

INSTALLA SIGNAL PRIVATE MESSENGER

Signal permette di usare la crittografia end-to-end per rendere sicuri i nostri messaggi e chiamate. Installala!



USA CRITTOGRAFIA END-TO-END SU ZOOM

Vai su **Profilo** —> **Impostazioni** —> **Usa crittografia end-to-end** —> **Attiva**. Così puoi proteggere le tue chiamate anche dallo staff di zoom. Però, Breakout Rooms e Messaggi Diretti alle persone del meeting non funzionano se è attiva questa funzione.

USA WIRE SE VUOI MEETING CIFRATI CON END-TO-END

Prova Wire Personal per videochiamate fino a 12 persone o chiamate vocali in 25

<https://wire.com/en/products/personal-secure-messenger/>

IN STRADA NON USARE LO SBLOCCO CON VISO O IMPRONTA

Usa invece un **codice PIN**. Il più sicuro è un PIN di 10 cifre o di più. Ne usi uno di 4 o 6? Ripetilo finché non arrivi a 8-9 e poi aggiungi un'altra cifra. Boom! Ora hai un codice PIN di 10 cifre.

PROTEGGI LA PRIVACY DELLA TUA POSIZIONE

Su <https://maps.google.com/locationhistory> cancella i viaggi o usa il **cestino** per buttare tutto. Su <https://myactivity.google.com> elimina le attività private oppure **Elimina Sempre**.

IL TUO TELEFONO È SICURO SOLO QUANDO È SPENTO



PROTEGGI LA TUA EMAIL & I SOCIAL

Attiva l'**autenticazione a 2 fattori (2FA)** per i tuoi account. Aggiunge un livello di sicurezza ulteriore rispetto alla sola password. Scopri come fare per ogni piattaforma qui <https://twofactorauth.org>.

INSTALLA BRIDGEFY

Ti permette di inviare messaggi cifrati end-to-end a persone che ti sono fisicamente vicine quando la rete non funziona. Scaricala ora!

PROTEGGI VISO/TATTOO DAL RICONOSCIMENTO

Prima di condividere foto, copri visi, tattoo, e vestiti con emoji e sticker. Puoi usare anche app del tuo telefono per farlo. Ricorda di scattare uno screenshot alla foto e condividerlo per aumentare la tua sicurezza e protezione.