Proton mail

ProtonMail is unique because it has PGP fully integrated such that you do not need to take any additional steps to benefit from PGP encryption. This means that with ProtonMail, anybody can use PGP, regardless of their technical knowledge.

# Encryption

Proton mail combine 2 types of cryptography which are asymmetric and symmetric to offer end-to-end encryption. When creat protonmail, user will have a pair of pub and pri keys:

* The public key is used to encrypt email and data
* The private key used to decrypt user’s data which is symmetrically encrypted with the user's mailbox password.

Encryption is mad e in the user’s browser. When register new account, users have to provide a login password( authentication purpose) also the application offer a two-password mode which uses user password and mailbox password(used to encrypt user’s emails, contacts and information and private key) for logining in. The decryption takes place at client-side. The public and private key store on protonmail servers( both encrypted on servers) to avoid protonmail developers from resetting user mailbox passwords. This system absolves ProtonMail from:

* Storing either the unencrypted data or the mailbox password.
* Divulging the contents of past emails but not future emails.
* Decrypting the mailbox if requested or compelled by a court order.

# Email sending

An email sent from one ProtonMail account to another is automatically encrypted with the public key of the recipient. Once encrypted, only the private key of the recipient can decrypt the email. When the recipient logs in, their mailbox password decrypts their private key and unlocks their inbox.

Emails sent from ProtonMail to non-ProtonMail email addresses may optionally be sent in plain text or with end-to-end encryption. With encryption, the email is encrypted with AES under a user-supplied password. The recipient receives a link to the ProtonMail website on which they can enter the password and read the decrypted email. ProtonMail assumes that the sender and the recipient have exchanged this password through a backchannel Such emails can be set to self-destruct after a period of time

<https://protonmail.com/support/knowledge-base/how-to-use-pgp/> share protonmail nonprotonmal

<https://medium.com/swlh/secure-your-emails-in-5-minutes-using-pgp-5435ba007b3b> setup gpgmail

https://lifehacker.com/how-to-secure-your-email-now-that-pgp-is-compromised-1826008338