

HOW TO RECOGNIZE – AND STOP – PHONE SCAMS

In the online world, “phishing” is the term for scams that try to steal your identity or money. Similarly, “vishing” is a term coined for voice-phishing, where scammers use the phone to cheat people out of their money.

Whether you call it vishing or a plain old phone scam, there are ways to recognize when an incoming call could be a scam – and how to fight back. [The Federal Trade Commission](#) tracks phone scams and offers advice on how to avoid them.

“Phone scams come in many forms, but they tend to make similar promises and threats, or ask you to pay in certain ways,” according to a news release issued by the FTC.

Popular phone scams

Here are some of the most common scams you’re likely to encounter, according to the FTC:

Gift card scams – If anyone calls you asking for payment by gift card, it’s almost certainly a scam. Legitimate businesses don’t want to be paid with gift cards. A December [report from the FTC](#) noted that gift cards are the payment method of choice for scammers, leading to \$148 million stolen from consumers in the first nine months of 2021.

Calls from government agencies – It’s common for scammers to call pretending to be from a governmental agency. Never give out your social security number or other personal information when you receive an unexpected call.

Debt relief and credit repair scams – Don’t be fooled by scammers who offer to fix your credit, lower your credit card interest rate, or forgive student loans.

Extended car warranties – Scammers will try to get you to purchase an extended car warranty. They may even have information such as the make and model of your car.

Prize and lottery scams – With these, the caller says you’ve won a prize or a lottery. But to get it, you’ll need to pay money for them to cover the cost to ship the prize or pay the taxes on lottery earnings.

How to fight back

There’s no way to completely stop scammers from calling you, but here are some ways to you can fight back:

Don’t answer calls from unknown numbers – It’s likely the phone numbers of all your friends and family members are programmed into your cell phone. When they call, their name will appear on your phone. Let others go to voicemail.

Don’t be fooled by seemingly local numbers – It’s easy for scammers to “spoof” a phone number to make it look like it’s a local call or a specific business or government agency. Again, let those calls go to voicemail and be wary when listening to the message.

Hang up and call back – If you do answer a call from someone who purports to be from a company you do business with, simply end the call and call the company back. You can find contact numbers on a company’s website, or on billing statements you’ve received in the mail.

Sign up on the Do Not Call Registry – Legitimate companies shouldn’t be making sales calls if you’re signed up on the [National Do Not Call Registry](#). If you’re on the registry, an incoming call is more likely to be a scammer since they don’t abide by the registry.

Consider a call blocking or call labeling app – You may want to download an app to your cell phone that will completely block certain types of calls or at least label them as potentially a scam. Search for “Call Blocking” and “Call Labeling” apps in the app store for iPhone and Android phones. Read reviews to find one that’s highly rated and suitable for your needs.