How to encrypt email

(Gmail, Outlook iOS, OSX, Android, Webmail)

Email was one of the earliest forms of communication on the internet, and if you are reading this you almost undoubtedly have at least one email address. Critics today decry the eventual fall of email, but for now, it is still one of the universal means of communicating with other people that we have.

One of the biggest problems with this cornerstone of electronic communication is that it isn’t very private. By default, most email providers do not provide the means to encrypt messages or attachments. This leaves email users susceptible to hackers, snoops, and thieves.

Let’s start by saying that setting up email encryption yourself is not the most convenient process. Not only must the sender have the means to encrypt an email, but the recipient of your encrypted email must have the means to decrypt it.

**How email encryption works**

Encryption, put simply, is no more than scrambling up the contents of a message so that only those with a key can decrypt it. Sort of like those puzzles you did in school where every letter of the alphabet had to be converted to some other letter of the alphabet so as to decode the final message. Computers make the scrambling far more complex and impossible for a human to crack by hand. When you encrypt an email, its contents are scrambled, and only the recipient has the key to unscramble it.

To make sure, only the intended recipient can decrypt the message, email encryption uses something called **public key cryptography**. Each person has a pair of keys–the digital codes that allow you to encrypt and decrypt messages. Your public key is stored on a key server where anyone can find it, along with your name and email address. Conversely, you can find other people’s public keys on key servers to send them encrypted email.

When you encrypt an email, you use the recipient’s public key to scramble the message. Due to the technology behind this type of cryptography, the public key cannot be used to decrypt it. The email can then only be decrypted by the recipient’s private key, which is stored somewhere safe and private on his or her computer.

Note that **you cannot send encrypted email to someone without access to his or her public key**. We’ll talk about a couple different types of email encryption and explain how key sharing works in each.

**Types of email encryption**

There are two main types of email encryption methods you need to know exist: S/MIME and PGP/MIME. In order for the recipient to decrypt an email encrypted by the sender, both parties must use the same type of encryption.

**S/MIME** is built into most OSX and iOS devices. When you receive an email sent from a Macbook or iPhone, you’ll sometimes see a 5-kilobyte attachment called “smime.p7s”. This attachment verifies the identity of the receiver so only he or she can read the email.

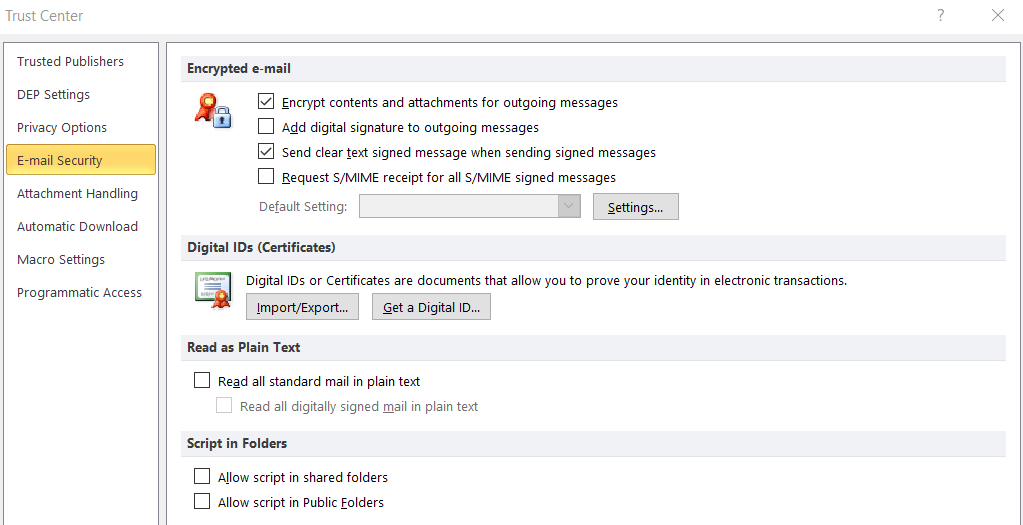
* Recipients must be in sender’s organization or have received at least one signed email from the sender in the past
* S/MIME relies on a centralized authority to choose the encryption algorithm and key size
* Easy to maintain
* Harder to set up with web-based email clients like Gmail
* More widely distributed thanks to Apple and Outlook built-in support

The other heavyweight in email encryption is **PGP/MIME**, which is what we’re going to focus on in the latter part of this tutorial.

* Recipient must have both public and private encryption keys, and the public key must be available to sender
* Relies on a decentralized, distributed trust model
* Fairly easy to use with web-based email clients
* Free to get a certificate, which S/MIME is usually not (you buy an S/MIME certificate when you buy an iPhone or Macbook)
* Choose how you encrypt and how well-encrypted the messages you receive must be
* Not widely supported by email clients, so requires third-party tools

This makes PGP/MIME cheaper and more flexible, but before we get into that, we’ll look at the S/MIME encryption features built into Outlook and Apple products.

**Encrypting email with Outlook**



Before you start sending secret admirer notes on Outlook, a couple requirements stand in your way. The first is that **you must have a digital certificate**. If you don’t already have a digital certificate, either one you created or from your organization, then you’ll need to create one:

* Go to **File > Options > Trust Center > Trust Center Settings > Email Security, Get a Digital ID.**
* Choose which certification authority you want to receive a digital ID from (we recommend **Comodo**).
* You will receive your digital ID in an email.

Now that you have a digital certificate/ID, follow these instructions to get it into Outlook:

* Select **Tools > Options** and click the **Security** tab
* Input a name of your choice into the **Security Settings Name** field
* Make sure **S/MIME** is selected on the **Secure Message Format** box
* The **Default Security Setting** should be checked
* Under **Certificates and Algorithms**, go to the **Signing Certificate** section and click **Choose**
* In the **Select Certificate** box, choose your **Secure Email Certificate** if it hasn’t been selected by default
* Check **Send these Certificates with Signed Messages**
* Click **OK** to save your settings and return to Outlook

Okay, so now you’ve got a digital signature to put on your emails, but they won’t appear by default. To attach your digital signature:

* Click **New Message**
* Go to **Tools > Customize** and click the **Commands** tab
* In the **Categories** list, choose **Standard**
* In the **Commands** list, click **Digitally Sign Message**
* You can click and drag the listing onto your toolbar, so from now on just click that to add your digital signature
* While we’re at it, click and drag **Encrypt Message Contents and Attachments** onto the toolbar as well

At this point we want to remind you that **digitally signing an email is not the same as encrypting it**. However, if you want to send someone an encrypted message on Outlook, that person needs to have sent you at least one email with his or her digital signature attached. This is how Outlook knows it can trust the sender.

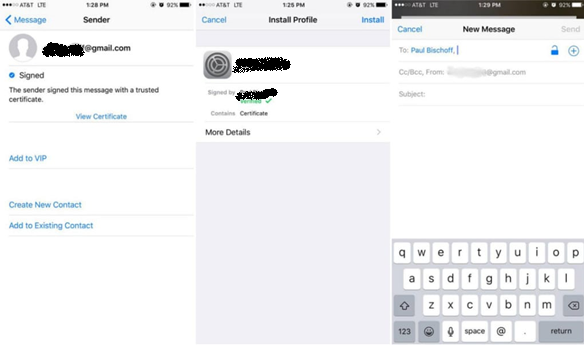
Conversely, if you want to receive an encrypted email from someone else, you will need to send them one unencrypted email first with your digital signature on it. This is a tedious downside to S/MIME. You can digitally sign your email just by clicking the new Sign button before sending.

Now that you have each other’s digital signatures and certificates saved into your respective key chains (address books), you can start exchanging encrypted emails. Just click the **Encrypt** button that we added before hitting send, and that’s all there is to it!

**Encrypting email on iOS**

S/MIME support is built into the default email app on iOS devices. Go into the advanced settings, switch S/MIME on, and change Encrypt by Default to Yes. Now when you compose a new message, lock icons will appear next to recipients’ names. Simply click the lock icon closed to encrypt the email.

iOS consults the global address list (GAL), a sort of keyserver for S/MIME certificates, to find contacts in your exchange environment. If found, the lock icon will be blue.



You’ll probably notice a red lock icon next to some recipients’ email addresses. This means they are either not in your exchange environment (e.g. you don’t work at the same company) or you haven’t installed that person’s certificate, and you cannot send them encrypted messages. In this case, the process is similar to Outlook above.

That person needs to send you at least one email with a digital signature attached. The option to attach signatures to your emails by default is found in the same advanced settings menu as the encryption options.

When you receive that email, do the following:

* Click the sender’s address
* A red question mark icon will appear indicating the signature is untrusted. Tap **View Certificate**
* Tap **install**. When done, the install button will change colors to red and say “Remove.” Click **Done** on the top right corner.
* Now when you compose a message to that person, the lock icon will be blue. Tap it to close the lock and encrypt your message.

**OSX email encryption**

To send encrypted messages in the default mail program in Mac OSX requires the same condition as iOS and Outlook: you must first have the recipient’s digital signature stored on your device. When you compose a message and type in the recipient’s email, a checkmark icon will appear to show the message will be signed.

Next to the signature icon, a lock icon also appears. Unlike iOS where you can select which recipients will receive encrypted email and which don’t, OSX is an all-or-nothing affair. If you don’t have the certificate for all of the recipients, the email cannot be encrypted.

Remember to sign emails only after you’ve finished writing them. If it’s been altered, the certificate will show up as untrusted.

**Android email encryption**

On Android, you’ve got a couple options for how to encrypt your email. The [**CipherMail app**](https://play.google.com/store/apps/details?id=com.djigzo.android.application&hl=en) **allows you to send and receive S/MIME encrypted mail** using the default Gmail app and some 3rd-party apps like K-9. It follows the same certificate rules as what we already discussed above.

The other option is to use PGP/MIME, which requires both an email app and a keychain to store certificates.

PGP requires a bit more setup, but you don’t need to receive someone’s digital signature in advance to send them encrypted email.

[**OpenKeychain**](https://play.google.com/store/apps/details?id=org.sufficientlysecure.keychain) **is a simple and free keychain tool for storing other people’s certificates and PGP public keys.** It works well with K-9 Mail, but some other email apps might also be compatible.

In OpenKeychain, you can create your own public and private keys. Input your email address, name, and password, and it will generate these keys for you. If you have an existing key, you can import it. To use a generated key with other devices and apps, you may export it.

OpenKeychain also helps you search for other people’s public keys online so you can send them encrypted email. After you’ve added someone’s public key to your keychain, they will be saved for more convenient use later.

To use OpenKeyChain with an email app, go into the email app’s settings and make OpenKeyChain your default OpenPGP provider.

This process varies from app to app, but it should just take a bit of digging through settings menus to find it. Not all email apps (including Gmail) will support encryption, however.

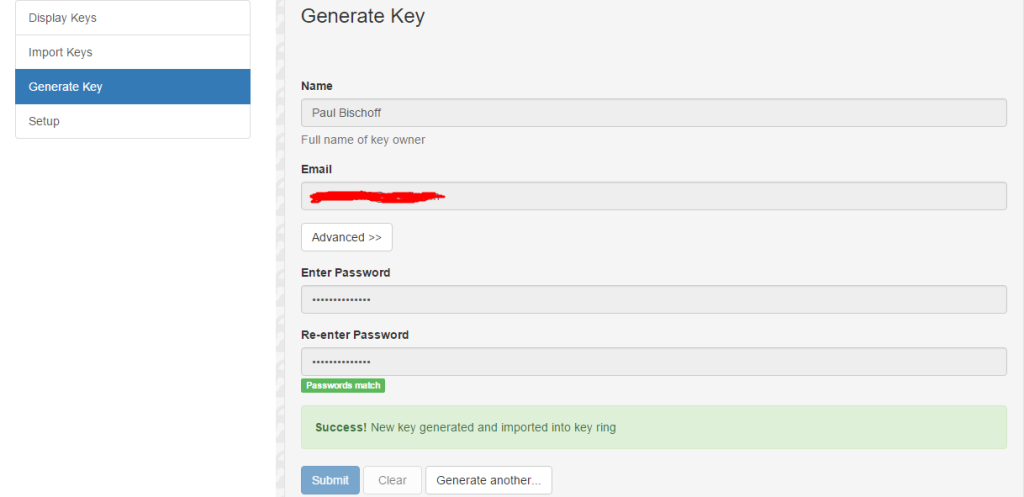
**Webmail encryption (Gmail)**

For web-based email clients like Gmail, we recommend a PGP/MIME encryption solution, as they are far easier to incorporate than S/MIME. For the purposes of this tutorial, we’re going to use a Chrome extension called[**Mailvelope**](https://www.mailvelope.com/)with Gmail.

Most browser extensions work in a similar manner, however, and follow the same basic principles. You can also consider **EnigMail, GPGTools, and GNU Privacy Guard**.

To get started, install the extension and open the options menu. Start by generating your own key: enter a name, email, and password and click Generate.

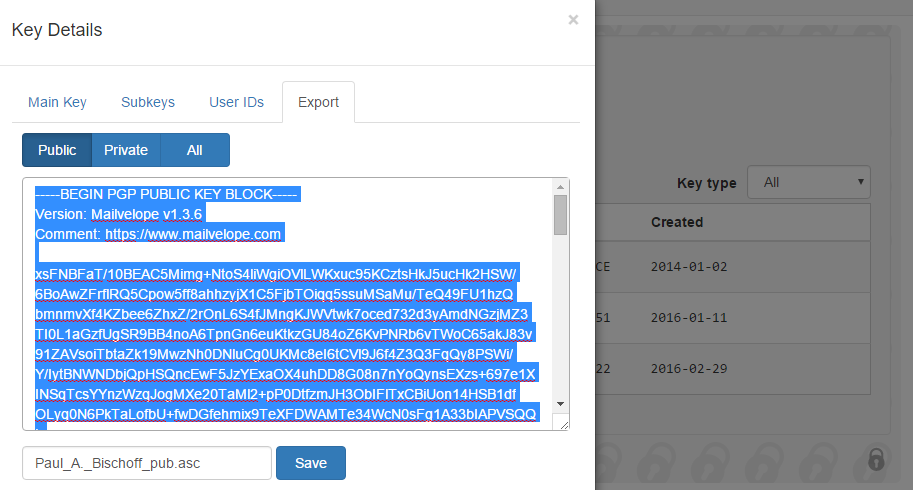
Most email encryption extensions come with a built-in key generator and key ring. If you already have a key, just select the option to import it via copy and paste.



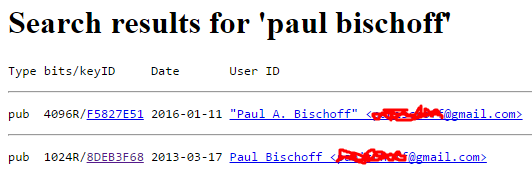
Now you’ve got an encryption key, but it doesn’t do much good if no one can find your public key to send you encrypted mail. You can **upload your public key** to a keyserver.

We suggest MIT’s keyserver because it’s popular, free, and easy to use.

1. In the Mailvenvelope **settings**, navigate to **Display Keys** and click on the one you just made.
2. Go to **Export** to see the plain text of your public key. Copy it to your clipboard.

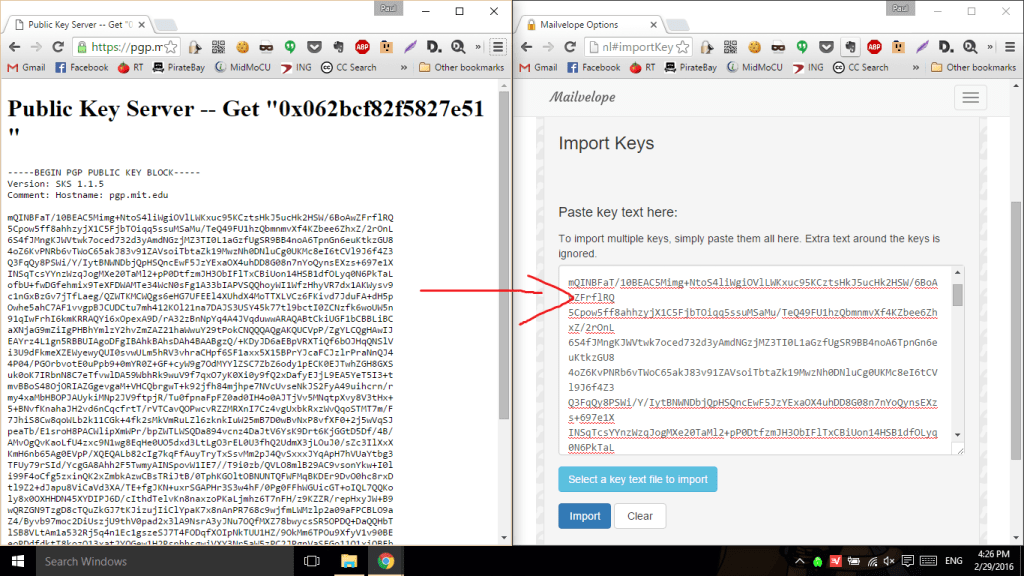


1. Head to the [MIT PGP Keyserver](https://pgp.mit.edu/) and paste your key into the “Submit a Key” field and hit submit. Now go back to the MIT keyserver homepage and search the name you entered. You should see your key listed.



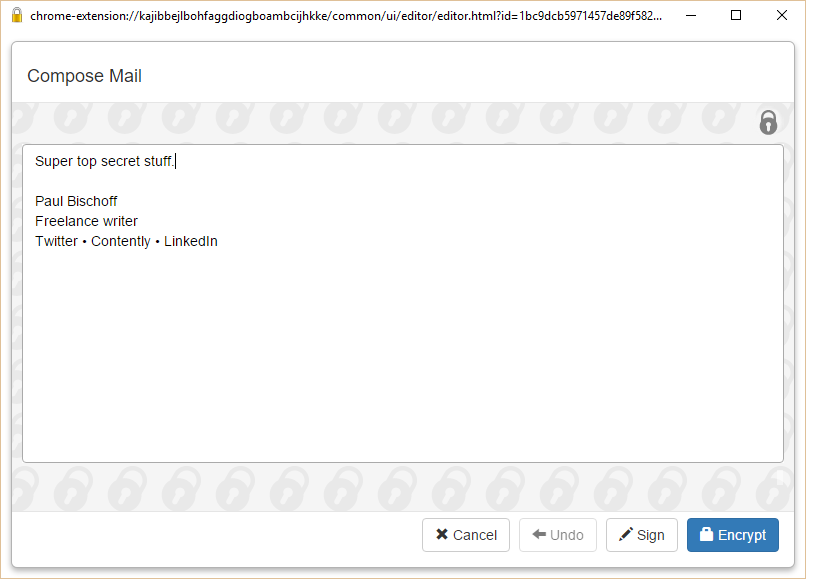
Take note of the **key ID**, which is displayed both in the Mailvelope settings and on the MIT listing. This is useful if you have the same name as someone else on the keyserver because it serves as a unique identifier. Journalists, for instance, often publish their key ID onto their online profiles and social media so sources know for certain that they are emailing the right person.

While we’re on the MIT keyserver site, you can use it to search for the public keys of others. Click on the key ID of the person you are searching for to display the plain text of their key. Copy it and paste it into the “import” section of Mailvelope to add it to your keyring.

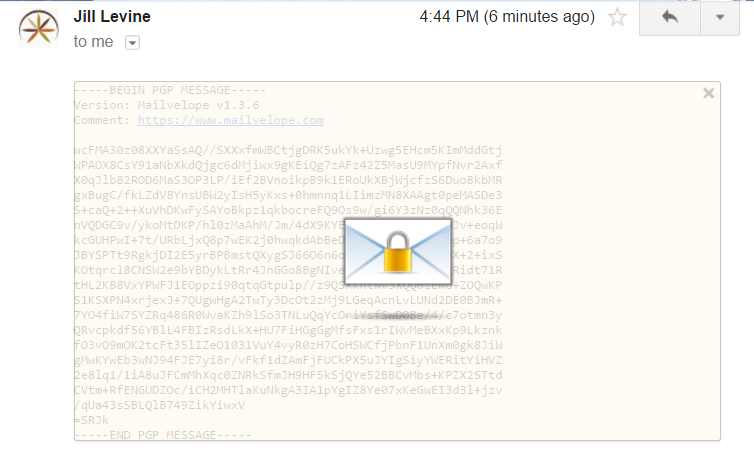


Now that you’ve added recipients to your key ring and made your own public key available to others, you can start sending and receiving encrypted mail. Mailvelope adds a button to the Gmail composer that opens another window where you can type out the message you want to encrypt.

When you’re done, hit the encrypt button, choose the recipient, and transfer the encrypted text into the email. You can add unencrypted text in the email as well, but don’t tamper with the encrypted text.



When you receive an encrypted email, the browser extension you chose should automatically recognize it and offer to decrypt it. The recipient will need an extension or some sort of PGP decryptor app on their end. In Mailvelope’s case, I just click the icon that appears hovering over the encrypted text, enter my password, and voila!



The downside to Mailvelope, and indeed most web-based encryption extensions, is that **they don’t encrypt attachments**. You can use Gnu Privacy Guard to encrypt attachments with PGP before uploading them, which allows you to encrypt using the same key pair. Or you can opt for any one of these [file encryption apps](https://www.comparitech.com/blog/cloud-online-backup/6-apps-to-encrypt-your-files-before-uploading-to-the-cloud/).

**Burner email addresses**

Encryption only hides the content of the message, not the sender’s email address. For any number of reasons, a time may come when you need to send an email anonymously to hide your identity. To do this, a few burner email services will give you a temporary “fake” email address.

[Guerrilla Mail](https://www.guerrillamail.com/inbox) is our top choice. You can set up a disposable email address from which you can send and receive messages. It includes a password manager so you don’t have to memorize passwords for multiple burner accounts. Best of all, it’s completely web-based with no registration required, which makes hiding your identity that much more effective.

[Zmail](http://zmail.sourceforge.net/) is another solid option for sending fake email if you prefer a desktop client rather than a web app.

**Best practices for protecting your email**

Nine out of 10 viruses that infect computers come from email attachments. No level of encryption will protect you from being careless. It’s therefore very important to scan all email attachments before opening them, especially from senders you don’t recognize. Viruses disguised as Microsoft Office documents are especially common. Many email clients, including Gmail, will automatically scan attachments for you, but others will require you do so manually.

Don’t click on links in emails from unreliable sources. In fact, just don’t open emails altogether if they don’t look trustworthy. A spam blocker will go a long way toward avoiding these.

If you email a large group of people, use BCC so spammers can’t get a hold of the list.

Conversely, if someone includes you in a long list of CC’ed email addresses, don’t hit “reply all” without carefully considering the alternatives.

Finally, set a strong password on your email account. Read through our guidelines if you’re not sure [what constitutes a strong password](https://www.comparitech.com/blog/information-security/how-to-create-a-strong-password/)  or use a [password strength checker](https://www.comparitech.com/privacy-security-tools/password-strength-test/) if you’re still unsure how strong yours is.

**Related:** [Cyber security statistics](https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/)

**Alternative email encryption apps**

If fiddling with certificates and key pairs sounds like too much trouble, you can use an off-the-shelf encrypted email client.

[Tutanota](https://tutanota.com/) is one such secure email service, with apps for mobile and a web mail client. It even encrypts your attachments and contact lists. Tutanota is open-source, so it can be audited by third parties to ensure it’s safe. All encryption takes place in the background.

[Hushmail](https://www.hushmail.com/personal/) is a paid web-based email client that allows you to send encrypted email to anyone even if recipients don’t have any email decryption tools. Recipients will receive an email notification to let them know they need to visit the Hushmail site, enter the code provided in the notification, and then correctly answer your challenge question. Check out our full tutorial on [how to use Hushmail](https://www.comparitech.com/blog/information-security/how-to-use-hushmail-to-encrypt-your-email/).

While we can vouch for Tutanota and Hushmail, it’s worth mentioning that there are a lot of email apps out there that claim to offer end-to-end encryption, but many contain security vulnerabilities and other shortcomings. Do your research before choosing an off-the-shelf secure email app.

**Be wary of encrypted email apps that don’t use S/MIME or PGP/MIME**

Many apps and email services out there promise email encryption but don’t use S/MIME or PGP/MIME. These are indeed much easier and faster to set up, but be aware that they roll their own encryption and may not strive for the same privacy standards. SafeGmail and Virtru are examples of these, and we don’t recommend them.

We encourage you to upload your public PGP key to a keyserver, but it’s not required. Instead, you can just send the plain text of your public key to the person(s) that you want to receive encrypted emails from.

Email encryption provides a secure means of sending messages containing sensitive material as well as a means for others to send you sensitive material. [Journalists use it](https://www.comparitech.com/blog/vpn-privacy/protection-of-journalistic-sources/) to correspond confidentially with sources. Businesses use it to relay trade secrets and classified documents. Lawyers use it to keep sensitive client and case information safe. You get the idea.

In our opinion, email encryption is something you should have readily available when the need arises, but it’s not necessary for everyday communication.

**How to Encrypt Email (And the Best Encrypted Email Services)**

Despite being one of our oldest methods of online communication, email is still one of the most popular. Untold billions of email messages fly around the world every day, carrying personal and business messages that we depend on, making email a prime target for snoops and spies of all types.

Unfortunately, experience shows that most **large email providers** **do not respect the privacy of your inbox**. For example,

* **Gmail** was caught giving [third parties full access](https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442) to user emails and also [tracking all of your purchases](https://www.cnbc.com/2019/05/17/google-gmail-tracks-purchase-history-how-to-delete-it.html).
* Advertisers are [allowed to scan](https://thenextweb.com/insider/2018/08/29/both-yahoo-and-aol-are-scanning-customer-emails-to-attract-advertisers/) **Yahoo** and **AOL** accounts to “identify and segment potential customers by picking up on contextual buying signals, and past purchases.”
* **Yahoo** was also caught [scanning emails in real-time](http://news.trust.org/item/20161004170601-99f8c) for US surveillance agencies.

And the problem runs deeper than the policies of your email provider.

**Where your email service is located** can have a huge impact on your email privacy. While jurisdictions like Switzerland have laws that protect your online privacy, others (unfortunately including the United States and its [Five Eyes](https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/) friends) have laws in place to erode it.

Leaving aside all the folks who can legally stick their nose into your email communications, there are also the illegal peeping Toms. While email services take steps to protect your messages from outsiders (aside from themselves), these **steps are not foolproof**.

Data breaches do result in crooks getting their hands on the passwords of email accounts, which can result in [identity theft](https://restoreprivacy.com/identity-theft-fraud/), fraud, and other crimes. Hackers do manage to get access to people’s inboxes. If some creep gets access to your inbox, there is nothing to stop them from reading your email and stealing all that juicy personal information.

As you can see, **email security is a big issue** today. There are a lot of different ways in which your email privacy can be compromised. In this post we’ll talk about various scenarios in more detail, and I’ll show you how to encrypt your email to protect against at least some of these problems.

**Why is email encryption important?**

Once you see the scope of the problem, we think you’ll agree that you need to encrypt at least some of your emails.

**Data breaches** – Breaches of the databases at companies large and small [expose hundreds of millions](https://restoreprivacy.com/cyber-security-statistics-2020/), if not billions of records per year. Some unknown number of those records are email messages, stored on mail servers around the world. Bad guys of all stripes target email messages because they can contain valuable information that can be sold or used for fraudulent activities. Financial data, vacation plans, corporate strategies, and personal data are all juicy targets.

**Pervasive surveillance** – Years ago, Snowden and others revealed the [vast scope of surveillance programs](https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013–present)) (many of at best marginal legality) that are being run around the world. Since then, the problem has only grown, with governments around the world sucking up every bit of email data they can get their hands on. Private companies are in on the act too, who may collect and sell your email content, or use it to target you with heads.

Because most email services store your data on their servers in unencrypted form, you have no real privacy. Hoping that big providers of free email services like Gmail won’t read your messages and use what they find for their own purposes, is foolish in the extreme.

We know that Gmail, for example, reads through every message you send or receive looking for information like airline reservations to add to your calendar. Then there is [Smart Reply](https://www.theverge.com/2019/4/5/18296953/how-to-enable-use-gmail-smart-compose-smart-reply-auto-response), an optional feature that reads messages so it can suggest short replies that might be relevant to the content of that message. While features like these can be useful, they can only work if Gmail can read and understand (at least a little bit) your email messages.

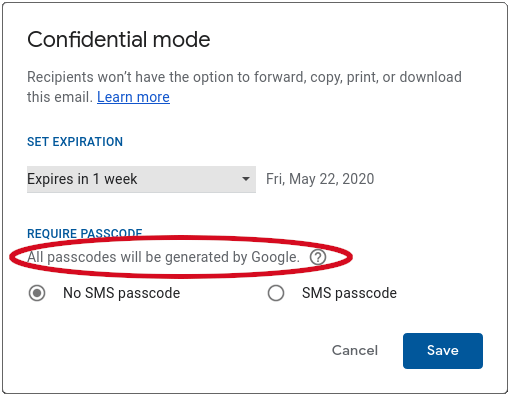
**How can you protect your email messages?**

There are a few approaches you can take to protecting your email messages from being read by the wrong people. The easiest solutions are ones where the email provider makes sure that only the intended recipient can read the messages you send.

**Gmail’s Confidential mode**

Gmail’s [Confidential mode](https://support.google.com/mail/answer/7674059?co=GENIE.Platform%3DDesktop&hl=en) is an example of an approach where the email provider makes sure that only the intended recipient can read messages. Beyond controlling access to the message, Confidential mode **restricts what the recipient can do with the message** (no forwarding, etc.), and causes the message to be inaccessible after a set amount of time. This sounds good, so let’s keep going with it.

To use Confidential mode, you compose your message normally. When you are ready to send the message, you select **Confidential mode**. Gmail displays the following dialog box:



This looks promising. For someone to read the message, they will need to enter the passcode. But there are a couple of drawbacks to this approach.

First is that passcode. Note the sentence circled in red, “All passcodes will be generated by Google.” In other words, **Google is in control of the code** that gives access to the message, not you, and not the recipient.

Second is the fact that selecting Confidential mode **doesn’t hide the contents of your message from Google**. Confidential mode protects your mail from everyone **except** Google. It doesn’t create an encrypted email message. It simply prevents someone from seeing the message unless they enter the password. A solution like this is only useful if you don’t mind your email provider continuing to have access to your email.

If you really want to protect the privacy of your inbox, you can’t rely on solutions like Confidential mode. It is time to talk encryption.

**About email encryption**

If we start talking about the details of various ciphers and encryption algorithms we’ll be here for a very long time… and your email may never get encrypted. So we’re going to try to keep this discussion at a high level.

To protect your email against any and all of the attackers we discussed at the top of this article, we need to use something called end-to-end encryption. This is often abbreviated as E2E encryption (or even E2EE).

**Why use E2E encryption with email**

E2E encryption means that you encrypt something (email in our case) on your computer or mobile device, and the recipient decrypts it on their computer or mobile device. Why is this important?

Think about how an email message gets from you to the recipient. You create the message in some email program. When you hit **Send**, the message passes out of your computer onto a connection controlled by your Internet Service Provider (ISP). The message then goes to your email provider, who passes it along another connection controlled by some other service, and so on. Eventually, the message arrives in the recipient’s inbox at their email provider. Then it goes through another set of connections controlled by other entities until it ends up on the recipient’s computer to be read.

That’s an awful lot of steps. At any one of those steps it is theoretically possible for someone to try to read your email.

E2EE solves this problem. Done right, no one read encrypted messages except the sender and the recipient.

If you encrypt your email before it leaves your device, and the recipient decrypts it once it arrives on their device, no one in the middle will be able to read it.

Since E2E encryption is the way to go, we’ll show you one way you can do it. But first we have to discuss…

**The drawbacks of E2E encryption**

While E2E encryption is the only way to protect your email from the various threats out there, it does have some real drawbacks, such as:

* It is more complicated than just sending email the old way. You’ll see what we mean in the next section.
* The people who receive encrypted emails need to know what to do with them. This too will become clear shortly.
* The powers that be don’t much like any kind of encryption. Encryption makes it harder for governments and law enforcement to spy on you, corporations to earn money from your personal data, and social media companies to censor you.

**How to encrypt email**

There are two ways to E2E encrypt email. On the assumption that you are not prepared to change email services right now, we are going to talk about how you can E2EE the bodies of your emails before letting providers like Gmail and company see them.

**Recommended**: The alternative approach is to **switch to a secure email provider** that respects your privacy and **builds E2E encryption right into their product**. For more on this approach, check out our review of the best [private and secure email providers](https://restoreprivacy.com/private-secure-email/).

**How email encryption works**

The essence of the process is that regular readable text (also called [plaintext](https://simplicable.com/new/plaintext-vs-cleartext)) gets converted into encrypted text (also known as ciphertext). The “key” to the encryption process is that the algorithms use an encryption key to turn plaintext into ciphertext.

Likewise, the decryption algorithm that turns ciphertext back into plaintext depends on a decryption key.

Encrypting an email message turns the body of the message into **ciphertext**. Some encryption approaches also encrypt additional parts of the message, possibly including the subject line and/or any attachments.

However, certain parts of the email need to remain unencrypted. For example, the email address of the recipient cannot be encrypted if you want the message to actually arrive at its destination! Other metadata is also readable, one of the key drawbacks of email in general (but we’ll discuss more secure alternatives below).

**Symmetric vs asymmetric encryption**

There is one more aspect of how encryption works that you need to know about before we can move forward. Remember that we said turning your message into ciphertext requires an encryption key, and turning it back into plaintext requires a decryption key.

The relationship between the encryption key and the decryption key can be either symmetric or asymmetric. In [symmetric-key encryption](https://en.wikipedia.org/wiki/Symmetric-key_algorithm), the encryption key and the decryption key are identical or related by a simple transformation. In effect, the encryption/decryption key pair is a secret shared between the sender and the recipient.

To send a message using symmetric key encryption, the sender encrypts the message using their copy of the secret key and the recipient decrypts it using their copy of the secret key.

In [asymmetric-key encryption](https://en.wikipedia.org/wiki/Public-key_cryptography) (more commonly known as public-key encryption) the relationship between the encryption and decryption keys is much more complex. Each person has both a public key and a private key.

The public keys can be shared publicly and are used to convert plaintext to ciphertext. The private keys are kept secret, and used to convert ciphertext back into plaintext.

With asymmetric-key encryption, there is no need for a shared secret. Both parties publish their own public keys and keep secret their own private keys.

To send a message using asymmetric key encryption, the sender encrypts the message using the recipient’s public key and the recipient decrypts it using the recipient’s private key.

**Pros & cons of encryption methods**

As you might expect, each approach has pros and cons.

**Symmetric-key encryption** is easier to implement, and generally faster to encrypt/decrypt messages, but require the sender and receiver to somehow agree on an encryption key and share it (securely). This could require a phone call, face-to-face meeting, or some other creative methods.

**Asymmetric-key encryption** is more complicated, in that it needs some system for discovering the public key of a person you want to communicate with. [Certificate Authorities](https://en.wikipedia.org/wiki/Certificate_authority) issue digital certificates that certify that a particular public key is owned by a particular person.

Certificate Authorities need to be trusted services for this approach to work, but they make it possible to send encrypted messages to someone you have never communicated with before.

**How to encrypt email using InfoEncrypt**

There are several tools out there for encrypting email messages. Some only work on a particular [operating system (OS)](https://www.britannica.com/technology/operating-system). Others only work in conjunction with specific email programs.

In the interest of presenting something that anyone can use on any OS, with any email program, without making this post truly enormous, let me present [Infoencrypt](https://www.infoencrypt.com/).



As you can see, InfoEncrypt is a free, browser-based encryption service that lets you encrypt any text using the AES 128 encryption algorithm. You can use InfoEncrypt on any device, with any browser that supports [Javascript](https://en.wikipedia.org/wiki/JavaScript).

**Note**: You probably wouldn’t want to rely on a free web service if you are trying to secure data from powerful adversaries. However, this service should be fine for protecting the contents of your email from run-of-the-mill hackers and similar snoops.

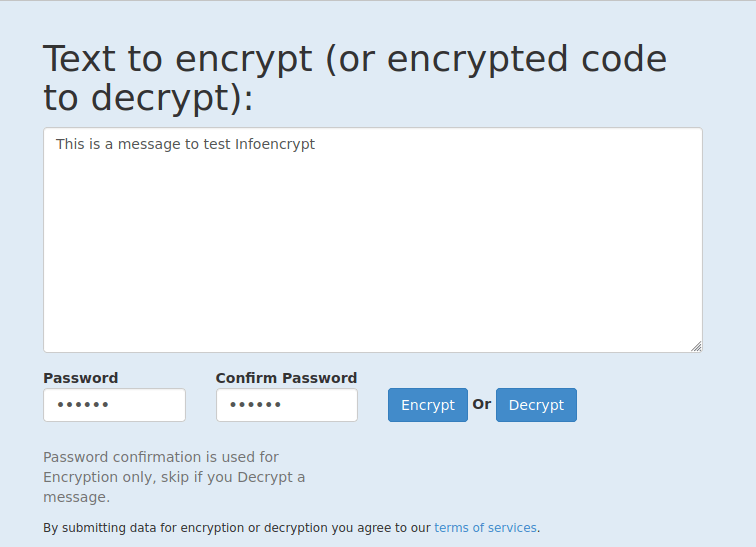
**AES 128** is a **symmetric-key encryption** algorithm that is fast and efficient, yet secure. Because it is symmetric-key, you will need to find a secure way to share the encryption key with the recipient.

Let’s see how this works. In this example, a secret information source (the sender) will encrypt a short message using InfoEncrypt, then email it to me (the recipient).

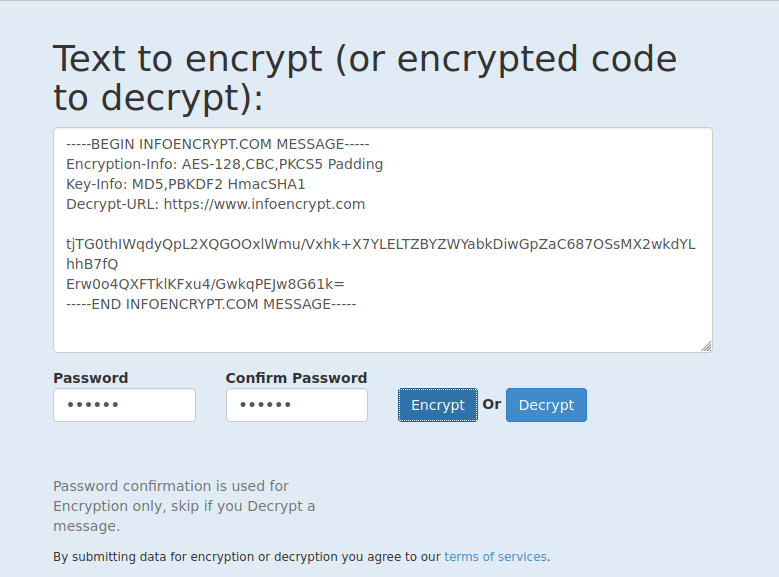
Since the sender and I have already shared the encryption key (the password), I will be able to use that key to decrypt the text of the message using InfoEncrypt.

Follow along to see how to encrypt email and decrypt it on the receiving end using InfoEncrypt:

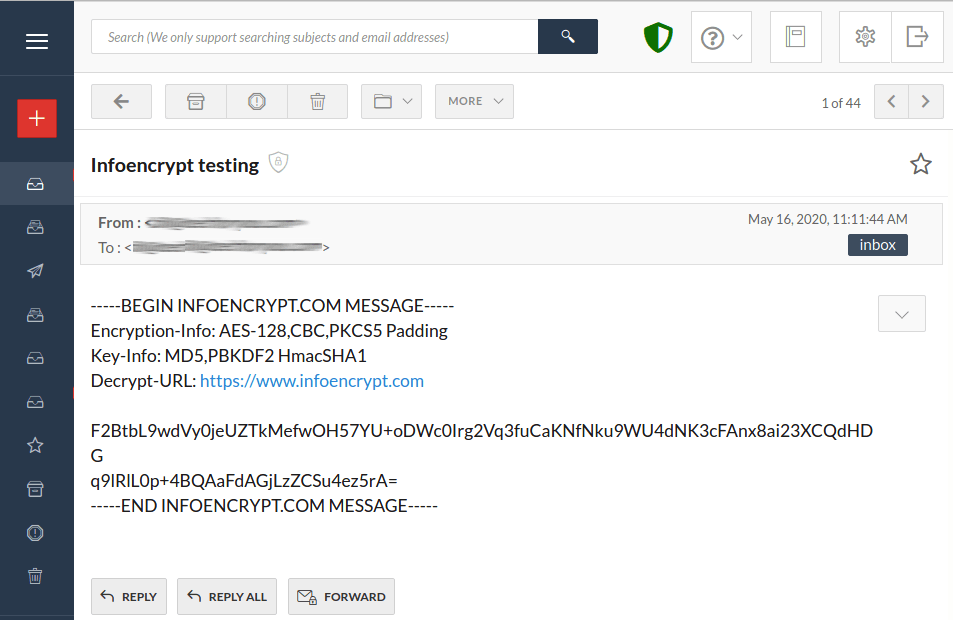
1. The sender goes to **InfoEncrypt.com**, then scrolls down to the Text to encrypt (or encrypted code to decrypt) box.
2. The sender enters the text they want to encrypt, then enters a strong **password** into the Password and Confirm Password boxes.



1. The sender clicks the **Encrypt** button. InfoEncrypt uses AES 128 and the password to encrypt the message. It replaces the plaintext with something like the following, which is both the ciphertext generated from the plaintext and some additional information that the recipient will need to decrypt the message.



1. To send the encrypted message to the recipient, the sender copies the entire contents of the “Text to encrypt…” box, pastes it into the body of the email message, then sends it like any other email message to the recipient.
2. When the recipient opens the message, the body of the email will contain the contents of the “Text to encrypt…” box:



1. The recipient then reverses the process by copying all the text beginning with, “—–BEGIN INFOENCRYPT.COM MESSAGE—–” and ending with, “—–END INFOENCRYPT.COM MESSAGE—–” and pastes that text into InfoEncrypt.com.
2. The recipient enters the shared password into the Password field then clicks **Decrypt** to see the original message.

Using a tool like InfoEncrypt is clumsy, and takes more steps than you might like, but it is an easy, free, and broadly useful way to send encrypted text by email without having to install new software, change email services, or anything like that.