Cybercrime Prevention Flyer

CPF 0011-2022-CID361-9H 30 March 2022

Juice Jacking

Be cautious where you charge your electronic device the next time it is dead when traveling. Public charging stations at airports, hotels, and restaurants are a target for cybercriminals to juice jack and collect information or install malware to further criminal activity.

What is Juice Jacking?

Juice jacking is a cyber-attack in which a compromised Universal Serial Bus (USB) charging station transfers malware to or steals personal information from the connected device. Juice jacking, also known as port jacking, is not limited to cell phones but any device capable of being charged via USB plug.

As you may or may not know, USB plugs are designed for two way transferring. When a USB plug is connected to an electronic device and a charging station, there is a trusted established relationship. The connected device is receiving a charge while the charging station has access to the entire database, including sensitive data, of the device. Unless the charging station was compromised, charging stations are not concerned with what is on a person's device.

Are You a Victim?

Often times in a juice jacking attack, the victim is unaware of the attack. But there are some telltale signs your device was juice jacked. The electronic device may:

- Consume more battery life than usual.
- Operate at a slower speed.
- Take longer to load.
- Crash frequently due to abnormal data usage.

Security and Protection

On many new devices, the automatic two way transfer of data is often disabled. If you really need to charge your device, proceed with caution and take some necessary precautions before plugging in.

- Avoid using public USB charging stations.
- Carry a portable charger or battery pack.
- Use electrical outlets with your own charging cable and wall plug in.

Report a crime to U.S. Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"Do What Has To Be Done"

- Bring a charge only USB adaptor.
- Keep your software updated. Software updates are likely to have security hole resolutions and bug fixes. For example, many updated cellular phones will now ask permission before data is transferred when you plug into an unknown station or device.
- Decline data transfer requests.
- Add two-factor authentication or biometric log-ins.

Additional Resources

Juice Jacking Foundation

What is juice jacking? Think twice before using public USB ports

'Juice Jacking': The Dangers of Public USB Charging Stations

Press Statement: NCC-CSIRT Identifies Two Cyber Vulnerabilities

The Cyber Crime of Juice Jacking in Developing Economies: Susceptibilities, Consequences and Control Measures

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF