**What are the best encrypted email services?**

As noted above, we think the best solution is to switch to an email provider that offers support for end-to-end encryption. Many email services offer support for various encryption options:

1. One of the most popular encryption methods for email is PGP, which stands for [Pretty Good Privacy](https://en.wikipedia.org/wiki/Pretty_Good_Privacy). Support for PGP is built into most secure email providers.
2. Some email services rely on a unique encryption method, outside of PGP. One popular example of this is with the email provider Tutanota.
3. Email services also allow you to send a link to an encrypted message that can be accessed with a shared password.

If you are open to switching to a secure email service that supports built-in encryption, we’d encourage you to explore our guide on [secure and private email services](https://restoreprivacy.com/private-secure-email/).

Here are the best encrypted email services:

1. [Tutanota](https://restoreprivacy.com/tutanota/) – Based in Germany; free plans; very secure and open source email with full encryption of email inbox, contacts, calendar, and subject lines. (Tutanota does not use PGP due to concerns over [PGP limitations and weaknesses](https://restoreprivacy.com/let-pgp-die/).)
2. [ProtonMail](https://restoreprivacy.com/protonmail/) – Based in Switzerland; free plans; secure and open source email that is based on PGP encryption
3. [Mailbox.org](https://restoreprivacy.com/mailbox-org/) – Secure and private email based in Germany; fully-featured, support for PGP encryption
4. [Posteo](https://restoreprivacy.com/posteo/) – Privacy-focused email service based in Germany; anonymous payment options; no support for custom domains; strong PGP encryption standards
5. [Mailfence](https://restoreprivacy.com/mailfence/) – Secure email based in Belgium, free plans up to 500 MB, fully-featured with built-in support for PGP encryption
6. [Runbox](https://restoreprivacy.com/runbox/) – A private email service in Norway, support for PGP encryption
7. [CounterMail](https://countermail.com) – Based in Sweden, this email offers strong encryption options (based on PGP).
8. [CTemplar](https://ctemplar.com/) – This open source email provider in Iceland uses strong encryption standards and is very privacy-focused.
9. [Kolab Now](https://kolabnow.com/) – A higher-priced email service in Switzerland, Kolab Now has some good encryption options while also being fully-featured.
10. [StartMail](https://www.startmail.com/en/) – Based in The Netherlands, StartMail offers built-in PGP encryption support.

We have personally tested (and use) many different encrypted email services. We not only do this to write reviews, we take data privacy seriously. Below I’m testing out the feature with ProtonMail to send an encrypted message to a person who does not use ProtonMail.

With ProtonMail, you can send encrypted emails to non-ProtonMail users.

If you are serious about encrypting your email, it would be wise to first start out by switching to a secure email provider. Finding the best encrypted email service is very subjective and all comes down to your own unique needs. Check out our [email reviews](https://restoreprivacy.com/category/email-reviews/) for an in-depth look at many providers.

**What about encrypted email services based in the US?**

Did you notice above that none of our recommended encrypted email services are based in the United States?

There’s a reason for this. And that is concerns about privacy and data security. There are many examples of US tech companies being forced to hand over private data to US authorities. This is particularly important with email services. Here are just two examples that we know about:

1. **Lavabit** – Lavabit was a privacy-focused email based in the US that was [forced to shut down](https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email) when the owner refused to give up the encryption keys to government agents.
2. **Riseup** – Another US email service catering to privacy-minded users, Riseup was hit with data requests and was forced to comply.

Here’s a quote describing the Riseup [situation](https://riseup.net/en/about-us/press/canary-statement), which could affect any US-based email service:

After exhausting our legal options, Riseup recently chose to comply with **two sealed warrants from the FBI**, rather than facing contempt of court (which would have resulted in jail time for Riseup birds and/or termination of the Riseup organization).

There was a **“gag order” that prevented us from disclosing even the existence of these warrants** until now. This was also the reason why we could not update our “Canary” [warrant canary that warns users about these events].

**Recommendation**: Choose an encrypted email service located in a good privacy jurisdiction. If you don’t, your data could be at risk.

**Encrypted email alternatives**

One of the fundamental problems with email is [**metadata**](https://en.wikipedia.org/wiki/Metadata).

Email is structured in such a way that metadata is very difficult to conceal from third parties. Email headers can reveal a lot of private data. What’s worse, PGP, the most widely-used encryption protocol, does not encrypt subject lines. This exposes further data to third parties and potential adversaries.

Another problem is that most people simply do not want to use an encrypted email service and/or encrypt messages. This isn’t an easy problem to get around — unless you use an alternative to email.

**Best alternative: encrypted messaging service**

We’d recommend using a good encrypted messaging service if you are really concerned about privacy and data security. Most encrypted messaging services do a very good job encrypting data, collect little (or no) metadata, and offer stronger encryption than most email services.

Some of our favorite options are [Signal](https://restoreprivacy.com/signal-messenger/), Session, [WickrMe](https://restoreprivacy.com/wickr-messenger/), and others. Check out the [best secure messaging services](https://restoreprivacy.com/secure-encrypted-messaging-services/) for more options.

**Conclusion on encrypting email**

In this world where the assaults on our privacy grow by the day, it behooves us to take whatever steps we can to defend ourselves. One place you can fight back is in your email inbox. Unless you want a vast number of entities (from Google AIs to foreign spies) reading your email messages and doing who knows what with the information they find there, you need to encrypt your email.

**Remember**: If you aren’t up for rolling your own end-to-end encryption system, you can move your most important email connections to one of the private email services.

[ProtonMail](https://restoreprivacy.com/protonmail/), for example, has a free version that handles E2EE for you and uses a system much like Gmail’s Confidential mode to send private messages to people who don’t use ProtonMail. And if your encrypted messaging needs aren’t too intense, you can get by just fine with the free version of ProtonMail or another one of our recommended encrypted email providers.

# **Email Encryption FAQs**

## Why is encryption in transit important?

Encryption in transit helps protect your emails from being snooped on while they travel between you and your intended recipients. Unfortunately, billions of unencrypted emails are sent and received every day “in the clear,” presenting a prime target for eavesdropping and mass interception as they cross dozens of optical fibers and routers.

## If my email is encrypted in transit, does it mean that no one can ever snoop on my email?

Security is an ongoing challenge where no solution is perfect and progress is incremental. Encryption in transit makes it more difficult to snoop on email and universal encryption of email in transit would be a huge step forward for security and privacy online. But encryption doesn’t make snooping impossible. Moreover, email is not only vulnerable in transit—it can also be snooped on after it’s delivered. For example, unauthorized parties could still gain access to your email by installing malware on the computer you use to read it.

## What do you mean by encryption of email in transit?

When an email is encrypted in transit, that means it’s protected against being read by someone with access to the networks through which the email is traveling, on its way from the sender to the destination. You can think of it as a temporary envelope of security that is wrapped around your email to keep it private while it is being transmitted to its intended recipient. Transport Layer Security (TLS) is the standard means of performing encryption in transit for email.

What TLS doesn’t do is encrypt data at rest—that is to say, it does not encrypt email while it is stored on a server. There are ways to do this, such as using PGP (see below).

## Is TLS the be-all, end-all solution for protecting my email while it’s in transit?

No single Internet security solution is perfect, but unencrypted email is a major vulnerability. Encrypting email when it travels between email providers is a big improvement that can be implemented fairly easily without any inconvenience to users.  Some more information about the state of TLS for email, and its flaws, can be found in [this detailed blog post from Facebook](https://www.facebook.com/notes/protect-the-graph/the-current-state-of-smtp-starttls-deployment/1453015901605223).

## Is email from Google users to other Google users encrypted in transit?

Yes.  This includes Gmail, GSuite and notifications from Google+.  That's why this report is focused on email deliveries where Google is only one of two providers involved.

## How does encryption in transit relate to HTTPS access to Gmail?

Since 2010, [HTTPS has been the default](http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html) when you’re signed into Gmail. This means that while your email travels between Google’s data centers and the computer you use to read your email, it’s encrypted and secure. This report is about something different: whether or not your email is protected by TLS when it travels outside Google’s data centers to the external mail server of the person you’re emailing.

We’ve turned on HTTPS for Gmail on our own, but when email is sent between different mail providers, both providers need to support TLS in order for the email to be encrypted in transit.

## How does encryption in transit relate to other forms of email encryption, like PGP?

[PGP](http://en.wikipedia.org/wiki/Pretty_Good_Privacy) encrypts the content of your email in such a way that, if you do everything perfectly, nobody but you and the intended recipient will ever be able to see it. When a Gmail user receives a PGP-encrypted email, for example, Gmail is unable to index the content of the email for later searching, because Gmail cannot see the content.

This tradeoff of convenience for additional security is especially appropriate for people who are at risk, and adds an additional layer of security not provided by encryption in transit.

But encryption in transit adds a significant privacy benefit to PGP. PGP encrypts only the content of your email, but not its headers (e.g. who is sending and receiving the email). An eavesdropper who “overhears” the delivery of a PGP-encrypted email will be able to see what address the message was delivered to, but not the content of the message. But when a PGP-encrypted message is also encrypted by TLS while in transit, the sender and receiver of the message will not be visible to an eavesdropper.

## Why isn’t all email sent to or from Gmail encrypted in transit?

For decades, the default has been for email to travel across the Internet unencrypted—as if it was written on a postcard. Gmail is capable of encrypting the email it sends and receives, but only when the other email provider supports TLS encryption.

In other words, encrypting 100% of all email on the Internet requires the cooperation of all online mail providers.

## What is being counted in this report?

We count message recipients, not SMTP connections.  We don’t count emails our systems flag as spam.  We don’t count inbound messages from hosts whose forward or reverse DNS is missing or inconsistent.  This is to ensure that inbound messages can be meaningfully attributed, since a message sender can assert any “From” address that he wants.

## What does “From X via Y” mean?

“From: gmail.com via google.com” means all messages with an envelope sender ending in @gmail.com or a subdomain, from a host in the domain google.com or a subdomain. When the "via" domain is the same, it is elided.

An ellipsis, as in “google.{...}”, means that several domains, such as google.com and google.co.uk, have been counted together. We try to do this only when we believe that like-named hosts process mail in the same way, which is not always.

# **How to Encrypt Email in Gmail, Yahoo, and Outlook**

Contrary to what many people believe, email was not designed with privacy and security in mind. To protect your personal information against [malicious hackers](https://clean.email/how-email-spammer-gets-your-address), learn how to encrypt email in Gmail, Yahoo, and Outlook.

## What Does Encrypted Mean?

Humans have been encrypting sensitive information since Roman times. Even though Roman ciphers are a far cry from modern encryption algorithms, they accomplish the same goal: convert information into secret code that hides its true meaning.

Imagine that your inbox is as safe and your emails are important documents that you don't want anyone else to see. Without email encryption, all that cybercriminals need to do to read the content of your emails is to know the right password to your inbox.

Unfortunately, large-scale data breaches are becoming increasingly common, and there's a chance that cybercriminals already know the [password to your inbox](https://clean.email/have-you-been-pwned). Even if they don't, they can attempt to intercept your emails while they're being delivered.

By converting messages from readable plain text into ciphertext, email encryption introduces another layer of security and ensures that only authorized parties can read them. While the technology behind encrypted email is incredibly complex, its practical implementations by major email service providers are easy to use.

## How to Encrypt Email in Gmail?

If you're a Gmail user, we have good news for you: **Google automatically encrypts all emails in transit using Transport Layer Security (TLS)**, the standard means of performing this type of encryption.

TLS, a set of cryptographic protocols designed to [provide communications security](https://clean.email/free-private-email-providers) over a computer network, makes it impossible for unauthorized third parties to snoop on your email communication when sharing the same network, such as the WiFi at your favorite coffee shop.

You can imagine TLS as a magical envelope for messages. Even if someone steals this envelope, the person won't be able to read your email unless they know how to unlock it.

Besides TLS, Gmail also supports S/MIME, which is an advanced encryption standard that encrypts the actual message, instead of simply providing an encrypted envelope for it. S/MIME is only available with G Suite Enterprise, G Suite for Education, and G Suite Enterprise for Education, and each sender and recipient must have it enabled for it to work.

**To enable S/MIME**:

1. Log in to your [Google Admin console](https://support.google.com/a/answer/182076).
2. Go to Apps → G Suite → Gmail → User settings.
3. Select the domain or organization you want to configure.
4. Check the Enable S/MIME encryption for sending and receiving emails box.
5. Click Save.

## How to Encrypt Email in Outlook?

Just like Gmail, Outlook.com uses TLS encryption to protect the connection with a recipient's email provider. The problem with TLS is that it protects messages only while they're in transit and doesn't guarantee that they'll stay encrypted after they reach the recipient's service provider.

Microsoft implemented its own Outlook email encryption system, which ensures that your messages always remain encrypted and don't leave Microsoft's servers. Outlook email encryption is available to Office 365 Home or Office 365 Personal subscribers, and it could hardly be any easier to use.

**To send an encrypted email message in Outlook.com**:

1. Log in to your Outlook.com account.
2. Click the blue New message button in the top-left corner.
3. Select the encryption option from the ribbon.
4. Click Encrypt or Encrypt & Prevent Forwarding (the latter makes it impossible for your message to be copied or forwarded).
5. Compose your message and click Send.

Outlook.com users can read encrypted email messages just like regular messages. The users of third-party email services receive a message with instructions for how to read the encrypted message.

## How to Encrypt Yahoo Email?

Yahoo protects your messages in transit using TLS, but you need to use a free email encryption browser plugin to enable end-to-end encryption. There used to be a [first-party encryption plugin](https://github.com/YahooArchive/end-to-end) for Yahoo Mail, but the project seems to be abandoned now.

Instead, we recommend you use [Mailvelope](https://www.mailvelope.com/), which adds missing encryption features to the user interface of common webmail providers, including Yahoo Mail, Gmail, and Outlook.com, among others.

**To encrypt a Yahoo email message using Mailvelope**:

1. Download Mailvelope for [Google Chrome](https://chrome.google.com/webstore/detail/mailvelope/kajibbejlbohfaggdiogboambcijhkke) or [Mozilla Firefox](https://addons.mozilla.org/firefox/downloads/latest/mailvelope/).
2. Configure Mailvelope to get started.
3. Open a new message in Yahoo Mail as usual.
4. Click the Mailvelope icon in the top-right corner.
5. Write your message and click Encrypt.
6. Send the encrypted email message.

## Improve Your Email Management to Increase Your Security

Password theft or email snooping are not the only two traps users can fall into. Experts estimate that phishing (a type of social engineering attack that occurs when an attacker posing as a legitimate institution or someone else tricks the victim into giving up personal information) accounts for [90 percent](https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html) of data breaches.

Since [phishing email messages](https://clean.email/phishing-email-and-how-to-avoid-phishing-attacks) are essentially just malicious spam emails, you can effectively protect yourself against them by keeping your inbox organized and well managed.

Instead of wasting hours every week manually sorting new emails, we recommend you use an automatic inbox cleaner like [Clean Email](https://clean.email/). This powerful tool works with Gmail, Yahoo, and Outlook, and has multiple features that can take your [email management](https://clean.email/email-management-tips) to the next level.

You can quickly organize older emails into easy-to-review bundles to free up storage space and make your inbox less cluttered, instantly unsubscribe from mass emailings, and automatically apply selected actions to future emails. All features Clean Email has to offer are intuitive and work the same way regardless of which email service you use.

## Conclusion

Email encryption is a must-have when it comes to [sending highly sensitive email](https://clean.email/how-to-send-a-secure-email) messages over public networks. When combined with a strong password and a well-thought-out email management strategy, it greatly improves the usefulness and reliability of email as a communication tool.

**How to send encrypted email in Office 365 and the Outlook desktop client on Windows and Mac** **Print**

Modified on: Fri, Apr 17, 2020 at 11:38 AM

This document shows how to send an encrypted email with your Lesley email account.  Recipients can be inside or outside Lesley University.

[Sending encrypted emails - Office 365](https://support.lesley.edu/support/solutions/articles/4000113814-how-to-send-encrypted-email-in-office-365-and-the-outlook-desktop-client-on-windows-and-mac#office365)

[Sending encrypted emails - Outlook desktop on your Windows computer](https://support.lesley.edu/support/solutions/articles/4000113814-how-to-send-encrypted-email-in-office-365-and-the-outlook-desktop-client-on-windows-and-mac#windows)

[Sending encrypted emails - Outlook desktop on your Mac](https://support.lesley.edu/support/solutions/articles/4000113814-how-to-send-encrypted-email-in-office-365-and-the-outlook-desktop-client-on-windows-and-mac#mac)

[Receiving encrypted emails](https://support.lesley.edu/support/solutions/articles/4000113814-how-to-send-encrypted-email-in-office-365-and-the-outlook-desktop-client-on-windows-and-mac#receiving)

Sending encrypted email through Office 365

1. Log into web mail at <http://www.lesley.edu/office365>.

2. Click the **Mail app** to access your email.



3. Click **New**or **New message** (depending on the version of Office 365 you're viewing) to start a new email.



4. On the new email, click **Protect**(old version of Office 365) or **Encrypt** (new version of Office 365) to add encryption.

Current Office 365:



New Office 365:



5. Fill in the To, Subject, and message body fields as normal and click **Send**.

Sending encrypted email through the Outlook desktop client on a Windows computer

In order to use the encryption feature, you must have the current Office 365 version of Outlook installed.

1. Choose **New Email**.



2. Click on **Options**.



3. Click on the **Encrypt**button.



4. Fill in the To, Subject, and message body fields as normal and click **Send**.

Sending encrypted email through the Outlook desktop client on a Mac computer

In order to use the encryption feature, you must have the current Office 365 version of Outlook installed.

1. Press the **New Email** button.



2. Press the **Options** button.



3. Press the **Encrypt**button, then press the Message button to get back to the window that allows you to send the email.



4. Fill in the To, Subject, and message body fields as normal and click **Send**.

Receiving Encrypted Email

Here’s what the recipient will receive depending on which type of email client they use.

* On-campus Lesley people using Outlook on MAC or PC will see a red stop sign symbol in front of the email to indicate it is encrypted. When they click on the email link, they will see a message that they must authenticate their credentials. They will enter their email address and password.



* People accessing their Lesley email using a web browser, on or off campus, will see a lock symbol next to the email.



* Non-Lesley email addresses will receive a message prompting them to click a **Read the message** button within the email.  This will bring them to a web page where they will log in with a one-time passcode which will also be sent to their email address.



* After entering the passcode and clicking **Continue**, they’ll be presented with the contents of the email.  They can also download any attachments that were on the email.



If they click the Reply button, their reply message back to the original Lesley sender will be encrypted.

# What is an Encrypted Email and How Does Encryption Work?

(**1** votes, average: **5.00** out of 5)

## Using Secure Email Ensures That Only Your Intended Recipients Can Read Your Messages

What is an encrypted email? Email encryption refers to the method of securing email messages by making them unreadable by an attacker who listens in over the network. So, what makes them so secure? An encrypted email is one that’s sent out over an encrypted communication channel and is secured using standard encryption protocols.

If you use an untrusted connection (like a public Wi-Fi), details such as your email login credentials, or any messages sent or received can be captured by an attacker. Apart from sensitive information, attackers can also access your attachments, stored messages, and may also have the ability to take control of your account.

However, emails may also be vulnerable in a relatively protected setting such as a corporate network, which typically has security solutions to prevent data breaches. Encryption adds another layer of protection to ensure that your communication remains secure. With an email signing certificate, you not only ensure that the messages are encrypted but also help your recipients verify your identity to prevent spoofing.

## Buy Sectigo Email S/MIME Certificate – Save 21%

**Save 21%** on Sectigo Email S/MIME Certificate. It ensures message integrity and helps you to set up DMARC.

[**Shop for Sectigo Email S/MIME Certificate**](https://sectigostore.com/id/email-signing-certificate)

### **Why You Should Encrypt Your Email**

It’s pertinent we discuss the most common email security threats to understand why encrypting emails is the way forward. Let’s look at some of them:

1. **Eavesdropping.**  When an attacker uses a computer to intercept the radio signals between your computer and a wireless router. With encrypted email communication, the information can’t be read by anyone unless they have the private key.
2. **Spamming and Phishing.** While unsolicited spam mails from advertisers are simply junk mails that clutter your mailbox, phishing emails pose a serious security threat. Phish often imitate legitimate entities and are sent out with the intention of stealing your private information like banking information, credentials, etc. Storing passwords as hashes, implementing DMARC (Domain-based Message Authentication, Reporting, and Conformance), encrypting sensitive information adds a layer of protection.
3. **Spoofing.** Just like with postal services, email services do not require an accurate return address to deliver a message. A cybercriminal can fake a return address on an email to make it look as though the message came from a trusted account (even though it didn’t). You can take a look at the full email header to distinguish a spoofed email from a legitimate one. [Email signing certificates](https://sectigostore.com/id/email-signing-certificate) can be used to prevent this type of attack by ensuring that every employee within your organization is signing their emails to indicate trust.
4. **Malicious Email Attachments.** Cybercriminals might deliver harmful scripts as attachments that execute right on your computer when you open them. Email signing certs are extremely useful when it comes to verifying sender’s identity so you can be assured that the message is from a trusted source.

Keep in mind that it takes almost the same amount of effort and time to send one malicious email to one person as it does to thousands of users. We’re all susceptible to become victims of the attacks mentioned above. As such, it’s imperative that we use encryption to secure our communications.

What is secure email, you ask? Well, the three things that need to be encrypted to secure your email communication effectively are as follows:

1. **The connection between your device and the email provider.** SSL/TLS certificates installed on your email servers ensure that the communication channel between your computer and the servers stays encrypted. Check if your email provider supports SSL/TLS. An easy way to do that is to log in to your email using a web browser and see whether you get an HTTPS at the beginning of the URL. If you use a desktop client program, you can typically activate encryption under advanced settings in the email settings window.
2. **The email message itself that you want to send.** You can encrypt individual messages either by using built-in services or by relying on trusted third-party solutions. OpenPGP and S/MIME are the two most common email encryption protocols.
3. **The email messages that you have stored or archived.** If you use an email client or an app in place of a web browser and are storing or saving emails to your local computer or phone, make sure that these messages are encrypted. For example, in the case of Windows, you can use the built-in Encrypted File System (EFS) feature to secure your data at rest.