Lookout

Mobile Threat of the Month

July 2025

ChoiceJacking: The Evolution of USB-Based Mobile Attacks

What is ChoiceJacking?

ChoiceJacking is an advanced attack that builds on the concept of JuiceJacking (malicious USB charging cables). While modern phones have security features to stop unauthorised data transfers when you plug them in, ChoiceJacking gets around these by tricking your phone into thinking you've given permission. It simulates the physical touch input to accept data connection prompts, bypassing Apple and Google's built-in safeguards.

The effectiveness of ChoiceJacking attacks largely stems from its exploitation of fundamental human behaviours and environmental factors. Public charging stations are often perceived as convenient and essential "lifesavers" when a mobile device's battery is critically low. Attackers strategically leverage this sense of urgency and the inherent trust users place in public infrastructure.

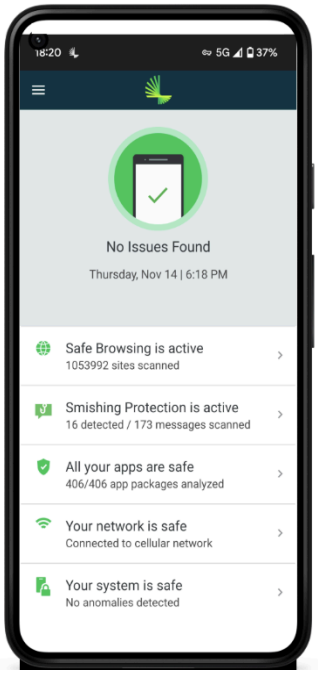
Potential Impact

This threat exploits the dual functionality of USB ports, which are designed for both power delivery and data transfer. When a device is connected, a "trusted relationship" can be established, potentially granting the charging station access to the device's database. The resulting impact may include:

Data exfiltration—the unauthorised theft of sensitive information such as contacts, emails, passwords, MFA tokens or sensitive documents accessible from mobile devices.

Malware installation - which can introduce adware, ransomware, Trojans, or spyware. Malware can monitor activities, steal additional data over time, or even lock users out of their devices. The malware can then exploit system vulnerabilities to gain "root" or "superuser" access, giving attackers full control over the device.

Lookout Mobile Security



Educating employees and promoting proactive vigilance is an important first step to safeguard mobile devices from ChoiceJacking attacks; however, it is not always possible for remote employees to use personal wall chargers, cables, or carry a portable power bank.

Lookout Mobile Security provides security coverage from these attacks through:

- Enforcement of regular mobile operating systems and application updates to ensure that exploitable vulnerabilities are patched.
- Rooted device detection to gain immediate visibility if a mobile device has been compromised.
- Mobile malware detection with simple end-user remediation guidance.
- Risk-based access control ensures that mobile devices at risk are prevented from accessing company apps or data.

Lookout provides leading mobile endpoint detection and response for iOS, Android and Chrome OS devices.