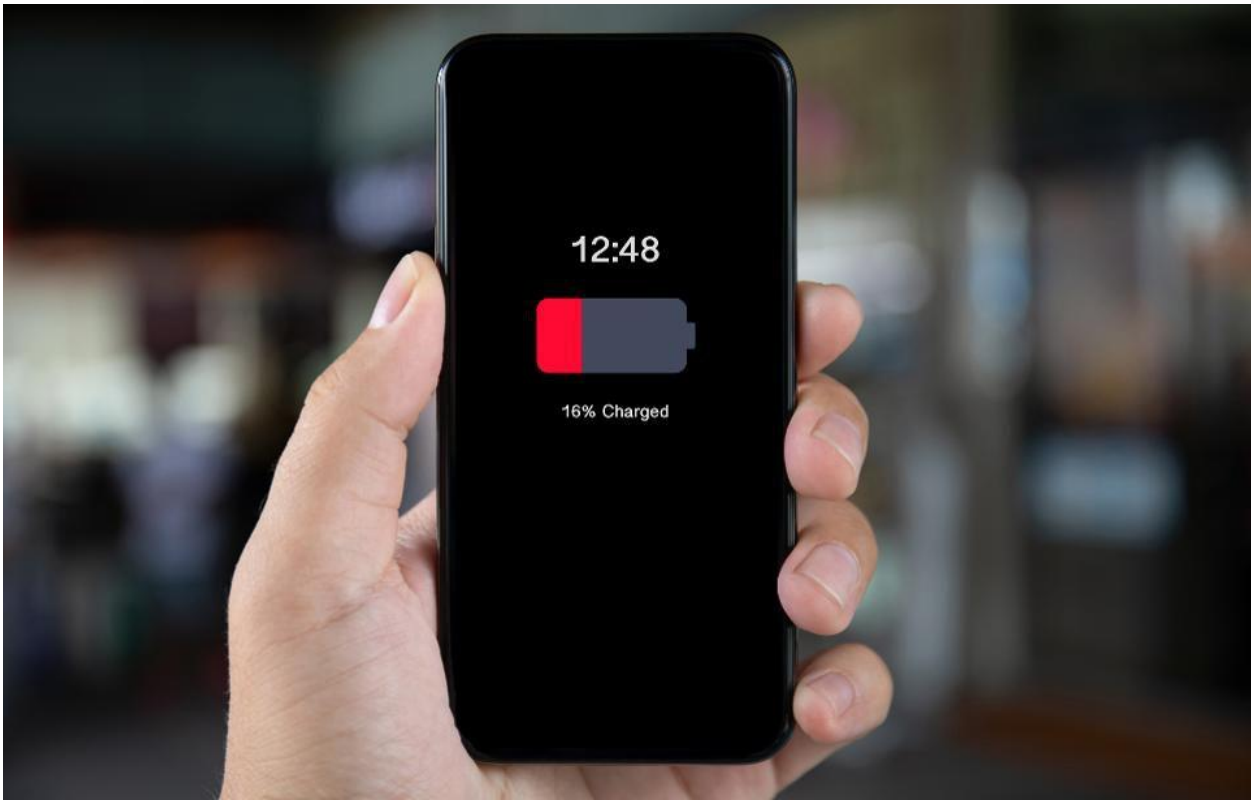
Forbes

May 21, 2019, 10:25am

Why You Should Never Use Airport USB Charging Stations

Suzanne Rowan Kelleher
Contributor

Travel



Almost out of juice? Be careful of where you turn for a power boost.

GETTY

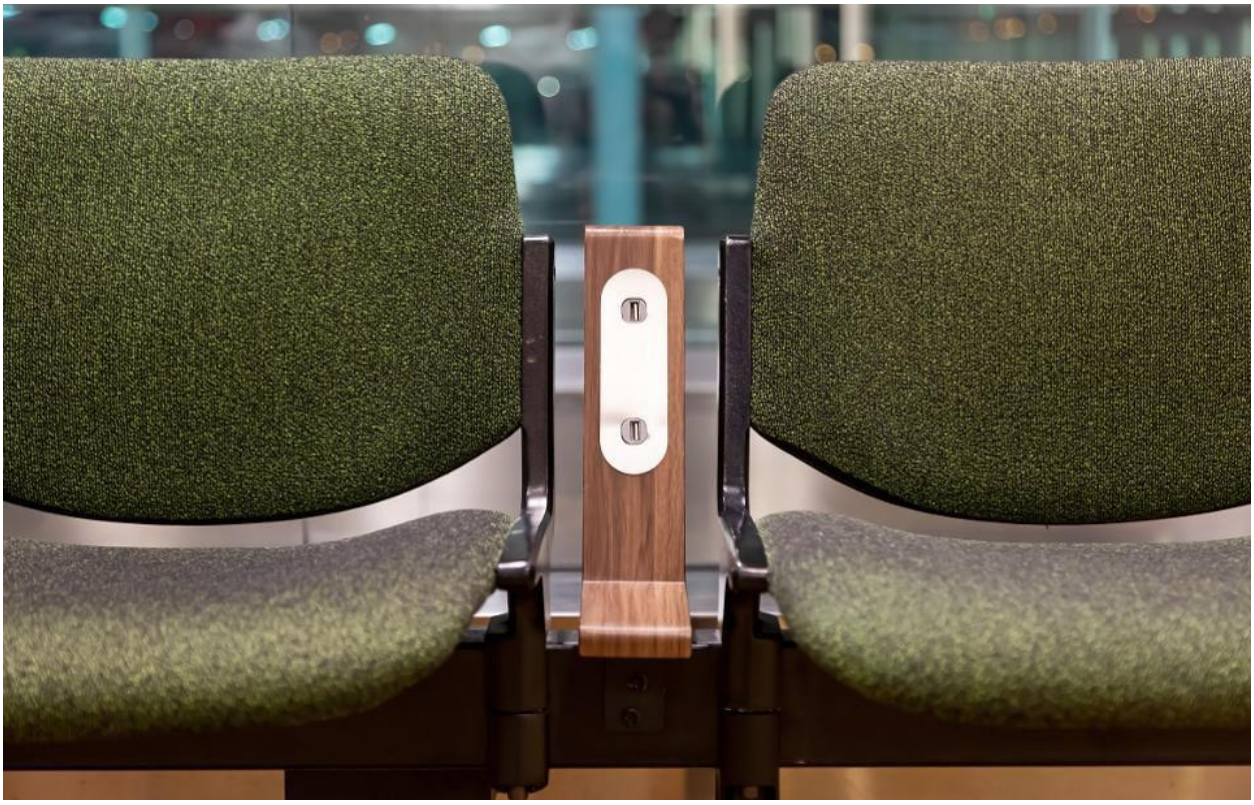
Those oh-so-handy USB power charging stations in the airport may come with a cost you can't see. Cybercriminals can modify those USB connections to install malware on your phone or download data without your knowledge.

"Plugging into a public USB port is kind of like finding a toothbrush on the side of the road and deciding to stick it in your mouth. You have no idea where that thing has been," says Caleb

Barlow, Vice President of X-Force Threat Intelligence at IBM Security. "And remember that that USB port can pass data."

It's much safer to bring your regular charger along and plug it into a wall outlet or, alternatively, bring a portable power bank to recharge your phone when you're low on bars.

If you insist on using public USB ports, Barlow recommends investing $10 for something called a Juice-Jack Defender. "It's a little dongle you can put in front of your charging cord that basically blocks any data from passing down the cord. It only passes the voltage," says Barlow.



They're handy, but airport USB charging stations may pose a risk to your personal data.

GETTY

While these precautions may seem excessive to the average traveler, Barlow says it's smart to worry about public USB power stations. A growing number of nation-state hackers are now training their sights on travelers, according to new research from IBM Security. The 2019 IBM X-Force Threat Intelligence Index reveals that the transportation industry has become a priority target for cybercriminals as the second-most attacked industry — up from tenth in 2017. Since January 2018, 566 million records from the travel and transportation industry have been leaked or compromised in publicly reported breaches.

Barlow also advises steering clear of random tech accessories left behind by other travelers. "My favorite of which is a simple Apple charging cord," he says.

“Let's say I’m a bad guy. I go into an airport. I’m not going to easily take apart the charging station but it’s easy to just leave my cord behind. Now, if you see an Apple charging cord, you're likely to grab it or just plug into it. But inside this cord is an extra chip that deploys the malware, so it charges your phone but now I own your computer.”

You take a similar risk if you use any old USB stick you find lying around. “A lot of companies now are banning the use of USB storage devices because at the end of the day they're dangerous,” says Barlow. “If you want to get into a company, go buy a couple hundred USB sticks and cast them around in places where you know company will go. Guaranteed, one of them will get plugged into a company laptop.”

For more travel insights, follow me on Instagram (@suzannekelleher), Pinterest (@suzannerowankelleher) and Flipboard (@SRKelleher).