USB charging outlets Travellers warned of 'juice jacking' scams that lock phones, steal data

Rigged free USB charging stations can be used by scammers to access your data.

Many thoughts can go through your mind at the airport as your phone's battery dwindles from green to yellow to red. How is it already dead? What if I can't call Uber when I land? Where is my charger? But when you find a place to plug in and charge, it may not be as simple - or safe - as you think.

The Los Angeles County district attorney's office is warning travellers using Los Angeles International Airport of a new scheme targeting people who need a quick boost at public USB charging stations. The USB charging scam, also known as "juice jacking," involves hackers spoofing charging stations to steal information.

Similar to credit-card skimming, fake charging stations are set up via port or cable, and unknowing users who plug into them expose their devices to malware attacks that can lock their devices and export sensitive contents such as passwords and bank account numbers into the hands of waiting information thieves.

Avoid using public USB charging stations at airports and other locations," the district attorney's office wrote on Twitter.

Sometimes phone security is taken for granted, he says, along with the knowledge that the phone's charging port is also how the phone sends and receives data.

"The big thing we tell people is to try to use [a power] adaptor instead of finding a random USB socket somewhere," he says. He also cautioned people to be aware of actions such as habitually using the cables in ride-share cars, hotels or, if travelling abroad, in internet cafes.

A key thing to look out for is whether your phone displays a "Do you trust this computer?" message when you plug into a USB outlet. Sisak said that's an easy giveaway that a data device has been connected to it. On anything that's not your home computer, the answer should always be "no."

Scammers rely on the easy access that the multiuse charging stations provide to catch flyers off-guard.

Sisak recommends avoiding USB charging stations in airports and hotels, and he says travellers should make sure their packing list includes a charger for quick plug-ins to wall outlets.

"It doesn't seem like it's happening daily, but it is something that's very hard to track," Sisak says. "It's just far better to try to be safe than sorry."

But for passengers who would like the added peace of mind and extra security, he recommends buying a "USB condom" to protect them from any security vulnerabilities.

The device is an add-on USB connector, usually costing around $US10 ($A14), that blocks the data pins on the end of a USB cable so that the only thing that flows from an outlet to a device is power.

Schneier is skeptical that a hacker would be able to pull off the kind of effort it would take to rig a public charging station, given how public and busy airports are.

There's ultimately, he says, a very simple step to reduce the chances it can happen to you: "Honestly, if you worry**, just plug it into a power outlet."**