Beware of Juice-Jacking

Published: 2011-08-22 · Archived: 2026-04-05 21:12:59 UTC

You're out and about, and your smartphone's battery is about to die. Maybe you're at an airport, hotel, or shopping mall. You don't have the power cable needed to charge the device, but you do have a USB cord that can supply the needed juice. Then you spot an oasis: A free charging kiosk. Do you hesitate before connecting your phone to this unknown device that could be configured to read most of the data on your phone, and perhaps even upload malware?

A DefCon attendee using the charging kiosk.

The answer, for most folks, is probably not. The few people I've asked while researching this story said they use these charging kiosks all the time (usually while on travel), but then said they'd think twice next time after I mentioned the possible security ramifications of doing so. Everyone I asked was a security professional.

Granted, a charging kiosk at an airport may be less suspect than, say, a slightly sketchy-looking tower of power stationed at **DefCon**, a massive hacker conference held each year in Las Vegas. At a conference where attendees are warned to stay off the wireless networks and avoid using the local ATMs, one might expect that security experts and enthusiasts would avoid using random power stations.

But some people will brave nearly any risk to power up their mobiles. In the three and a half days of this year's DefCon, at least 360 attendees plugged their smartphones into the charging kiosk built by the same guys who run the infamous Wall of Sheep, a public shaming exercise at DefCon aimed at educating people about the dangers of sending email and other online communications over open wireless networks.

Brian Markus, president of Aires Security, said he and fellow researchers **Joseph Mlodzianowski** and **Robert Rowley** built the charging kiosk to educate attendees about the potential perils of juicing up at random power stations. Markus explains the motivation behind the experiment:

"We'd been talking about how dangerous these charging stations could be. Most smartphones are configured to just connect and dump off data," Markus said. "Anyone who had an inclination to could put a system inside of one of these kiosks that when someone connects their phone can suck down all of the photos and data, or write malware to the device."

To make their charging station more attractive to passersby, Markus and his pals equipped it with a variety of charging cables to fit the most popular wireless devices. When no device was connected, the LCD screen fitted into the charging station displayed a blue image with the words "Free Cell Phone Charging Kiosk." The screen switched to a red warning sign when users plugged in any devices. The warning message read:

> "You should not trust public kiosks with your smart phone. Information can be retrieved or downloaded without your consent. Luckily for you, this station has taken the ethical route and your data is safe. Enjoy the free charge!"

Markus said the comments from those who chose to juice up their phones at the kiosk were the most rewarding part of the project.

"One guy that clearly seemed stressed and in a hurry to get his phone topped off said, 'I don't care, take my data, I need my phone charged to make a phone call!'" Others said they planned to wipe their phones after leaving the hacker conference anyway.

"One attendee claimed his phone had USB transfer off and he would be fine. When he plugged in, it instantly went into USB transfer mode," Markus recalls. "He then sheepishly said, 'Guess that setting doesn't work.'"

Another DefCon attendee remarked, "This freaked my boss out so much he sent an email across the entire company stating employees are now required to bring power cables and/or extra batteries on travel, and no longer allowed to use charging kiosks for smart devices in open public areas."

Inside the charging kiosk.

The safest route for charging your device on-the-go is to use the supplied power cord that plugs into a regular electrical outlet (assuming you can find an available outlet). Battery-powered mobile charging devices also work well in a pinch and are available at many airports. If you must use a random charging kiosk, the safest option may be to completely power off the device before plugging it in.

"One thing we discovered: On certain devices, if you power them completely off, then charge them, they don't expose the data," Markus said.

Source: http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/