FACT SHEET

U.S. Army Cyber Command

www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

THE FACTS: "JUICE JACKING"

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, a 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.

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

How do I know if I'm a victim of juice jacking?

Victims are often unaware that they have been "juice jacked", but there are some telltale signs that a device may be compromised. The device may:

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

How can I protect myself?

On many new devices, automatic two-way transfer of data is disabled. But if you really need to charge a device on the go, take some precautions:

-- Avoid using public USB charging stations
-- Decline data transfer request
-- Use two-factor authentication or biometric log-ins when available
-- Carry a portable charger or battery pack
-- Use electrical outlets with your own charging cable and wall plug-in charger

ABOUT US: U.S. Army Cyber Command integrates and conducts cyberspace operations, electromagnetic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information dimension, while denying the same to our adversaries.

As of 23 March 2022

-- Use a charge-only USB adaptor that allows your devices to be charged but does not transfer data

-- Keep your software updated. Software updates are likely to have current security protection, patches and bug fixes. For example, many updated cellular phones now ask permission before allowing data to be transferred when they are plugged into an unknown station or device.

The bottom line: Be cautious where you charge your electronic device. Public charging stations at airports, hotels and restaurants are a prime target for cybercriminals to juice jack and collect your information or install malware to further criminal activity.

FOLLOW ARCYBER ON (Click the images to visit sites):

ABOUT US: U.S. Army Cyber Command integrates and conducts cyberspace operations, electromagnetic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information dimension, while denying the same to our adversaries.

As of 23 March 2022