State Attorney William Scheiner

The Monthly Brief

Volume 13 Issue 2 February 2025

Protect Yourself From the No. 1 Scam Targeting Seniors: 'Tech Support'

The No. 1 scam targeting seniors is phony tech support, as measured by complaints received through January by the FBI's Internet Crime Complaint Center.

Fraudsters posing as technical support representatives ask for remote access to victims' computers to fix nonexistent computer issues. Once in, they steal funds and sensitive information.

Four ways to protect yourself:

Learn the Signs: Tech support scams start with unsolicited calls, emails, or pop-up messages claiming that your computer has a virus or another issue. Be wary of any communication that pressures you into immediate action.

Remote Access Caution: Never allow remote access to your computer unless *you* have initiated the contact with a verified company technician.

Verify the Source: Never give out personal or financial information based on an unsolicited contact. Verify the identity of the support by calling the official support number from the company's official website.

What If You Already Paid a Scammer?

With a credit or debit card ...	Contact the company or bank that issued the credit card or debit card. Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.
Through a money-transfer app ...	Report the fraudulent transaction to the company behind the money transfer app and ask them to reverse the payment. If you linked the app to a credit card or debit card, ask your card company or bank to reverse the charge.
With a gift card ...	Keep the gift card itself, and the gift card receipt. Contact the company that issued the gift card, Tell them it was used in a scam and ask them to refund your money.

Toll-Collection Fraud Starts With Text Message

If you receive a text message that says you owe unpaid expressway tolls and asks you to click a link to pay up, just delete it. It's a scam.

The Central Florida Expressway Authority, which operates toll roads and E-PASS accounts, says it never texts drivers about toll balances.

The authority has alerted customers of an ongoing national text-phishing scam, a practice the FBI now refers to as "smishing."

The scam has been reported in several states, including Florida. Thousands of people have been targeted.

The scammers appear to be choosing recipients' phone numbers at random and not based on their use of toll roads or E-PASS accounts.

E-PASS account holders who receive suspicious text messages should play it safe and check or pay their accounts on the official E-PASS website or the E-PASS app available from the Apple App Store, or Google Play store.

Question or Suggestion?

Email Mreed@SA18.org