T2025_31 Be Cautious When Using Public Charging Stations (October 14th, 2025)

Public charging stations in airports, hospitals, and other public places may seem convenient, but they can also expose your device to serious cybersecurity risks. Cybercriminals can compromise USB ports in these charging hubs to perform "juice jacking," a technique that installs malware or secretly extracts data while your device charges. Once infected, your phone or tablet could transmit sensitive information, grant unauthorized access, or be remotely controlled without your knowledge. To stay safe, always use your own charger and plug it directly into a wall outlet instead of a public USB port. Carry a portable power bank for emergencies or use a "USB data blocker" that allows power flow but disables data transfer. Keep your device's operating system and security software updated and never grant trust permission when connecting to unfamiliar ports.

References

- Federal Communications Commission. (2023, April 11). Juice jacking: Tips to avoid it. Federal Communications Commission. Retrieved October 13, 2025, from https://www.fcc.gov/juice-jacking-tips-to-avoid-it

- Malwarebytes. (2025, June 5). Juice jacking warnings are back, with a new twist. Malwarebytes Labs. Retrieved October 13, 2025, from https://www.malwarebytes.com/blog/news/2025/06/juice-jacking-warnings-are-back-with-a-new-twist