Stop! Don’t Charge Your Phone This Way

nytimes.com/2019/11/18/technology/personaltech/usb-warning-juice-jacking.html

By Aimee Ortiz

18 novembre 2019

A dead or dying phone or laptop is enough to send anybody on a mad dash to find a way to charge the device, but you might want to think twice before using that random cable found at an airport charging station or docking into that hotel USB port — hackers could be waiting.

As the busy holiday season approaches, the Los Angeles County District Attorney’s Office iswarning travelers about a USB charger scam, or “juice jacking.”

“A free charge could end up draining your bank account,” Luke Sisak, a deputy district attorney, said in a video posted online this month.

Juice jacking happens when unsuspecting users plug their electronic devices into USB ports or use USB cables that have been loaded with malware.

The malware then infects the devices, giving hackers a way in. They can then read and export your data, including your passwords, and even lock up the gadgets, making them unusable.

Juice jacking exploits the fact that somebody doesn’t have a full battery, saidLiviu Arsene, a cyber security expert at BitDefender, a Romanian cybersecurity and antivirus software company.

Mr. Arsene cautioned against using USB cables found already plugged into charging stations or even given away as promotional gifts.

“You can easily brand these things so you can make it look like any other cable,” he said, adding, “When people see it, they don’t really think or expect it to be malicious in any way.”

Other ways to protect yourself include carrying your own charging wires, only charging directly from an electrical outlet and using portable batteries that were bought from known vendors, Mr. Arsene said.

“Don’t believe everything you see, and don’t believe everything you get your hands on,” he said, noting that starting with Black Friday, if it looks too good to be true, it probably is.

But it isn’t just cables that pose a risk for tech consumers; it’s the ports, too.

Like scammers who steal debit card numbers by putting illegal card-reading devices, or skimmers, on A.T.M.s, hackers can easily rip out USB ports and replace them with their own malicious hardware, said Vyas Sekar, a professor at CyLab, a security and privacy research institute at Carnegie Mellon University.

“It’s easy to modify the outlet if the attacker has physical access,” Professor Sekar said.

Though Mr. Arsene and Professor Sekar said they were unsure of how often hacking attacks like these happened, the growing ubiquity of USB charging ports in places like hotels, airports and public transportation has translated into an increased risk of falling victim to such scams.

“People want the convenience of charging their phones and tablets wherever they go,” Professor Sekar said, adding, “Obviously I would like it too, but there is a risk.”

Professor Sekar said consumers could also use attachable protective devices on USB cables known as “USB condoms.”

“What they do is a very simple trick,” he said. “They essentially disable the data pin on the USB charger.”

This means that the device will charge, but the cable will be unable to send or receive data.

“For less than five bucks you can buy it,” he said, “and that can actually save you.”

The Los Angeles County district attorney’s office echoed cybersecurity experts in its tips for consumers, including using a power outlet and not a USB charging station, carrying your own AC and car chargers and keeping a portable charger for emergencies.