Linked Devices, Technique T1676 - Mobile

Archived: 2026-04-05 13:30:42 UTC

Adversaries may abuse the "linked devices" feature on messaging applications, such as Signal and WhatsApp, to register the user’s account to an adversary-controlled device. By abusing the "linked devices" feature, adversaries may achieve and maintain persistence through the user’s account, may collect information, such as the user’s messages and contacts list, and may send future messages from the linked device.

Signal is a messaging application that uses the open-source Signal Protocol to encrypt messages and calls; similarly, WhatsApp is a messaging application that has end-to-end encryption and other security measures to protect messages and calls. Both applications have a "linked devices" feature that allows users to access their Signal and/or WhatsApp accounts from different devices, such as a Windows or Mac desktop, an iPad or an Android tablet.[1][2]

Adversaries may use Phishing techniques to trick the user into scanning a quick-response (QR) code, which is used to link the user’s Signal and/or WhatsApp account to an adversary-controlled device. For example, adversaries may masquerade QR codes as group invites, security alerts or as legitimate instructions for pairing linked devices.
Upon scanning the QR code in Signal, users may click on the "Transfer Message History" option to sync the linked devices, which may allow adversaries to collect more information about the user. Upon scanning the QR code in WhatsApp, the user’s device will automatically send an end-to-end encrypted copy of recent message history to the adversary-controlled device.
