

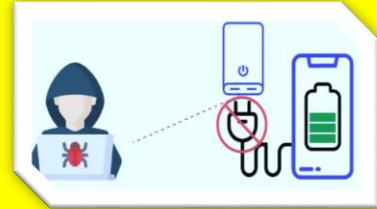
Where service is a way of life

JUICE JACKING ATTACK

CYBER JAAGROOKTA DIWAS - 06.03.2024

What is Juice Jacking ?

Juice jacking enables an intruder to copy sensitive data from a mobile device, such as passwords, files, contacts, texts and other personal financial data.



How Juice Jacking scam works?

Malicious Public Mobile Charging Stations:

Scammers set up Mobile charging stations that appear legitimate and convenient. These stations are rigged to collect data from connected devices.

Malware Injection: It involves malware injection directly into the user's device while it charges, giving scammers control over the victim's phone or tablet.



Safety Measures and Precautions

- ✓ Bring your own charger: Whenever possible, use your personal charger and plug it into an electrical outlet. Avoid using public charging stations, especially in high-risk locations.
- ✓ Portable power banks: Invest in a high-quality portable power bank to keep your devices charged on the go.
- ✓ USB data blockers: Consider using USB data blockers, which are small adapters that only allow charging functionality and block data transfer.
- ✓ Disable auto-connect: Disable the automatic connection feature for transfer of files on your device.
- ✓ Update software regularly: Keep your device's software, apps, and operating systems up to date.
- ✓ Use secure networks: Stick to reputable and secure Wi-Fi networks whenever possible.
- ✓ Avoid unlocking of Mobile: Refrain from using your phone while it's charging on a public station. As it may leave it vulnerable to unauthorized access.



Be Alert , Stay Safe , Cyber Safe !!!

