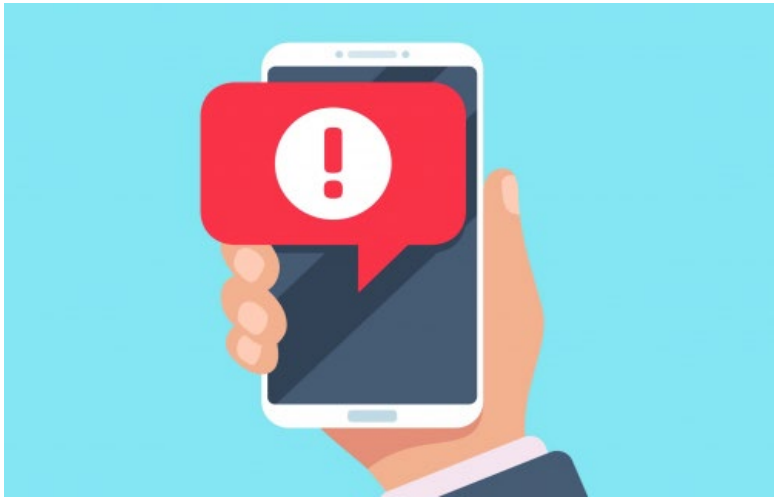
How to Recognize and Report Spam Text Messages



Today, texting is a major part of our everyday life, and scammers are relying on the ding or vibration of an incoming text message being hard for people to ignore. In 2022, the FTC reported that $330 million was lost due to text scams with a median reported loss of $1,000 – more than double the amount reported in 2021!

You may be wondering why these scams work. Scammers use the speed of communication via text to their advantage and hope you won't slow down and carefully read over what's in the message. Some text messages include the promise of a good thing such as a free gift, cash back, or even a job. While other text messages try to alert you and make you panic, thinking someone else has used your financial or personal information. This is just one of the ways scammers try to attack consumers.

There are countless types of text scams, however the top five described below account for more than 40% of text frauds reported last year. You'll see all five have one thing in common – they often impersonate well-known businesses.

1. Fraud prevention alerts: You may receive a text message impersonating your bank asking you to call a fake phone number about supposed suspicious activity. Or the text may say "reply yes or no to verify a large transaction" (that you did not make). If you do reply, you'll get a call from the fake fraud department which is actually the scammer. People who have fallen for the scam, say they really believed the bank was helping them get their money back, but instead, money was taken out of their account. What's even worse is many people reported giving out their Social Security number and other personal information to scammers, which can lead to possible identity theft.

2. Bogus "little gifts": If you receive a text that says you won a free gift, reward, or prize and it may look like it came from a company you know like your cell phone company or a big retailer, you should still be cautious. If it says you need to click the link and pay a small "shipping fee" in order to claim your reward, don't do it! If you actually won something, you shouldn't have to provide your credit card number to pay for anything.

3. Fake package delivery issues: If you're expecting a package, there's a text scam coming for you. Unfortunately, it has become more common to receive a text posing as the U.S. Postal Service, FedEx, and UPS that says there's a problem with your delivery. The text message usually includes a link to a website that looks legitimate – but isn't. They also say you need to pay a small "redelivery fee," which many people have reported, is a way for the scammers to retrieve your credit card number. If there's a delivery issue with any package you've ordered, only trust legitimate emails from the retailer you purchased the item(s) from.

4. Phony job offers: A scam that is an oldie, but a goodie is the promise of getting paid fast for mystery shopping at well-known stores like Trader Joe's and Target. Scammers will text you with bogus offers to make money by just driving your car around after wrapping it in retailer ads. Scammers will also target people who have their resumes posted on employment websites like Indeed and text them to provide their bank account information as part of onboarding for the new job. Remember, legitimate companies will not communicate with you via text for your personal or financial information.

5. Fake Amazon security alerts: Similar to bogus texts from your bank, there are text messages going out that say they're "Amazon" and look like automated fraud prevention alerts. Most of the time, the message will ask you to verify a big-ticket order that you didn't place and to call the phone number provided, which goes to a phony Amazon representative who offers to "fix" your account. People have reported giving the "representative" remote access to their phone to fix things and get their refund. However, the representative says a couple of zeros were accidently added to the refund amount, so you need to return that money to them by purchasing gift cards. Remember, any security alert will come directly and securely from Amazon via email or the Amazon app, do not trust any phony alert text messages.

In any of these text message scam cases, reporting them immediately can help stop them:

- Forward the scam message to 7726 (SPAM) to report it to your wireless provider so they can block similar messages
- Block phone numbers and report spam or junk in the Apple iMessages app or Google's Messages app for Android users
- Report it to the FTC

To avoid text scams, don't ever click on links or respond to unexpected text messages. If you're not sure if it's legitimate or not, contact the company directly by calling a phone number you know is real. Don't use the information that's in the text message. You can also filter unwanted texts before they even reach you as well as block them too. To learn more about text scams, how to spot and avoid them and how to recover money if you've paid a scammer – visit ftc.gov/scam. As always, we're here to help, contact us at 218-456-2187.