

SPOT FAKE TEXTS

Scammers leave lots of clues. Here are 9 to look for

BY AMY NOFZIGER

Phone scammers hire professional-sounding speakers to make their robocalls more convincing. But many crooks who rely on emails and text messages apparently don't bother to hire an editor—giving you an advantage in figuring out their authenticity.

Sadly, fraudulent texts are on the rise. Across the U.S., \$86 million was reported lost in 2020 from frauds originating in scam texts, according to the Federal Trade Commission. That doesn't surprise those of us working with the AARP Fraud Watch Network helpline. A third of the scam attempts we've heard about recently started as a text message or an email.

If you haven't been a target yet, you almost certainly will be. Check out these real examples of fraud messages so that you can learn to spot the red flags.

Have questions related to scams?
Call the AARP Fraud Watch Network helpline toll-free at **877-908-3360**. For the latest fraud news and advice, go to aarp.org/fraudwatchnetwork.



3 The sender uses emojis. Legitimate companies rarely insert these into messages.

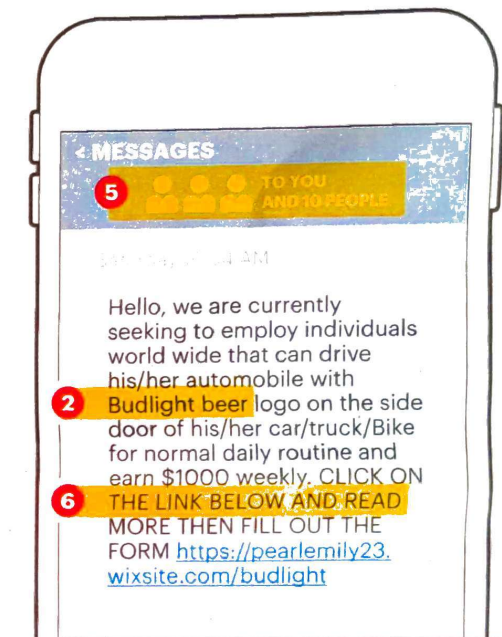
4 The message has a website link not associated with the company that's supposedly reaching out.

5 The email or text is directed to multiple phone numbers and people. Real businesses don't send out chain messages.

6 The sender uses ALL CAPITAL LETTERS. Scammers see this as a way to grab your attention. It is far less common in legitimate texts and emails.

1 The text or email suggests a relationship that doesn't exist. For example, you get a friendly, personalized email from a bank you don't use or a text referring to a package you never ordered.

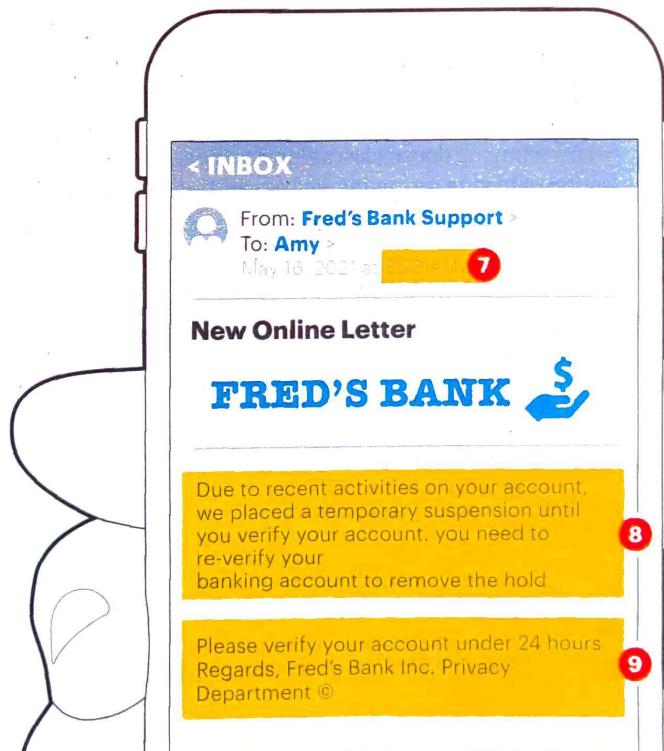
2 Spelling mistakes and poor grammar. The crooks writing these are doing it fast and blasting out thousands. They don't pay close attention to basic mistakes in punctuation, spelling and word choice.



5 The message is directed to multiple recipients.

2 The message contains a brand name (Budlight beer logo) not associated with the sender.

6 The message contains a link in all caps and a URL.



7 A "sent" time on a personalized email or text that suggests it originated in a foreign country.

8 A request for you to text your phone number or other personal information. Legitimate companies don't seek information this way.

9 Language that creates an unnecessary urgency. The goal, of course, is to spark emotions that spur you to take action without first thinking it through carefully. Don't be stamped into a mistake.