



스푸핑 스캠 방지하기

전화 스캐머는 때로 불법 스푸핑 기술을 사용하여 발신인 ID 디스플레이에 잘못된 정보를 보내 자신의 정체성을 위장합니다. 귀하를 속여 전화를 받도록 하기 위해, 스푸핑 스캐머는 익숙한 지역 번호와 전화번호를 사용할 수 있습니다. 또한 거래하는 회사, 지역 공공 시설 또는 정부 기관으로 가장할 수도 있습니다.

스푸핑을 피할 수 있는 몇 가지 좋은 방법이 있습니다:

- 알 수 없는 발신인으로부터 걸려온 전화를 받지 마십시오.
- 화를 받았으나 알고 있는 발신인이 아닌 경우, 받지 말고 끊으십시오.
- 발신인이 더 이상 전화를 받지 않으려면 버튼을 누르라고 해도, 그냥 전화를 끊으십시오.
- 예기치 않은 전화의 발신자 ID가 합법적일 것이라고 가정하지 마십시오. 전화를 끊고 청구서, 명세서 또는 공식 웹 사이트에서 확인할 수 있는 번호로 전화를 거십시오.
- 의심하십시오. 사기꾼들은 매우 설득력이 있습니다. 악의 없는 질문을 하거나, 위협적인 말을 하거나, 믿을 수 없을 만큼 선하게 느껴질 때도 있습니다.
- 계좌 번호, 사회 보장 번호 또는 비밀번호와 같은 개인 신상 정보를 알려주거나 보안 관련 질문에 대답하지 마십시오.
- 즉시 지불을 하라고 압력을 가한다면 세심한 주의가 필요합니다.
- 귀하의 전화 회사에 유선 또는 휴대 기기용 애플리케이션의 통화 차단 도구를 요청하십시오.
- 법 집행 기관, FCC 및 FTC에 스푸핑 스캠을 신고하십시오.



Avoid Spoofing Scams

Phone scammers often disguise their identity by using illegal spoofing techniques to send false information to your caller ID display. To trick you into answering, spoofer may use local area codes and numbers that look familiar. Or they may impersonate a company you do business with, such as a local utility, or even a government agency.

Here are some good ways to avoid being spoofed:

- Don't answer calls from unknown numbers.
- If you answer and it's not who you expected, don't hang on, hang up.
- If a caller asks you to hit a button to stop getting calls, just hang up.
- Never assume an unexpected call is legitimate. Hang up and call back using a number you can verify on a bill, a statement, or an official website.
- Be suspicious. Con artists can be very convincing: They may ask innocuous questions, or sound threatening, or sometimes seem too good to be true.
- Don't give out personal information – account numbers, Social Security numbers or passwords – or answer security questions.
- Use extreme caution if you are being pressured for immediate payment.
- Ask your phone company about call blocking tools for landlines or apps for mobile devices.
- Report spoofing scams to law enforcement, the FCC and the FTC.

