

Privacy & Security

Help keep your data safe, private and secure with Pixel

Pixel puts business security first with built-in protections designed to safeguard sensitive data, detect threats, and keep work and personal life separate. With features like the Titan M2™ chip, regular security updates, and phishing and theft protection, Pixel helps keep your team protected right out of the box.^{ΔΔ}

Next-level threat protection

Help keep business data safe and secure with:

- **Multiple layers of security**, including the Tensor security core and the certified Titan M2™ chip, to help protect sensitive business data.[‡]
- **Seven years of security updates** to help protect against evolving threats.^Δ
- **Passkeys** for password-free, phishing-resistant sign-ins using biometrics.
- **Android Theft Protection**, a suite of proactive features including Theft Detection Lock, Offline Device Lock and Remote Lock.^Δ
- **Safe Browsing** to warn users about phishing, malware and deceptive sites.^Δ
- **SecurityLog** to help IT teams review logs, identify vulnerabilities and ensure compliance with the latest audit logging requirements.
- **Call Screen** to help avoid spam by screening unknown callers using Google AI.[⊖]

Robust mobile security

Pixel is consistently recognised for its robust security features, earning top marks in independent security analyses.[⊖]

With dedicated hardware security and a multi-layered approach, Pixel is designed to protect against a wide range of mobile threats.

- Pixel provides **strong overall security** with **multiple layers of defence** designed to block malware and spyware, and to be resilient to advanced threats like zero-click exploits.
- Robust **lost-device protections**, including the ability to locate, lock or erase a lost phone remotely with **Find My Device**, and locate devices even when they are offline via the Find My Device network.^Δ
- Timely **security updates** from Google, provided for seven years, to help guard against evolving threats.^Δ
- **Dedicated hardware security**, with the Tensor security core and Titan M2™ chip providing protection for sensitive data.

Security and privacy settings

All your key security and privacy settings, in one place, including:

- **Google Play Protect** regularly checks your apps and devices for harmful behaviour. You'll be notified of any security risks found.
- **Find My Device** helps locate your phone if it gets lost or stolen.⁴
- **Security update** lets you see whether your system is up to date.
- **Screen lock** lets you lock your phone with a PIN, pattern or password.
- **Face & fingerprint unlock** lets you unlock your phone and authorise purchases using your fingerprint or face.
- **Google security checkup** lets you review signed-in devices, saved passwords, recent activity and more related to your Google Account.
- **Google Play system update** lets you check for updates to your Android operating system.



Separate business from personal

Keep work apps and data separate from personal life with:

- **Work Profile** encrypts and separates business apps and data from personal use, giving IT teams control over work apps while preserving employee privacy.³
- **Private Space** lets users create a separate, locked folder for sensitive apps and content within their personal profile, supporting dual use without compromising privacy.⁵

Personal Safety

Get help during emergencies with:

- **Satellite SOS** lets you contact emergency services and share your location when you're outside of mobile network coverage.⁸
- **Car Crash Detection** automatically detects car crashes and can connect you to emergency services, even if you're unresponsive.⁹
- **Crisis Alerts** provide timely updates about local emergencies or disasters, helping you stay informed and prepared.⁷

Security that's certified

Security features and services from Android are backed by independent analysts and researchers. That means industry-approved and regulation-certified protections for your business.

These certifications and standards help demonstrate that commitment:

- **GDPR compliance**, supporting secure data handling and user privacy in accordance with EU regulations.
- **ISO 27001 certification**, confirming that Android Enterprise information security practices meet ISO's strict industry standards for managing sensitive company and customer data.
- **FIDO2 certification**, ensuring that devices running Android 7+ meet FIDO Alliance standards for secure, passwordless authentication.
- **NIAP compliance**, confirming that Android supports the Common Criteria Protection Profile, with certification built into AOSP and AMAPI.
- **SOC 2 and 3 reports**, verifying that Android Management API, zero-touch enrolment and managed Google Play are SOC-audited for controls around security, availability, confidentiality and privacy.

Top security needs for business

When it comes to mobile security, businesses know what they need. From phishing protection to secure access controls, these are the features that matter most to IT teams and end-users alike.

Business-ready mobile security features include:

Anti-phishing protection

- **Safe Browsing** helps protect users from phishing, malware and deceptive sites.¹⁴
- **Call Screen** identifies unknown callers and shows their intent to help avoid spam and scams.¹⁵

Hardware security

- **Multiple layers of security** help protect user privacy and make Pixel devices resilient to attacks.¹

Anti-malware protection

- **Google Play Protect** scans apps and devices to block harmful behaviour.
- **Titan M2™ security chip** works with the Tensor security core to safeguard data like passwords and PINs.

Files and photos protection

- **Work Profile** separates work and personal data with dedicated controls.²
- **Private Space** creates a locked folder in the personal profile for sensitive apps and data.⁵

Identity protection

- **Screen lock** secures access with a PIN, pattern or password.
- **Face & fingerprint unlock** provides quick, secure access to apps and data.
- **Passkeys** enable phishing-resistant, password-free sign-ins using biometrics or a PIN.

Lost-device protection

- **Find My Device** lets users locate, lock or erase a lost phone remotely.¹¹
- **Android Theft Protection** includes Theft Detection Lock, Offline Device Lock and Remote Lock via android.com/lock.¹¹



Disclaimer

- ¹ Common Criteria certification for hardware and cryptographic library (CC PP0084 EAL4+, AVA_VAN.5 and ALC_DVS.2). See g.co/pixel/certifications for details.
- ² Pixel updates for seven years from when the device first became available on the Google Store in the US. See g.co/pixel/certifications for details.
- ³ Theft Detection Lock, Offline Device Lock and Remote Lock require Android 10+ and an Internet connection. Android Go devices are not supported. Support may vary based on your device model. The user must be using the phone while it is unlocked.
- ⁴ See safebrowsing.google.com to learn more.
- ⁵ Available in select countries and languages. See g.co/pixel/callassist for details.
- ⁶ Based on third-party global research firm evaluating Pixel 6 through Pixel 9. Evaluations considered features that may not be available in all countries. See [Mobile Device Security 2021](#), [Mobile Device Security 2022](#), [Mobile Device Security 2023](#), and [Mobile Device Security 2024](#) for more information.
- ⁷ Find My Device network requires location services and Bluetooth to be turned on. Requires mobile network service or Internet connection. Works on Android 9+ and in certain countries for age-eligible users.
- ⁸ Some features require Android Enterprise.
- ⁹ Private Space on COPE devices are subject to the same security requirements as the personal profile. Admins will be able to block the user from having a Private Space and remove an existing Private Space in COPE.

- ¹⁰ Restrictions apply. Setup required. Service included at no additional charge for the first two years after activation of devices. Available in the US. Connection and response times vary based on location, site conditions and other factors. See g.co/pixel/satellitesos for details.
- ¹¹ Car Crash Detection not available in all languages or countries. Car Crash Detection may not detect all accidents. High-impact activities may trigger calls to emergency services. This feature is dependent upon network connectivity and other factors, and may not be reliable for emergency communications or available in all areas. For country and language availability and more information see g.co/pixel/carcrashdetection.
- ¹² Crisis Alerts available in Personal Safety app. Personal Safety app features are dependent upon network connectivity and other factors, and may not be reliable for emergency communications or available in all areas. For more information, see g.co/pixel/personalsafety.