

Scammers are Active in Many Ways

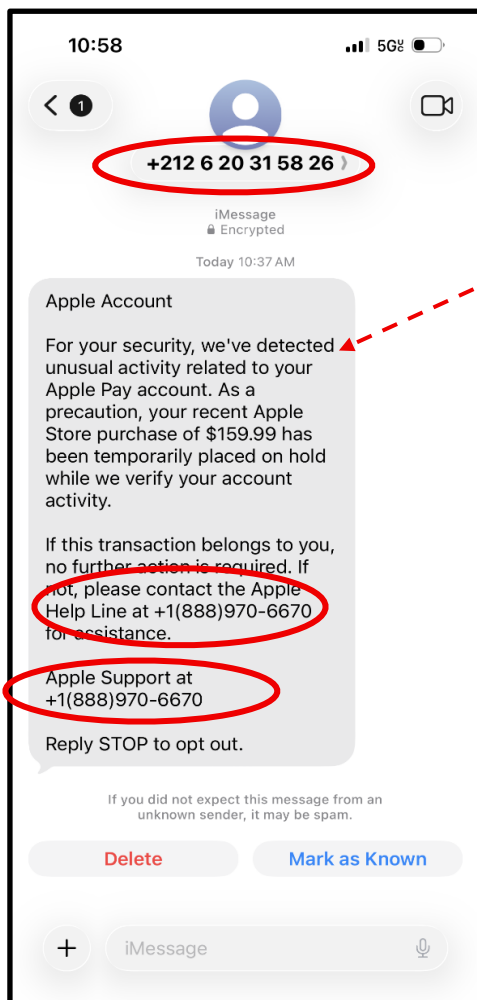
by

Mike Pancione

Computer Club Newsletter Editor

The threat posed by scams is ever present so you have to remain vigilant to protect yourself. One of the best lines of defense is to always be skeptical of emails, text messages, and phone calls you receive, especially those you were not expecting.

Recently, I received a text from “Apple” helpfully telling me that they intercepted a suspicious purchase of \$159.99. I was told to do nothing if I recognized the charge, or to contact “Apple” to resolve the issue. I’ve copied the message and included it below:



There are a few ways to verify the legitimacy of a text message, but there are differences, depending on who the scam text is supposed to be from. This text is a good example of a phishing scam – i.e. scammers “throw something out there” to see if someone bites. Here are some clues that this text is a scam:

1. Scam messages always try to make you worry and scare you to take some kind of immediate action.
2. Messages from Apple always show **Apple** as the sender. This message was not sent by Apple. Unfortunately, legitimate senders don’t always follow Apple’s example.
3. A good way to check if Apple (or a legitimate organization) was the sender is to by-pass the contact information in the text and to contact the sender’s customer service by going to its website, *in this case:* <https://support.apple.com>. There you will find the real phone number. ***Do not accept any contact information in the text as legitimate.***

4. Finally, you can also log into your Apple account (or your sender’s account) and check your purchase history.

I talked with an Apple support representative who sent the email below as a follow up. Check out the link as there is some useful information about how to spot, and avoid, phishing attempts like

this one.

Thanks for contacting us.

Case ID: 20000150190999

Hi Michael,

Glad we were able to assist you.

Based on your recent conversation, your Advisor recommends the following articles:



Recognize and avoid social engineering schemes including phishing messages, phony support calls, and other scams

If you still need help with this issue after reviewing the articles, [contact Apple Support](#) to reopen this case.

Thanks,
Apple Support