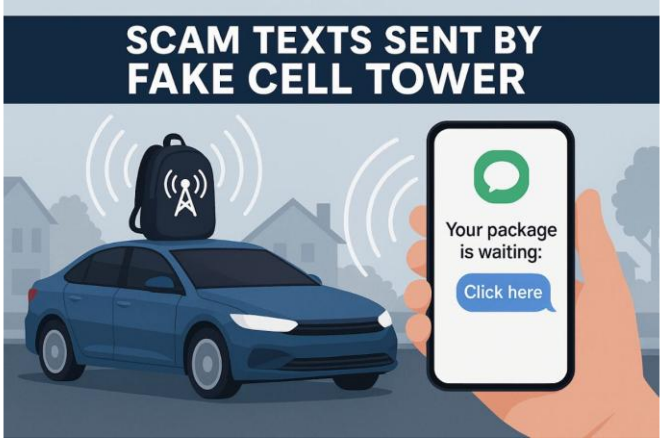
Spam on wheels

The Current, Komando.com, 9/23/25



Ever get one of those weird texts that says something like, “Your package is waiting” or “Click here to unlock your cash reward”? We all have. Most people figure it’s just a scammy mass text from some sketchy website.

You can’t be so sure anymore. What if I told you those shady texts didn’t come through the usual networks? They were broadcast by a random car driving through your neighborhood?

That’s the new trick. Scammers are using devices called SMS blasters, and they’re not just annoying, they’re downright dangerous.

A cell tower in a backpack?

Here’s the deal: These devices pretend to be a real cell tower.

Your phone gets tricked into connecting, even if just for a second, and then BAM, a scam text pops up like it came from nowhere. These setups can be mobile, too. I’m talking about backpacks, parked vans, rental cars on the move.

They don’t need your number. They don’t even need a list. They just hijack every phone nearby and blast out messages like spam on steroids.

Why this should freak you out

These scam texts can look *really* convincing. Delivery updates, IRS warnings, bank fraud alerts, the kind of stuff you click without thinking twice. One wrong tap, and they’ve got you. Personal info, passwords, credit card numbers, all wide open.

Here’s the kicker: Even the scam filters on your phone can’t stop them because these texts are basically cheating the system.

Your checklist

1. Turn off old connections: Scammers love older networks because they're easier to spoof. Disabling 2G or older on your phone blocks one of their favorite tricks. I checked the steps below, but they may be different on your device, depending on make, model and operating system. Just keep poking around until you find them.

- **iPhone:**
  Go to **Settings** > **Cellular** > **Cellular Data Options**. Under **Voice & Data**, select **LTE** or **5G**, then under **Data Mode**, turn off **Allow More Data on 5G** if it's enabled. iPhones don't always offer a "disable 2G" option, but choosing the most secure data setting helps.

- **Android (Pixel/Samsung):**
  Go to **Settings** > **Connections** or **Network & internet** > **Mobile networks** or **SIMs** > **Network Mode** or **Preferred network type**, then select **5G/4G/3G** only. If you see "Allow 2G" (available on newer models), **toggle it OFF**.

2. Don't click sketchy links: If a text or email comes out of the blue with weird grammar and an urgent tone, don't tap. Visit the company's website manually or call their official number to check if the message is legit.

3. Report and warn others: Don't just delete scam texts. Report them to your carrier (forward to 7726) or the FTC at **reportfraud.ftc.gov**.