The Indian EXPRESS
JOURNALISM OF COURAGE

Why you should think twice before using public charging ports while travelling

Do you charge your phone at airports, cafes, or other public places? Then this edition of The Safe Side is for you. We break down how juice jacking works and what you can do to stay safe.

Your phone's battery is at three per cent, and you are desperate to recharge it. Next, you spot a charging point at the airport, or a railway station, or a cafe, and gladly plug in your phone without thinking much.

Instant relief that the phone is back up, and you proceed to respond to the urgent text or call and ease yourself into waiting for the battery to reach at least 20 per cent. In all of this, one thing most of us would overlook is that this simple act of plugging a phone into a public USB port may also silently open the door to a lesser-known cybercrime.

This cybercrime is known as juice jacking, a scam in which compromised charging points or look-alike power devices are used to access data, install malware, or even spy on unsuspecting users.

What is juice jacking?

Pavan Karthick M, threat researcher III at CloudSEK, told indianexpress.com, "Juice jacking may sound like a new term, but the technique itself has existed for a long time, earlier seen in attacks using malicious USB pen drives or 'Rubber Ducky' devices (USB devices that mimic a keyboard to execute malicious scripts rapidly on any system). What has changed today is the form factor — attackers can now hide this behaviour inside something that looks like a

normal charging cable or power bank."

"Technically, the USB device you plug in can behave like a keyboard or mouse, also called a Human Interface Device (HID). An HID is not malicious by default, but it can automatically type commands, enter text, or click through screens in milliseconds. You might briefly see something open and close, but in the background, malware could be installed, or data could be accessed," Karthick explained.

Dr Sanjay Katkar, joint managing director of Quick Heal Technologies Limited, described this cybercrime as a form of smartphone compromise. He said, "Attackers hide malicious hardware inside public charging points, fake power banks, or tampered cables and then persuade users to plug in and unlock their phones under the pretext of just checking if it's charging."

"Once the connection is established, the rogue device can silently attempt to access files, copy contacts, steal authentication tokens, or push malware onto the phone without any visible alert. In crowded places like cafes, stations, or airports, this social engineering layer is critical – the scam works because it feels like a harmless, time-saving favour."

"This makes juice jacking a combination of technology and social engineering. If users do not unlock their device or grant permissions when prompted, modern smartphones are generally safe," Karthick added.

Targeted threat

"Juice jacking is often described as a common cyber risk, but in practice, it is unlikely to be used randomly against the general public. Attackers have much easier and cheaper ways to collect data at scale. USB-based attacks require physical access, planning, and custom hardware, which makes them inefficient for mass targeting," said Kaushal Bheda, director at Pelorus Technology.

"The real risk lies in targeted operations," he said. "People who carry sensitive information, such as government officials or senior executives handling sensitive, strategic or intelligence-related data, are more realistic targets. In such cases, attackers may use modified charging cables, compromised power banks, or social engineering to gain access."

"For anyone in a high-risk role, simple precautions work well. Use your own charger and cable, carry a personal power bank, and avoid unknown USB accessories, especially if someone offers them directly. For most people, juice jacking remains a low-probability threat rather than a day-to-day concern," Bheda added.

Evolution of the scam

"Juice jacking may evolve beyond isolated incidents into large-scale supply-chain attacks. In such scenarios, state actors could compromise charging hardware, cables, or device components at scale, enabling the silent infection of thousands of devices through trusted infrastructure. This would provide persistent access to sensitive communications and data flows across national networks, turning everyday charging points into strategic surveillance vectors and posing serious long-term risks to digital sovereignty and national security," Kaushal Bheda added.

"The future of juice jacking is no longer about careless users; it is about losing control altogether. What began as a niche cyber threat is rapidly evolving as public charging points become ubiquitous across airports, railway stations, malls, EV charging stations/ hubs, and smart cities in India and globally," opined Vaibhav Koul, managing director, Protiviti Member Firm for India.

"First-generation juice jacking relied largely on user error or inaction. Second-generation Juice Jacking attacks, known as 'Choice Jacking', change the rules entirely. In these scenarios, malicious cables or chargers force a data-enabled connection, bypassing the user's on-screen choice altogether. Consent is no longer tricked; it is overridden," said Koul.

"What makes choice jacking dangerous is its precision. These devices can impersonate keyboards or mouse, inject commands in milliseconds, defeat 'charge-only' prompts, and operate even against security-aware users. Because the attack mimics legitimate hardware behaviour, it is significantly harder for mobile operating systems to detect," added Koul.

"As these techniques converge with AI-driven malware that activates only during sensitive actions, such as UPI payments, banking logins, or corporate email access, the future of juice jacking shifts from opportunistic data theft to targeted financial fraud and enterprise compromise. Juice jacking once relied on users making the wrong choice. NextGen version of the scam removes the choice altogether, your phone says 'charge only,' but the malicious cable can decide otherwise and leak sensitive information," Koul said.

What threats does the scam pose to users?

The risks of juice jacking go far beyond a phone being briefly compromised and can lead to long-term financial and privacy damage, said Dr Sanjay Katkar, of Quick Heal Technologies Limited.

1. Once a malicious cable or charging port gains access, attackers may steal personal data stored on the device.

2. Passwords, authentication cookies, and login credentials can be harvested without the user's knowledge.
3. Messaging apps may be hijacked, allowing attackers to read private conversations or impersonate the user.
4. Spyware can be silently installed to track keystrokes, app activity, and user behaviour over time.
5. In India, where smartphones are closely linked to UPI, banking apps, and OTP-based verification, such access can enable account takeovers and fraudulent fund transfers.
6. Stolen contacts and messages can be misused for impersonation, scams, or social engineering attacks.

"According to our India Cyber Threat Report 2026, the Android threat landscape is becoming increasingly sophisticated by the day, with banking trojans, spyware, fake apps and honey traps already causing considerable financial distress to unsuspecting users. Amidst this, it is recommended to install robust security solutions for mobile and detect anomalous activity, block malware, and flag suspicious financial or communication patterns that may follow such a compromise," said Dr Katkar.

How to protect your phone?

Karthick discussed preventive measures to protect your devices against juice jacking.

1. Never unlock your phone when connecting it to an untrusted cable, power bank, or public charging port
2. Even if your phone is already unlocked, always plug and unplug the cable yourself and do not hand your phone to strangers
3. Pay close attention to any permission prompts that appear while charging
4. On newer smartphones, accessories require explicit user approval to perform actions, which helps reduce the risk of data theft. A genuine power bank or charging port should never ask for accessory permissions; charging should start automatically without any prompts.

What to do in case users suspect falling prey to this scam?

Dr Sanjay Katkar and Karthick listed some points on what to do if someone falls victim to this scam.

1. Immediately disconnect the device from the charging source and, if possible, power it off briefly.
2. After restarting, run a full device scan using a trusted security solution to detect and remove any malware or trojans that may have been introduced.
3. Change passwords for critical accounts, including email, banking, UPI apps, and social media, from a known clean and trusted device.

4. Review recent login history and transaction activity across all important accounts.
5. Enable or recheck multi-factor authentication (MFA) wherever available
6. Watch for signs of fraud such as suspicious UPI transfers, newly linked devices, or unusual messages sent from your accounts.
7. If any fraudulent activity is detected, immediately inform the bank or payment service provider.
8. File a formal complaint with the local cybercrime authorities without delay.

The safe side

As the world evolves, the digital landscape evolves as well, bringing new opportunities—and new risks. Scammers are becoming more sophisticated, exploiting vulnerabilities to their advantage. In our special feature series, we delve into the latest cybercrime trends and provide practical tips to help you stay informed, secure, and vigilant online.