What is SMS Spoofing?

SMS spoofing is a technique/activity in which people replace or alter the originating mobile number (Sender ID) of a text message [sent via SMS] to an alphanumeric text of their choice. To put it into simple terms, the Sender ID of an SMS message is reset to change who the sender appears to be.

Spoofing an SMS message completely changes vital information like sender name, phone number or even both simultaneously.

In terms of legality, there is a huge grey area for whether or not this practice is legal. Because while SMS spoofing sounds malicious in concept, there are a lot of legitimate reasons why text messages can be spoofed. Consequently, spoofing has a varying degree of legality globally.

For example, a company altering its Sender ID from a random phone number to their company name would be a legitimate use of SMS spoofing. This is done so customers are alerted of the identity of the sender.

Nevertheless, spoofing can also be used to attack unsuspecting people by sending SMS messages to targets under the assumed identity of others (companies or phone numbers).

How to Protect Yourself from SMS Spoofing?

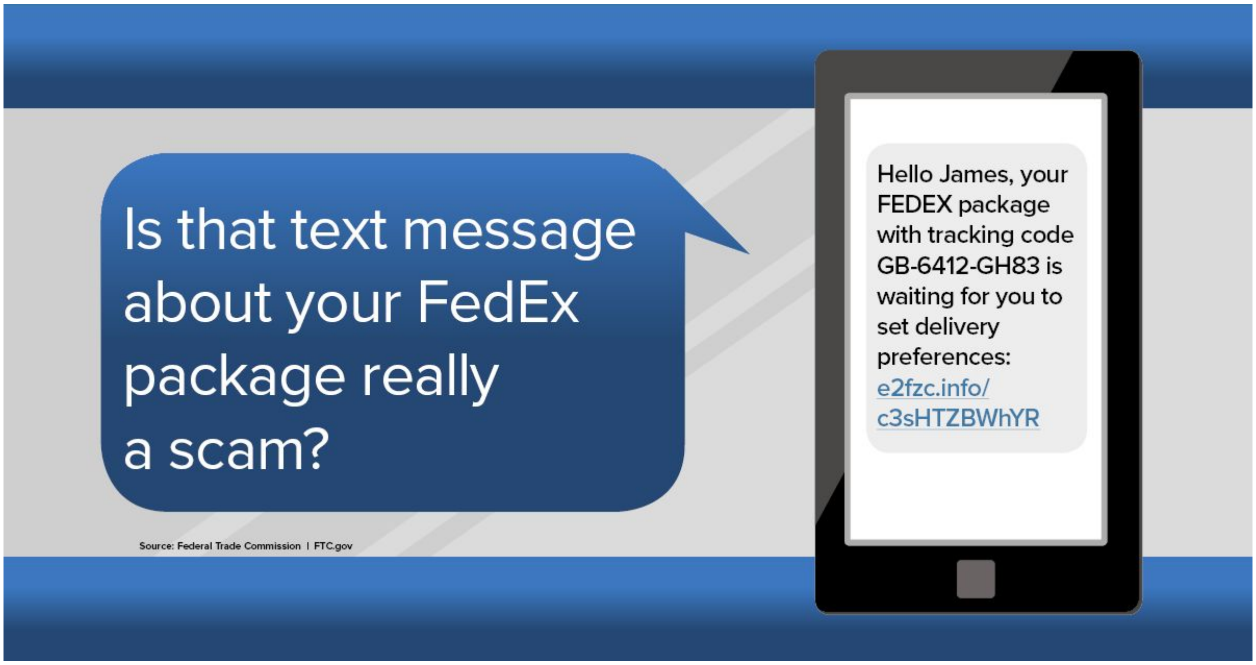
No one can be 100% safe from spoofing. Whether scammers use your number for spoofing or are attacking you, you should always proceed by reporting it to your carrier and law enforcement, who can then track where SMS messages came from. This way you can prevent SMS spoofing in the future.

Spam Text Messages and Phishing

Scammers send fake text messages to trick you into giving them your personal information – things like your password, account number, or Social Security number. If they get that information, they could gain access to your email, bank, or other accounts. Or they could sell your information to other scammers.

The messages might ask you to give some personal information — like how much money you make, how much you owe, or your bank account, credit card, or Social Security number — to claim your gift or pursue the offer. Or they may tell you to click on a link to learn more about the issue. Some links may take you to a spoofed website that looks real but isn't. If you log in, the scammers can then steal your user name and password.

Other messages may install harmful malware on your phone that steals your personal information without you realizing it.


Is that text message about your FedEx package really a scam?

Hello James, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e2fzc.info/c3sHTZBWhYR

Source: Federal Trade Commission | FTC.gov

What to Do About Spam Text Messages

If you get a text message that you weren't expecting and it asks you to give some personal information, don't click on any links. Legitimate companies won't ask for information about your account by text.

If you think the message might be real, contact the company using a phone number or website you know is real. Not the information in the text message.

There are many ways you can filter unwanted text messages or stop them before they reach you.

Here are a few tips that may help you deal with spam texts.

Don't reply directly to any spam text message

Directly replying to a spam text message lets a spammer know that your number is genuine. What happens next? They can sell your phone number to other spammers who might bombard you with promises of free gifts and product offers.

Do treat your personal information like it's cash

Spam text messages may lure you into disclosing personal information like how much money you make, how much you owe the bank, your Social Security number, and credit card details. Most legitimate companies do not request personal information like passwords, account details, and other personal details via text messages. When in doubt, look up the company phone number, call them, and verify if a legitimate request was made. Don't call the number sent in the text message.

Don't click on any links in the text message

Clicking on a link in a spam text message could install malware that can collect information from your phone. It can take you to spoof sites that look real, but are designed to steal your information. Malware can also slow down your cell phone's performance by taking up space on your phone's memory. Once the spammer has your information, it can be sold to marketers or, worse, identity thieves.

It can also lead to unwanted charges on your cell phone bill. Your wireless carrier may charge you for receiving a text message, regardless of whether you requested it.

Do place your cell phone number on the National Do Not Call Registry

Adding your phone number to the Federal Trade Commission’s National Do Not Call Registry lets you opt you out of receiving most telemarketing calls. If you receive an unwanted call after your number is on the registry for 31 days, you can report it to the FTC.

Do check to see if your carrier offers a call-blocking service

Most major carriers offer call-blocking services or plans that let you block calls from unknown numbers for a specific period of time. You can also see if one of the third-party call-blocking apps and services will work with your carrier’s wireless service.

Do report spam texts to your wireless carrier

Send any suspicious or spam messages to 7726, which spells SPAM, so your carrier can investigate. Don’t worry, messages forwarded to 7726 are free and don’t count against your text plan.

Do check your phone’s settings

Your phone probably has built-in features to help block unwanted calls and text messages. Type in “block” using your device’s search function or read below for more help.

iOS users: Block a phone number or contact

There are a few ways that you can block phone numbers, contacts, and emails.

Phone

If you're in the Phone app under Recents, tap the Info button ⓘ next to the phone number or contact that you want to block. Scroll down, then tap Block this Caller.

FaceTime

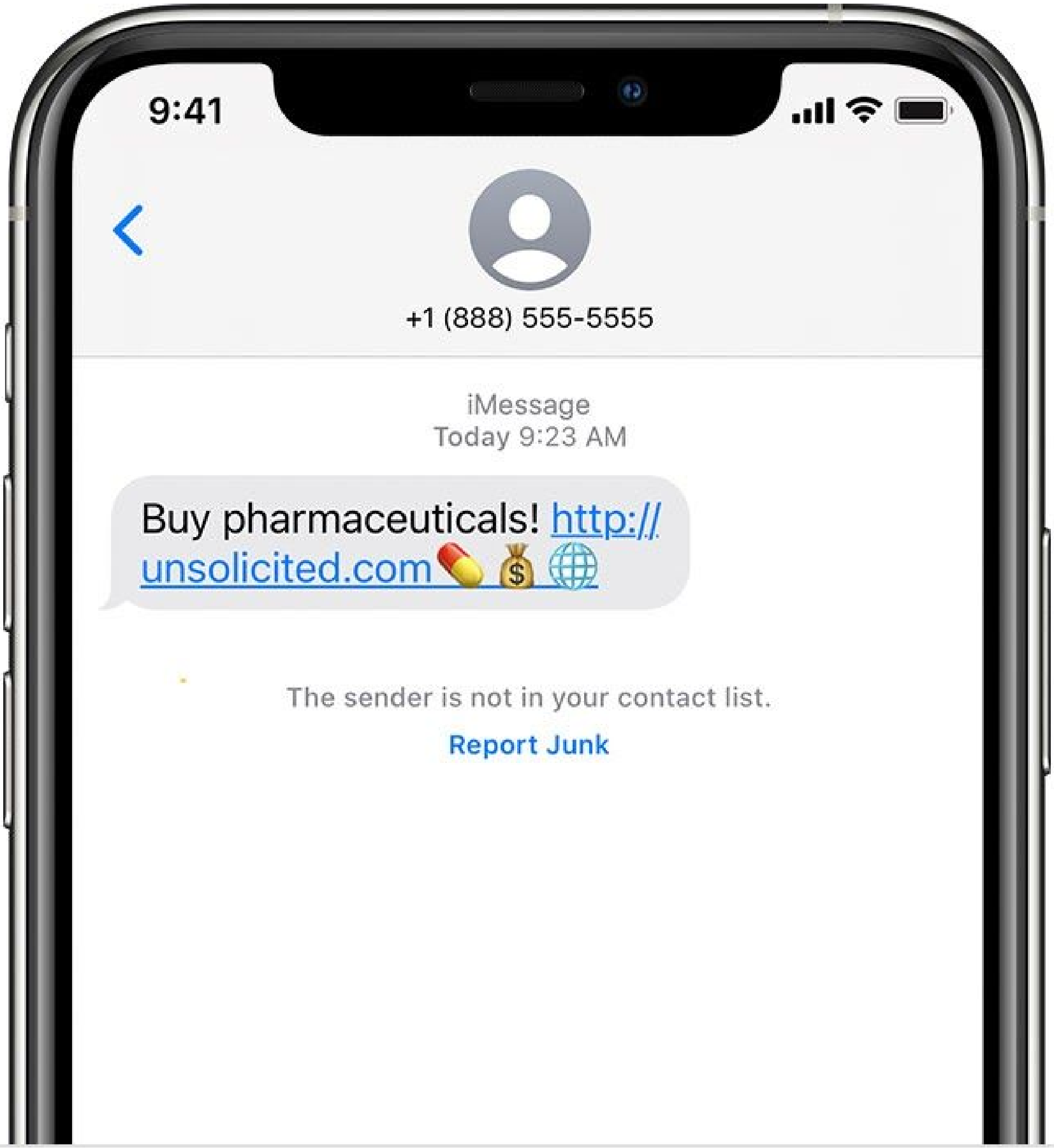
If you're in the FaceTime app, tap the Info button ⓘ next to the phone number, contact, or email address that you want to block. Scroll down, then tap Block this Caller.

Messages

If you're in Messages, open the conversation, tap the contact at the top of the conversation, then tap the Info button ⓘ. Tap info 👤 scroll down, then tap Block this Caller.

Report spam or junk in the Messages app

You can report iMessages that look like spam or junk from the Messages app. If you get an iMessage from someone who's not saved in your Contacts, you'll see a Report Junk link under the message.



Buy pharmaceuticals! http://unsolicited.com💊💰🌐

The sender is not in your contact list.

Tap Report Junk, then tap Delete and Report Junk. Messages will forward the sender's information and the message to Apple, as well as delete the message from your device. You can't undo deleting a message.

Reporting junk doesn't block the sender from being able to send another message.

If you don't want to receive these messages, you need to block the contact.

Android Users: Report spam and Block Sender

When you report a conversation as spam, you can also block the sender and move the message to your "Spam & blocked" folder.

1. On your Android phone or tablet, open the Messages app .
2. Touch and hold the conversation you want to report.
3. Tap Block ⊘ › Report spam › OK.

You can also open the conversation to report it as spam. From the conversation, tap More ⋮ › Details › Block & report spam › Report spam › OK.

Notes:

The contact will be reported as spam and the message will be sent to your “Spam & blocked” folder.
You can report spam without blocking the contact.

Report spam in a group message

When you report spam in a group message, the spammer is reported and the message is sent to your “Spam & blocked” folder.

1. On your Android phone or tablet, open the Messages app .
2. Open the conversation you want to report.
3. Tap More ⋮ › Group details › Report spam.
4. Tap Report spam.