How to send encrypted email on Android using OpenKeychain

Today's article will show you how to encrypt email on Android using OpenKeychain. The best thing is that OpenKeychain is completely free. Using OpenKeychain for email encryption is quick, easy and effective.

Encryption is very important, especially when you send and receive email on the go. You never know if the free public WiFi connection in use is absolutely safe. Fortunately, you can minimize those risks by 'wrapping' your private emails in an encryption layer.

Today's article will show you how to encrypt email on Android using OpenKeychain. The best thing is that OpenKeychain is completely free. Using OpenKeychain for email encryption is quick, easy and effective.

Encrypt and decrypt email on Android using OpenKeychain

What is encryption?

Encryption is the process of concealing or tampering with information. Encryption uses a complex algorithm called cryptography to turn ordinary data into a string of garbled and unreadable data. When users encrypt their data, no one can read that data until the data is decrypted with a special key.

Encryption is everywhere in modern digital life. Do you use WhatsApp? This application secures users' messages with end-to-end encryption. Are you logged into online banking? If so, you are using encryption. When you go to a friend's house, do you ask for WiFi password? That's how your friend encrypts and keeps data safe.

You can also use encryption to send email securely from your Android device.

OpenKeychain.org is an open source application that implements OpenPGP encryption standards on Android devices. OpenPGP is an open source version of the PGP encryption standard. Users will find it in hundreds, if not thousands of different applications.

Most modern encoders use asymmetric encryption. Asymmetric encryption uses a system of keys to protect user data.

You have a public key that anyone can know. Someone with this public key can encrypt the message then send it to you. Only you can open it because you have a private key. The private key is linked by password with the public key.

However, you cannot let anyone else know your private key. If not, they can fake your name, read your message, etc.

Encrypt email with OpenKeychain

OpenKeychain makes it easy to use OpenPGP encryption. The process will take place as the sequence below. The article will also show you how to decode an email. Here's how you set up OpenKeychain on your device.

Step 1: Download and install OpenKeychain

First, go to Google Play Store and download OpenKeychain.

Step 2: Configure OpenKeychain user accounts

Next, follow these steps to set up:

1. Launch the OpenKeychain application. The user will come to the initial setup screen. From here, select **Create My Key** .

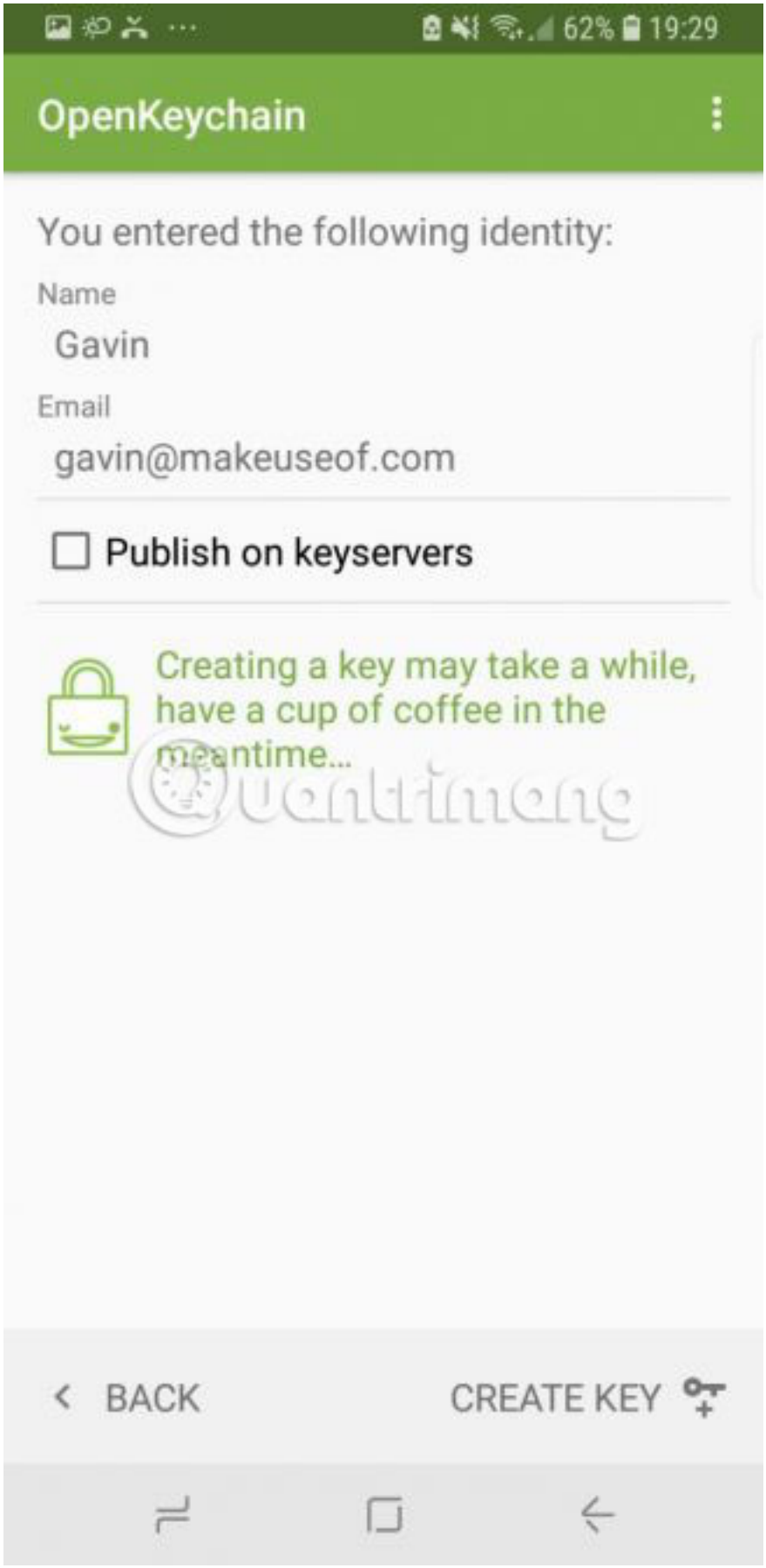
2. Add the name you want to associate with the key. No need to use proper names. Next, add the email address you want to link to the key.

3. On the last page, create the key. Confirm your name and email address, uncheck the **Publish on keyservers option** , then select **Create Key.**


62% 19:28
OpenKeychain
CREATE MY KEY
USE SECURITY TOKEN
(Fidesmo, YubiKey NEO, SIGILANCE, ...)
IMPORT KEY FROM FILE
SECURE WIFI TRANSFER
SKIP SETUP


62% 19:28
OpenKeychain
Choose a name associated with this key. This can be a full name, e.g., 'John Doe', or a nickname, e.g., 'Johnny'.
Full Name or Nickname
BACK
NEXT


57% 20:10
Manage my keys
Enter your main email address used for secure communication.
Email
Add additional email address
BACK
NEXT


62% 19:29
OpenKeychain
You entered the following identity:
Name
Gavin
Email
gavin@makeuseof.com
Publish on keyservers
Creating a key may take a while, have a cup of coffee in the meantime...
BACK
CREATE KEY

The application will indicate that key generation may take a while. However, often OpenKeychain creates encryption keys very quickly.

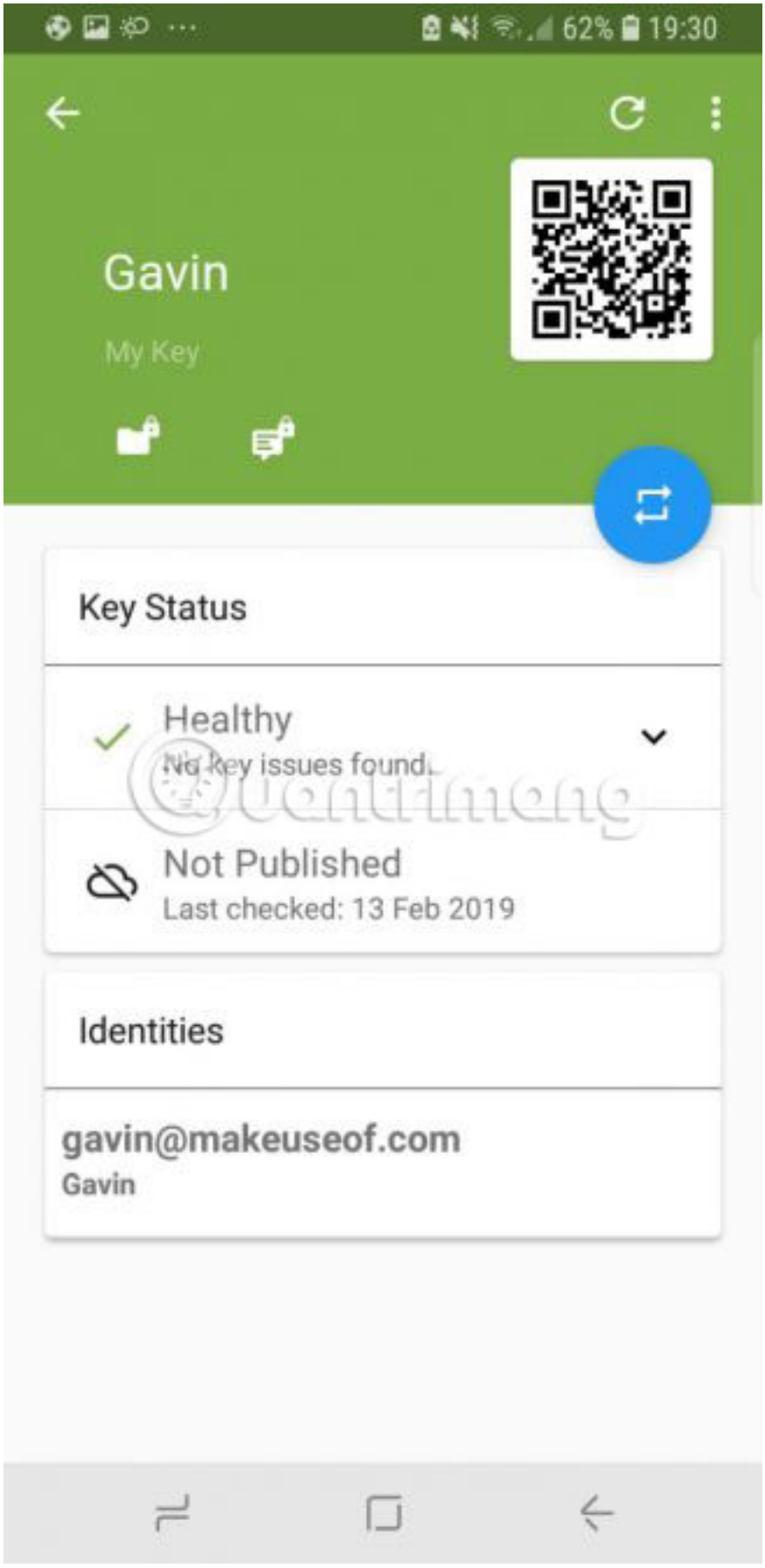
Now, users can view the key management section in the OpenKeychain user account. From here, users can share their keys with links or QR codes, encrypt and send files or email, export keys on keyserver and more.

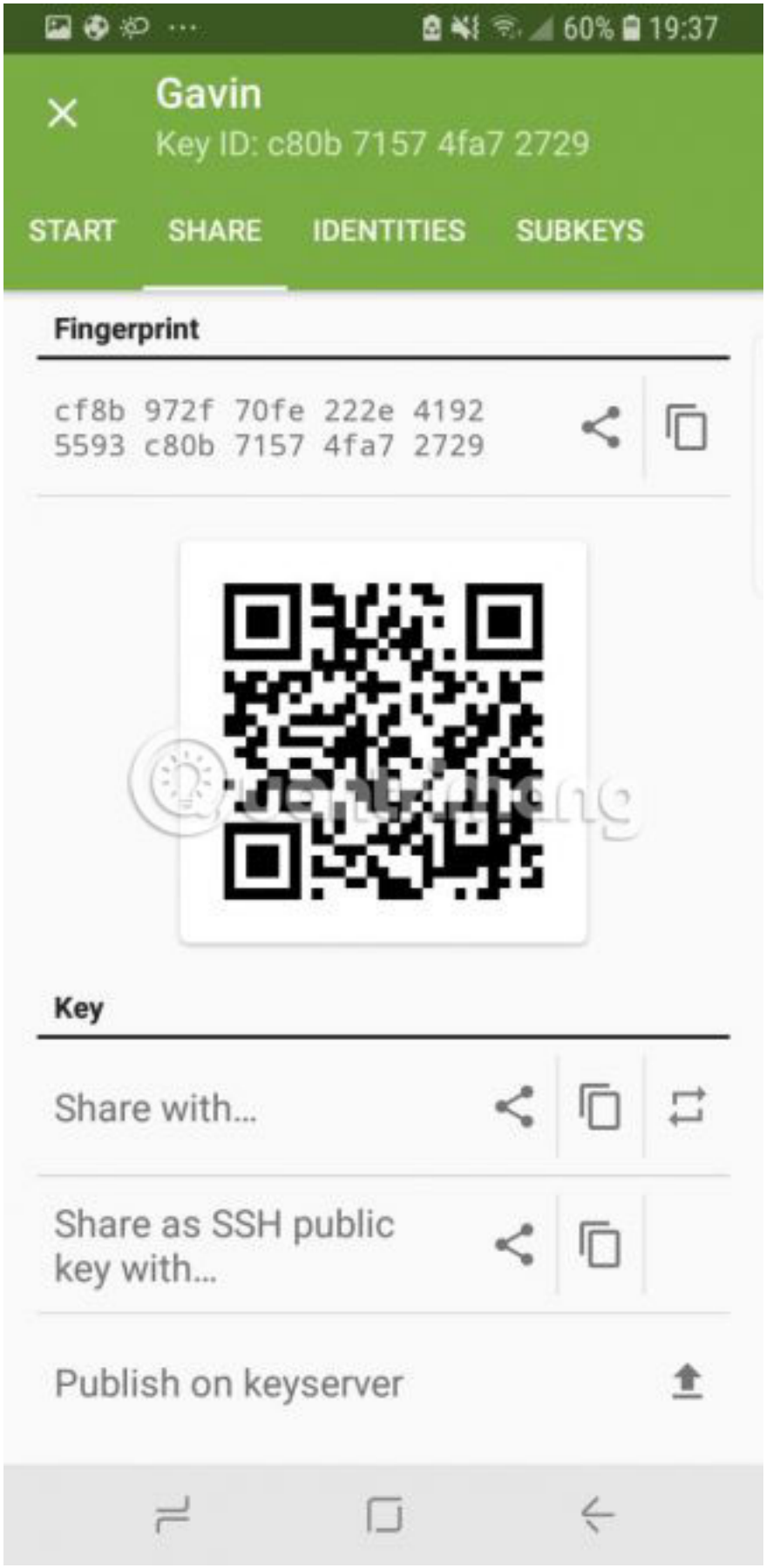
Step 3: Share the public key

The next step is to share the public key with the recipient. If not, when you email them, they will not be able to decrypt it. There are several ways to share keys with OpenKeychain. Here are two easiest ways.

1. First, from the main account page, select the **Settings** menu **icon** (three dots) in the upper right corner, then select **Advanced.** Switch to the **Share** tab **.** Here, you will see QR codes that can be shared. If at the same location as the recipient, they can scan the QR code with their encryption application to automatically enter your key.

2. If they cannot scan the code or are not nearby, you can use the Android sharing function. On the same page, in the **Key** section **,** select **Share with.** You can now share your key with any option on your Android device.

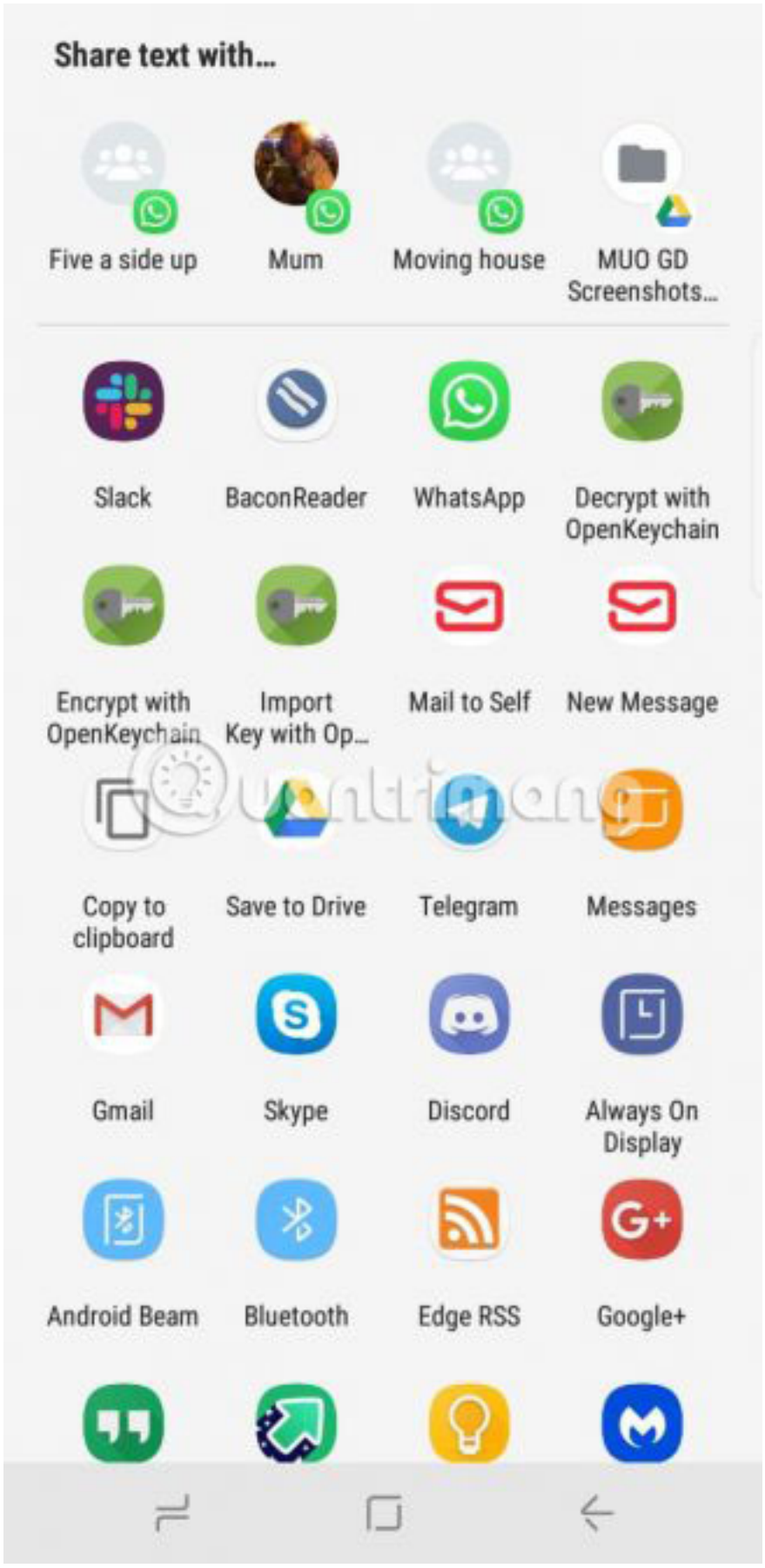

62% 19:30
Gavin
My Key
Key Status
Healthy
No key issues found.
Not Published
Last checked: 13 Feb 2019
Identities
gavin@makeuseof.com
Gavin


60% 19:37
Gavin
Key ID: c80b 7157 4fa7 2729
START
SHARE
IDENTITIES
SUBKEYS
Fingerprint
cf8b 972f 70fe 222e 4192
5593 c80b 7157 4fa7 2729
Key
Share with...
Share as SSH public key with...
Publish on keyserver

It is important for recipients to have OpenKeychain or alternative encryption key management application to enter your key. The recipient can enter the key into any compatible application, mobile device or desktop. For example, you can share the OpenKeychain public key with your own desktop computer, then enter the key into Gpg4win's Kleopatra certificate and key management program.

Step 4: Encrypt email first


61% 19:32
Encrypt
Gavin
Sign with:
Gavin
gavin@makeuseo...
Created 13 Feb
Look at my secret messages!


Share text with...
Five a side up
Mum
Moving house
MUO GD Screenshots...
Slack
BaconReader
WhatsApp
Decrypt with OpenKeychain
Encrypt with OpenKeychain
Import Key with Op...
Mail to Self
New Message
Copy to clipboard
Save to Drive
Telegram
Messages
Gmail
Skype
Discord
Always On Display
Android Beam
Bluetooth
Edge RSS
Google+


60% 19:35
theshed.place
gavin (you)
Today
gavin 19:35
-----BEGIN PGP MESSAGE-----
hQGMA1KVGVNbWUhpAQwApsGgR
wvXXrH7RlWerqM2TrCLFhAlexiP1
48shtCqTm+U
A5XP/9QvuZ67z1fsnSxoSlgsvUW1hlKG
mXicyyVMltwo5kYtKCNjtsqCexk50ER3
ZEdJ8JQ7YYn4JpnboA7azeycWfXJ1
ThRalpnfxxnZA8BPmSu5HY8cckO
QOP1SvvP
aLvVPO1NTaaluRoeF1fJS54K7D4
1dEzBoteFj27ayHGSBk3F6yjr7/
xxYYuZwqR2
BYKoRbu/kBQEDwbluzDSvzt/
0RKL/d9A6j+IRrR/
TQGMtEph3EUp0HjsucWYdkJM
BVB7Vben4OA3phf9Uf3vLSieQT
vaeSTCoqDsF/OiW+P2QWZi4V/
F+4Ain73BXkV1
FD0qI1SKNa1ylzwXWB
0xkKtLW1Fmpr83JC3/
slzyWJS+gUJ3h3jhPZGFbZVgDAtI
Fo7kqa6Eo+fQOY+CaA2Ad0OTabo
sDfthNtxXb6bcuSCxUuzV63lhPUW0
Jot something down


60% 19:36
Message
bcuSCxUuzV63lhPUW07HWqaw5e
fr2qgylMX2+WVJiQPclV0sFeAbwlb1xkAaKG6PQ
JtpbP2ogqO1amT1xScjR5Li3o
1fmj/S5+7YsRhgF4pINk+Zho5Q63KUreFvfD2My
oklynlZd9iPcroJdsGLZglyQq
TpSo33LLiGyD4CRL7GmlC8kmKkOqx
NvUvC4CU2SAV/fBFhJx9GA59ki+kb/
R2RGj
WXYWlnM0KPKVJByJD1T2Jvp3N2WZai5rr/ls0/
p1G412+etplRl9gil5Fq4beEL/
/END6rCTMlpRdsoQaILmxFgqgYFTnzIGmaJ/
gwkFHpFPdxuuTHJiTujqWFtwbfFU
wpDVKcdSDKOXDWKLHe5C7GExbzWNWTB3tI
5n0mivfVt9ChoSRiVBszwSg1U73opd
w2mDxZM9t1Dwx0EWLzomV3FAG4snMAGcfa9
grYRITCaVMS0PPA3CvooX6Smg4uZQ
q1LIxKmUBJ9SLz9K20dAkhjNyRI0bvsN5nukheci
GnsDP9ZaBcZpLBFThN53T0Y+
yGFDuNW6UR2KI20dPv0FVnchf75rN2ZUL1P0f
dUfCJ2FOaGp0TZ3DQe6hvekuV7h
JBOSSVLnUOnLkX6bdOaWxaiTjNX17Ygwe6MLI
EPKdKyNFbzjhAqYwPImvy+aoCIh
zZz6suMYhwd0Bo/Ii40x6xDYJvRZihYCd9/
JDvnKrEO3m8ZgbZ4OwortYQ9LeSEM
mPKkWZrbIOholMXqIyqbV0i/
vDaHSnMhAzMr8HcBHmM=
=0Uii
-----END PGP MESSAGE-----
Start a thread

After the recipient enters the public key, you can start sending them secure emails.

On the OpenKeychain key identification page, the sender will find two icons below his name. One is folder icon with small padlock; the other is a message icon with a small padlock. The sender uses the first icon to encrypt the file and the second to encrypt the email.

Open the email screen and enter the content. When ready, use one of the two icons:

1. Direct copy icon to copy and encrypt email content to paste into another application.
2. Share icon to encrypt email content while sharing it into another application.

Both icons are located in the upper right corner of the screen.

Decrypt email with OpenKeychain

Readers already know how to send encrypted email. But what about when an encrypted email is sent to your inbox?

OpenKeychain makes it easy to decrypt emails. Highlight content of PGP email. Make sure you have selected the entire content. When the prompt appears, select **Share> Decrypt with OpenKeychain** . Email content immediately enters OpenKeychain. If the sender used your public key to encrypt the email, the email content will be displayed!

Hope you are succesful.