JUICE JACKING: RISKS AND REMEDIES

If you're stuck somewhere with a dying smartphone battery, you may not think twice about plugging in at the nearest USB charging station.

Beware!

Possible that someone has loaded malware on the USB port or the USB cable attached to these public charging stations. While your phone is charging, the perpetrator might infect your device with a virus or malware that could track your keystrokes or steal sensitive data from your mobile device, including passwords, files, contacts, texts and voicemails.

Juice jacking does not yet appear to be widespread threat, but it's still a good idea to understand your risks before giving your battery a boost at public charging stations like those at airports, hotels or long distance AC Volvo buses.

How does juice jacking work?

Whether you have an iPhone, BlackBerry or an Android device, smartphones have one thing in common: The power supply and the data stream pass through the same cable. Juice jacking works because the port used for charging a device can also transfer data.

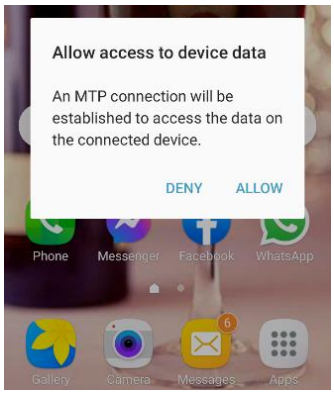
In this hardware-focused Man in the Middle (MitM) attack the attacker uses a USB connection to load malware directly onto the charging station or infect a connection cable.

When your phone connects to another device, it pairs to that device and establishes a trusted relationship. So during the charging process also, the USB cord opens a trusted pathway into your device to share information which the cybercriminal can exploit.

A regular USB connector has five pins, where **only one is needed to charge the device**. Two of the other pins are used for data transfers.

Pin	Name	Wire Colour	Description
1	V_{BUS}	Red	+5 V
2	D–	White	Data –
3	D+	Green	Data +
4	ID	No wire	Permits distinction of a host connection from device connection • "A" Plug (host) : Connected to the signal ground • "B" Plug (device) : Not connected
5	GND	Black	Signal Ground

← **USB Connection Table**



Unless you have made changes in your settings, on most phones the data transfer mode is disabled by default (except on devices running older Android versions). For instance, when you plug your phone into your computer, a message pops up to ask whether to trust the device.

In the case of USB charging points, the device owner won't see what the USB port connects to. The connection is only visible on the end that provides the power. That means, when a user connects to a USB port for a charge, a pathway to move data may be established without knowledge of the user.

Although USB ports and phone charging cables are the most common devices used in juice-jacking attacks, other less common devices like USB ports in video arcade consoles and portable battery power banks can also be used in this type of exploit.

Types of juice jacking attacks

Data theft

In data theft juice-jacking attacks, sensitive information is stolen from connected device. Depending on how long a device is left plugged into a compromised cable or port, very large amounts of data may be compromised. Given enough time and storage space, hackers may even be able to make a full backup of the data on a device.

Using a crawler program on your device, a cybercriminal could then search for personally identifiable information (PII), account credentials, banking-related or credit card data. These crawlers have the ability to copy all information to their own devices. There are also many malicious apps that can clone all your phones' data to another phone and to impersonate you or access your financial accounts.

Malware installation

When malware installation juice-jacking attacks occur, malware is automatically installed in the connected device. The malware remains on the device until it is detected and removed by the user. The malware placed on the device may do a great deal of damage, including manipulation of a phone or computer, spying on a user, locking the user out of the device or stealing information.

Cybercriminals may use a malware app to clone your phone data, your GPS location, purchases, social media interactions, photos, and call logs and transfer it back to their own device. There are many categories of malware that cybercriminals can install through juice jacking, including adware, cryptominers, ransomware, spyware, or Trojans. Once your device is frozen or encrypted with one of these types of malware, the cyber-thief may demand payment to restore the information.

Multi-device attack

On top of harming the device plugged into a compromised charger, a device charged by infected cables may in turn infect other cables and ports with the same malware as an unknowing carrier of the virus.

Disabling attack

Some malware uploaded through a charging device can lock the owner out of their device, giving full access to the hacker.

Remedies

The best defense against any such attack is awareness. Here are few tips to avoid juice jacking attacks:

1. **Keep your devices fully charged**

This is the most obvious precaution. Make it a practice to charge your phone full before you step out. Charge your phone at work, in the car, or at home, when you're not using it. Try and reduce instances of low battery while you are traveling.

2. **Carry personal charger with you**

Avoid public charging stations or portable wall chargers. Plan ahead. Always keep your charger in your bag for charging.

3. **Choose a different method to charge your phone**

Options can include external batteries, wireless charging stations, or power banks — devices you can charge at home and power your device on the go.

4. **If you must charge your phone, use an AC wall outlet**

Data cannot be transferred from your device at a regular AC wall outlet. So if you're in public and desperately need a charge, consider using a wall socket. And if you're traveling, make sure you have the correct adaptor before heading out on your trip.

5. **Switch off or Power the phone down**

Switch your phone off if you are using a charger/adapter that is not yours, especially in public places. There is a one-way flow that allows the power to travel to the phone without having any data transit taking place.

This technique only works on few mobile models as some phones, despite being powered down, still powers on the entire USB circuit and allows access to the flash storage in the device. Hence, this may not be an optimum solution always.

6. **Lock Your Phone**

When your phone is locked, it cannot be paired with any device. Be cautious not to use your face/finger print id since pairing can happen unintentionally within a flick of a second. So you have to make sure that the phone is really locked and don't unlock it while it is in the charging station.

7. **Use specialized cables**

You can buy a special Charge-Only USB cable that doesn't have pinout connections for pins 2 and 3. Therefore it's impossible to transmit data across the connection. These are two conductor cables meant for charging only and prevents data transfer.

8. **Use USB pass-through devices**

These adapters allow power to flow through but disable the data pin on the USB charger. That means the device charges, but data won't transfer.

9. **Reject data transfer request**

Do not accept the request to allow the cable to be used for data transfer. In case only a data cable is accessible, 'cancel' the request to transfer data hence blocking the data flow and allowing it to only charge.

10. **Use a USB condom**

It is a device that goes between your normal data charging cable and a USB port to block data transfer through the connection. The USB Condom is a small and unobtrusive dongle that effectively turns any USB cable into a secure 'charge-only' cable to allow safe recharging from untrusted USB ports.

Ref:
https://en.wikipedia.org/wiki/Juice_jacking
https://us.norton.com/internetsecurity-mobile-what-is-juice-jacking.html
https://timesofindia.indiatimes.com/blogs/tastefully-contemporary/beware-of-juice-jacking-a-new-way-to-steal-your-data/
https://searchsecurity.techtarget.com/definition/juice-jacking
https://blog.malwarebytes.com/explained/2019/11/explained-juice-jacking/
https://en.wikipedia.org/wiki/USB_hardware
https://www.youtube.com/watch?v=ezy03Y6xbbw
Image: https://www.dailymail.co.uk/