**Tools**

*These links are for your use only, as sources of images used below if they are not high quality enough in this doc.*

1. Adium tool guide [– Link](https://ssd.eff.org/en/module/how-use-otr-mac)
2. Basic Security Setup for Android - [Link](https://securityinabox.org/android_basic)
3. ChatSecure tool guide - [Link](https://ssd.eff.org/en/module/how-install-and-use-chatsecure)
4. Cobian Backup Guide - [Link](https://securityinabox.org/cobian_main)
5. How to change your Facebook privacy settings - [Link](https://www.eff.org/deeplinks/2013/01/how-protect-your-privacy-facebooks-graph-search)
6. How to opt-out of Facebook's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook)
7. How to opt-out of Twitter's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/07/how-opt-out-twitters-tailored-advertisements-and-more)
8. Jitsi Tool guide – [Link](https://securityinabox.org/jitsi)
9. K9 & APG tool guide – [Link](https://securityinabox.org/k9_apg_main)
10. KeePassX tool guide – [Link](https://www.keepassx.org/screenshots/)
11. ObscuraCamTool guide – [Link](https://securityinabox.org/obscuracam_main)
12. Orbot & Orweb tool guide – [Link](https://securityinabox.org/Orbot_main), [Link](https://securityinabox.org/orweb_main)
13. PGP for Linux tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-linux)
14. PGP for Mac O SX tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-mac-os-x)
15. PGP for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-windows-pc)
16. Pidgin tool guide – [Link](https://ssd.eff.org/en/module/how-use-otr-windows)
17. Psiphon3 tool guide – [Link](https://www.level-up.cc/leading-trainings/training-curriculum/deepening/psiphon3)
18. Recuva – File Recovery Guide – [Link](https://securityinabox.org/recuva_main)
19. Redphone Tool guide – [Link](https://ssd.eff.org/en/module/how-use-redphone-android)
20. Signal Tool guide – [Link](https://ssd.eff.org/en/module/how-use-signal-%E2%80%93-private-messenger)
21. TextSecure tool guide – [Link](https://ssd.eff.org/en/module/how-use-textsecure-android)
22. Tor for Mac tool guide – [Link](https://www.torproject.org/projects/torbrowser.html.en#macosx)
23. Tor for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/)
24. TrueCrypt Tool Guide – [Link](https://securityinabox.org/truecrypt_main)

**K9 & APG TOOL GUIDE**

# K9 & APG Tool Guide

# Encrypted email for Android

**Lesson to read: Email**

**Download Location:**

* [**APG homepage**](http://www.thialfihar.org/projects/apg/)
* [**K-9 Mail homepage**](https://code.google.com/p/k9mail)

**Phone requirements:**

* Android 1.5 or up
* APG must be installed before installing K-9 Mail

**Version used in this guide:**

* APG 1.1.1
* K-9 5.001

**License:**

* APG: Free and Open Source Software (Gnu GPL v3)
* K-9: Free and Open Source Software (Apache 2.0)

**Other reading:**

* Passwords
* Mobile Phones

**Level:**Advanced

**Time required:** 30-40 minutes

**Using K-9 & APG will give you**:

* APG can be used to encrypt, decrypt and sign emails and single files locally on your phone.
* When APG is used with K-9 it gives you the ability to use encrypted email easily on your phone.

**Android Privacy Guard (APG) for Android Devices**

****

## 1. How to Install and Use APG

1.0 How To Install APG

1.1 Key Management

1.1.1 Key Management - Create Your Public And Private Keys

1.1.2 Key Management - Import Keys From A File

1.1.3 Key Management - Import Keys From The Clipboard

1.1.4 Key Management - Share Your Public Key As A File

1.1.5 Key Management - Share Your Public Key From The Clipboard

1.1.6 Key Management - Verify Identities

1.2 Message Encryption

1.2.1 Message Encryption - Public Key

1.2.2 Message Encryption - PassPhrase

1.2.3 Message Decryption

1.3 File Encryption

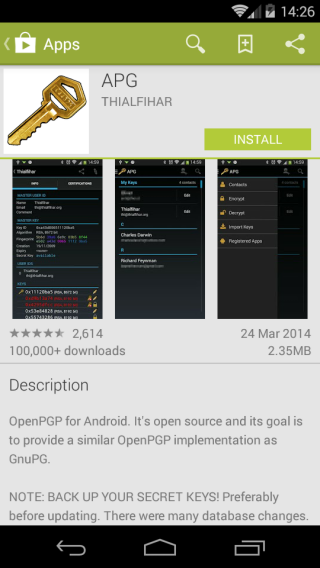
1.3.1 File Encryption - Public Key

1.3.2 File Encryption – PassPhrase

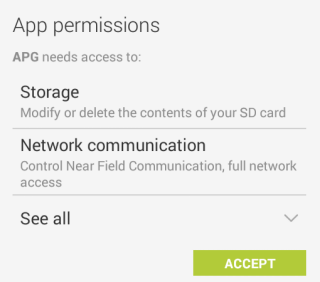
1.3.3 File Decryption

## 1.0 How To Install APG

**Step 1.** On your Android device, **download**and **install**the app from [**Google Play here**](https://play.google.com/store/apps/details?id=org.thialfihar.android.apg) by pressing, “Install”.

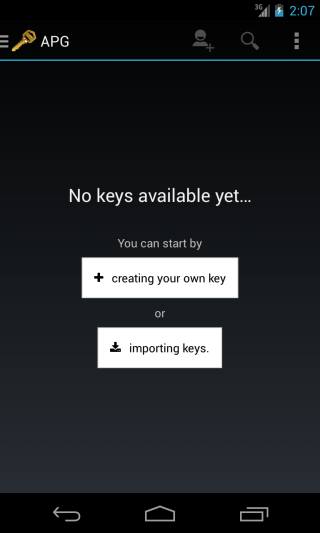


**Step 2:** Before the installation process begins, you will be prompted to review the access that the application will have on your phone. Review this carefully. Once you are happy with the permissions that will be granted, press “Accept” and the installation will complete. If you do not agree with the permissions that will be granted, press the back button and the installation will be cancelled.



## 1.1 Key Management

In order to encrypt files or messages when you first start **APG**, you will be asked to either importexisting GPG keys or createa new public and private key on your phone.



**Note:** If you want to send encrypted files or messages to other people, you will either need to import their public keys or decide on a shared password.

## 1.1.1 Key Management - Create Your Public And Private Keys

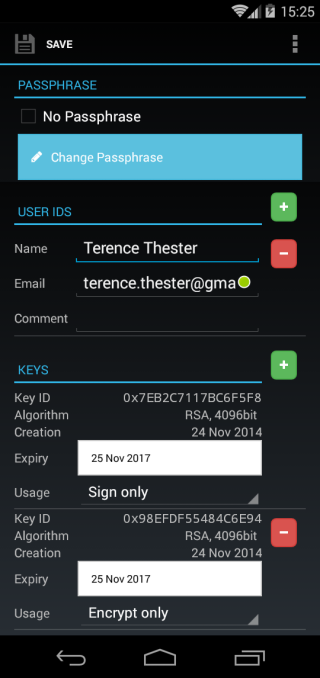
If you do not already have your private and public GPG key or wish to use a separate GPG keys for your Android device you can use **APG** to create them.

**Step 1:** When you open **APG**for the first time click the “Creating your own key” button, as shown above.

**Step 2:** Wait 2 - 3 minutes while your GPG keys are generated. You will be able to assign your name and email address to the key in the next step.

**Step 3:** In the following screen, below:

* We strongly recommend that you protect your GPG keys with **password**. To do this press “Set Passphrase” and provide strong password. See the **Passwords** **lesson** on how best to do this;
* Fill in your name**,** email address;
* It is important that you set an **expiry date**on the GPG keys, after which time the keys can no longer be used to encrypt files.



**Step 4:** Once all the information is correct, tap “Save” at the top of the screen to be brought back to the main **APG**screen, as shown above, where you will see a list of all your keys.

## 1.1.2 Key Management - Import Keys From A File

To use GPG keys that you created on another device or computer, or to import the public keys of your contact:

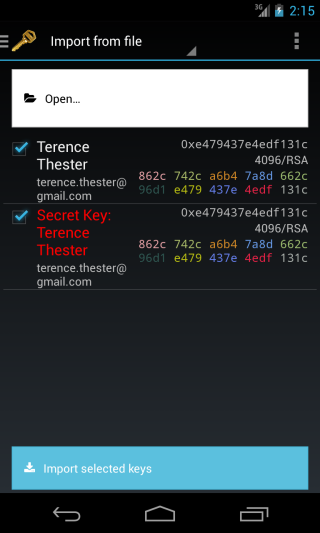
**Step 1:** Copy the GPG key(s) to your Android device via USB or save them from the email that you received on the Android device.

**Step 2:** In APG, click the “Importing Keys” button.

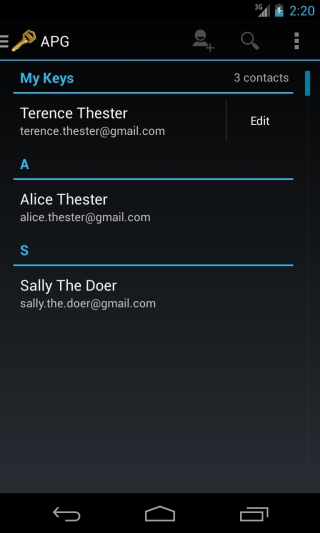
**Step 3:** On the following screen click the “Open” button at the top of your screen to open a file browser.

**Step 4:** From the file browser, select the key(s) you wish to import.

**Step 5:** Review the keys you will import and tap “Import Selected Keys” to add the GPG keys to APG. You may decide which keys you do not wish to import by deselecting appropriate checkbox for the keys.

**

**Step 6:** Once you have imported all the desired GPG keys you will be brought back to the main screen where you will see a list of all your keys.



## 1.1.3 Key Management - Import Keys From The Clipboard

GPG keys can be sent in the body of an email instead of as an attachment to import such a key

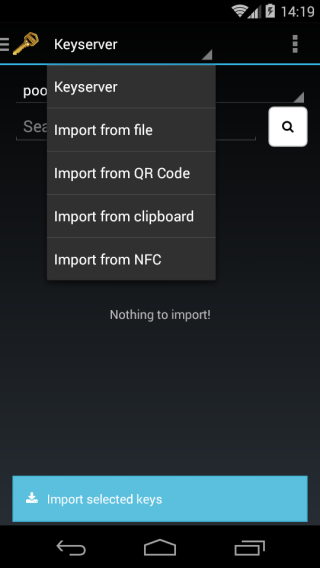
**Step 1:** Copy the GPG key from your email to the clipboard. The image below shows a GPG key in the body of an email.



**Step 2:** Open **APG**and expand the side menu on any **APG**screen by pressing “APG” at the top left of your screen.

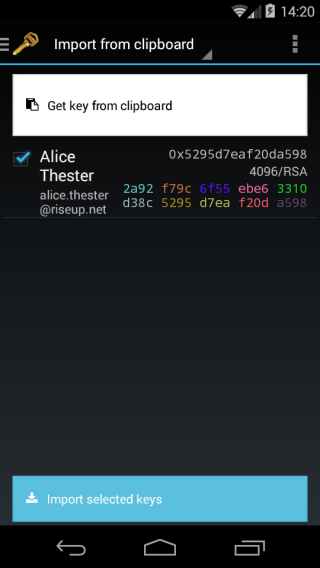
**Step 3:** Select “Import Keys” to bring up the import key screen.

**Step 4:** Tap “Keyserver” at the top of the screen to display the import options menu and select “Import form clipboard”.



**Step 5:** Tap “Get key from the clipboard” to copy the key from the clipboard.

**Step 6:** Tap “Import selected keys” at the bottom of the screen to finish importing the key into **APG**

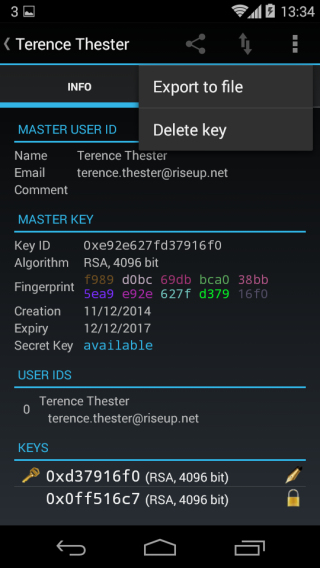


## 1.1.4 Key Management - Share Your Public Key As A File

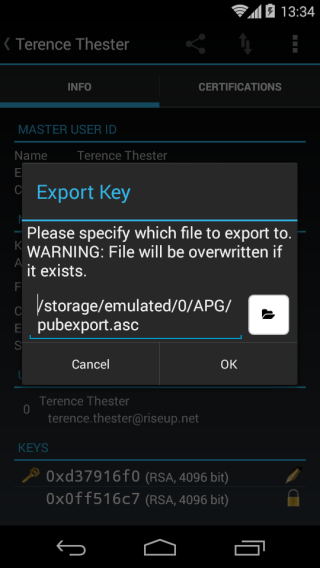
In order for your contacts to be able to send you encrypted email, you will first need to send them your public key

**Step 1:** From the main **APG** window tap on your key's entry to bring you to the info screen (as above) for your GPG key.

**Step 2:** Tap on the three vertical dots in the top right corner to display the menu and select “Export to file”.



**Step 3:** Select the location and file name you want to save your public key to and press “OK”.



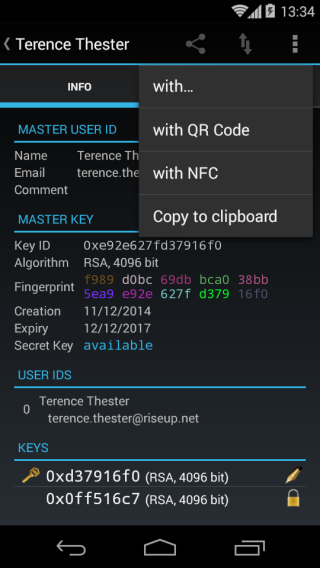
**Step 4:** The saved file cannot be given to your contacts, for example via email or IM.

## 1.1.5 Key Management - Share Your Public Key From The Clipboard

**Step 1:** From the main **APG**window tap on your key's entry to bring you to the info screen for your GPG key.

**Step 2:** Tap the three connected dots at the top of the screen to bring up sharing options and select “Share whole key”.

**Step 3:** In the following menu select “Copy to clipboard” to copy your GPG public key to the clipboard.

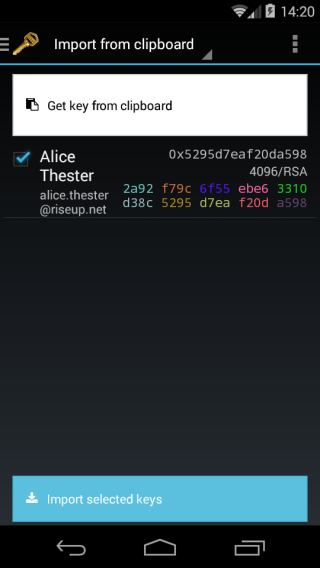


**Step 4:** Paste the public key into an email or IM chat session to your contact.

## 1.1.6 Key Management - Verify Identities

In order to ensure that you have received the correct GPG public key for your colleague and not someone trying to impersonate them, it is very important that you verify the GPG keys fingerprints either in person or via a medium that you can verify who you are talking to such as a video call or telephone call.

**Step 1:** From the main **APG** window tap on your key's entry to bring you to the info screen for your GPG key. Your contact should do the same and tap on the key they have for you.



**Step 2:** Locate the **Fingerprint** line under the **MASTER KEY** heading and read out the 40 character long string one line at a time.

**

**Step 3:** Your contact should verify that the fingerprint you read out, is the fingerprint displayed for your key on their phone or computer.

**Step 4:** Repeat steps 1 to 3 but tap on your contacts key at the first step.

## 1.2 Message Encryption

**APG**provides two ways for you to encrypt files on your Android device. **Public key** encryption is the desired option to use when sending files to other people as you will not have to share any passphrase with them. However you will need to receive public key from each person you wish to encrypt files to in advance. **Passphrase**encryption can be useful to be able to decrypt a file at a later date without the need to have access to a public key. But this method requires sharing the passphrase used to encrypt the file in order to decrypt it later.

Message encryption in **APG** can be useful if you want to store encrypted notes in another application or send encrypted email or message via a service that you can not use K-9 Mail with (eg. webmail, social networking message, etc.).

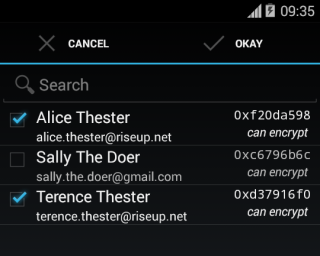
## 1.2.1 Message Encryption - Public Key

**Step 1:** Expand the side menu on any **APG** screen by pressing “APG” at the top left of your screen.

**Step 2:** Select “Encrypt” to bring up the encryption screen.

**Step 3:** To view the list of possible recipients press “Select” button with the person icon. **Note:** If you want to be able to decrypt the message at a later time, you will need to remember to include yourself in the list of recipients.

**Step 4:** On the Recipient selection screen, tick all the people that need to be able to decrypt the message and press “Okay”.



**Step 5:** Choose how to encrypt your message. Tapping “Share with…” will allow you to send the encrypted message to another application on your phone such as an email client. Tapping “Clipboard” will copy the encrypted message to your clipboard allowing you to paste the message anywhere that you can paste, such as an online forum.

## 1.2.2 Message Encryption - PassPhrase

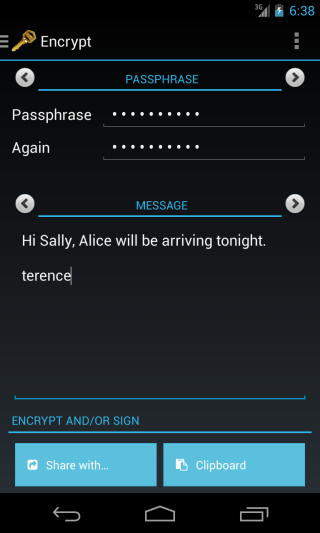
**Step 1:** Expand the side menu on any **APG**screen by pressing “APG” at the top left of your screen.

**Step 2:** Select “Encrypt” to bring up the encryption screen.

**Step 3:** Press the < or > buttons to either side of **PUBLIC KEY** to change the encryption type to **PASSPHRASE**.

**Step 4:** Enter a strong password in the fields provided.

**Step 5:** Enter the message you want to encrypt



**Step 5:** Choose how to use your encrypted message. Tapping “Share with…” will allow you to send the encrypted message to another application on your phone such as an email client. Tapping “Clipboard” will copy the encrypted message to your clipboard allowing you to paste the message anywhere that you can paste, such as an online forum.

**Note**: If you plan to share the encrypted message with a contact you will need to relay the passphrase to them in a secure way, such as in person. It should never be sent to anyone over email or IM if it is not encrypted.

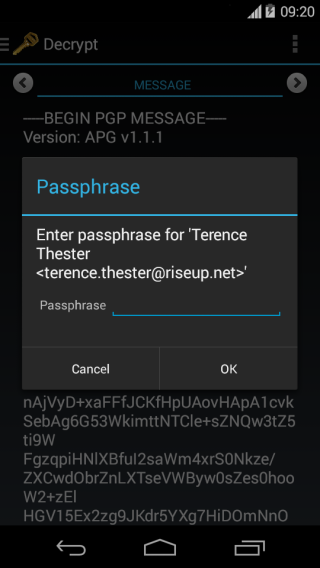
## 1.2.3 Message Decryption

**Step 1:** Copy the entire contents of the encrypted message that you received in the other app to the clipboard by long-taping on the message and selecting copy button.

**Step 2:** Switch to APG app and expand the side menu on any **APG**screen by pressing “APG” at the top left of your screen.

**Step 3:** Select “Decrypt” to bring up the encryption screen.

**Step 4:** APG will automatically detect that the clipboard has an encrypted message in it and ask you for either your GPG password, if the sender used public key encryption, or for the message password, if you used the passphrase encryption.



**Step 5** The decrypted message will be displayed in a text window inside APG.

## 

## 1.3 File Encryption

As with message encryption **public key**is the preferred encryption method but password encryption will allow you to decrypt on a phone or computer that does not have a **private key** installed but does have **APG**or **GPG**software.

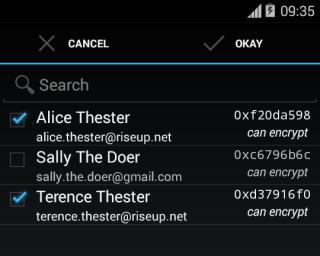
## 1.3.1 File Encryption - Public Key

**Step 1:** Expand the side menu on any **APG**screen by pressing “APG” at the top left of your screen.

**Step 2:** Select “Encrypt” to bring up the encryption screen.

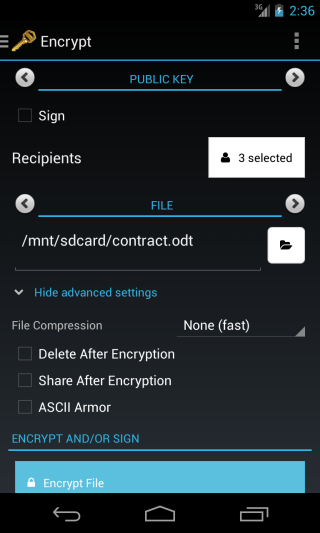
**Step 3:** To view the list of possible recipients press “Select” by the person icon. **Note:** If you want to be able to decrypt the file yourself at a later time, you will need to remember to include yourself in the list of recipients.

**Step 4:** On the Recipient selection screen, tick all the people you want to be able to decrypt the file and press “Okay”.

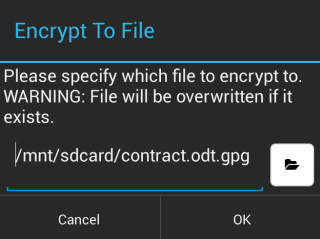


**Step 5:** Press the < or > buttons to either side of **MESSAGE** to change the encryption type to **FILE**.

**Step 6:** Tap the open file icon to open the file browser and select the file you want to encrypt.



**Step 7:** press “Encrypt File” to choose a file name and location to save the file to.



**Step 8:** Tap “OK” to complete the encryption process.

## 1.3.2 File Encryption - PassPhrase

**Step 1:** Expand the side menu on any **APG**screen by pressing “APG” at the top left of your screen.

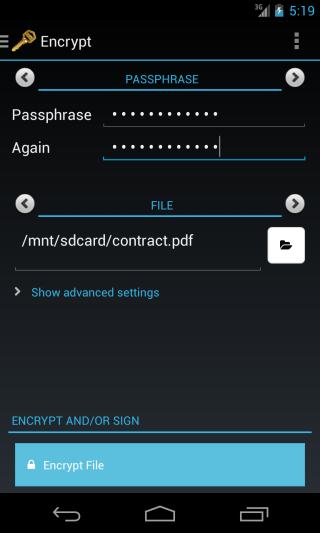
**Step 2:** Select “Encrypt” to bring up the encryption screen.

**Step 3:** Press the < or > buttons to either side of **PUBLIC KEY** to change the encryption type to **PASSPHRASE**.

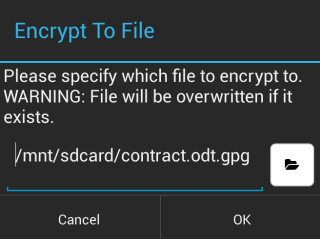
**Step 4:** Enter a strong password in the fields provided.

**Step 5:** Press the < or > buttons to either side of **MESSAGE** to change the encryption type to **FILE**.

**Step 6:** Tap the open file icon to open the file browser and select the file you want to encrypt.



**Step 7:** press “Encrypt file” to choose a file name and location to save the file to.



**Step 8:** Tap “OK” to complete the encryption process.

**Note**: If you plan to share the encrypted file with a contact you will need to relay the passphrase to them in a secure way, such as in person. It should never be sent to anyone over email or IM if it is not encrypted.

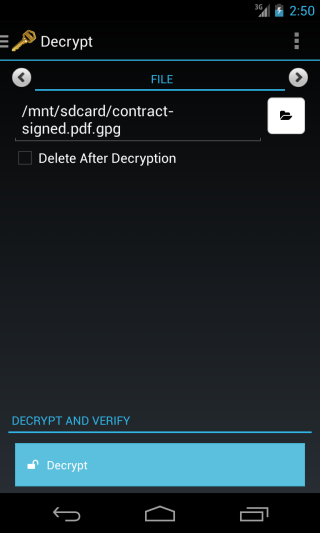
## 1.3.3 File Decryption

**Step 1:** Expand the side menu on any **APG**screen by pressing “APG” at the top left of your screen.

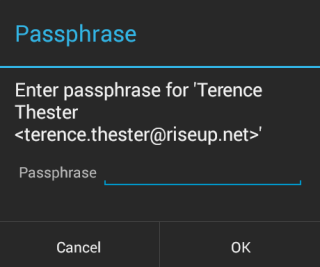
**Step 2:** Select “Decrypt” to bring up the encryption screen.

**Step 3:** Tap the < or > buttons to either side of **MESSAGE** to change the encryption type to **FILE**.

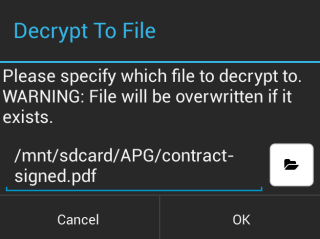
**Step 4:** Tap the open file icon to open the file browser and select the file you want to decrypt.



**Step 7:** press “Decyrpt” after which you will be prompted for your GPG keys password if public key encryption was used or for the file password if you used the passphrase encryption.



**Step 8:** Tap “OK” to choose a location to save the decrypted document.



**Step 9:** Tap “OK” to complete the decryption process.

**……………………………………………………………**

**K-9 Mail with APG**

****

**2. How to Install and Use K-9 Mail with APG**

2.0 How to Install K-9 Mail

2.1 How to configure K-9 Mail

2.1.1 Automatic account setup

2.1.2 Manual account setup

2.2 How to send and receive encrypted eMail

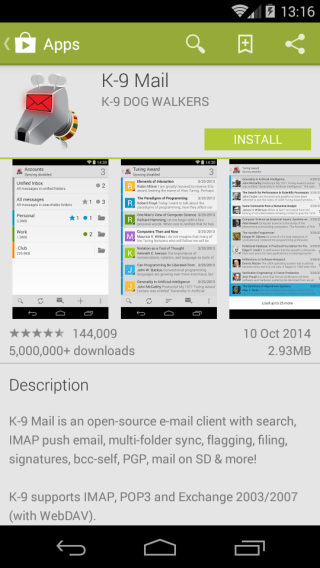
2.2.1 Sending encrypted email

2.2.2 Receiving encrypted email

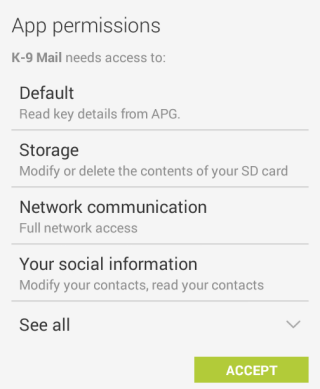
## 2.0 How to Install K-9 Mail

**Note**: Before you start using K-9 Mail you will need to have an email account, such as Gmail, that supports either secure POP3 or IMAP connections.

**Step 1.** On your Android device, **download** and **install** the app from the [Google Play store here](https://play.google.com/store/apps/details?id=com.fsck.k9) store by tapping “Install”.

**

**Step 2:**. Before the installation process begins, you will be prompted to review the access that the application will have on your phone. Review this carefully. Once you are happy with the permissions that will be granted, tap “Accept” and the installation will complete. If you do not agree with the permissions that will be granted, tap the back button and the installation will be cancelled.



**Step 3.** **Tap “**Open”to run the app for the first time

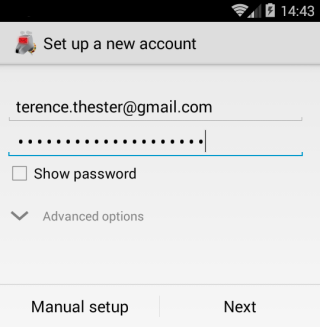
## 2.1 How to configure ****K-9 Mail****

After installing **K-9 Mail**and running it for the first time you will be presented with a welcome screen describing the features of the mail client. Press “Next” to begin the account setup.

Where possible, **K-9 Mail**will attempt to **automatically configure**your email account for you. If this is not possible or you wish to have more control over the account setup you can also **manually configure**your account.

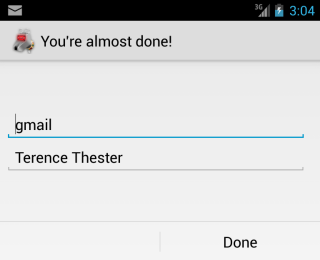
## 2.1.1 Automatic account setup

**Step 1:** Enter your email address and email password in the fields provided and tap “Next”.

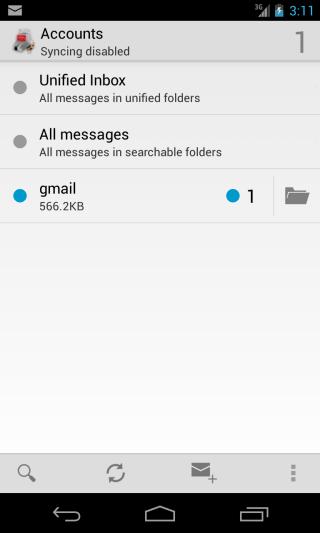


**Step 2:** **K-9 Mail** will connect to the internet and attempt to get your account settings.

**Step 3**: Once the settings have been retrieved you will be asked to enter your name as you want it to be displayed on all outgoing email and to give the account a name. The account name will allow you to distinguish between multiple accounts, should you want to add more. Tap “Done” to complete the account setup.



**Step 4:** **K-9 Mail**will display changes to the program since the last version, tap “OK” to dismiss this window and be brought to your mail account.



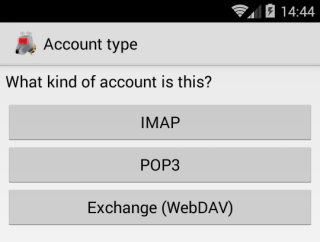
**Step 5:** To make sure the account is working in **K-9 Mail, send**yourself an email from your computer and download it from the **K-9 Mail**client.

## 2.1.2 Manual account setup

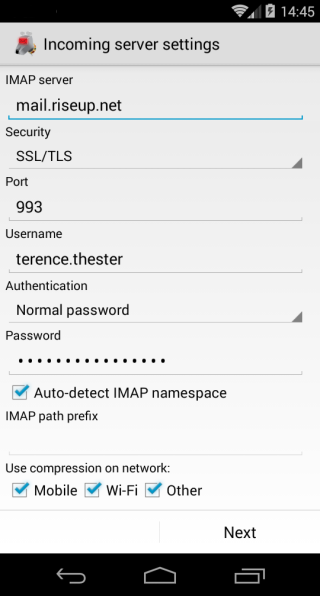
**Step 1:** Enter your email address and email password in the fields provided and tap “Manual setup”.

**Step 2:** Select the account type your email is (IMAP/POP/Exchange) and tap the relevant button as in the image below.

**Note:** you will need to refer to your email client settings on your computer to know what account type your email server uses.

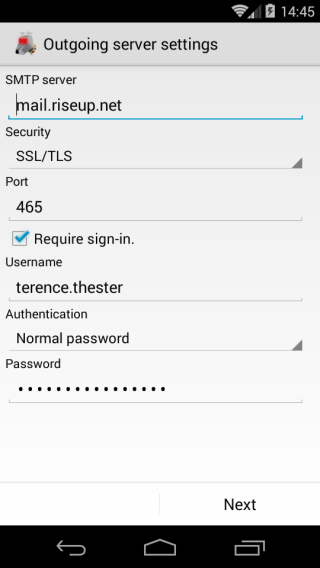


**Step 3:** Next are the incoming server settings. If unsure, refer to the email client on your computer for settings. Always ensure that the security type is set to either STARTTLS or SSL/TLS. **Never** use the none option.

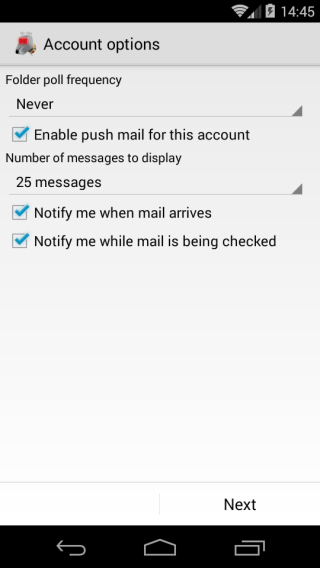


**Step 4.** **K-9 Mail** will then connect to your mail server to check if your settings are correct. It might display a warning about the certificate of your secured connection. Do not ignore this! This is the only time you can verify that the certificate really belongs to your mail server. If you ignore this, you can not be sure if you are not subject to a Man-in-the-Middle attack, and your communications could be intercepted. You can see a SHA-1 fingerprint at the very end of the warning. Either **check** on your computer if the installed certificate from your mail server has the same fingerprint, or find a way to check your mail server's certificate directly from your provider.

**Step 5.** **K-9 Mail** asks you to configure your outgoing server settings. Again, **ensure** that Security Type is STARTTLS or SSL/TLS. For all additional settings, **check** your computer's email client or the settings of your email provider.



**Step 6.** **K-9 Mail**now asks you how often you want it to automatically poll for email. **Set**the option to never and uncheck enable push mail for this account, if you only want to receive email when you manually check, otherwise leave the settings as they are to automatically receive email as they arrive to your account.



**Step 7.** The last pieces of information to provide are a nickname for the email account which will be displayed in **K-9 Mail**and to set up the name you wish to be displayed on all outgoing email.

**Step 8:** To make sure the account is working in **K-9 Mail, send**yourself an email from your computer and download it from the **K-9 Mail**client.

We recommend that you use **K-9 Mail**only in addition to your computer's email client. Therefore it is important that when you download email with your Android phone, it does not delete the email on the server, since you want to receive the email later with your computer, too. By default, **K-9 Mail**is set up this way, but you may want to learn more about the settings which can be found in accounts; this can be reached by long pressing on the account you have just set up and selecting account settings from the menu. You may also wish to check the fetching mail and sending mail account option for settings.

## 2.2 How to Send and Receive Encrypted eMail

One of the main benefits of using **K-9 Mail**over other email clients is that it lets you send and receive GPG encrypted email. Before you can start sending and receiving encrypted email, you need to ensure that you have all your OpenPGP keys imported into APG, as outlined in the APG section above. If you followed all the necessary steps in the APG keys section your keys will be imported.

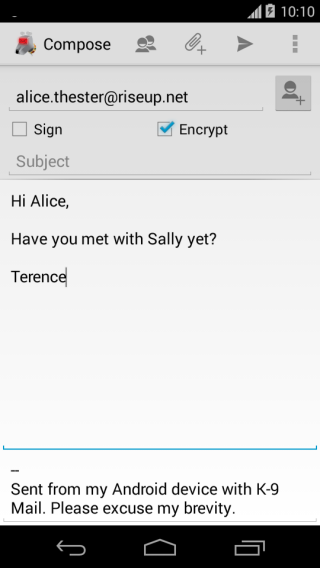
## 2.2.1 Sending encrypted email

**Step 1:** From any screen in **K-9 Mail**tap the  icon to start a new email.

**Step 2:** On the email composition screen add your recipient by either typing in an email address or pressing  and selecting one from your address book.

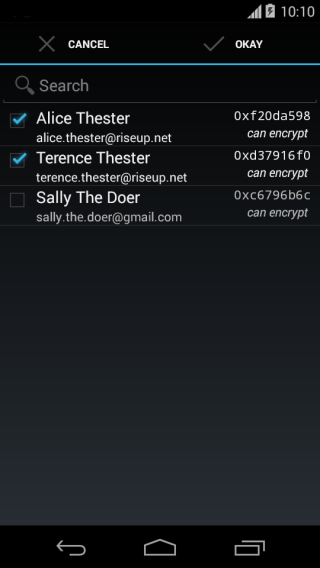
**Step 3:** Enable encrypted email by checking the box next to encrypt.

**Step 4:** When finished writing your email, press  to send.



**Step 5:** The following screen will ask you to select which GPG keys to encrypt to. Be default the recipient key and your own should already be selected.

**Note:** You should always ensure that your key is selected so that you can read the encrypted email that you had send.

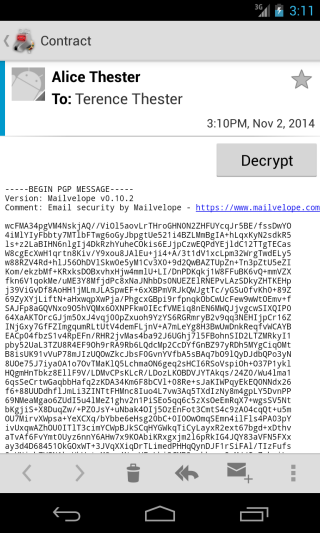


**Step 6:** Once all recipient keys have been selected, press “OKAY” to send the email.

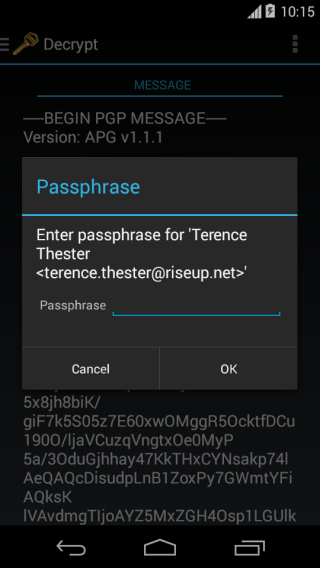
**Note:** Currently **K-9 Mail**cannot encrypt attachments, so you will need to encrypt any files with **APG**that you wish to send, before you compose the email. This is explained in the APG encryption section above. To attach the files tap the paperclip attachement icon and select the encrypted file (ending in .gpg).

## 2.2.2 Receiving encrypted email

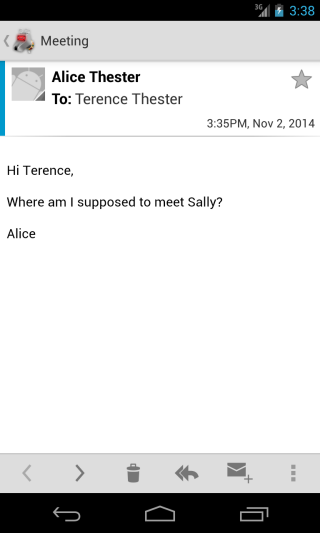
**Step 1:** Open your inbox and tap the email you wish to read.



**Step 2:** Tap the “Decrypt” button.



**Step 3:** Enter the passphrase for your GPG key when prompted and press “OK” to decrypt the email.



**Note:** as **K-9 Mail** is currently not able to decrypt encrypted attachments, you will need to save the attachments to your phone and decrypt them with APG, as explained in the APG decryption section above.

**KEEPASSX TOOL GUIDE**

# KeePassX Tool Guide

**Secure password management**

**Lesson to read: Passwords**

**Download Location:** <https://www.keepassx.org/downloads>

**Computer requirements** Windows 2000 or higher, Mac OS X 10.4-10.9

**Version used in this guide:** KeePassX 0.4.3 (KeePassX is a cross-platform version of the Windows-only KeePass program.)

**License:** Free and Open-Source Software (primarily GPLv2)

**Other Reading**: <https://www.keepassx.org/forum/>

**Level:**Beginner

**Time required:** 5 minutes

**Using KeePassX will give you:**

* The ability to save all your passwords in one convenient and secure database
* The ability to create and store many strong passwords without having to remember them

# 1.0 Things to consider with KeePassX

KeePassX is a password safe—a program you can use to store all your passwords for various websites and services. A password safe is a great tool because it allows you to use different difficult-to-guess passwords for all your services, without needing to remember them. Instead, you only need to remember one master password that allows you to decrypt a database of all your passwords. Password safes are convenient and allow you to organize all of your passwords in one location.

It should be noted that using a password safe creates a single point of failure and establishes an obvious target for bad actors or adversaries. Research has suggested that many commonly used passwords safes have vulnerabilities, so use caution when determining whether or not this is the right tool for you.

## 1.1 How KeePassX works

KeePassX works with files called password databases, which are exactly what they sound like—files that store a database of all your passwords. These databases are encrypted when they’re stored on your computer’s hard disk, so if your computer is off and someone steals it they won’t be able to read your passwords.

Password databases can be encrypted via three methods: using a master password, using a keyfile, or both. Let’s look at the pros and cons of each.

## 1.2 Using a master password

A master password acts like a key—in order to open the password database, you need the correct master password. Without it, nobody can see what’s inside the password database. There are a few things to keep in mind when using a master password to secure your password database.

* This password willdecryptall of your passwords, so it needs to be strong!That means it shouldn’t be something easy to guess, and it should also be long—the longer the better! Also, the longer it is, the less you need to worry about having special characters or capitals or numbers. A password that is only made up of six random words (in all lower case, with spaces in between) can be harder to break than a 12-character password made up of upper and lower case letters, numbers, and symbols.
* You need to be able to remember this password! Since this one password will allow access to all your other passwords, you need to be able to make sure you can remember it without writing it down. This is another reason to use something like [Diceware](http://world.std.com/~reinhold/diceware.html" \t "_blank)—you can use regular words that are easy to remember, instead of trying to remember unnatural combinations of symbols and capital letters.

## 1.3 Using a keyfile

Alternatively, you can use a keyfile to encrypt your password database. A keyfile acts the same way a password would—every time you want to decrypt your password database you will need to provide that keyfile to KeePassX. A keyfile should be stored on a USB drive or some other portable media, and only inserted into your computer when you want to open your password database. The benefit of this is that even if somebody gets access to your computer’s hard disk (and thus your password database) they still won’t be able to decrypt it without the keyfile stored in the external media. (Additionally, a keyfile can be much harder for an adversary to guess than a normal password.) The downside is that any time you want to access your password database, you’ll need to have that external media handy (and if you lose it or it gets damaged, then you won’t be able to open your password database).

Using a keyfile instead of a password is the closest thing to having an actual physical key to open your password database—all you need to do is insert your USB drive, select the keyfile, and presto! If you do choose to use a keyfile instead of a master password, though, make sure your USB drive is stored somewhere safe—anyone who finds it will be able to open your password database.

## 1.4 Using both

The most secure method for encrypting your password database is to use both a master password and a keyfile. This way, your ability to decrypt your password database depends on what you know (your master password) and what you have (your keyfile)—and any malicious entity who wants to get access to your passwords will need both. (With that said, keep in mind your threat model—for most home users who just want to store their passwords, a strong master password should be sufficient. But if you’re worried about protecting against state-level actors with access to huge computational resources, then the more security the better.)

Now that you understand how KeePassX works, let’s get started with actually using it!

## 2.0 Getting started with KeePassX

Once you’ve installed KeePassX from [here](https://www.keepassx.org/downloads), go ahead and launch it.

Once it’s started, select “New Database” from the File menu.

A dialog will pop up which will ask you to enter a master password and/or use a keyfile. Select the appropriate checkbox(es) based on your choice.

Note that if you want to see the password you’re typing in (instead of obscuring it with dots) you can click the button with the “eye” to the right.

Also note that you can use any existing file as a keyfile—an image of your cat for example, could be used as a keyfile. You’ll just need to make sure the file you choose never gets modified, because if its contents are changed then it will no longer work for decrypting your password database.

Also be aware that sometimes opening a file in another program can be enough to modify it; the best practice is to not open the file except to unlock KeePassX. (It is safe to move or rename the keyfile, though.)

Once you’ve successfully initialized your password database, you should save it by choosing “Save Database” from the File menu. (Note that if you want, you can move the password database file later to wherever you like on your hard disk, or move it to other computers—you’ll still be able to open it using KeePassX and the password/keyfile you specified before.)

## 2.1 Organizing passwords

KeePassX allows you to organize passwords into “Groups,” which are basically just folders. You can create, delete, or edit Groups or Subgroups by going to the “Groups” menu in the menubar, or by right-clicking on a Group in the left-hand pane of the KeePassX window. Grouping passwords doesn’t affect any of the functionality of KeePassX—it’s just a handy organizational tool.

## 2.2 Storing/generating/editing passwords

To create a new password or store a password you already have, right-click on the Group in which you want to store the password, and choose “Add New Entry” (you can also choose “Entries > Add New Entry” from the menubar). For basic password usage, do the following:

* Enter a descriptive title you can use to recognize this password entry in the “Title” field.
* Enter the username associated with this password entry in the “Username” field. (This can be blank if there is no username.)
* Enter your password in the “Password” field. If you’re creating a new password (i.e. if you’re signing up for a new website and you want to create a new, unique, random password) click the “Gen” button to the right. This will pop up a password generator dialog, which you can use to generate a random password. There are several options in this dialog, including what sorts of characters to include and how long to make the password.
  + Note that if you generate a random password, it’s not necessary that you remember (or even know!) what that password is! KeePassX stores it for you, and any time you need it you’ll be able to copy/paste it into the appropriate program. This is the whole point of a password safe—you can use different long random passwords for eachwebsite/service, without even knowing what the passwords are!
  + Because of this, you should make the password as long as the service will allow and use as many different types of characters as possible.
  + Once you’re satisfied with the options, click “Generate” in the lower right to generate the password, and then click “OK.” The generated random password will automatically be entered in the “Password” and “Repeat” fields for you. (If you’re not generating a random password, then you’ll need to enter your chosen password again in the “Repeat” field.)
* Finally, click “OK”. Your password is now stored in your password database. To make sure the changes are saved, be sure to save the edited password database by going to “File > Save Database.” (Alternatively, if you made a mistake, you can close and then re-open the database file and all changes will be lost.)

If you ever need to change/edit the stored password, you can just choose the Group it’s in and then double-click on its title in the right-hand pane, and the “New Entry” dialog will pop up again.

## 2.3 Normal use

In order to use an entry in your password database, simply right-click on the entry and choose “Copy Username to Clipboard” or “Copy Password to Clipboard,” and then go to the window/website where you want to enter your username/password, and simply paste in the appropriate field. (Instead of right-clicking on the entry, you can also double-click on the username or password of the entry you want, and the username or password will be automatically copied to your clipboard.)

## 2.4 Advanced use

One of the most useful features of KeePassX is that it can automatically type in usernames and passwords for you into other programs when you press a special combination of keys on your keyboard. Note that although this feature is only available under Linux, other password safes like KeePass (on which KeePassX was based) support this feature on other operating systems, and it works similarly.

To enable this feature, do the following.

1. Choose your global hotkey. Choose “Settings” from the “Extras” menu, and then choose “Advanced” in the pane on the left. Click inside the “Global Auto-Type Shortcut” field, and then press the shortcut-key combination you wish to use. (For example, press and hold Ctrl, Alt, and Shift, and then hit “p.” You can use any key combination you like, but you’ll want to make sure that it doesn’t conflict with hotkeys other applications use, so try to stay away from things like Ctrl+X or Alt+F4.) Once you’re satisfied, click “OK.”

2. Setup auto-type for a specific password. Make sure that you have the window open where you’ll want to enter the password. Then go to KeePassX, find the entry for which you want to enable auto-type, and double-click on the entry’s title to open up the “New Entry” dialog.

3. Click the “Tools” button in the bottom left, and select “Auto-Type: Select target window.” In the dialog that pops up, expand the drop-down box and choose the title of the window in which you want the username and password to be entered. Click OK, and then click OK again.

Test it out! Now in order to autotype your username and password, go to the window/website where you want KeePassX to autotype your username/password for you. Make sure your cursor is in the text box for your username, and then hit the combination of keys you chose above for the global hotkey. As long as KeePassX is open (even if it’s minimized or not focused) your username and password should automatically be entered.

Note that depending on how the website/window is set up, this feature may not work 100% correctly right off the bat. (It might enter the username but not the password, for example.) You can troubleshoot and customize this feature, though—for more information we recommend looking at the KeePass documentation [here](http://keepass.info/help/base/autotype.html" \t "_blank). (Although there are some differences between KeePass and KeePassX, that page should be enough to guide you in the right direction.)

It is recommended that you use a key combination that is difficult to hit accidentally. You don't want to accidentally paste your bank account password into a Facebook post!

## 2.5 Other features

You can search your database by typing something in the search box (the text box in the toolbar of the main KeePassX window) and hitting enter.

You can also sort your entries by clicking on the column header in the main window.

You can also “lock” KeePassX by choosing “File > Lock Workspace,” so that you can leave KeePassX open, but have it ask for your master password (and/or keyfile) before you can access your password database again. You can also have KeePassX automatically lock itself after a certain period of inactivity. This can prevent someone from accessing your passwords if you step away from your computer. To enable this feature, choose “Extras > Settings” from the menu and click on the security options. Then check the box that says “Lock database after inactivity of {number} seconds.”

KeePassX can also store more than just usernames and passwords. For example, you can create entries to store important things like account numbers, or product keys, or serial numbers, or anything else. There’s no requirement that the data you put in the “Password” field actually has to be a password. It can be anything you want—just input what you want to store in the “Password” field instead of an actual password (and leave the “Username” field blank if there’s no username) and KeePassX will safely and securely remember it for you.