Android

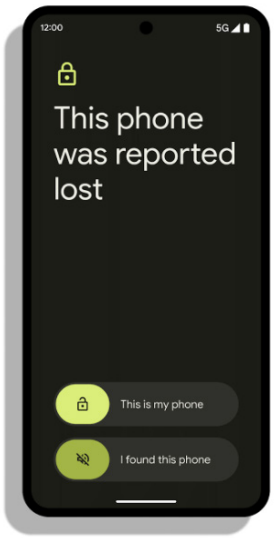
Recover devices and protect corporate data with lost mode

To help employees work while on the go, many organizations provide employees with company-owned devices. While great for productivity, this can make it difficult to protect corporate data if a device is lost or stolen. IT teams need to take steps to mitigate these risks.

The average cost of a data breach in 2022 is up 2.6% from 2021, and remote work is a key liability for enterprises.
(Source: 2022 IBM Cost of Data Breach Report)

$200k is the average cost of a data breach.
(Source: National Cyber Security Association, 2019)

83% of organizations experience more than one data breach in their lifetime.
(Source: Gartner, 2023)



Lost mode on Android Management API allows IT admins to disable access to lost or stolen company-owned devices, and report locations to IT on a recurring basis. When activated, the device remains locked and access to data is restricted. IT teams can help locate lost devices with the Android Management API.

Help protect corporate data

Once lost mode is activated, access beyond the lock screen is prohibited, ensuring all corporate data remains protected and accessible by only authorized users and IT admins.

Remotely manage lost devices

IT admins can remotely wipe devices, receive location data, push custom messages to help retrieve devices, and more - all while preserving user location data from unauthorized access.

Protect employee privacy

Once activated, a lost device rings for a short period before sharing location data. This gives employees a chance to exit lost mode and prevent IT from accidentally or intentionally misusing location data.

Learn more at www.android.com/enterprise/security