FCC | CONSUMER CONNECTIONS

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, spoofers 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.

FCC **Learn more at fcc.gov/spoofing**