

Beware of Fake Toll Texts: A Nationwide Scam Targeting Drivers

February 26, 2025 - A new wave of text message scams is hitting phones across the U.S., demanding payment for bogus unpaid tolls. The scheme, which has been reported in multiple states, impersonates official toll services and tricks consumers into handing over personal and financial information.

It works like this. Scammers send text messages claiming to be from a toll agency, such as EZ Pass in the Northeast or FastTrak in California. The messages often include urgent warnings about overdue tolls, threatening excessive late fees or even legal action if the recipient does not pay immediately. Some of these messages also contain links to fraudulent websites that closely mimic real toll service sites.

In some cases, scammers instruct victims to copy and paste a link instead of clicking it directly, adding another layer of deception. One such message states:

While scammers try to make their messages look legitimate, there are several warning signs that can help you identify a fraudulent toll text:

If the message refers to a toll service from a state you haven't recently visited, includes misspellings or awkward language, the URL in the message does not match the official toll service website or the message pressures you to act quickly to avoid penalties, it is probably a scam.

The FBI reported receiving more than 2,000 complaints last year about toll-related text scams in just three states. The Federal Trade Commission (FTC) issued a fresh warning in January, stating that scammers are pretending to be toll agencies from coast to coast.

If you receive a suspicious toll-related text, follow these steps to stay safe:

- Do not click on any links. Instead, visit the official website of your state's toll agency directly to check your account balance.
- Delete the message. Use your phone's "report junk" feature to flag the scam before removing it.
- Secure your accounts. If you accidentally clicked the link or entered personal information, monitor your financial accounts for suspicious activity and report any unauthorized transactions immediately.
- Report the scam. File a complaint with the FBI's Internet Crime Complaint Center and include details such as the sender's phone number and the fraudulent website link.

Scammers continue to refine their tactics, but vigilance and skepticism can help protect you from falling victim to fraud. When in doubt, always verify toll charges through official sources and never share sensitive information through unsolicited messages.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS

