

Protected Computing

Protected Computing trasforma le modalità, i tempi e i luoghi di elaborazione dei dati per **garantire tecnicamente la privacy e la sicurezza dei tuoi dati.**

L'elaborazione dei dati non avviene più solo su un computer o su un telefono, ma anche a casa, in auto, al polso e nel cloud. Creare esperienze personalizzate e utili proteggendo allo stesso tempo la privacy degli utenti in un ambiente sempre più complesso, presenta sfide tecniche nuove.

Per questo motivo abbiamo progettato Protected Computing, una soluzione tecnica nuova per mantenere i dati personali privati e al sicuro.

Oggi Protected Computing:

- ✓ Permette ad Android di suggerire la prossima parola nei tuoi messaggi, ma le conversazioni rimangono del tutto private
- ✓ Aiuta Pixel a sapere quando tenere acceso lo schermo, eliminando continuamente i segnali ambientali man mano che vengono elaborati
- ✓ Permette a Chrome di avvisarti in caso di password compromesse, senza conoscerne nemmeno una

 **Più al sicuro con Google**

I principi di Protected Computing

Minimizzare l'impronta dei dati

Riduciamo la quantità di dati personali identificabili, raccogliendone meno e cancellandone di più, sfruttando tecniche come l'edge processing e l'effimero. Se i dati non esistono, non possono essere violati.

Anonimizzazione dei dati

Utilizziamo una serie di tecniche di anonimizzazione, come l'offuscamento, la randomizzazione dei segnali identificabili e l'aggiunta di rumore statistico per dissociare la tua identità dai tuoi dati, in modo che non siano più collegati a te.

Limitare l'accesso ai dati

Limitiamo l'accesso tramite tecnologie come la crittografia end-to-end e le enclavi sicure. In questo modo rendiamo tecnicamente impossibile per chiunque, incluso Google, l'accesso ai tuoi dati sensibili.



Scopri di più su come Google protegge online più persone di chiunque altro su safety.google