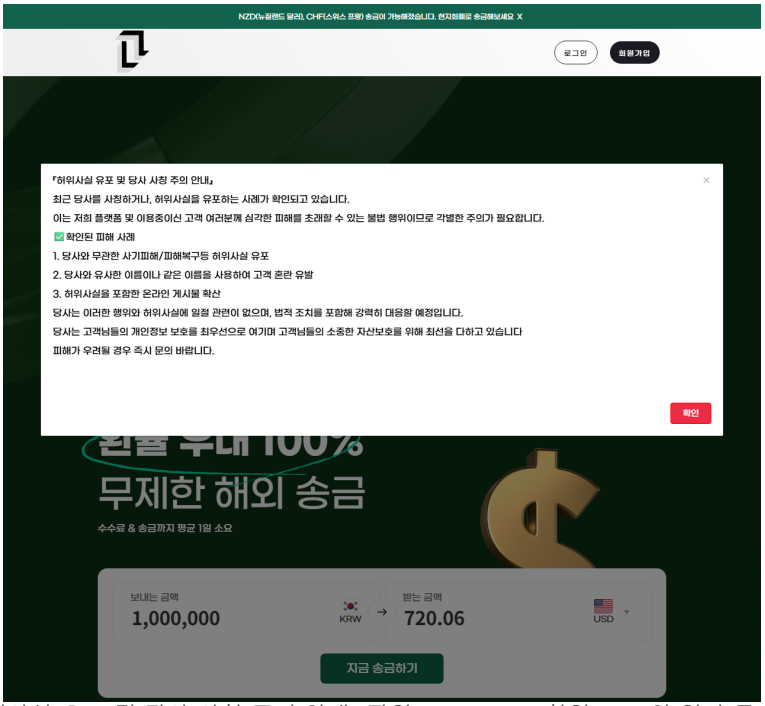
## 5. 나만의 방식

- 사람이 범위와 원칙을 정하고 AI가 반복 작업을 수행(공개 정보 한정, 로그인·입금 금지).
- 증거 보존을 첫 단계로: 내려받자마자 수집 시각·출처·SHA-256 해시를 기록.
- "확인된 사실 / 추정 / 요청"을 분리해 쓰게 해 과장 없는 신고서 작성.
- 신고 대상 층별 체크리스트를 만들어 다음 사건에도 재사용 가능.

## 6. 따라 하는 방법과 주의점

- 이미 입금했다면 가장 먼저 은행 지급정지 요청과 경찰 신고(경찰청 사이버범죄 신고시스템)를 한다.
- 의심 사이트에 가입·로그인·입금을 하지 않고, 화면 캡처와 주소를 보관한다.
- AI에게 공개 정보만 수집하도록 하고, 수집 시각·출처·SHA-256 해시를 함께 남기게 한다.
- AI에게 사실·추정·요청을 구분한 신고서를 쓰게 한 뒤, 사람이 원본과 대조해 확인한다.
- 호스팅·CDN·도메인 등록 기관·메일·채팅 서비스·은행·경찰·KISA·금융감독원 신고처 목록을 AI와 함께 만든다.
- 확인되지 않은 사람이나 업체를 범인으로 단정하지 않는다. 도용된 정보의 주인은 피해자일 수 있다.
- 개인정보와 비공개 정보는 신고서 외에 공개하지 않는다. 이 설명서도 도메인을 일부 가리고 도용 추정 업체·관리자 이메일·채팅 키·IP·신고 번호를 뺐다.

## 7. 첨부2 사이트 화면(주소·계좌·이메일 등 식별정보가 화면에 없음)




접속 즉시 표시되는 "허위사실 유포 및 당사 사칭 주의 안내" 팝업(2026-10-12 촬영, 로그인 없이 공개 화면). 피해 경고를 허위로 몰아 무력화하는 장치로 보인다.