🤫 Hush Line FAQ

🙈 How anonymous is Hush Line?

Hush Line requires no personally identifying information (PII) for tip line owners to use the service, including an email address. We scrub IP addresses and country codes from access logs and don't timestamp messages or relate account data in any way.

We offer an Onion service for users with advanced privacy needs, which can be accessed using the Tor Browser, making connections and activity completely anonymous.

Message submitters are not required to create an account and may also choose to use our Onion service to access the app.

🔒 Is Hush Line end-to-end encrypted?

Hush Line uses OpenPGP.js for client-side encryption, giving users who add their public PGP key end-to-end encryption for their messages. Users who disable JavaScript use server-side encryption.

Adding your PGP key enables only you to have technical access to your decrypted messages. Neither the server administrators nor an attacker with access to the server can learn their contents. Setting up PGP is easy using our getting started guide.

Hush Line uses TLS encryption for data in transit, message data is stored encrypted at rest on our database, and server access is limited to relevant members of the technical staff.

Learn more at hushline.app