사기일까요?

누르기 전에, 돈 보내기 전에, 답하기 전에 확인하세요

흔한 사기의 네 가지 신호

1. **사칭.** 은행, 정부 기관, 잘 아는 회사, 또는 가족인 척합니다.
2. **문제나 당첨.** 계좌가 막혔다, 돈을 내야 한다, 상품에 당첨됐다고 합니다.
3. **재촉.** 지금 바로 하라고 합니다. 전화를 끊지 말라, 아무한테도 말하지 말라고 합니다.
4. **돈 요구.** 기프트카드, 송금, 결제 앱, 암호화폐, 현금, 또는 받은 수표에서 돈을 일부 돌려보내라고 합니다.

이런 연락이 오면? 잠깐 멈추고 전화를 끊으세요. 카드 뒷면에 있는 번호처럼, 진짜 번호를 직접 찾아서 거세요.

꼭 기억할 FTC(미국 연방거래위원회) 원칙

- 휴대폰으로 온 인증번호를 알려 달라는 사람은 사기꾼입니다.
- 기프트카드로 돈을 내라는 사람은 사기꾼입니다.
- 돈을 지키려면 다른 곳으로 옮기라는 사람은 사기꾼입니다.
- 진짜 보안 경고창은 절대 전화를 걸라고 하지 않습니다.

이렇게 하세요

- 링크를 누르거나 답장하지 마세요. 그 회사 앱을 직접 열거나, 웹 주소를 직접 입력하세요.
- 사기 문자는 7726(SPAM)으로 전달하세요.
- 사기는 ReportFraud.ftc.gov에 신고하세요. 60세 이상이시면 노인 사기 핫라인(Elder Fraud Hotline) 833-372-8311에 전화하셔도 됩니다.

수상한 점 찾기

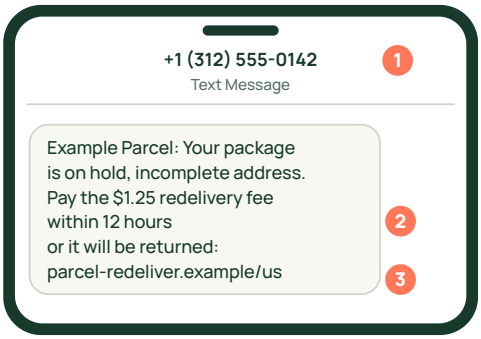


그림 예시입니다. 미국에서 실제로 받는 문자처럼 영어로 보여 드립니다. 회사 이름, 번호, 링크는 모두 지어낸 것입니다.

1. 모르는 번호입니다. 이 회사 문자를 받겠다고 신청하신 적이 있나요?
2. 아주 적은 수수료에 마감 시간까지 붙어 있습니다. 진짜 노리는 건 카드 번호입니다.
3. "해결하려면" 누르라는 링크가 있습니다. USPS(미국 우체국)는 배송 알림을 신청한 경우에만 문자를 보내고, 그 문자에는 링크가 없습니다.

로고 말고 웹 주소를 보세요

https:// 다음에 나오는 첫 번째 빗금(/)을 찾으세요. 그 바로 앞에 있는 이름이 진짜 주인입니다.

https://www.**examplebank.example**/login
✓ **진짜 사이트입니다. 첫 빗금 바로 앞 이름이 은행 자기 이름입니다.**

https://examplebank.example.**account-check.example**/login
✕ 은행 이름이 들어 있지만 미끼입니다. 진짜 주인은 account-check.example입니다.

https://www.**examp1ebank.example**/sign-in
✕ 비슷하게 만든 가짜입니다. 영어 l 자리에 숫자 1이 들어갔습니다.

https://**examplebank-secure.example**/verify
✕ 뒤에 단어가 하나 더 붙었습니다. 은행 주소가 아닙니다.

AI에게 한 번 더 물어보기

> 이 문자를 받았는데 아직 아무것도 누르지 않았어요. 제 개인 정보는 지웠어요. 쉬운 말로 알려 주세요. 누가 보냈다고 하는지, 저한테 뭘 하라고 하는지, 사기일 수 있는 신호가 있는지요. 그리고 문자에 있는 링크나 번호를 쓰지 않고 제가 직접 확인할 방법도 알려 주세요. 문자 내용: **[여기에 문자 붙여넣기]**

이름, 계좌번호, 인증번호는 먼저 지우세요. ChatGPT 같은 AI 앱에는 한국어로 물어보셔도 됩니다. AI도 틀릴 수 있으니 꼭 그 회사에 직접 확인하세요.

영어로 된 전체 안내서 **Is This a Scam?**에는 흔한 사기 십여 가지와 표시된 예시, 피해 후 대처법, 인쇄용 카드, AI 질문 25개가 들어 있습니다. aiveryhuman.com에서 보실 수 있습니다.

일반 정보이며 법률이나 금융 조언이 아닙니다. 2026년 10월 23일 FTC, FBI, CISA, USPIS, 사회보장국(SSA) 자료로 확인했습니다. 결과를 보장하지 않습니다. 피해를 입으셨다면 은행에 연락하고 신고하세요. 예시는 모두 지어낸 것입니다. 상표는 각 소유자의 것이며, aiveryhuman은 언급된 기관이나 회사와 관계가 없습니다.

aiveryhuman