Juice jacking

March 1, 2024 • vajiramandravi.com

About Juice jacking

- The term “juice jacking” was first coined in 2011 by investigative journalist Brian Krebs.
- It is a form of cyberattack where a public USB charging port is tampered with and infected using hardware and software changes to steal data or install malware on devices connected to it.
- The attack is used by hackers to steal users’ passwords, credit card information, addresses, and other sensitive data stored on the targeted device.
- This type of attack has been a growing concern, with incidents reported in various public spaces such as airports, hotels, and shopping centres.
- RBI emphasised the importance of protecting personal and financial data while using mobile devices.
- How to prevent such attacks?
    - To protect themselves from juice jacking and other cyber threats, mobile phone users have to use their personal chargers and avoid connecting their devices to public USB ports.
    - Additionally, using a virtual private network (VPN) and ensuring that devices have the latest security updates installed can help mitigate the risk of cyberattacks.

Q1) What is the Chameleon Trojan?

It is a malware that has the ability to disable biometric authentication methods, including fingerprint and face unlock, to sneakily access sensitive information.

Source: Juice jacking: RBI issues warning against charging mobile phones using public ports

---