Free privacy tools for Android phones and tablets

TextSecure Private Text and Chat

This is a replacement for the standard SMS messaging app and provides support for end-to-end encryption of text messages.

The TextSecure application will ask a keyserver for the public key for each recipient. If found then the text message will be encrypted; if not then it will be sent plain text like a standard SMS.

Messages are sent over wifi or mobile data connection so are charged as data instead of SMS.

All messages are encrypted locally so are secure even if your phone is lost.

Install Text Secure from the Google Play store.

More info: https://whispersystems.org

Redphone Private Calls

End-to-end encryption for your mobile telephone calls.

Use your default system dialer and contacts apps to make calls as you normally would.

Redphone will offer encrypted call as an option if the other person has Redphone (Android) or Signal (iPhone) installed.

Uses your normal phone number as your identifier to make and receive calls

Install Redphone from the Google Play store

More info: https://whispersystems.org

OpenKeyChain (GPG Key Management)

Key management app – required for setting up email encryption with the K9 email client

1. Install OpenKeyChain from the Google Play Store
2. If you already have your private key stored on your SD card then Select 'Import from file'
3. Click 'Open' and then complete action with a file manager app to browse the disk and locate your keyring files. Public and private keys are normally stored in separate keyrings so you will need to do this once for each keyring.
4. If you don't already have a private key then use the 'Create Key' facility to create a new set of subkeys. Choose a passphrase that you will be able to remember and use on your phone (You will need to enter it each time you encrypt or decrypt your email)

Subkeys: OpenKeyChain creates a master key-pair which is the key that is used for signing to build up the web-of trust. Sub-key pairs are then generated for encryption of email. This allows you to revoke a sub-key without losing your web of trust.

OI (Open Intents) File Manager

Free, Open Source file manager for Android that doesn't request network access permissions or install adverts.

A useful utility for browsing your device storage and SD card to load your encryption keys into OpenKeyChain

Install OI File Manager from the Google Play store

K-9 Send and receive encrypted email

K-9 is an email client for Android with support for PGP public/private key encryption.

Uses the Android Privacy Guard (APG) or OpenKeyChain apps to manage keys and perform encryption/decryption. (OpenKeyChain is the most mature of the two PGP provider applications)

1. Install OpenKeyChain from the Google Play store and install your keys or create new ones (Instructions overleaf)
2. Install K9 from the Google Play store and set it up to connect to your existing email account
3. View your inbox and select [Menu]->'Settings'->'Account Settings'->'Cryptography'->'Open PGP Provider' and select OpenKeyChain.

Every time you send an email you will see checkboxes for 'sign email' and 'encrypt email'. If you tick either then you will be prompted to enter your passphrase to unlock you private key to sign or encrypt the email.

If you receive an encrypted email then you will be prompted to enter your passphrase to decrypt the email.

ChatSecure

Encrypted chat client for iPhone and Android that supports OTR (off the record) encryption.

Install ChatSecure from the Google Play store

More info at https://chatsecure.org

X-Privacy – 'The ultimate yet easy to use privacy manager'

Fine control over what privileges are granted to each Android application.

Requires root access to install.

Revoke privileges that application require on install (e.g. deny the Facebook app access to your contacts).

Feeds fake data to applications when privileges are revoked.

Information about rooting your device is available at http://www.androidcentral.com/root – Each device is different.