**Email Encryption**

**ON THIS PAGE**

* [**WINDOWS**](https://www.openpgp.org/software/#windows)
* [**MAC OS**](https://www.openpgp.org/software/#mac-os)
* [**ANDROID**](https://www.openpgp.org/software/#android)
* [**IOS**](https://www.openpgp.org/software/#ios)
* [**LINUX**](https://www.openpgp.org/software/#linux)
* [**BROWSER PLUGINS**](https://www.openpgp.org/software/#browser-plugins)
* [**WEBMAIL PROVIDER WITH BROWSER PLUGINS**](https://www.openpgp.org/software/#webmail-provider-with-browser-plugins)
* [**WEBMAIL PROVIDER WITH IN-BROWSER CRYPTOGRAPHY**](https://www.openpgp.org/software/#webmail-provider-with-in-browser-cryptography)
* [**PROJECT MISSING?**](https://www.openpgp.org/software/#project-missing)

All email applications on this page support the OpenPGP standard either directly or with additional software. The authors of this webpage are not actively participating in the development of each of these third-party apps. No security audits have been done by us and, thus, we cannot provide any security guarantees.

**Windows**

* [Claws Mail](https://www.openpgp.org/software/claws/)
* [eM Client](https://www.openpgp.org/software/emclient/)
* [EverDesk](https://www.openpgp.org/software/everdesk/)
* [The Bat!](https://www.openpgp.org/software/thebat/)
* Outlook:
  + [gpg4o](https://www.openpgp.org/software/gpg4o/)
  + [Gpg4win](https://www.openpgp.org/software/gpg4win/)
  + [p≡p](https://www.openpgp.org/software/pep/)
* [Postbox](https://www.openpgp.org/software/postbox/) using [Enigmail](https://www.openpgp.org/software/enigmail/)
* Thunderbird:
  + [Autocrypt](https://www.openpgp.org/software/autocrypt/)
  + [Enigmail](https://www.openpgp.org/software/enigmail/)

**Mac OS**

* [Apple Mail: GPGTools](https://www.openpgp.org/software/gpgtools/)
* [Canary Mail](https://www.openpgp.org/software/canary-mail/)
* [Mutt](https://www.openpgp.org/software/mutt/)
* [Postbox](https://www.openpgp.org/software/postbox/) using [Enigmail](https://www.openpgp.org/software/enigmail/)
* Thunderbird:
  + [Autocrypt](https://www.openpgp.org/software/autocrypt/)
  + [Enigmail](https://www.openpgp.org/software/enigmail/)

**Android**

* [FairEmail](https://www.openpgp.org/software/fairemail/)
* [K-9 Mail: OpenKeychain](https://www.openpgp.org/software/openkeychain/)
* [p≡p](https://www.openpgp.org/software/pep/)
* [R2Mail2](https://www.openpgp.org/software/r2mail2/)

**iOS**

* [Canary Mail](https://www.openpgp.org/software/canary-mail/)
* [iPGMail](https://www.openpgp.org/software/ipgmail/)
* [Safe Easy Privacy](https://www.openpgp.org/software/safe/)

**Linux**

* [Claws Mail](https://www.openpgp.org/software/claws/)
* [Evolution: Seahorse](https://www.openpgp.org/software/seahorse/)
* [KMail: Kleopatra](https://www.openpgp.org/software/kleopatra/)
* [Mutt](https://www.openpgp.org/software/mutt/)
* Thunderbird:
  + [Autocrypt](https://www.openpgp.org/software/autocrypt/)
  + [Enigmail](https://www.openpgp.org/software/enigmail/)

**Browser Plugins**

* [Mailvelope](https://www.openpgp.org/software/mailvelope/)
* [FlowCrypt (Gmail)](https://flowcrypt.com/)
* [Psono](https://www.openpgp.org/software/psono/)

**Webmail Provider with Browser Plugins**

A lot of webmail providers support email encryption via the OpenPGP standard using [Mailvelope](https://www.openpgp.org/software/mailvelope/). The Mailvelope website provides a list of [supported webmail providers](https://www.mailvelope.com/en/faq#mailer_list).

Providers with help pages:

* [GMX](https://hilfe.gmx.net/sicherheit/pgp/mailvelope-installieren.html)
* [Posteo](https://posteo.de/hilfe/wie-installiere-ich-eine-ende-zu-ende-verschluesselung-pgp-im-browser)
* [WEB.DE](https://hilfe.web.de/sicherheit/pgp/index.html)

Pre-configured (authorized) providers:

* [Gmail](https://mail.google.com/)
* [mail.ru](https://mail.ru/)
* [Outlook.com](https://outlook.live.com/owa/)
* [volny.cz](https://volny.cz/)
* [Yahoo](https://login.yahoo.com/)
* [Zoho Mail](https://www.zoho.eu/mail/)

Other authorized providers with API support:

* [mailbox.org](https://mailbox.org/)
* [riseup.net](https://mail.riseup.net/)
* [Roundcube](https://roundcube.net/)

**Webmail Provider with In-Browser Cryptography**

In contrast to the previous section, the following webmail providers do not require the installation of additional browser plugins, instead OpenPGP is implemented in JavaScript provided directly by the website. While these are easier to set up and provide basic security guarantees with OpenPGP, [some people don’t consider these “end-to-end secure”](https://tonyarcieri.com/whats-wrong-with-webcrypto).

* [Hushmail](https://www.hushmail.com/) (limited OpenPGP support)
* [Mailfence](https://www.mailfence.com/)
* [postale.io](https://postale.io/)
* [ProtonMail](https://protonmail.com/)

**Project Missing?**

If a project is missing and you would like it included, please open a pull request at [github.com/OpenPGP/openpgp.org](https://github.com/OpenPGP/openpgp.org). Please note that we only include published, working software, which implements the standard. The software is ordered alphabetically within the sections.