What Cryptocat Doesn't Do

Cryptocat is a work in progress that aims to offer strongly encrypted, private Instant Messaging, so it's important to note what Cryptocat does not protect you against:

Cryptocat does not anonymize you: While your communications are encrypted, your identity can still be traced since Cryptocat does not mask your IP address. For anonymization, we highly recommend using Tor.

Cryptocat does not protect against key loggers: Your messages are encrypted as they go through the wire, but that doesn't mean that your keyboard is necessarily safe. Cryptocat does not protect against hardware or software key loggers which might be snooping on your keyboard strokes and sending them to an undesired third party.

Cryptocat does not protect against untrustworthy people: Parties you're conversing with may still leak your messages without your knowledge. Cryptocat aims to make sure that only the parties you're talking to get your messages, but that doesn't mean these parties are necessarily trustworthy.

www.crypto.cat

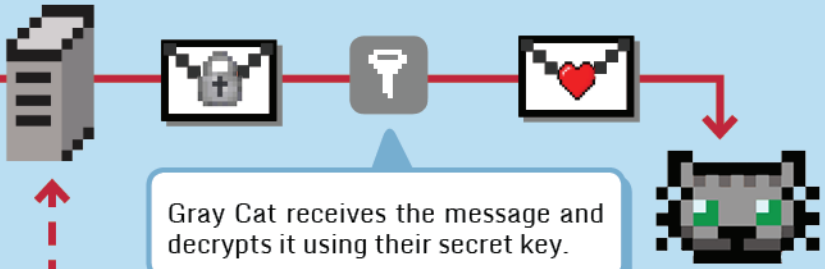
CRYPTOCAT

ENCRYPTED CHAT MINI GUIDE

www.crypto.cat

HOW CRYPTOCAT WORKS

When you write a message using Cryptocat, each message is **encrypted on your own computer before being sent**. Only the intended recipient(s) have the key to decrypt and read the message, preventing the it from being revealed to a third party.



Gray Cat receives the message and decrypts it using their secret key.

Orange Cat encrypts their chat message using their **secret key**. They set the message so that **only Gray Cat can decrypt it** using Gray Cat's secret key. When the message passes through the server, it is already encrypted--if it's intercepted, Spy Dog can't read it.

SPYDOG THWARTED!!

Verifying Identities

A fingerprint is a user's public identifier (key) in Cryptocat. Users have an OTR key (for private conversations) and a group conversation fingerprint. Confirming someone's key using a third channel (voice, DM) is one way to verify that the person you're talking to is who you think it is. **Every time you use Cryptocat, you get a new fingerprint set**. So you need to verify that identity every time.

WHAT IT IS

Cryptocat is a free browser plugin that provides an **encrypted Instant Messaging environment** for your conversations. Different than Facebook Chat or Skype, Cryptocat is a secure and encrypted message environment to protect your privacy.

When you use most chat services, the messages you send go from you to a server to the person you're chatting with. Throughout this process, the messages remain **unencrypted.** This means that someone else who isn't in your conversation can potentially **intercept** it.

Conversation Name can be whatever you want. Everyone you want to chat with must use the same conversation name to be in the same chat. Pick a conversation name that's hard to guess (i.e., not "test" or "chat") if you don't want people barging in randomly.

Nickname is your name in the conversation.

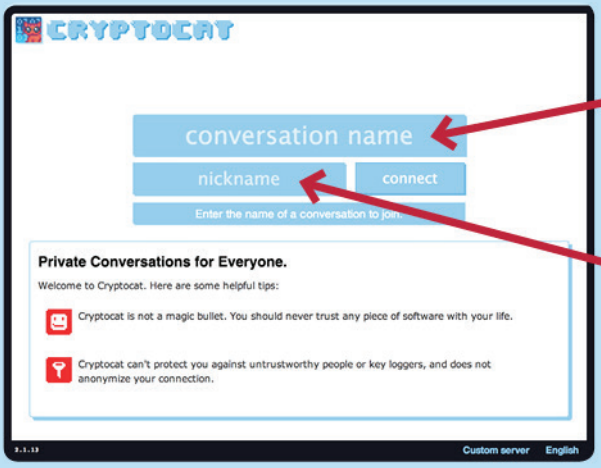
Click on a user's name to start a private conversation with them. Click the white arrow to view their key information, send files, or block the user.

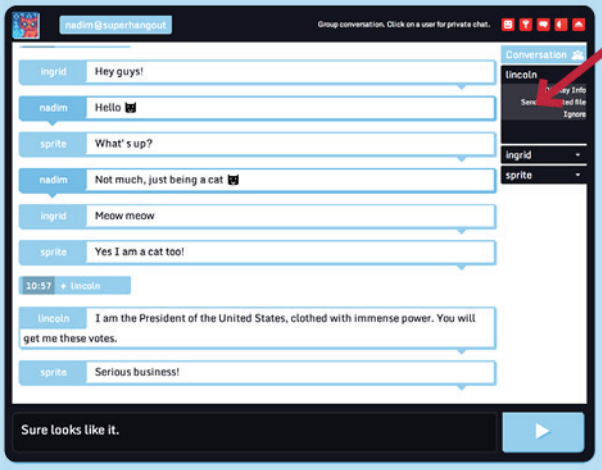
Change your status to away or available.

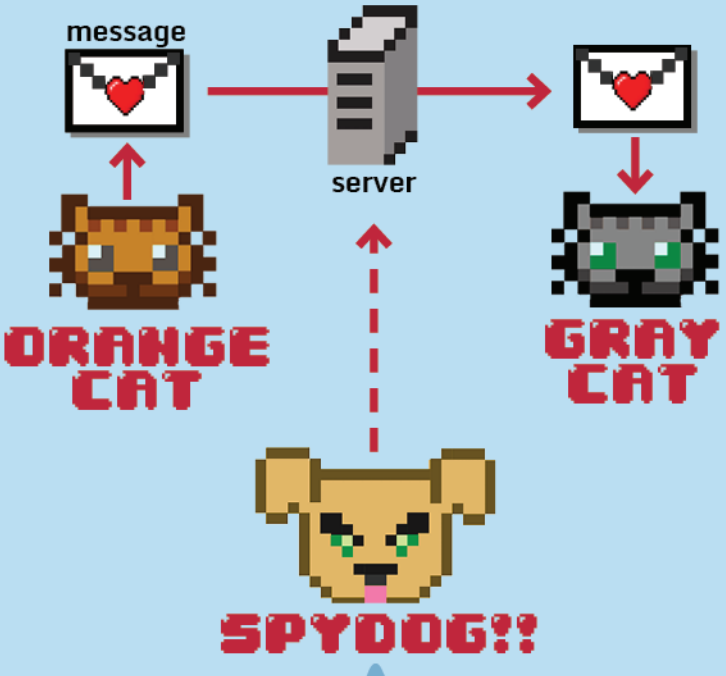
View your fingerprint for the conversation.

Turn the sound on and off.

Leave the conversation!







HOW NORMAL CHAT WORKS