Charging your phone using a public USB port? Beware of 'juice jacking'

6 February 2020, by Ritesh Chugh

Credit: AL Robinson/Shutterstock

Have you ever used a public charging station to charge your mobile phone when it runs out of battery? If so, watch out for "juice jacking."

Cybercriminals are on the prowl to infect your mobile devices such as smartphones and tablet computers and access your personal data, or install malware while you charge them.

Specifically, juice jacking is a cyber attack in which criminals use publicly accessible USB charging ports or cables to install malicious software on your mobile device and/or steal personal data from it.

Even a 60-second power-up can be enough to compromise your phone's data. This is because USB cables allow the transmission of both power and data streams simultaneously. Victims can be left vulnerable to identity theft, financial fraud, and significant stress.

USB charging stations are a common sight in shopping centres, airports, hotels, fast-food restaurants, and even on public transport. While juice jacking is neither new nor particularly widespread so far, it was recently highlighted by Los Angeles County District Attorney's Office as a significant threat, especially to travellers who can easily find themselves caught short and in need of a battery boost.

How does it work?

First, the attackers tamper with the charging stations or cables in public areas, and install malicious software on them. This software then infects the phones of unsuspecting users who subsequently plug into the tampered charger.

The software can invade, damage or even disable your phone. It can also steal or delete data from your phone and possibly spy on your usage activity, to the extent of transmitting your personal information such as account numbers, usernames, passwords, photos, and emails to the perpetrator.

How can I tell if I've been juice jacked?

Hacked mobile devices will often go undetected. But there are a few telltale signs that your device may have been hacked. These include:

- a sudden surge in battery consumption or rapid loss of charge, indicating a malicious app may be running in the background
- the device operating slower than usual, or restarting without notice
- apps taking a long time to load or frequently crashing
- excessive heating
- changes to device settings that you did not make
- increased or abnormal data usage.

How do I protect myself?

The tampering of USB charging stations or USB cables is almost impossible to identify. But there are some simple ways to guard against juice jacking:

- avoid USB power charging stations

- use AC power outlets rather than USB ports
- use a portable battery power bank (your own, not a borrowed one!)
- carry your own charging cable and adaptor
- use a data-blocker device such as SyncStop or Juice-Jack Defender. These devices physically prevent data transfer and only allow power to go through while charging
- use power-only USB cables such as PortaPow, which don't pass any data.

And finally, if you must use a charging station, keep your phone locked while doing so. USB ports typically don't sync data from a phone that is locked. Most mobile phones will ask your permission to give the USB port access to your phone's data when you plug in. If you're using an unknown or untrustworthy port, make sure you decline.

I think I might have been juice jacked—what can I do?

If you suspect you have fallen prey, there are several things you can do to protect your device's integrity:

- monitor your device for unusual activity
- delete suspicious apps you don't recall installing
- restore your device to its factory settings
- install anti-virus software, such as Avast Antivirus or AVG AntiVirus
- keep your mobile device's system software up to date. Developers continually release patches against common types of malware.

A lot of data is stored on our mobile devices these days, and protecting our privacy is crucial. While juice jacking may not be a widespread threat, it is important to ensure the safety of our mobile devices. So, the next time you consider using a public USB charging station or cable, ask yourself if it is worth it, particularly as your personal information is at stake.

Provided by The Conversation