Who is Most at Risk?

Tourists and Visitors

Millions of tourists use Florida toll roads each year and may be unfamiliar with how the state's toll systems, like SunPass, operate. Scammers may exploit this confusion by sending fake toll violation notices after a trip ends.

Commuters

Floridians who regularly use toll roads, especially those commuting for work, are also frequently targets. With an automated system like SunPass, scammers attempt to trick these users into thinking there may have been an issue with a recent payment.

Elderly Drivers

Senior Floridians may be less familiar with digital scams and scammers may exploit an elder Floridian's concern about potential legal or financial issues by pressuring for quick payments.

Florida Attorney General's Office Scams at a Glance:

SunPass Safety

Visit MyFloridaLegal.com to find consumer tips or to file a complaint.

Report fraud by calling
1-866-9-NO-SCAM
(1-866-966-7226)

View other Scams at a Glance resources at:
MyFloridaLegal.com/ScamsAtAGlance

Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399-1050

03/2025

MyFloridaLegal.com

Scams at a Glance:

SunPass Safety

OFFICE OF ATTORNEY GENERAL

JAMES UTHMEIER

SAFE ★ STRONG ★ FREE

What are Toll Scams?

Toll scams occur when bad actors impersonate legitimate toll services, like SunPass and E-ZPass, to trick consumers into providing personal information or paying fraudulent fees. These scams will often threaten a target with penalties if fees are not immediately paid.

Types of Toll Scams

Fake Emails and Texts – Scammers send phishing emails or text messages that appear to come from SunPass or E-ZPass. These messages often include alarming language about overdue tolls and penalties to create urgency. They may also contain links to fake websites that mimic the legitimate toll service.

Phone Calls – Scammers may also impersonate toll service representatives over the phone, claiming unpaid toll fees and requesting immediate payment.

Fake Websites – Some scams direct a target to fraudulent websites designed to look like official SunPass or E-ZPass portals. These sites request personal information such as credit card information, billing address and account details, putting identity and finances at risk.

Tips to Stay Protected:

Verify the Source
SunPass and E-ZPass will never ask for sensitive information via text message or email. If a suspicious message is received, contact SunPass or E-ZPass directly using the customer service numbers listed on their official websites.

Look for Red Flags
Be cautious of messages that create a sense of urgency or threaten penalties if immediate payment is not made. Also, watch for poor grammar, misspelled words or links that seem slightly different than the official site as these are all common signs of phishing attempts.

Check an Account
Log into a SunPass or E-ZPass account through their official websites or apps to verify a balance and check for unpaid tolls before responding to unexpected notifications.

Never Share Personal Information
Do not provide personal information or payment details over the phone or through email unless absolutely certain that a legitimate toll line representative is on the other line.

Fake Emails and Texts — Fake Phone Calls — Fake Websites