The Text in Disguise

How to Spot Scam Texts

DEER BROOK

Once upon a time, scam texts were some of the easiest to spot. Similar to popup ads, these first scam texts would claim you won a grand prize, you were entitled to millions of dollars or free items you never signed up to receive, and more. They were clear as day to avoid.

But scammers have evolved and adapted their techniques, and scam texts nowadays are far more compelling and believable than those of yesterday. And with generative AI, long gone are the days where you could rely on typos and grammatical errors to spot something suspicious.

But in the fight against scam texts, not all hope is lost. There's still ways you can check to see if texts are the real deal.

Signs You're Reading a Scam Text

Fake texts commonly claim to be from a credible organization creating urgency, or they try to prey on your curiosity. Here's some clear-cut signs that a text is probably a scam:

The Message Makes You Panic

At the start of 2025, fake texts about parking violations and other automobile-related fines heavily circulated around the United States.

In a classic case of creating urgency, scammers were hoping people would click the dubious links and interact with these texts without a second thought.

Fake texts and emails share a lot in common, and the tactic of creating panic and urgency is a core element of both. These texts often attempt to lead people onto websites where they're tricked into "logging in," and giving up their account information. In other cases, scammers disguise malware as an app and convince the user to install it on their device.

Scam texts often contain legal or financial threats, both of which are meant to kick in your "fight or flight" instincts and get you to lower your guard as you reply, click links, or download their malware.

It Preys on Your Vulnerability or Curiosity

Another fake text, linked to romance or "pig butchering" scams, revolved around the scammer purposely mis-texting the victim, leading them on for months to get into an online romantic relationship before stealing their money through wire fraud or investment schemes.

When you get an unexpected text from a stranger, be aware of how the message you're reading makes you feel. Don't fall for any pitches, prompts, or conversations that feel like they're preying on your curiosity.

Likewise, romantic relationships don't just bloom from out of nowhere. Be hesitant of any text message exchange in which a stranger is forcing the conversation to continue at every turn.

You're Prompted to Login

Be wary of any text that asks you to click a link and log in to confirm your details or approve/deny an action.

We don't advise clicking any links, but if you do and you've downloaded the app of the business in question, make note of whether you're redirected to the app. In most cases, you should be. Otherwise, you need to double-check and verify the URL is legitimate. But we recommend just not clicking on any links at all.

The Text Combines Many or All of These Signs

Scammers will try and create text messages that combine the panic factor, pique your interest, and ask you to click on links. They often use personal data stolen in data breaches to make these messages appear convincing, too.

Another popular scam text going around in 2025 told potential victims that their banking account information was changed, and prompted them to log in and deny the action. These texts leveraged personal information like

account numbers and the name of a legitimate financial institution to make themselves look as credible as possible.

Checking a Scam Text Message

Ask Yourself These Questions

When you receive a suspicious text message, take a step back and ask yourself these sorts of questions:

- Do I have an account with this company, or is it reasonable that this person has my phone number?
- Was I expecting this text, or have I ever received a text like this ever?
- Has this company or this person ever communicated with me like this?

Don't be fooled and think to yourself that this must be a new way the organization or person is reaching out to you. If you answered "no" to one or many of those questions, you're probably looking at a scam text.

Institutions that handle your sensitive or private information, such as banks, won't likely ever try to contact you through text (or email, for that matter). They especially won't disclose your unfiltered private information in these communications either.

Look Up and Compare Phone Numbers

It's important not to click any links or respond to the text, even if the message is strongly encouraging you to.

Instead, navigate to the legitimate website of the company or whoever is contacting you, and compare their contact details to those of the text message. If the information doesn't match up, block the sender's number and move on.

When in doubt, always take a look at your records. Reach out to organizations or people using contact info you have saved yourself, or use contact info from official records you've received from them in the past.

Search the Sender's Number Online

You can also search the sender's number online to see if others have reported fraud attempts, phishing attempts, and other scams originating from that phone number.

Don't use this technique as a be-all end-all though, because many phone numbers don't have an online history, and even fewer people take the time to report scam texts this way.

Trust Your Gut

If you have a bad feeling about a text, don't engage with it.

If a text message is claiming you need to pay someone, go to your laptop, or your tablet, or a new browser tab on your phone, and navigate straight to that service yourself. Check and see on official channels if there's any indication that the claims in the text are true.

Don't make excuses that legitimize the claims of the text message (such as "the company's systems must be out-of-sync" or "this must be a new contact method"). Sometimes what you see is what you get: a scam text.

Keep Your Cool, Follow Through

When a text message is laying out a dire situation and telling you to react immediately, your first reaction might be to panic and click links, log into suspicious websites, or hand over sensitive info that a few seconds of pause might have prevented.

Never click a link from a text message you weren't expecting, never give your credentials to webpages they link to, and be cautious in general when a stranger is contacting you out of the blue.

When you get a message that induces panic or any other impulse, take the opportunity to calm down and assess the situation as objectively as possible.

Just keep cool. Use your tools to double-check the validity of any suspicious text messages.