REVIEW

USING TUTANOTA

Review: Using Tutanota.

Out of 20+ email providers we've tested. Basically it quickly came down to Tutanota vs Protonmail. We use both of them...

Disclaimer: We are not affiliated with these companies. This article is based entirely on our own research findings, and there is no affiliate marketing involved through the links provided below for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo rigorous testing:

- Real-time usage on actual projects.
- Evaluation by diverse team members situated across various countries.
- Testing on a range of devices and operating systems.
- Minimum testing duration of two weeks, averaging four weeks.
- Peer review by team members precedes submission to the app's publisher for the final assessment.

1. Our specifications sheet:

- End-to-end, zero-knowledge encryption (1),
- Tailored to our business domain (2),
- Efficient administration of users (3),
- Resilience against state-sponsored threats (4),
- Cost-effectiveness for a large user base (5),
- Multi-platform compatibility (6),
- Open-source nature (7),
- Emergency support provided by the service provider.

This criteria swiftly narrowed down our choices, leading to a comparison between Tutanota and ProtonMail. Notably, both declined NSA's request for a backdoor. While we utilize both, Tutanota, with its Premium package, supports our domain name. Key distinctions lie in pricing and storage capacity (8).

2. Shared features between Tutanota and Protonmail:

- Open source.
- End-to-end encryption with keys stored on the user's computer (9).
- Android and iOS apps.
- Web-based add-ons for desktops.
- Password-protected emails for external users (10).
- Own domain.

- No logging of users' data.
    - Two-factor authentication.
- Encrypted calendar.
- Encrypted contacts.

3. Only with Tutanota:

- Administration of users.
- No recovery via email or SMS (considered insecure), but through a Recovery Code generated during account creation. The admin retains the ability to recover for a user from the admin panel.
- 1€/month/user.
- 1 GB storage.
- Servers located in Germany, subject to German privacy protection laws (11).
- Dual encryption mechanism (12).
- Local encryption (13).

4. Only with Protonmail:

- Auto-destruct emails between ProtonMail users, with the option for external users when setting up a password-protected email.
- Notification on the recovery email for new incoming emails.
- 5€/month/user.
- 5 GB storage.
- Option to disable the recovery email.
- PGP encryption available (11).
- Servers located in Switzerland, subject to Swiss privacy protection laws (15).
- IMAP/POP3 support (16).

5. Serious alternatives:

- Countermail
- Virtru
- Zeromail

6. Notes:

(1) End-to-end encryption is limited to users within the same platform. PGP is still a universal method for sending encrypted emails to anyone, though it is not widely used due to a lack of awareness. The security of the encryption key depends on its storage on the user's device, which helps protect against state-sponsored threats. While this doesn't completely prevent the government from accessing plain text messages, it makes it much harder by requiring an active attack on the user to obtain the necessary password. So far, such attacks have not occurred, and they are unlikely to happen in the near future.

(2) This potential vulnerability could open an attack opportunity for state-sponsored criminals through MX records. To reduce this risk, it is advisable to host your domain in a location that prioritizes access protection, ideally in a country not affiliated with the Fourteen Eyes alliance. Consider countries with a strong track record of respecting privacy and upholding democratic principles.

(3) Distinguishing between multiple users and multiple aliases is crucial. Each user has their own unique access credentials, including a distinct username, password, and mailbox. In contrast, aliases are email forwarding mechanisms that direct emails to and from the main email address. For example, the main email could be name.surname@yourdomain.com, with aliases like blabla01@yourdomain.com and blabla02@yourdomain.com. Emails sent to any alias are forwarded to the main name.surname@yourdomain.com address. While aliases make it easy to create and delete email addresses, sharing the inbox would require admin access, which is impractical in a business environment.

(4) Corrupt law enforcement and prosecutors can wield significant influence, making their actions appear legal. Such individuals pose a substantial threat to both individuals and countries. If involved in illicit activities, they can hide them by intercepting and reading IMAP, POP3, TLS, and SSL communications. They might manipulate your email provider's SSL certificate or gain access to your SMS and emails. This makes recovery options vulnerable, highlighting the importance of consistently using encryption software, securing devices, and obtaining hardware from trusted external sources.

(5) For our numerous contractors using our emails, a synchronized and unified solution is essential to minimize potential information leaks to third parties.

(6) For our numerous contractors using our emails, a synchronized and unified solution is essential to minimize potential information leaks to third parties.

(7) Open source doesn't automatically ensure thorough code audits for potential backdoors or weaknesses, but it does reflect a commitment to transparency. Tutanota, for example, asserts that it conducts regular code audits and has undergone a comprehensive penetration test by SySS GmbH, demonstrating their dedication to security.

(8) Tutanota, priced at $12 per year per user, is more economical than ProtonMail. Although Tutanota offers less storage space (1 GB vs. 5 GB), our minimal storage requirements make pricing the decisive factor in our choice.

(9) It also means the provider is unable to recover (decrypt) data if password is lost.

(10) You need to send the password through another communication channel.

(11) The uncertainty arises because Germany is a member of the Five Eyes alliance. While NSA hardware is present on German soil, acting as a surveillance hub for Europe, the resilience of the German people in resisting such activities is notable. Tutanota asserts a stance against providing backdoors to these agencies, adding a layer of assurance.

(12) Tutanota employs a dual encryption mechanism involving a private key and a password. Upon registration, a private key is generated in the browser for encryption and decryption purposes. This private key is then encrypted with the login password for added security.

(13) Emails are stored encrypted locally on the devices.

(14) Tutanota is planning to develop an API to allow users to use PGP in a user-friendly manner.

(15) By siting themselves outside US and EU jurisdictions, they establish a more secure location to safeguard confidential data.

(16) IMAP and POP3 are considered insecure because they download emails locally without encryption, making them susceptible to being read in transit and/or on the devices.

7. We've tested this and more:

- bulletmail.org (dead).
- chiaramailcorp.com (dead).
- confidantmail.org
- countermail.com
- darkmail.info
- invmail.io (dead).
- mailbox.org
- mailfence.com
- msgsafe.io
- mynigma.org (dead).
- openmailbox.org (dead).
- posteo.de
- riseup.net
- runbox.com
- safe-mail.net
- scryptmail.com (dead).
- shazzlemail.com
- unseen.is (dead).

- virtru.com
- zeromail (via zeronet)
- zwooky.com

