How to Spot Fake Texts

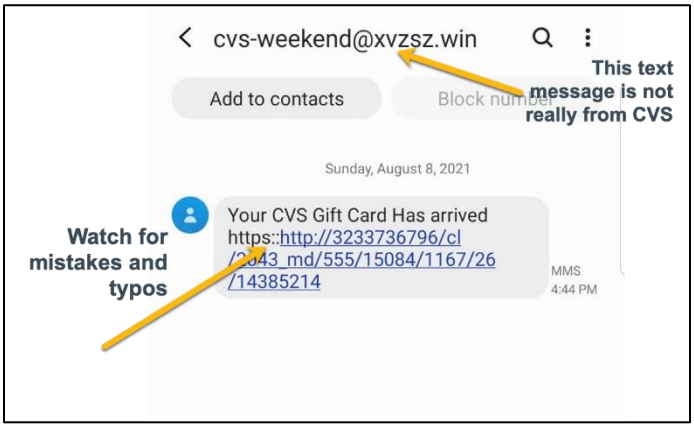
Don't Trust Unsolicited Messages

Scammers will try to get you to click a link or call a number in a text message claiming

- You've won a great prize
- Your subscription account is about to be deactivated
- There was a problem delivering a package to your home
- Fraudulent activity has been detected on your account

If an out-of-the-blue offer sounds too good to be true, it probably is. If you receive an unsettling text message from a company you do business with and you have never received a text from them in the past, look up their contact information on their official website and reach out to the business to investigate.

Watch Out for Suspicious Links



Most scam text messages contain a link for you to click. Scammers hope their message will make you feel so scared or excited that you'll click the link without thinking. Some of these links could download malware onto your device. Others may lead you to lookalike websites where scammers hope to harvest your personal information, login ID, and passwords.

Look for Spelling and Grammar Errors

Legitimate companies often hire professional writers and editors to craft their business communications. If you notice strange phrasing along with spelling and grammar errors, you're probably dealing with a scammer. Many fake texts originate with offshore companies where they may be written by someone who isn't completely fluent in the English language.

Know That a Personalized Message Doesn't Make the Sender Trustworthy

Thanks to data breaches and online directories, at least some of your personal information is online. Scammers may have access to your name, address, where you bank, your phone provider, and other details about your life. They may include some of your information in their text to appear more legitimate. When in doubt, contact the businesses directly from a website you've researched and NOT the provided link, and investigate.

If A Website Looks Real, Check Again Before Proceeding

If you do click on a link in a suspicious text message and it appears to take you to an official business website, don't presume it is safe. Scammers can create carbon copies of legitimate websites. If you log onto the fake site, scammers can retrieve your user name and password.

Look Up Phone Numbers Before You Call

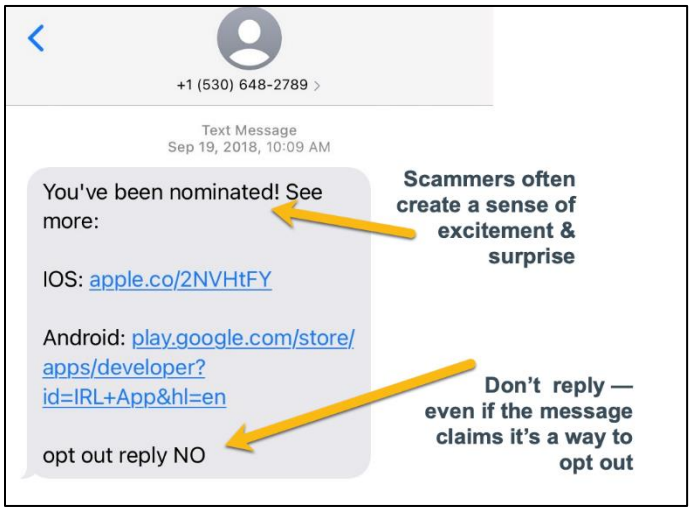
Scam texts may prompt you to call a number, claiming you need to resolve some kind of issue or register

to receive a prize. If the scammer gets you on the phone, they'll likely ask you to "confirm your identity" by having you tell them (state and verify) your PIN, password, social security number, or other personal details.

No legitimate company will ever ask you to reveal your security information over the phone. If you realize you're talking to a scammer, hang up and block the number.

If You Spot a Scam Text, Don't Reply

Some scam texts give you're the option to reply "STOP" or "NO," so you won't receive future texts. In fact, sending a reply text informs the scammer that they have a real, active phone number, and that could open you up to future attacks. If a text message seems suspicious, don't reply. Block the number and delete the message.



Keep Your Antivirus Software Up to Date. Antivirus software can alert you to fake and unsafe websites if you happen to click on a link in an unsolicited text message. Keep the software installed and up to date to protect yourself against scammers.

https://www.bbb.org/all/spot-a-scam/how-to-spot-a-phony-text-message