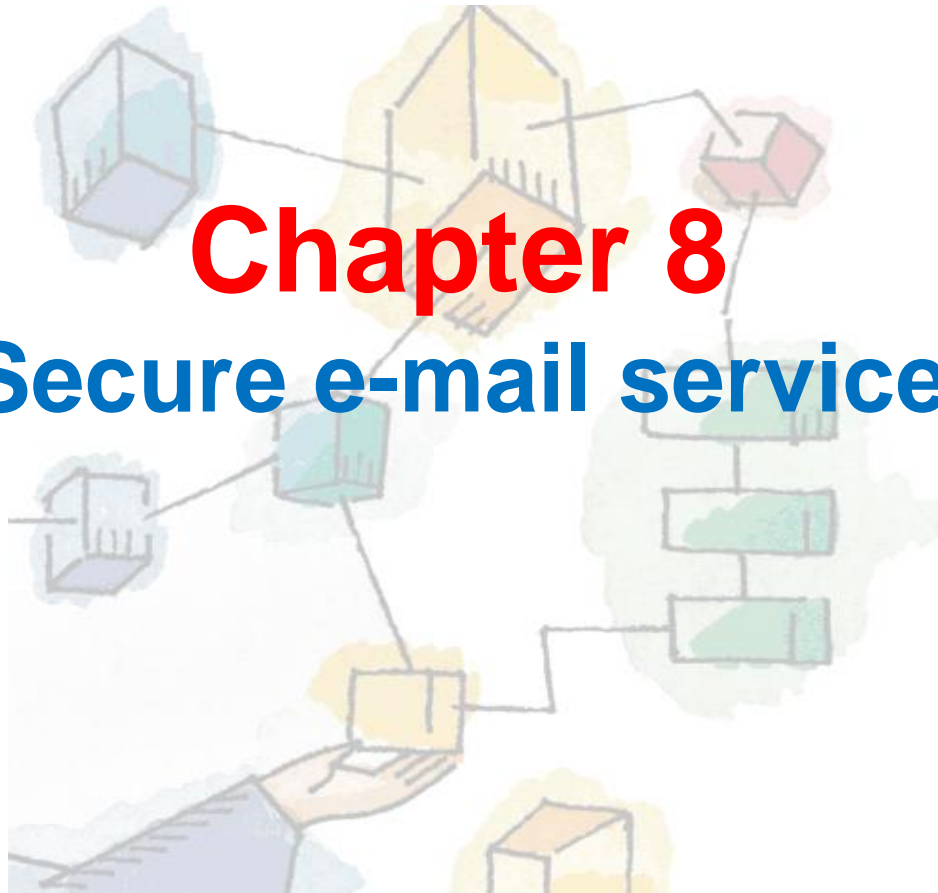


Cyber Security

Chapter 8 **Secure e-mail service**



Secure e-mail service

- **Secure e-mail service provider**

To protect customer accounts and data from attackers, email service providers have email protection measures in place. These steps involve email servers with robust frameworks for password and authentication, secure emails (both inbox and in transit); firewalls for web applications; and spam detection tools.

- **What is E-mail Security?**

As a platform for delivering viruses, spam, and phishing attacks, e-mail is prominent with attackers. To manipulate users into disclosing personal information, they use misleading texts, culminating in identity fraud. They tempt users to register files or click URLs on the user's computer that allow maliciously (like email malware). For threats, anyone wants to penetrate network architecture and hack sensitive customer information, email is often a key entry point. The characteristics of E-mail security are often flexible, and according to the user's requirements, some of the common features are given below-



Secure e-mail service

Features of the e-mail service provider

- It's not like, all reliable email services are confidential and protected indeed. Several free alternatives may do further damage. Therefore, it meets some or most of the following requirements when looking for the most reliable email provider:
- Some of the most common features of e-mail service providers are mentioned-below:
- **1. End-to-end encryption**
- No email service can call itself secure without end-to-end encryption. Your message is only encoded till it hits Gmail or yahoo mail when you're using a standard service. If end-to-end encryption is used, the text can only be read by the sender and the receiver. The most popular end-to-end encryption for protected messages is the so-called Pretty Good Protection or PGP in general.



Secure e-mail service



2. Two-factor-authentication (2FA)

- It gives you great protection and protects your accounts in case anyone learns your password. You find it more difficult to hack into your inbox by incorporating anything that you must have, like a mobile. There are several 2FA options, varying from Google and other SMS to authorization apps.

3. Stripping headers from metadata.

- Each message includes the data of data (metadata), like the internet browser, and even the receiver. For the sake of the sender and recipient confidentiality, protected email providers wipe out the header's metadata.

4. Position of the server.

- Many nations are not private information-friendly. Some even have regulations for data protection that enable your personal information to be retained for a certain time. Representatives of the Five Eyes intelligence organization are the USA, United Kingdom, Canada, and Australia. They exchange intelligence information about indicators and are among the hardest locations for a safe email provider to enroll.



Secure e-mail service



- **The Need of secure e-mail service**

- The benefits of using a protected email service must be evident to you. When you still have some questions, although, while switching to Gmail, please ensure to take a look at the following considerations:
- **1. Protect the emails**
- After the message hits their servers, Gmail, Hotmail, and other popular services don't encode your confidential information. This implies that they can translate them and make reading easier for attackers as well.
- **2. Metadata header hiding**
- It doesn't immediately imply covering the headers with metadata if your daily email system authenticates your mail. It also covers your email account, laptop, browser, and network, as well as the receiver.



Secure e-mail service

3. Do not be a commodity.

If your email is good and free to use, there may be some possibilities that you are treated as a commodity. However, very few users realize that Gmail constantly searches the mailbox for words and utilizes them to display customized advertisements. By using this way, you are helping Google to earn money from your data with the help of Gmail.

4. In a private information-friendly place, save your emails.

- The USA and any cognitive ability-sharing nation with Fourteen Eyes will someday wish to access your mailbox. If the vendor's database is in one of those nations, it would be much quicker to do that than to obtain access to any of Switzerland's nuclear bunkers.
- Ultimately, please remember that the email system is as protected as the passwords you have selected. If someone can hack your password in a couple of minutes, all end-to-end authentication and no-logs regulations go over the roof.





Secure e-mail service

• Working of secure email service

- End-to-end authentication is the distinguishing characteristic of encrypted messaging. It implies that there is no option for the mail service or a third party to decode your letter, which can only be achieved by the receiver. On the counter, your messages can be read by any standard email service provider such as Google (they are screening emails for words already!) and making them simpler for attackers to get.
- For protection, **Pretty Good Privacy (PGP)** and **Secure/multipurpose internet mail extension (S/MIME)** are the most prominent options. PGP incorporates symmetrical and asymmetrical protection, whereas S / MIME provide the certificates that must be approved by the certification authority at the regional or public level. Utilizing a certificate guarantees that you are the message provider and that it has not been interfered by others.
- Because of the encryption, neither perpetrators nor the government, like email accounts, will peer into your communication or metadata.



Secure e-mail service

- **Encryption Levels**

- Here, we have discussed some different types of encryption levels that are used to secure email communication.
- **Transport-level Encryption**
- Transport-level authentication guarantees that your email moves securely across the network, as discussed before. After all, the provider will see the non-encrypted edition once it appears on their server, it would not be sufficient to allow safe mail transmission. Although the latter is still used, Transport layer security, is counterpart of Secured socket layer. It is configured for encrypting emails (IMAP, SMTP) as well as other protocols, like **HTTP (Hyper-text transfer protocol)** or **FTP (File transfer protocol)**, on **top of TCP (Transmission Control Protocol)**. It is still not included in all mail systems, unfortunately. For a frequent user, this may not be obvious since there is no easy ability to determine when transport-level encryption is in effect while using mail, unlike an internet browser displaying a green lock or equivalent icon.



Secure e-mail service



- **End-to-end Encryption**

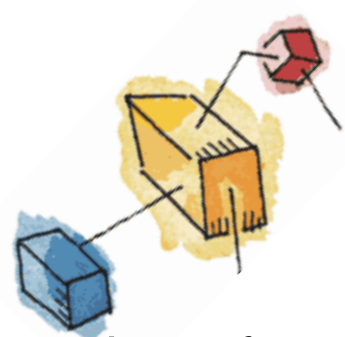
- End-to-end encryption means that your text can be decrypted neither by the email service provider nor any other third party. Only the sender and the receiver contain the public and private keys that are required to unlock it.

- **Working of End-to-end encryption**

- You encode the text with the public key of your partner. Now, this can only be decoded with the private key of your partner. Before it hits your partner, your encoded data passes via servers. He or she utilizes the private key to decode your message in exchange.
- **PGP email encryption**
- There is no need for users to share private keys; PGP email authentication incorporates a hashing algorithm, symmetric encryption and public-key authentication. Behind this, a safe email system does it, so you do not have to think about the pros and cons.



Secure e-mail service



- **How the PGP operates**

- Just after the session key is created by Pretty Good Privacy protocol, the shared key of the receiver encodes it. The sender provides this encoded session key and it is decrypted with his or her private key by the recipient.
 - Ultimately, the non-encrypted session key is used by the receiver to interpret the email.
-
- **Best Secure email service provider**
 - Here, the list involves paid and unpaid safe email providers that can offer independent options for various platforms (ubuntu will be the focus in this) or simply provide the normal web-based email services.



Secure e-mail service

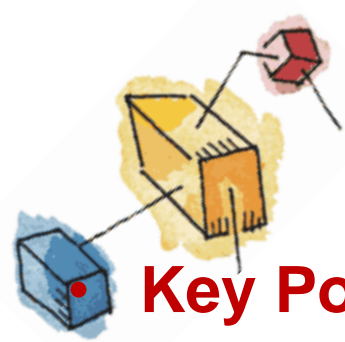
1. Tutanota



- Tutanota is an email service provider that is secure and suitable for personal and business usage. It offers 1 Gb of space (rather than 500 MB) for free users, unlike Proton Mail. And, to your account, you may also attach more space. To attach a domain name, users need a paid subscription plan. You may also choose for the option to white-label the system for your company if you like. Several other tools are also offered by Tutanota to protect your confidential data. Some few instances of the increasing stock include resources such as free encrypted calendars or end-to-end encryption types.



Secure e-mail service



• Key Points

- It is an open-source tool.
- It uses end-to-end encryption approach.
- This tool is accessible with two-factor-authentication.
- Tutanota is available in paid and unpaid versions.
- It supports the custom domain that needs a premium subscription.
- It also supports white label for organizations.
- It supports the **free version up to 1 GB**.
- The **subscription price for this tool is \$1.18/ month**.
- It can **store 1to10 GB of data**.
- Tutanota is **located in Germany**.



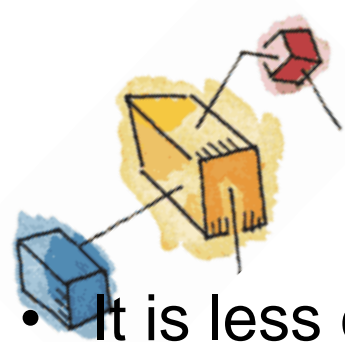
Secure e-mail service

• **Advantages of Tutanota**

- It is less costly.
- This tool doesn't contain the log policies.
- It supports the feature of spam filter.
- Tutanota tool supports more than 20 languages.

• **Disadvantages of Tutanota**

- It doesn't support the Pretty Good Privacy (PGP) and IMAP (Internet message access protocol).
- Tutanota comes under the fourteen Eyes country.
- It has very costly extra memory space.



Secure e-mail service

• 2. Hush Mail



- Several other tools are also offered by Tutanota to protect for individuals concerned with confidentiality, Hush mail is an authenticated email service provider. It makes possible for you to utilize a 14-day trial period for private use.
- However, for organizations, it classifies them and provides different rates. For instance, if you want to use your health insurance company's safe email service, it provides you with a Health insurance portability and accountability (HIPAA) compliant system. Some few instances of the increasing stock include resources such as free encrypted calendars or end-to-end encryption types.



Secure e-mail service

Key Points

- It supports 2 weeks trial version for private use.
- It provides different plans and costs for business customers.
- It includes open Pretty Good Privacy (PGP) end-to-end encryption.
- It has capacity to create multiple web forms.
- The **paid version is available at price of \$4.18/month.**
- It can **store 10 GB of data.**
- Hush Mail is **located in Canada.**
 - **Advantages of Hush mail**
- It is a user-friendly tool.
- This tool supports Touch ID.
- Hush mail facilitates users with spam filter.
- It uses Internet message access protocol (IMAP) and POP3.



Secure e-mail service

- **Disadvantages of Hush mail**

- This tool comes under the five Eyes country.
- It doesn't support the free version.
- You cannot access it with Android app.

- **3. Proton Mail**



- To protect your personal information, Proton Mail is a very prominent Swiss-based email system that implements an ad-free layout. It helps you to set an expiration period for the self-destructing email itself. It is open - source software in default, in contrast to all of the safety features. So, to be certain, you should check the open-source authentication repositories or other stuff.

Secure e-mail service



- You are required to have a premium account to enable a custom domain. With minimal functionality, you will use it for unpaid or choose to update it to a paid subscription (for organization).

- **Key Points**

- It is an open-source mail service provider.
- It provides an end-to-end encryption.
- It is a Swiss-based tool.
- This tool provides both paid and free version.
- It supports self-destruct message functionality.
- It also supports two-factor-authentication.
- The paid version is available at **\$4/ month**.
- It provides **5 to 20 GB memory storage**.



Secure e-mail service



• i) Not a one-time thing

• Cyber security requires constant monitoring and updating with regular intervals of time for its benefit because it is not designed in a few minutes. This states that cyber security is not a one-time installation process that you set and forget. It takes years of effort, study, and experimentation to make a cyber security program and put it into place. It needs constant attention.

• **Benefits of Proton Mail**

- It doesn't have any log policy.
- It provides the message encryption to the users.
- It supports more than 20 languages.

• **Drawbacks of Proton Mail**

- It has the costly visionary plan.
- Sometimes the client is treated as an outdated client.
- It doesn't support POP3.



Secure e-mail service

• 4. Counter Mail



- Counter Mail is just an option available to be described as a secure email service provider. It allows you to try the service completely free of charge for 7 days. It allows you to get your own domain name and build online application in contrast to the authentication, no matter which type of membership you have.
- The more you pay, the more you get a little more memory space. But the characteristics remain the same, which is a pleasant thing.

• Key Points

- It supports Open Pretty Good Privacy (PGP) end-to-end encryption.
- Counter Mail supports the custom domain.
- It provides a facility for users to use web forms.
- Counter Mail supports Windows, Linux, and Mac Operating system.
- The paid version is available at **\$3.29/ month.**
- It provides **4 GB memory storage.**
- **It is located in Sweden.**



Secure e-mail service

• Advantages of Counter Mail

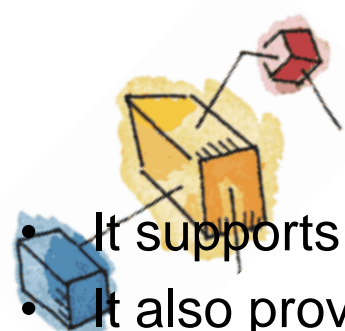
- It supports anonymous payment method.
- It also provides the protection from MITM (Man-in-the-middle) attacks.
- Counter Mail facilitates you with the safe box storage.
- It uses PGP encryption standard.

• Disadvantages of Counter Mail

- The counter Mail lies under the fourteen eyes country.
- It has limited and costly memory space.
- It doesn't support the POP3.
- There is no unpaid version of Counter Mail.

• 5. Zoho Mail

- Among the best protected mail servers, Zoho Mail is not really that always encountered. This provider is simply focused to business customers, but that has little to do with its efficiency. But as it can also be used by users, we are including it to our Top 10 secure email service provider.




Secure e-mail service



- Zoho provides a range of Information technology solutions, such as a password manager, so when you combine it with other things, your email functions better. This solution offers a protected network infrastructure that can be retrieved only with biometric security, putting that aside. Then there's security from malicious software & spam, and end-to-end encryption (SSL, S/MIME, TLS). For additional account protection, this protected email support Two - factor authentication (2FA). Users are able to access the encryption application, one-time password (OTP), QR code, or fingerprint Reader from Zoho.
- Zoho Mail functions with your mobile as an internet browser or an application. You may also use any other third-party email users to customize it. The interface is eye-pleasing and elegant, which is essential if you are willing to use your protected email on a continuous basis.



Secure e-mail service

- 
- With a 25 MB connection cap, the free plan has a big 5 GB of memory storage. Five members can access one account; however, you may only use the web application, making it a hassle to search your mobile email successfully.
 - Even so, you have the applications or other IMAP/POP users, a 10 times greater connection scale, and several domains for a dollar per month. Power allows users to transmit 1 GB of files, save 50 GB, backup addresses, and use white-labeling for \$4 / month with Email Premium. There is also a 15-day trial period.

- **Key points**

- You can purchase this tool at \$1/ month.
- It provides **5 GB memory storage**.
- **It is located in India.**

- **Advantages of Zoho Mail**

- It contains a sleek design.
- It provides an IMAP (Internet message access protocol)/ POP.
- This tool comes with the free version.
- It also facilitates users with malware protection.

- **Disadvantages of Zoho Mail**

- It is mostly focused on business to business client supports.
- Some data centers of Zoho mail are situated in USA and China.



Secure e-mail service

- **6. Start Mail**



- When one of the best personal email account programs offered, an email service from Startpage.com (best Google options) is perhaps a worthy option.
- It provides a 30-day free trial with restricted functionality. You may want to update if you really like the service. There is something really significant, in contrast to all the characteristics such as domain name, customized aliases, and PGP email authentication. StartMail allows you to make use of email addresses that are reusable. So, you may always use a provisional one because you may not want to reveal your actual email account.



Secure e-mail service

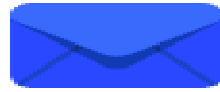
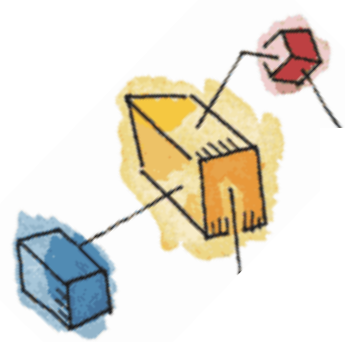
- **Key Points**

- This email service provider tool contains disposable email aliases.
- It provides a Pretty Good Privacy (PGP) email encryption.
- This tool comes with custom domain service with upgrade.
- It is compatible with Simple mail transfer protocol (SMTP) and Internet mail access protocol (IMAP).
- It contains the 10 GB of data storage.
- The subscription price of Start Mail is \$5/month.
- Start Mail is Europe based service provider.

- **7. Private-Mail from Tor Guard**

- Private Mail is a 100 percent protected encoded email service which is really easy to use. It is available for both people and enterprises. Private Mail tends to make your mailbox genuinely private - it doesn't just incorporate the absurd notion of confidentiality. For all files transferred via the network, it's configured with MITM security, an email alias function, and Paranoid authentication. With any web browser, your mailbox can be reached anywhere, without any need of apps.

Secure e-mail service



PrivateEmail

- In a private email service, private-mail hits all the spots you usually look for. You can still get 100 MB of space with authentication and web-based email access only if you'd like for free.
 - You may also want to update your membership if you want to use the service on portable platforms (including your mobile device). There is a web client available for Windows now. It is coming to Linux soon sufficient, however according to its download link.
- Key Points**
- It supports Open Pretty Good Privacy end-to-end encryption.
 - The users can also use the Desktop app but only in Windows.
 - This tool also provides a custom domain with premium subscription.
 - It also provides MITM prevention.
 - The users can also access it from anywhere.
 - It supports a simple email alias.
 - It offers private encrypted cloud storage.



Secure e-mail service

• 8. Mailbox



- Mailbox is an amazing encrypted email system that executes on green power. The information center of Mailbox is located in Germany that keeps it very private information-friendly.
- It will charge you 1 Euro / month, including 100 MB of safe storage in the cloud. The concept of providing storage space along with your emails is not new, but it is not provided by all privacy-oriented email providers.
- Besides that, to allow you to keep your messages secure, it offers a lot of security features.

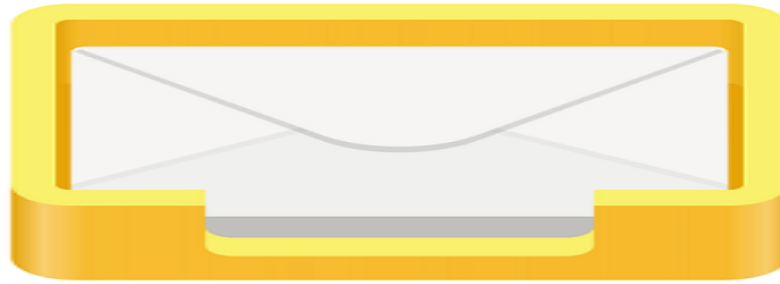
• Key Points

- This tool is mainly focused on privacy.
- It also provides a huge storage capacity on cloud.
- The Mailbox email service provider executes on the green energy.
- It also offers an end-to-end encryption.
- The data centers of Mailbox are situated in Germany.



Secure e-mail service

- **9. Librem Mail**



- Librem Mail is a portion of Librem One spectrum of tools provided by Purism. Unlike other secure mail service providers, it isn't unpaid. To get access to their private messaging service, Librem Mail, you will need to choose for a paid service to Librem One.
- If we consider the Purism's history of preserving the privacy of clients, it sounds like a fantastic end-to-end secured, ad-free email service. They are also developing a stable mobile called Librem 5, based on Linux.

- **Key Points**

- It is an end-to-end encrypted email service tool.
- This tool supports a secure VPN tunnel for safe browsing.
- It is convenient, ad-free email service provider.
- Librem mail uses K-9 mail and Open Key Chain.



Secure e-mail service

- **10. Mail fence**



- Mail fence is a reasonable email service platform focused on confidentiality, which imposes end-to-end authentication for Open PGP. With the help of restricted disk space (500 MB) and functionality, you may start using it for free. In any case, to boost the storage capacity, unleash the capacity to use a domain name, you may also get the opportunity to upgrade the subscription, etc.
- The absence of mobile applications is the only drawback that the user faces here. So, in attempt to use several devices, you are required to initiate a browser and log-in.

- **Key Points**

- It uses end-to-end encryption to protect the email privacy.
- This tool provides both paid and unpaid versions to the user.
- It supports the custom domain.
- This tool also provides a two-factor-authentication.
- It is only available on the web browser (No smart phone applications).

