zero messenger

The White Paper

Welcome

Zero Messenger is a secure live messaging app for iOS and Android that requires absolutely zero user information and data, and leaves complete control in the users' hands.

Zero Messenger uses the latest multi-ratchet encryption technologies and proprietary methods to protect your data from inception, through transit, to delivery, but never retains any of your messages, contacts' or data on its servers or third party servers.

Zero's three main design philosophies are:
Zero Registration, Zero Collection, and Zero Trace. Zero does not require users to sign up. Your messages live on your device and nowhere else, and you can remove any message(s) or complete contacts and their history from your device and the contact's devices at any time.

This white paper is intended to provide you with some understanding of how we accomplish what we do as well as further details our design decisions from a privacy and security perspective.

Contents

Zero Registration

We have meticulously designed Zero to protect users, their identity, and their individual communications when using Zero Messenger.

From the moment you download and open Zero, you are protected and your communications are secure. While there is an initial, one time registration when you install Zero, you DO NOT have to provide any phone number, email, username or any other identifying information. Once you download the Zero app, all you need to do to start your secure conversations is add your first contact.

Zero Collection

Zero Messenger requires that both users (you and the person you are communicating with) be online in order to exchange messages. This allows Zero users to pass data from one device to another while never having that data held on any servers. Zero relies on its proprietary network solely to transmit messages back and forth between Zero users and therefore, never stores your messages. Your communications are securely stored solely on your device and nowhere else.

Zero is not a cloud based application that distributes your messages or data to multiple devices. Therefore, in order to use Zero on multiple devices, you must download and install Zero on each separate device that you plan to use it on because each device is treated as a separate unique user.

Zero does not collect any metadata from users and everything a user does is on their device only. Given that both users must be online in order to communicate, Zero uses a single push notification to notify a user to come online and securely communicate.

Zero Trace

Zero does not collect any data of any kind from our users, therefore we do not know when you are using Zero or who you are using it with.

Zero does not leave behind any trace of your communications. Your communications are completely private and secure from inception, through transit, to delivery, and Zero never retains any of your messages or communications, contacts or data on its servers or any third party servers.

Individual messages, chats, and the entire app can be wiped using the “Burn” functionality which removes your messages from both your device and your contacts’ device.

Adding Contacts

Adding contacts is a simple process that is done solely by each Zero user. Users must individually enter each contact that they would like to communicate with using Zero Messenger. The reason for this is that Zero never scans the contacts on your device. Zero has no access to your contact information and makes no use of your private contact list in any way what-so-ever.

Messages

Zero is a live messenger that does not hold onto your messages or media at any given point. Therefore, we require both parties to be present in the app to maintain their connection to transmit their data back and forth.

You have the ability to draft messages in a chat but until the specific user comes online, you cannot send the messages.

A fully secure communication channel is established between two users once they are both online. All messages are end-to-end encrypted and sent over the secure channel that Zero creates for you, so that no other parties, including us can decrypt your message.

As a part of our security, each individual message is separately encrypted and protected using the latest multi-ratchet encryption technologies and proprietary methods so that even in the extremely unlikely event of one message being compromised, all other messages before and after stay completely secure. To help create future-secrecy, Zero uses a proprietary algorithm, so that even if the user's device is comprised in the future, all previous and subsequent messages remain fully protected on your device.

Voice Calls (VOIP)

All calls on Zero Messenger are routed through and facilitated by Zero Messenger so no two users can or will be linked together.

Zero Messenger uses Traversal Using Relays around NAT (TURN) servers to relay and facilitate Voice over IP (VoIP). Calls made using Zero use design philosophy making it so users do not reveal their IP Addresses to one another when communicating.

Burn

To Burn on Zero Messenger means you are removing all copies of that contact, message or entire chat from both yours and the recipients device. As those are the only two points that ever have a copy of your message.

Burn Contacts
Once a contact has added you and a mutual connection has been made, you still remain in control of what happens to your communications with each of your Zero contacts. You can Burn a contact at any time. This will remove them from your device and remove you from their device along with any current communications you may have with this contact. From this point forward, you two can no longer contact each other unless you add one another again.

Burn Messages
All messages on Zero get automatically burned after 24 hours. If you choose to, you have the ability to also burn individual messages and entire chats at any given point. Burning a message or chat will remove all copies of that specific message or entire chat from both you and your contact's devices, leaving no trace of the message or messages.

Burn App
All users have the ability to execute a Burn option which will purge their entire app and remove all messages and contacts from both the user's device and all of their contacts devices as well, leaving no trace that any communications ever took place.

Encryption

All communications between users are secured using the latest multi-ratchet encryption technologies and proprietary methods. The Zero network is responsible for relaying messages to the desired recipient, and is not able to decrypt those messages. Voice calls use the latest encryption technologies and protocols.

zero messenger

Made in the Imagination Room