Is That Text Message Real or Fake?

Cybercriminals send text messages posing as somebody you trust, such as government officials, friends, family, and others, with the goal to steal your money or personal information.

Their common tactics include:

- Threatening you unless you pay a fee or fine
- Offering a great product, service, or investment at a great price
- Asking for you to log in to an account
- Pretending they are friends or family and urgently need money because of some dire event, like getting arrested, hurt, or their money stolen

In general, just delete an unusual or unexpected text message.

Do not click on any links or attachments as they may lead to malicious websites or contain malicious software. Never respond to a fake text message, as that tells the cybercriminals that they reached a real person (and increases the likelihood you'll get more fake texts).

How to Assess a Text Message

Follow the steps below to investigate and assess a text message to determine if it is most likely real or fake. The steps use the text message above as an example.

STEP 1

Determine if it is a reasonable request.

Do you live in the state they are refering to? Would the government contact you via text message? Were you expecting this message?

If not, the text is likely fake.

STEP 2

Identify the sender.

Search for the sender's phone number on www.Google.com.

Identify where the sender seems to be located and if any of the results suggest the number is involved in scams.
(Don't click on any search results)

STEP 3

Expand the URL.

Type the URL *(don't click on it)* into a tool like www.expandurl.net. This will let you see the actual website the link leads to without clicking on it.

You'd expect the link to go to the state's DMV or government site. If it doesn't, that's a warning sign!

Determination: Based on our review, the text message is likely fake.