How to encrypt Gmail, Outlook and other webmail

Email account is very important. They hold the key to entering the digital 'kingdom' as well as the personal information of each user. Today's article will show you how to encrypt Gmail, Outlook.com and other webmail accounts.

Encryption plays a very important role for privacy and security. User privacy is under constant threat from social networks, governments, businesses and many other factors. Therefore, encrypting web traffic and email accounts is an important step to regain the privacy that was there decades ago.

Email account is very important. They hold the key to entering the digital 'kingdom' as well as the personal information of each user. Today's article will show you how to encrypt Gmail, Outlook.com and other webmail accounts.

How to secure email in Gmail, Outlook and other webmail?

Which encryption is best for webmail protection?

Before considering encryption tools, it is important to understand what type of encryption is available when using Gmail, Outlook.com or other webmail services. Users will use symmetric or asymmetric encryption to protect their data. But what do they mean?

Asymmetric encryption is the most common type of encryption found on the Internet today. An asymmetric encryption tool consists of two separate keys: **Private key** (**private key**) and **public key** (**public key**). Public key allows people to encrypt private messages for you. When the messages are encrypted to the inbox, you decrypt it with private key. Unlike public key, private key must always be secure. If someone gets it, they can unlock your emails. This asymmetric encryption method is also called **Public key cryptography** .

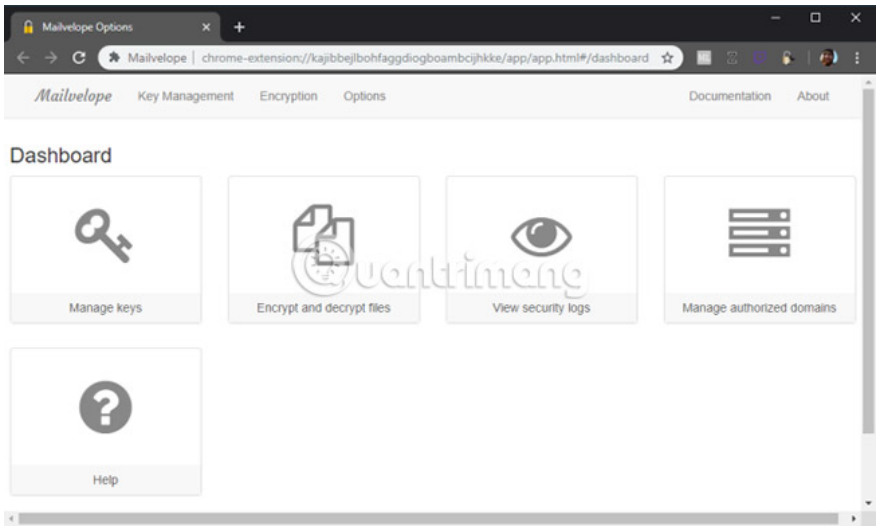
Symmetric encryption is a very secure but simpler encryption method. Basically, users encrypt their messages with a unique cryptographic key and the recipient cannot unlock the email without that key. Symmetric encryption is also called **Secret key cryptography** .

Both types of encryption have their advantages and disadvantages.

Encrypt email in webmail

The article will list some of the best webmail encryption tools, the right place to use them, and how they help send encrypted email.

1. Mailvelope



Mailvelope is still one of the best and simplest webmail encryption tools. It uses asymmetric encryption to secure email. Browser extension Mailvelope seamlessly integrates with webmail accounts in Gmail, Outlook.com, Yahoo Mail, GMX, mail.ru, Zoho Mail, etc.

Mailvelope works directly from the browser. When downloading the application, the Mailvelope icon will appear along the address bar. Clicking on this icon will give users some options: **Dashboard, Keyring** and **File Encryption.** To get started, follow these steps:

1. Select **Keyring> Generate Key.**

2. Enter the name and email address you want to link to the encryption key. Next, add a secure, unique password, then select **Generate** to create the key.

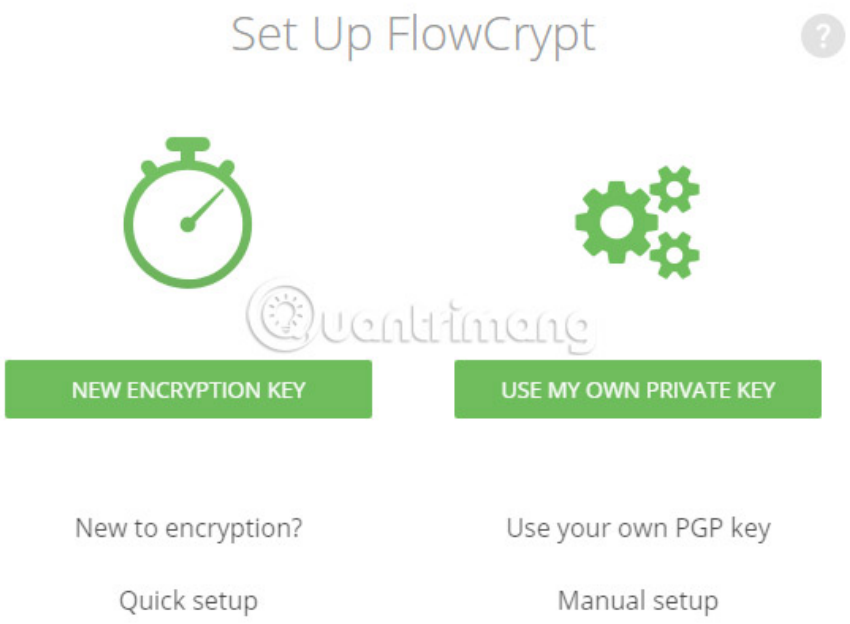
3. Go to the webmail account and authenticate the new key by opening the verification email, as well as confirming the unique password created from the previous section. When decrypting the email, the user can select the verification link.

4. After verification, you receive a link containing a public key. It is a long string of alphanumeric characters. You can share public key with others so they can encrypt email when sent to you.

Users can access public key from the **Keychain** option **.** If you want to send it to someone, locate the key, then select **Export** and one of the **Display Public Key options** or **Send Public Key by Mail** . When the recipient has the key, the user can send them a secure email from his own webmail account.

Download Mailvelope for Chrome | Firefox.

2. FlowCrypt



FlowCrypt is another great encryption option for Gmail users. Like Mailvelope, Flowcrypt seamlessly syncs with Gmail accounts, allowing users to send emails using PGP encryption standards.

When downloading Flowcrypt, select the Flowcrypt icon located along your Chrome address bar. To set up Flowcrypt, do the following:

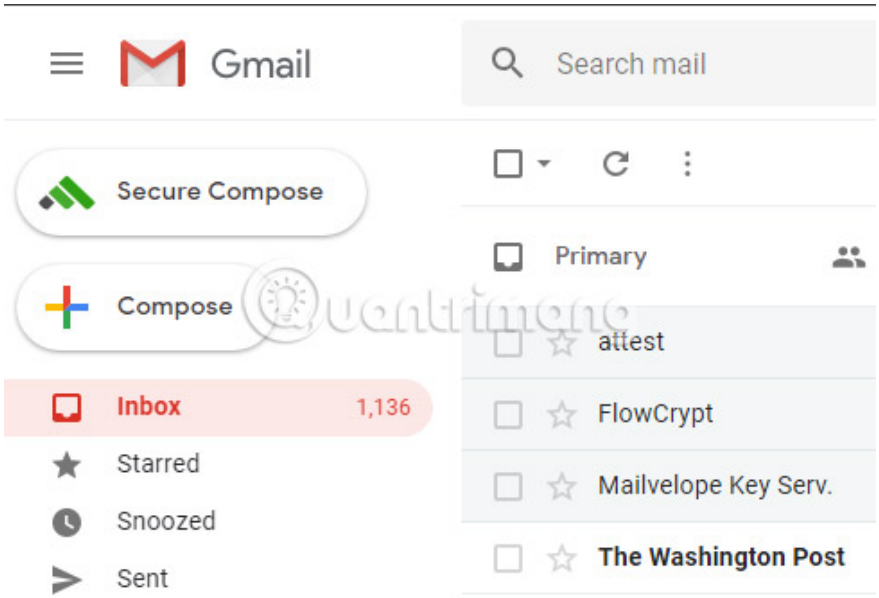
1. Select **Create a new key** .

2. Create a secure passphrase (The passphrase is a series of unique words, using letters, numbers and symbols).

3. Go to Gmail account. Above the usual **'Compose'** button is a new option: **Secure Compose.**

4. Select **Secure Compose** and enter the email content.

A handy FlowCrypt feature is a **PK** button in the lower right corner of the email compose window. The **PK** button adds public key to email so that recipients without FlowCrypt can still read the email.



FlowCrypt is available for Gmail on Chrome, Firefox and Android. In addition, users can use FlowCrypt with any webmail application on their Android device, expanding FlowCrypt's functionality for multiple accounts.

However, FlowCrypt is planning to become an application for Windows, macOS, Linux, iOS, Thunderbird and Outlook. The iOS version will be available in 2019. The development team is looking to expand FlowCrypt's mobile functionality before integrating other webmail services in the future.

Download FlowCrypt for Chrome | Firefox | Android Beta.

3. InfoEncrypt

InfoEncrypt differs from the previous two tools. It uses private key symmetric encryption, instead of public key encryption. That means that instead of sharing a public key to allow people to encrypt messages sent to you, you must sort your password or passphrase before you can send and receive emails securely. InfoEncrypt uses extremely powerful AES-128 encryption algorithm. This is one of the most powerful algorithms available.

InfoEncrypt is extremely simple to use.

1. Go to the website and enter the email content.

2. Enter the unique and secure password you shared earlier with the recipient.

3. Select **Encrypt** and the content will be encrypted.

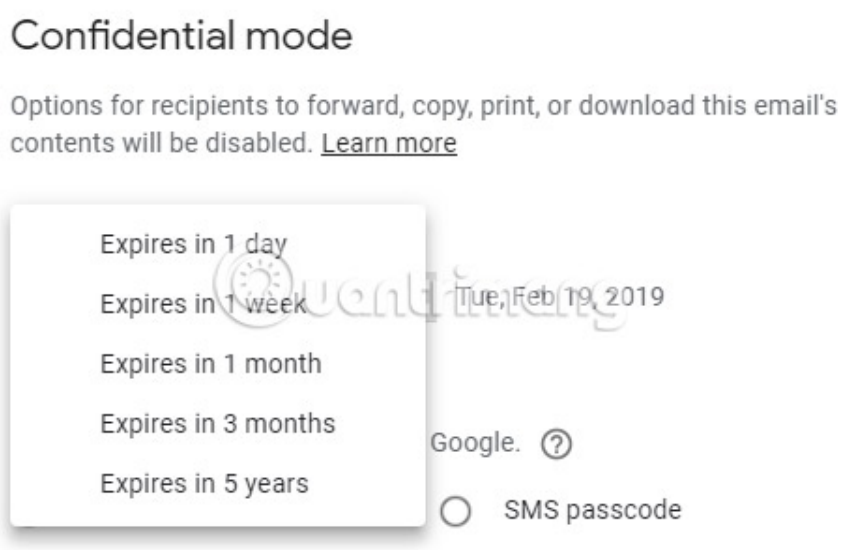
4. Then, copy the ciphertext (that's an encrypted text) into the webmail application and send it.

The recipient will receive the email, copy the content to the **InfoEncrypt** page **,** enter the password and select **Decrypt.**

4. Encryption in Outlook.com

For more details on how to encrypt email in Outlook, please refer to the article: How to encrypt email on Microsoft Outlook.

5. Send and open secret email with Gmail



Gmail recently introduced **'Confidential Mode'. 'Confidential Mode'** is a way of sending secure email in Gmail, using a password and expiring timer. Please note that at this time **Confidential Mode is** not available for users using the G Suite suite.

Here's how to use **Confidential Mode:**

1. Go to **Gmail.**

2. Next to the **Send** button **,** specify **Turn Confidential Mode On / Off.**

3. Change **Confidential Mode** settings **;** set an expiration date and select the user who requires the password to read the email, then select Save.

4. Send email as usual.

Recipients cannot forward, copy or print emails that use **Confidential Mode.** Also, be sure to enter the recipient's phone number if using the password option. If not, they will not be able to open your email!

Mailvelope and FlowCrypt are probably the two best options for fast and secure webmail encryption. InfoEncrypt is very handy, but users need to find a secure password before it is a drawback. Unfortunately, currently there are not many secure webmail encryption tools, focusing on security, privacy and data breaches.

Wish you success in securing your email content!