An official website of the United States government Here's how you know

Scam Glossary

For Consumers

- Help Center Overview
- Consumer Complaint Center
- Scam Glossary
- Disability Rights
- Headlines
- Social Media
- National Consumer Protection Week Toolkit

The FCC scam glossary describes robocall scams, spoofing scams and related consumer fraud, which the FCC tracks through complaints filed by consumers, news reports, and notices from other government agencies, consumer groups and industry sources. Glossary entries include links to more detailed information posted in the Consumer Help Center and to trusted external sources.

| A | B | C | D | E | F | G | H | I | L | M | N | O | P | R | S | T | V | W

#	
809 Scam	A scammer leaves an urgent voicemail and a call-back number with an 809 area code. While it appears to be a three-digit U.S. area code, it's actually an international number. If you call, you'll be charged international rates while the person answering tries to keep you on the line as long as possible. Similar to the "One Ring" Scam.
90# Scam	Someone impersonating a telephone company employee calls your landline phone and asks you to dial 90# to connect to an outside line. This enables them to bill their calls to your account.
A	
Auto Warranty Scam	A scammer calls you with a sales pitch for renewing your auto warranty or insurance policy. The scammer may have acquired information about your car and its existing warranty to make the offer seem more credible.

Return to Top

B	
Back-to-School Scams	Calls or messages to students and parents may offer school shopping deals, scholarships, college housing rentals, and student loan forgiveness. Regardless of the approach, ultimately fraudsters are trying to steal your personal information, your identity, and your money.
Bank Account Smishing	You get a text message that seems to be from a bank, telling you a hold has been placed on an account in your name and providing a link to reactivate it. Selecting the link may download malicious software, giving scammers access to banking and other information on your phone.
Bank Impersonation Scams	Scammers pretend to be your bank through calls, texts, or emails, often claiming there's suspicious activity on your account. They use urgency to trick

	you into sharing personal or financial information, sending money, or transferring funds to a so-called "safe" account.

Return to Top

C	
Cable & Streaming Service Discount Scam	Watch out for robocalls, voicemails, and texts offering 50% off of your cable or streaming service monthly bill. The callers urge customers to "act immediately" or lose the discount, then request payment with gift cards.
"Can You Hear Me" Scam	Scammers open by asking a yes-or-no question, such as: "Can you hear me?" or "Is this X?" Their goal is to record you saying "yes" in response. They then may use that recording to authorize charges over the phone.
Cellphone Fraud	Cellular fraud is defined as the unauthorized use, tampering or manipulation of a cellular phone or service. Types of cellular fraud include SIM swapping, cloning and subscriber fraud.
Charity Scams	Scammers call asking for charitable donations, often after large-scale disasters. They may make up phony charities or spoof a real charity to trick you out of your money.
Chinese Language Robocall Scams	Phone scam calls targeting Chinese speaking consumers appear to be trending up again. The FCC and law enforcement agencies have received multiple reports from members of the Chinese community about individuals impersonating health-care providers, federal employees (including the FCC), and police officers from China.
Cramming	Cramming is when phone companies or third-party billing companies place misleading, unauthorized, deceptive or poorly explained charges on a phone bill.
Credit Card/Interest Rate Scams	Scam callers pretending to represent banks and credit card companies use a variety of tactics, such as bogus fraud alerts or promises of lowered interest rates, to steal your personal information and your credit.
Cryptocurrency Scams (Federal Trade Commission)	A crypto scammer may call claiming to be from the government, a local utility company, or even a romantic interest directing you to withdraw money from your bank account.

Return to Top

D	
Disaster Relief Scam	After disasters, some callers may impersonate charities, seeking disaster aid. Before giving money, verify that you're talking with a real charity.

Return to Top

E	
Email/Phishing Scams (Federal Trade Commission)	Scammers often use email "phishing" to hook unsuspecting fraud victims. Treat all unsolicited email and spam as suspicious: Do not open or reply. To avoid loading malicious software onto your computer or device, never click a link – even from a trusted source – unless you've verified its authenticity. Be

	especially wary of emails asking for emergency funds or help from friends, family and colleagues. Their email accounts may have been hacked. Scammers will also pretend to be government agencies in scam emails.
Employment Scam (Better Business Bureau)	Bogus job postings, recruitment emails and online ads - often illegally using legitimate company names – are all tools scammers use to defraud people seeking employment. Always be suspicious of quick offers with high salaries or pre-payment requests for coaching, training or certifications, and never share personal information until you're certain a job posting is legitimate. Many employment scams also offer advanced payment for supplies. These checks will often bounce, costing you money.

Return to Top

F

How to Spot FCC Imposters	Identity thieves that impersonate the FCC in calls, texts and emails are using names of FCC employees, which are publicly available, to make the call seem more convincing. Always verify any contact from the FCC.
Free Trial Scams (Federal Trade Commission)	Free-trial product offers you receive over the phone may be too good to be true. You may be asked to pay a small fee by credit card, which can lead to other unwanted fraudulent charges, or you may be unable to cancel after the trial runs out, forcing you to pay for the product in question.
Flood Insurance Scam	After floods, scammers may target hard hit areas with fake calls about flood insurance to steal private information or money. They may spoof a legitimate flood insurance company to appear more convincing.

Return to Top

G

Gift Card Scams (Federal Trade Commission)	A telltale sign of phone scams is if the caller asks you to make a payment with a gift card. Many scammers prefer this non-refundable and hard to trace form of payment.
Google Listing Scams (Google My Business Help)	Some scammers claim that they can add or remove you or your business from Google searches or similar services. These callers, unaffiliated with Google, seek payment for services they can't deliver.
Government Grant Scam (Federal Trade Commission)	Scammers claim that you are eligible for a government grant and offer to forward it to your checking account as soon as you give them your account information, which they sell or use to steal your money. The scammer may spoof the number of the government agency they claim to be representing.
Grandparent/Family Emergency Scam	Scammers sometimes prey on grandparents by claiming their family members are in jail or in trouble and need money quickly. They use stolen personal information such as family member names and hometowns to seem more convincing.

Return to Top

H

Health Insurance Scam	In 2024, insurance scams topped the list of robocall complaints filed with the FCC. While these calls tend to spike during health care Open Enrollment season, fraudsters may use similar approaches year-round.
Holiday Scams	Don't let scammers stifle your giving spirit. Holiday scams come in various forms that include unsolicited calls and texts, fake ads and emails. A few of the most common scams making the rounds this holiday season involve fake charities.

Return to Top

I

Identity Theft Scams (USA.gov)	Callers posing as government officials, often from the Social Security Administration, claim that you've been a victim of identity theft. These scammers ask for personal information or payment of some kind, or access to your bank account.
Imposter Scam (Federal Trade Commission)	A caller poses as someone you know or trust in order to obtain money or personal information. They often spoof a legitimate caller's number to appear more realistic.
Interest Rate/Credit Card Scams	Scam callers pretending to represent banks and credit card companies use a variety of tactics, such as bogus fraud alerts or promises of lowered interest rates, to steal your personal information and your credit.
Investment Scams (Securities and Exchange Commission)	When a caller claims to have a promising investment opportunity that will help you get rich quick, it's likely a scam.
IRS Call Scam	Scammers sometimes pose as IRS agents, threatening legal action and demanding money or personal information over the phone. To appear legitimate, imposters may attempt to spoof an IRS number.

Return to Top

L

Low Power FM Radio Scam	LPFM Radio applicants may receive phone calls or messages offering to help with the application process or prompting them to buy a "Part 15" device for a fee. Their expertise or expensive devices aren't needed. The FCC authorizes all licenses for LPFM radio stations.

Return to Top

M

Medicare Scams	Older Americans with Medicare eligibility should be on alert for scam calls that can lead to health insurance fraud.
Mexico Collect Call Scam	Operators say you have a collect call from a family member in Mexico, sometimes even providing the family member's name. You accept the call, but it's from a stranger who offers no information about family members. You end up being billed regardless.

Return to Top

N	
Neighbor Spoofing	Scammers spoof caller ID information that displays the same initial digits as your own phone number (usually the first six), making it seem like someone else with a local number is trying to reach you.

Return to Top

O	
One Ring/Wangiri Scam	When your phone rings only once, late at night, you may be tempted to call back. But the call may be from a foreign country with an area code that looks deceptively like it's in the U.S. If you dial back, international calling fees may wind up on your bill. Such cons are also known by the Japanese term "Wangiri."
Open Enrollment Scams	During the yearly health-care open enrollment season, scam callers may offer fake insurance plans to swindle you out of money. They may spoof a legitimate insurance company's phone number so you'll think the call is authentic.

Return to Top

P	
Phishing/Email Scams (Federal Trade Commission)	Scammers often use email "phishing" to hook unsuspecting fraud victims. Treat all unsolicited email and spam as suspicious: Do not open or reply. To avoid loading malicious software onto your computer or device, never click a link – even from a trusted source – unless you've verified its authenticity. Be especially wary of emails asking for emergency funds or help from friends, family and colleagues. Their email accounts may have been hacked. Scammers will also pretend to be government agencies in scam emails.
Porting	A scammer gets your name and phone number, then gathers other identifiable information that can be used for identity theft. Pretending to be you, they then contact your mobile provider to report your phone as stolen or lost, and ask for the number to be "ported" to another provider and device. They can use your number to gain access to your financial accounts and other services with two-factor authentication enabled.

Return to Top

R	
Recovery Scams (Federal Trade Commission)	If you've already fallen for a scam, another scammer may call you and offer to get you your money back for a fee. Their goal is to double dip and steal more of your money.
Romance Scam	Romance scammers contact you through dating apps or social media to try to establish a romantic relationship with you in order to access your money or personal information. Scammers use fake identities and back stories to gain your trust.

Return to Top

S	
Slamming	Slamming is when a phone company illegally switches you from your existing phone service company to their own service without your permission, then bills you for service you did not request.
Smishing	Short for "SMS phishing," smishing often involves text messages claiming to be from your bank or another company. The message displays a phone number to call or a link to click, giving scammers the chance to trick you out of money or personal information.
Social Security Number Scam	Scammers may pose as government officials, often from the Social Security Administration, to request your Social Security Number or a payment of some sort. Sometimes, they claim your SSN is suspended. The call may spoof what appears to be a legitimate Social Security Administration number.
Spoofing	Spoofing occurs when a caller maliciously transmits false caller ID information to increase the likelihood that you'll answer. Scammers often spoof local numbers, private companies, government agencies and other institutions.
	Return to Top
T	
Tech Support Scams	Phone scammers may masquerade as tech support employees for a major company in order to take your money or install a virus on your computer. They may call from what seem to be legitimate company numbers using caller ID spoofing.
Toll Road Payment Scam Texts	Hoping the fear of unpaid tolls may help them make some quick money, scammers are sending out texts claiming you have a toll violation.
	Return to Top
U	
V	
Veteran Benefits Scam	These scams involve callers claiming that veterans are eligible for new benefits, often relating to home loans, to acquire personal and financial information. The caller may even spoof a legitimate benefits organization.
Voicemail/Callback Scams	Scam callers leave voicemails threatening legal action if you don't call back. Our guidance is: Never call back an unfamiliar number, because it may lead to a scam.
Voicemail Hacking Scam	Hackers guess default voicemail passwords (like "1234") and change voicemail greetings on phones to verbally accept collect call charges. They then use the phone to make international calls, costing you money.
	Return to Top
W	

Wangiri/One Ring Scam When your phone rings only once, late at night, you may be tempted to call back. But the call may be from a foreign country with an area code that looks deceptively like it's in the U.S. If you dial back, international calling fees may wind up on your bill. Such cons are known by the Japanese term "Wangiri."

Return to Top

Bureau/Office:
Consumer and Governmental Affairs

Tags:
Consumers - Fraud - Scams - Telephone Consumer Issues

Updated:
Wednesday, July 22, 2026

Federal Communications Commission
45 L Street NE
Washington, DC 20554

Phone: 1-888-225-5322

ASL Video Call: 1-844-432-2275

Fax: 1-866-418-0232

Contact Us

Visiting FCC Facilities