What are spam texts and how to get rid of them

Very few of us escape the nuisance of spam texts. Not only are unwanted text messages extremely annoying, but in many cases, they are a scam. This guide explains how you can fight back and reduce the number of spam text messages and phishing texts you receive.

What are spam texts?

Spam refers to messages which are unsolicited and unwanted. Usually, spam texts are not coming from another phone. They mainly originate from a computer and are sent to your phone via an email address or instant messaging account. Because they are sent online, they are cheap and easy for scammers to send. It's a numbers game for spammers – they send messages in bulk, often to randomly chosen or automatically generated numbers, and they only need a few responses to justify their efforts.

What are robotexts?

Robotexts are a type of spam text, however, they are less invasive than robocalls because they are easier to ignore. Still, it's annoying to hear the sound of an incoming text message and to check your phone — only to find it's spam. Worse than that, spam texts and robotexts are often the start of a scam, where the senders are hoping to obtain personal information about you, which they can use for fraudulent purposes.

These texts can expose you to identity theft and increase the risk of you accidentally downloading malware onto your phone. They can also lead to unwanted charges on your phone bill if your wireless carrier charges you for receiving a text message.

Spam text message examples

Not all spam text messages are scams, but they very often are. Scammers use a variety of stories to try to trick you.

Common examples include:

- You've won a prize, a gift card, or a coupon that you need to redeem.

- You're being offered a low or no interest credit card.
- You have been overcharged and are owed a refund, possibly from a government agency such as the IRS or HMRC.
- Your account has been deactivated for your protection, and you need to take steps to reactivate it.
- You can get help to pay off your student debt.
- There is negative information in your credit report which you can remove for a fee.
- Suspicious activity has been noticed on your account, and further action on your part is required.
- There's a problem with your payment information – you need to take action.
- There's a notification about a delivery package – perhaps asking you to rearrange a delivery slot or else pay a delivery charge to receive it.
- You're notified about a purchase or transaction and told to reply if it wasn't you.
- "Get rich quick" or "Be your own boss" type messages.

Fake text messages often try to create a sense of urgency – for example, by claiming that 'urgent action is required' or 'you only have two days to reply'.

Typically, the messages ask you to disclose some personal information – such as your bank or card details or Social Security number – to claim the gift or pursue the offer. Or you may be asked to click on a link to learn more about the issue. The link then takes you to a fake website where, if you log in, the scammers can steal your login credentials.

Other SMS spam may install malware on your phone, which steals your personal information without you realizing it.

How can you tell if a message is a scam?

Scammers are getting more sophisticated at making scam text messages look authentic and often use identity masking technology to change the name displayed as the caller ID. This is known as number spoofing. That said, if you're wondering how to tell if a message is a scam, there are a few signs to watch out for:

- **Unexpected contact.** Think about how an organization usually contacts you. If it isn't via a text message, contact them directly to check if it's legitimate. Remember, genuine organizations don't contact you out of the blue, asking you to disclose personal or financial details via a text message.
- **Spelling and grammatical errors.** If a message doesn't look professional, that's a red flag that it's probably a scam. Legitimate organizations rarely make glaring spelling or grammatical errors in customer communications.
- **Is the message relevant to you?** For example, if it informs you about a parcel delivery, did you order or were you expecting anything? If it informs you about a prize, did you enter a competition? If it's about a gift card, is it from somewhere you have previously shopped?

The golden rule of any scam, online or otherwise, is that if something sounds too good to be true, it probably is.

Why am I getting spam text messages?

There are many ways spammers get hold of your cell phone number so they can send SMS spam and sales texts:

- They may use technology to generate numbers automatically — so even if you have a brand-new number, you can still receive both robocalls and robotexts.

- Social media sites sell your data. Popular and well-known social networking platforms keep track of your online activity and pass the information on to advertisers. If you list your phone number publicly on social media, there's a high chance it exists in various marketing databases.
- There are many reasons people disclose their phone numbers online – filling out online forms, entering competitions or loyalty programs, and so on. Whenever you hand out your cell phone number online, there's the potential for it to end up in the wrong hands.
- In the US, you may have called an 800, 888, or 900 number. When you call phone numbers with these prefixes, your cell phone number is collected by an Automatic Number Identification (ANI) system. As well as identifying and storing your number, the ANI system can match it with other digital data associated with you.

Plus, if you've ever responded to a spam text message, even accidentally, your phone number was likely tagged as valid and may have been sold on to other spammers, increasing your odds of getting more junk messages and SMS spam.

What to do if you receive a spam text

1. **Never reply**

With any spam text messages, you should never reply to them. Doing so confirms to the spammers that you're a real person and a potential target. Sometimes spammers try to trick you into responding by saying, "text STOP to be removed from our mailing list" or something similar. Don't be fooled by this. If you reply, you can expect more spam texts and calls. You are better off not responding at all.

2. **Don't click on any links**

Clicking on a link from a spam text could take you to a fake website explicitly set up to steal your money or personal information. In some cases, the website could infect your phone with malware, which may spy on you and slow down your phone's performance by taking up space on your phone's memory.

3. **Don’t disclose any personal information**

Remember, legitimate organizations such as banks or government agencies don’t ask for personal or financial information via unsolicited text messages. So guard your personal data carefully and be careful about how you disclose it online. Be wary of any text message that asks you to ‘update’ or ‘verify’ account details.

4. **Visit an organization’s website directly**

If you are unsure whether a text message is real or not, the best thing to do is contact the relevant organization directly. You can search for their website via a search engine and then click through from the search engine results page, or else you can type in the URL directly into your address bar. Or you can find out their phone number and call them to check.

5. **Report the scammer**

In the UK, you can report spam text or robotexts to your cellular carrier by forwarding the unwanted text to 7726 (this spells SPAM). Make sure the original number is showing. This reporting method works for the primary network providers. You may receive an automated response thanking you for the report and giving you further instructions if needed. You will not be charged for sending texts to 7726.

You can also report spam texts on the messaging app you use. Look for the option to report junk or spam:

- How to report spam or junk for iPhone
- How to report spam or junk on an Android phone

6. **File a complaint**

It is illegal to send unsolicited commercial messages to users without their consent. The precise complaints procedure will vary by jurisdiction. For example:

- In the US, you can complain to the Federal Trade Commission (FTC)
- In the UK, you can complain to the Information Commissioner’s Office
- In Australia, you can complain to the Australian Communications & Media Authority

What to do if you’ve fallen victim to a scam message or phishing text

If you think you may have passed on personal or financial information to a scammer via a spam message:

- Contact your bank or financial institution immediately to alert them.
- Change all your usernames and passwords across all your accounts.
- Report the fraud to your phone service provider – they may have had other customers with the same experience and can take action if they see their customers experiencing similar spam texts.
- Involve law enforcement where financial loss is involved.

How to stop spam texts

Two simple ways to stop getting spam texts are blocking numbers and using spam filters on your mobile device.

Blocking numbers

Blocking numbers is easy to do, although precise instructions may vary according to your mobile device's manufacturer, model, and operating system. Remember that the scammers may try texting you from what appears to be a different number each time – by spoofing numbers – which makes the process of manually blocking more laborious.

How to block text messages on iPhone:

- Open the text from the number you wish to block and tap on the sender’s number.
- Click on the **info (i)**
- Under the **Details** screen, click on the phone number, choose **Block this Caller**, and **Block Contact**.

How to block spam texts on Android:

- On an Android, open your phone app and tap on the three-dot icon in the upper right corner and choose “**Settings”.**
- Tap on “**Block numbers**”.
- You will find several options, including unknown callers, recent calls, or from your contact list.
- Choose or manually enter a number you wish to block.

Filter unknown senders

Another way to help reduce spam messages and robotexts is by using spam filters on your mobile device.

Filtering out spam messages on iPhone:

- Go to the Settings app and tap “Messages.”
- Scroll down until you find the “Filter Unknown Senders.”
- Turn it on by swiping the button to the right. All messages from a number not in your contact list will be filtered to the “Unknown Senders” tab found under “Filters.”

Filtering out spam messages on Android:

- Go to the Messaging app and tap the three dots icon in the upper right-hand of the screen.
- Tap on “Settings” –> “Spam Protection.”
- Scroll down until you find “Enable Spam Protection.”
- Turn it on by swiping the button to the right.

Tips: How to protect yourself from spam texts

Don’t disclose your cell phone number online unless it’s essential

Often, online forms ask us to disclose phone numbers but remember that the details you submit can often end up on marketing lists or databases. Unless it’s essential or mandatory, avoid giving your number out to help reduce the number of unwanted texts and calls.

Don’t post your cell phone number publicly

For example, avoid listing your cell phone number on your social media profiles such as Facebook, Twitter, or elsewhere.

Keep an eye on your cell phone bill

Review your phone bill regularly. If you see any charges which don’t look right, contact your network carrier to check if you’re either receiving or unknowingly sending spam messages from your phone.

Check to see if your carrier offers call blocking

Many major carriers offer call-blocking services that allow you to block phone numbers from unknown callers for a set period. Several third-party apps can block spam texts – including Nomorobo, Robokiller, Truecaller, TrapCall, and others. Bear in mind, though, that using these apps involves sharing your data with them.

Place your number on a Do Not Call Registry

Different countries have different schemes, but in the US, the Federal Trade Commission operates a National Do Not Call Registry. This allows users to opt-out of receiving unwanted texts and marketing calls. However, note that actual scammers don't abide by this registry, so they will continue to send scam texts regardless.

Use antivirus protection for phones

So much of our personal information is stored in smartphones and tablets, so it's advisable to use mobile security to protect it.

Message spam and unwanted text messages are a real nuisance and often the start of a scam. As ever, a combination of awareness and practicing good cybersecurity hygiene is the key to staying safe.