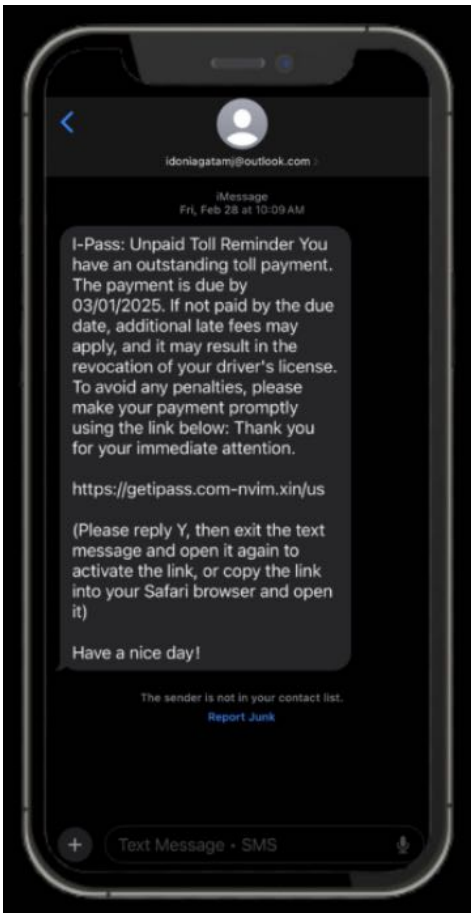
The Easiest Ways to Spot an Unpaid Tolls Scam Text

Joel Cunningham March 7, 2025



For one thing, the transportation administration doesn't use Gmail.

I've recently rented a car in two different states. Both times I was asked if I wanted to pay an extra fee per day to avoid worrying about paying tolls—a crucial issue in some states, like Florida, that no longer accept cash on the road and sometimes won't even allow you to pay online. Both times I declined, and set my Google Maps to "avoid tolls."

I was reasonably confident Google would keep me safe from an unpaid toll ticket, but my heart still skipped a beat when, a few weeks ago, I got a text message letting me know I had unpaid I-Pass tolls from Illinois. But then I took a closer look at the text.

Missed toll texts are the latest scam

It turns out that texts purporting to be from a tolling administration telling you you have unpaid tolls and you have to pay up, or else face fines or even lose your driver's license, are the latest in an unending stream of text-based phishing scams trying to get you to give up your personal info (and your money).

Transportation authorities in multiple states have issued warnings about these texts, which seem fairly legit at a glance. Typically they will purport to come from one of the major tolling programs—the E-ZPass in the northeast, FasTrak in California, I-Pass in Illinois. The text will inform you that you have an unpaid toll, provide a looming due date, and outline dire consequences for failing to pay up. Also included will be a handy, official-looking URL where you can make your payment.

Accessing that link will take you to a site that invites you to enter your credit card or banking information to settle your fine. And I'm sure you can imagine what happens from there, because you've just given your credit card number to a scammer.

How to spot a scam missed toll text

As scams go, this one isn't very sophisticated. The scammers aren't doing anything special to target you—they just have your phone number somehow and are including you in a mass spamming attempt in the hopes you'll be too distracted to notice the obvious signs the message isn't legit. So here are a few things to watch out for:

Do you even use this particular tolling service? In the last week, I've received half a dozen of these texts. Some of them are for services I've used and could conceivably owe money (like I-Pass, which operates in Illinois, one of the states I recently visited). Others, not so much: I didn't even know California used something called "FasTrak" until I googled it. So take a beat to think: Is there a legitimate reason *this* tolling agency is asking me for money? I might have a missed E-ZPass toll, but I definitely don't have a missed FasTrak toll.

Check the sender. One of the most obvious tells is the source of the text. Official automated texts will usually come from a 5-digit number. The texts I get telling me my E-ZPass has topped up, for example, come from "39769." Scam texts will more likely come from a full phone number, likely an international one, with an unfamiliar country code at the start (I recently got one from a number that began with "+44," indicating a number based in the U.K.). Another tell: If the sender is an email—especially if it's from a free email service like Gmail or Outlook (I've even gotten a few from Hotmail, which hasn't existed for years).

Non-hyperlinked URLs. When a message comes from a legitimate sender, any URLs included will likely be clickable. Scam texts will almost always have non-clickable URLs, with weird instructions either telling you to copy and paste the address into your browser, or to respond to the text with a Y, and then close and reopen it. This is an attempt to get around an iPhone security feature. Conveniently (for the scammer), once you've responded to a text and then reopened it, the link they sent you before will become clickable, taking you right to the site that will steal your payment info.

Look for other signs of an online scam. Chances are good the payment sites these URLs lead you to will also carry telltale signs of a phishing scam, like poor grammar, misspellings, or weird formatting. Luckily, all the ones I've been directed to visit via my most recent scam texts don't actually work, suggesting that the sites are being taken down as fast as the scammers can put them up. But I keep getting more of them, so they probably aren't going to stop trying.