NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

Toll and SunPass Text Scams: Don't Click “Pay Now”

A text claiming you owe money for an unpaid toll, from SunPass, E-ZPass, or another agency, is almost always a scam. This guide shows what the fake text looks like, how to spot the fake link, how to check your real toll account safely, and what to do if you already tapped the link or paid. (The phone number and link shown are made-up examples.)

How the scam works

A tiny amount, a big threat, and a link that wants your card.

A small unpaid toll
Usually just a few dollars, so it feels believable.

A scary deadline
“Pay today, or face a $50 fine, late fees, or legal action.”

A link that wants your card
It leads to a fake payment page built to steal your card or bank info.

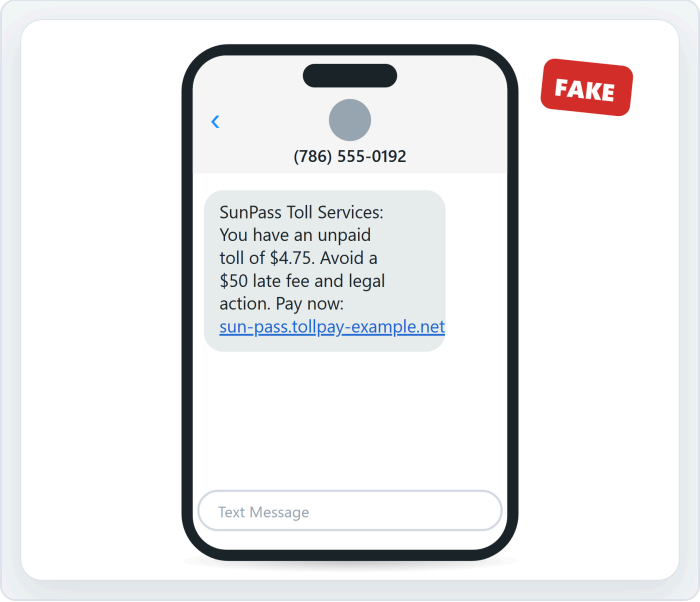
The warning signs of a toll text scam

WARNING SIGN

1 Here's what the scam text looks like

A short code or random number, claiming to be SunPass, with a link and a threat.

WHAT TO DO
Real toll agencies don't text you a bill with a “pay now” link and a threat.



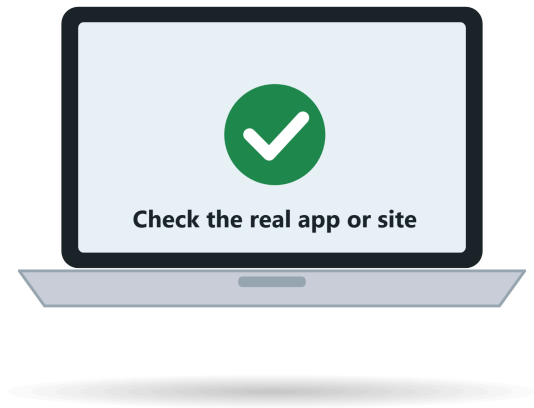
CHECK IT SAFELY

Check your real toll account instead

Open the official app, or type the agency's website address in yourself. Never tap the link in the text.

WHAT TO DO

If you really do have an unpaid toll, it'll be right there on your real account.



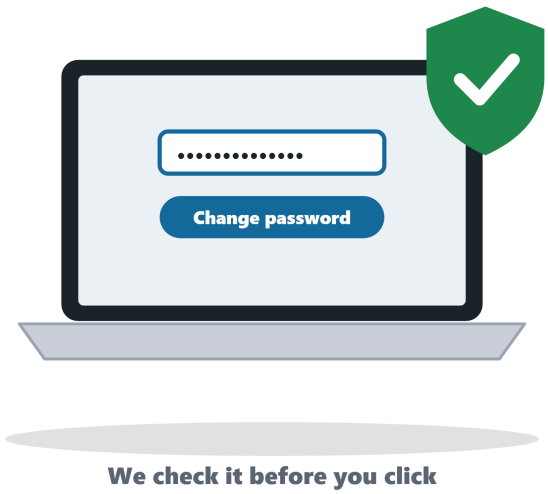
NAPLES COMPUTERS

Not sure if a toll text is real?

Forward it to us, or just call, and we'll check it before you tap anything.

WHAT TO DO

Already tapped a bad link? Call 239-513-1960, and we'll help you check your accounts.



Warning sign 2: look at the link

- [ ] It's not the agency's real website
  SunPass's real site is sunpass.com — nothing more, nothing less
- [ ] Extra words or a strange ending
  Like “-pay”, “-billing”, or a “.net”/“.xyz” instead of “.com”
- [ ] A text message, not an app or mail
  Toll agencies bill through their app, mail, or your online account, not a text link

3 rules to remember

- [ ] Never tap the link
  Go to the agency's app or real website instead, typed in yourself
- [ ] Delete it, don't reply
  Replying, even “STOP”, can confirm your number is active
- [ ] Report it
  Use your phone's “Report junk”, forward to 7726, or ReportFraud.ftc.gov

Already tapped it, or paid? Act fast.

- [ ] Entered card info on the fake page?
  Call your card company right away, and ask about a replacement card
- [ ] Just tapped the link, didn't enter anything?
  Close the page, and keep an eye on your accounts for anything odd
- [ ] Watch for follow-up scams
  Your number may get sold to other scammers; be extra alert for a while

Recap: toll text scams

- [ ] Small amount, big threat, a link — that's the pattern
- [ ] Check the link: not the agency's real, plain website
- [ ] Check your account in the real app or site instead
- [ ] Never tap the link; delete, don't reply
- [ ] Report it: Report junk, 7726, or ReportFraud.ftc.gov

The safest move is to never tap a link in an unexpected toll text. Open the official app, or type the agency's real website address in yourself, and check your account directly.

NAPLES COMPUTERS

Got a suspicious toll text? We'll check it for you.

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**