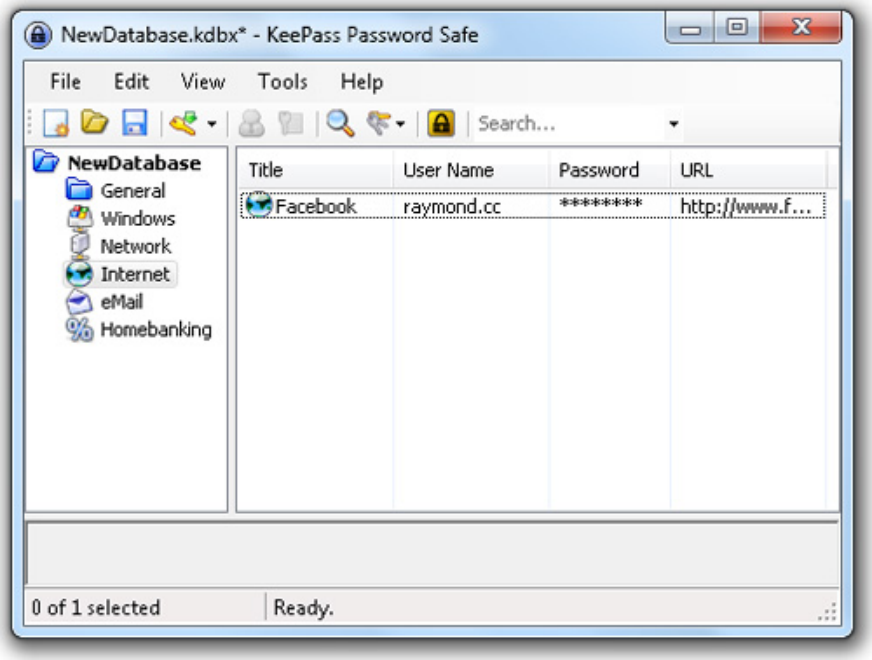
Experience Keepass, impressive password manager

In the following article, we will explore and discuss some more details about KeePass application - a popular password management tool today.

QuanTangMang - One of the rules to remember when using a password is that they should not be used many times. If the user's email inbox is peeked at by hackers, it is likely that all of their online accounts registered with this address will be easily detected .Conversely, if you set up and use different passwords, it will take time to recover each time you forget your password.So how do we do that?That's why password management software - Password Manager is as popular as it is today.

With the help of this Password Manager tool, users can be assured and comfortable with lengthy and complex characters including letters and numbers . All they need to do is remember 1 Unique Master Password parameter to manage all real passwords.However, any software has its advantages and disadvantages.In the following article, we will explore and discuss some more details about KeePass application - a popular password management tool today.



Pros and cons of KeePass

First, we will highlight the advantages of this program.

Convenience: KeePass has 2 main versions: **Installable** and **Portable** .Users can copy Portable files to USB and use them on any computer.

- This is an open source program, completely free.So anyone can download the source code and check for any malicious code inside.

- Automatically login with **TCATO (Two Channel Auto - Type Obfuscation)** : in fact, this is quite important, because it prevents others from using the first keyboard to log in, and this information Can be memorized by the usual keylogger program. On the other hand, TCATO is integrated enough to make keylogger applications 'confused' with the use of the Windows clipboard to turn each part of the application's auto-text string. But there is a slight inconvenience here that the default TCATO has not been activated yet, please select **Entry> Auto-Type** and check the **Two-channel auto-type obfuscation box.**

- Works with all browsers without support plug - ins: KeePass is a standalone application, so flexibility is very high, users do not need to install any plugin .

Next is a number of points to overcome :

- No **On - Screen** keyboard support: for many people this may be the biggest shortcoming of this program. Every time you start KeePass, the program will ask you to enter a Master Password, the point is that the password can still be recorded with the keylogger, and the hackers only need to download the database. KeePass, saved as **Database.kdb** (for version v1) or **NewDatabase.kdbx** for v2.On the other hand, users should be aware that the OSK (on screen keyboard) plug-in for KeePass v1 uses the Windows OSK function itself, and can still be recorded with keyloggers.

- Windows Clipboard processing capability is not secure enough: according to KeePass official information, this program can completely prevent the monitoring of clipboard characters but in our test it is not like so.When double-clicking on the Password field, this information is still copied to the Windows clipboard.

- No online support service.

Set up KeePass for the first time

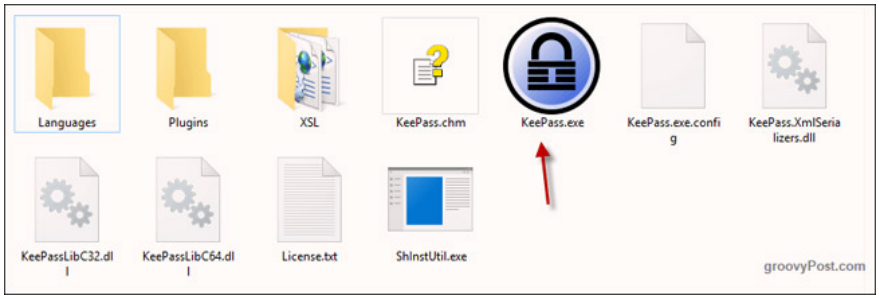
Download KeePass

This article will focus on the portable version. If you access the KeePass download page, you will see the latest Windows versions at the top and of course you should use these latest versions. Here, you will see Installable version on the left, Portable version on the right.

If you are a Mac or Linux or Android or iOS, there is also a KeePass version for these platforms. You will see them when scrolling the mouse down. As you can see, they cover all platforms like Blackberry, Palm, Windows Phone, Chromebook and Command Line.

They are not called KeePass but they are all compatible with KeePass password database - KeePass's password database.

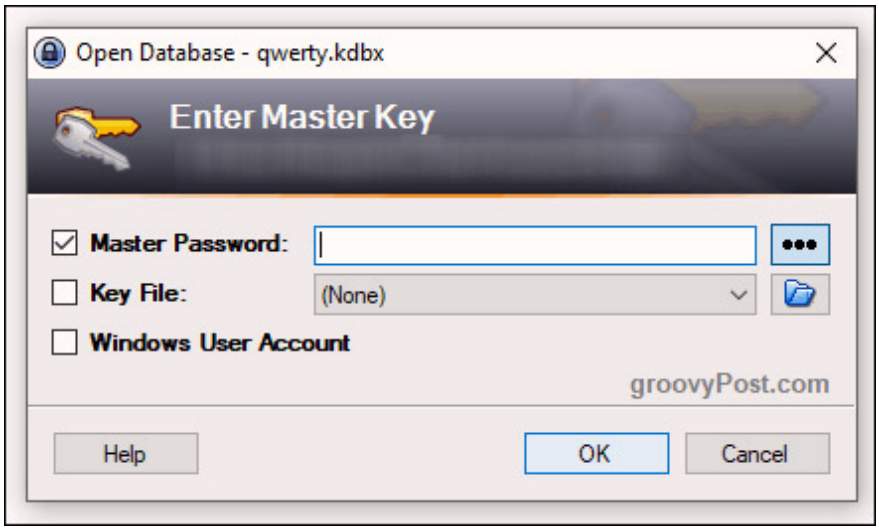
Open the main application



Once the zip file has been downloaded, open the file. If you have selected the installable version, install it on your computer. If you choose the portable version, create a KeePass folder on the cloud or USB memory. You

should synchronize cloud storage service for an additional 5GB for free.

Now click on **KeePass.exe** to start the program and you will see the login window to protect your database.

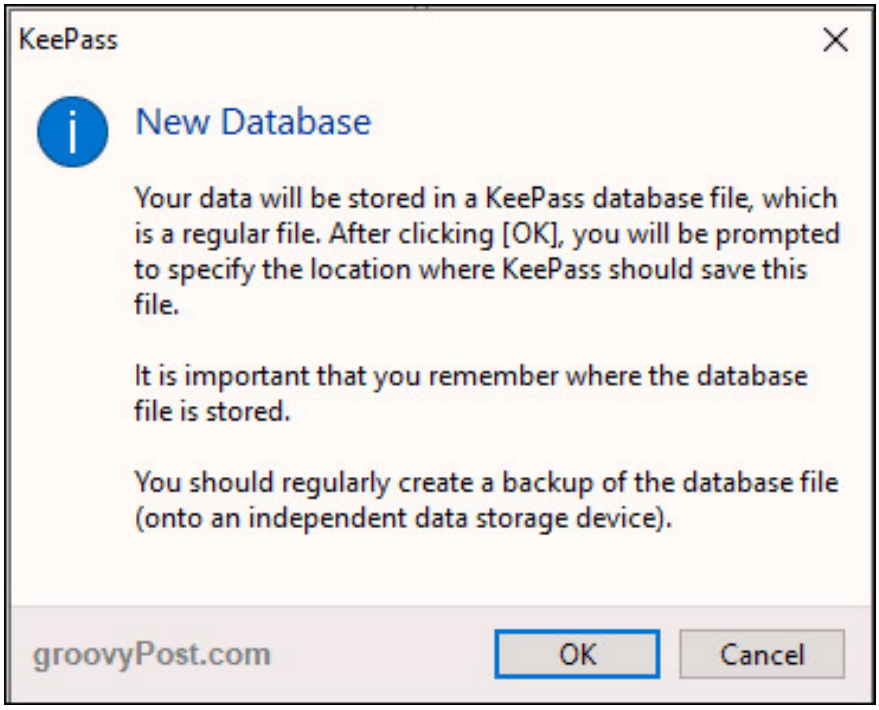


However, because you do not have a database, close this login window and an empty database window will appear.

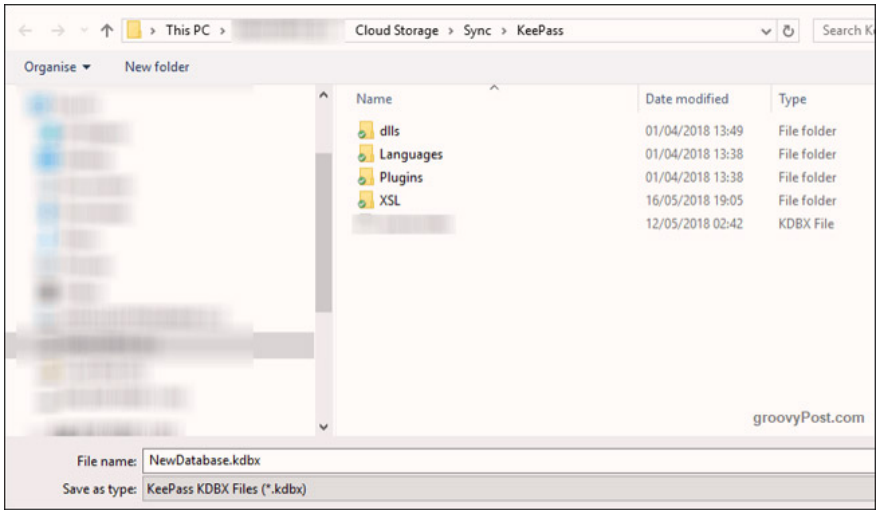
Create a database

Now we need to create a new encrypted database where the passwords will be stored securely.

First click **File -> New** . Then you will see this screen.



Click **OK** and you will be prompted to save a **KDBX** file (the file format of the KeePass password database).



Make sure it is in the same directory as the other KeePass components. You can put KDBX files somewhere on your computer, but saving these files in the same place (especially on cloud storage) is best.

You can also rename the KDBX file if you don't want to use the default name.

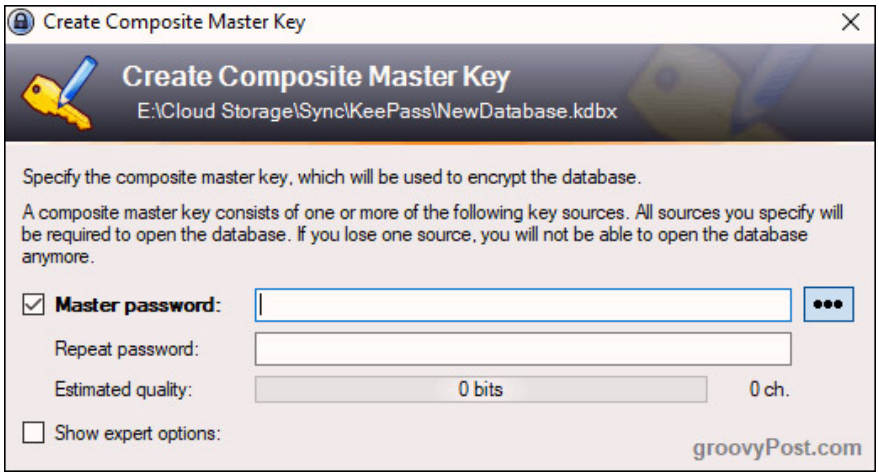
Create an unbreakable password

The encrypted database is only as strong as the master password protecting it. If you use an easy-to-guess password such as your name, your spouse's name, your dog's name, your birthday, etc., the KeePass database will be hard to protect safely. .

Conversely, if you take some time to set up a master password, your data will be really safe and no one will get it except you.

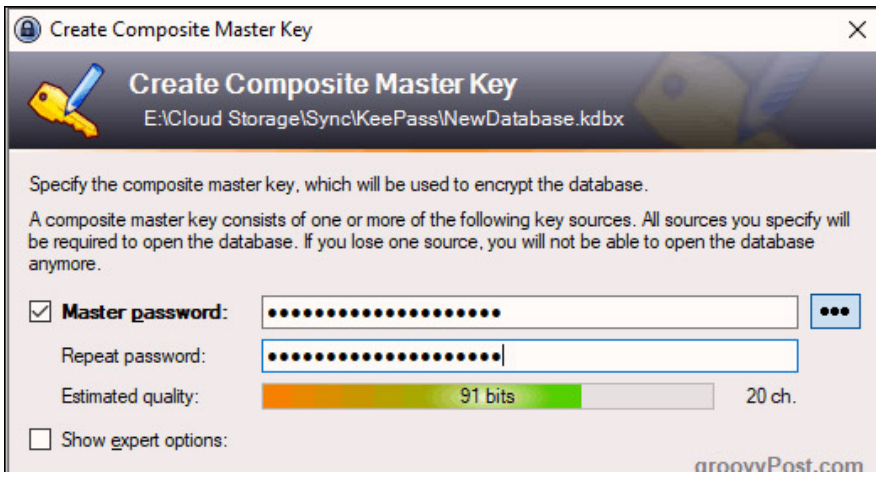
1. Summary of how to create strong passwords and manage the most secure passwords

So this sequel is the most important part of the process.

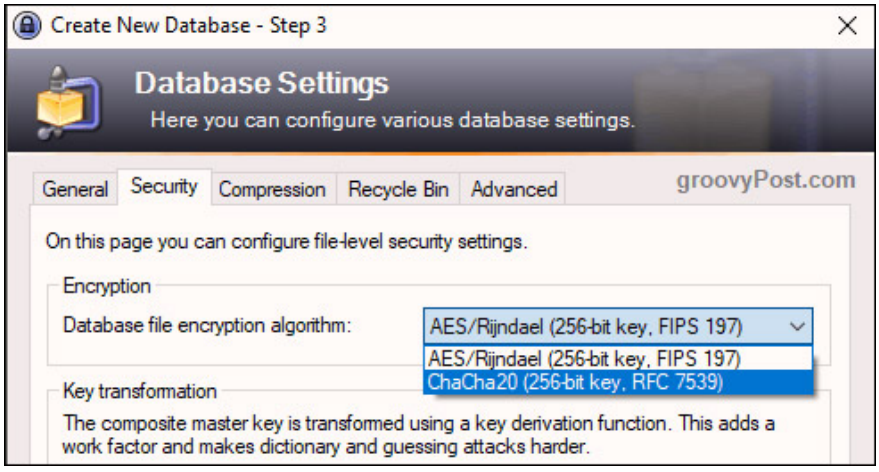


You should set your password at least 10 characters with lowercase, uppercase and numbers. If possible, include some special characters such as commas, periods, and semicolons. You need to make the password as difficult as possible to guess.

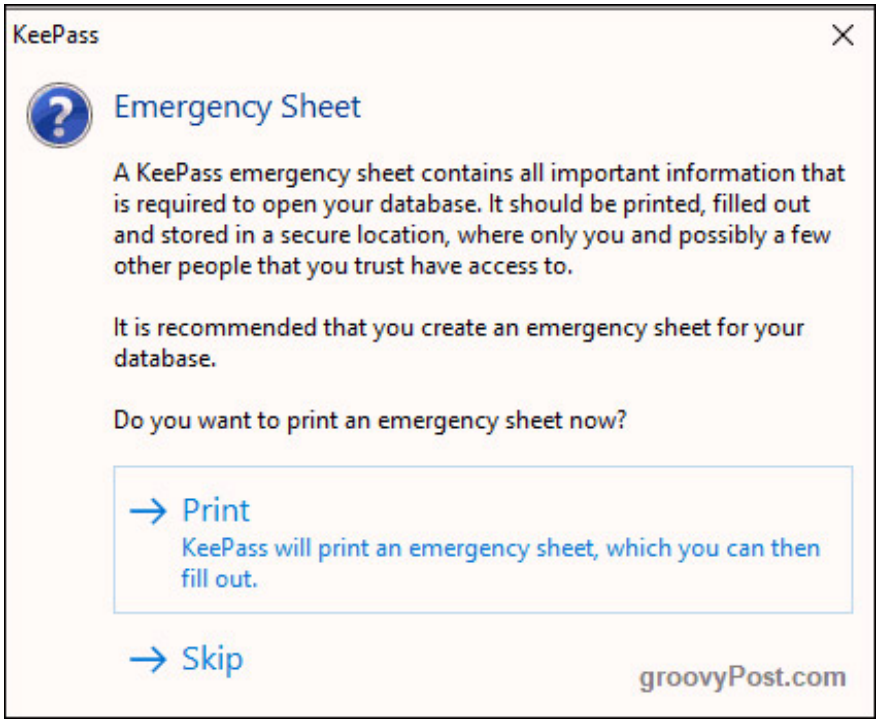
To ensure you are entering it correctly, repeat the password where indicated, ' **Estimated Quality** ' - **Estimated** quality - of the password will be displayed. The higher the number, the better. In this example, Estimated Quality only reaches 91 bits because this is just a temporary database in this article. If you are creating a real database, keep Estimated Quality at more than 100 bits, maybe 120 for example.



In step 3, the only thing that will be changed is the **ChaCha20** encoding standard. This is a much stronger encryption protocol than the **AES-256** standard.



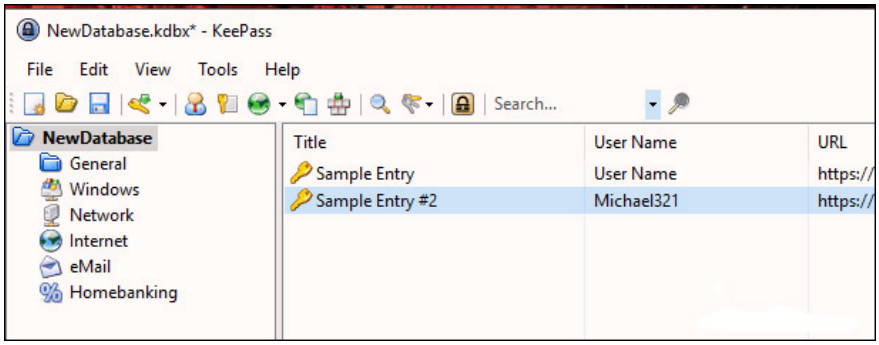
Print out the Emergency Sheet



One last thing before the database is created and opened. You will be asked if you want to print an " **Emergency Sheet** ". We recommend doing this. For very obvious reasons, there is no ' **Forgot Your Password** ' option **? Click Here To Reset It** '. So if you forget the master password, or your loved one needs this password when you die, this will become a big problem.

So print out the Emergency Sheet, write master pasword KeePass, then hide it somewhere. If this Emergency Sheet is for your loved one, put it in a sealed envelope with a life insurance policy where your loved one can easily find it. And if you later change the master pasword, remember to update this Emergency Sheet!

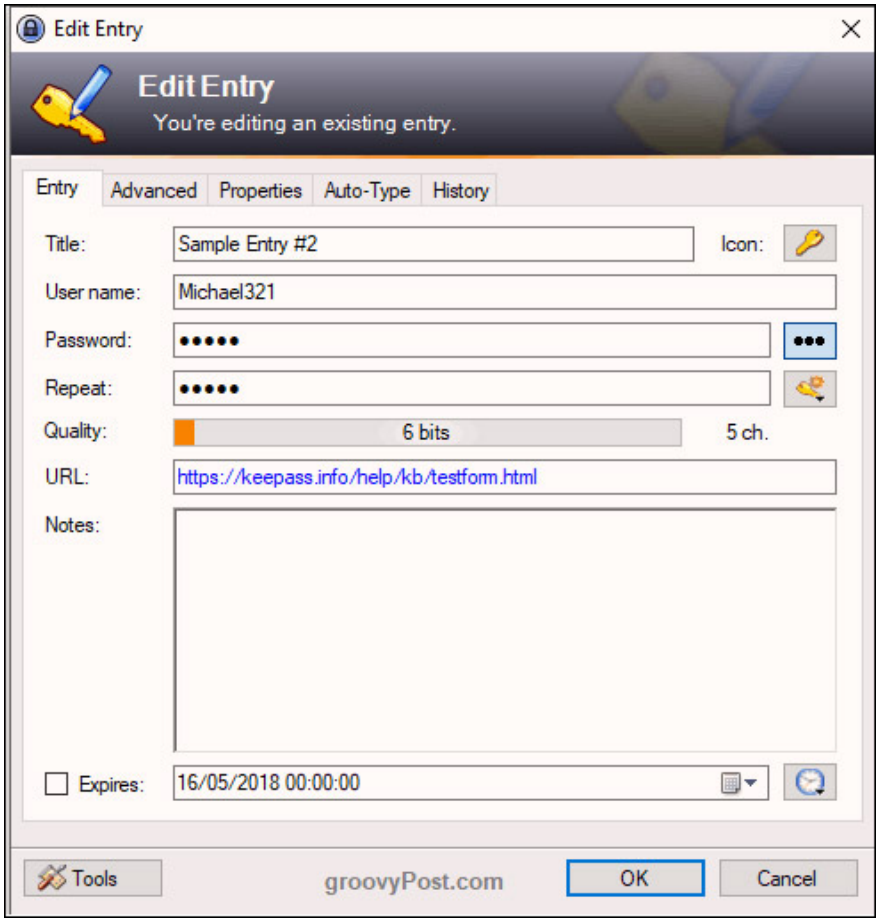
Customize your database



Your database will now open and you can start creating and saving passwords.

On the left are groups where you can classify your login information. These are KeePass groups available to you, but you can delete or rename them if you wish. You can also create an unlimited number of new groups.

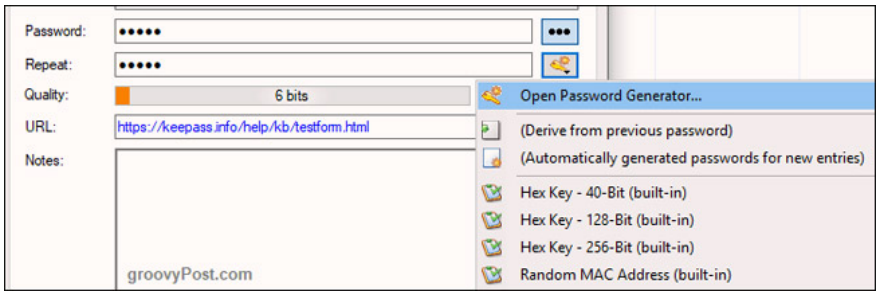
KeePass will have two sample items saved on the right and you can continue and delete those items. But before you do this, open one of them to see what the sample password entry will look like.



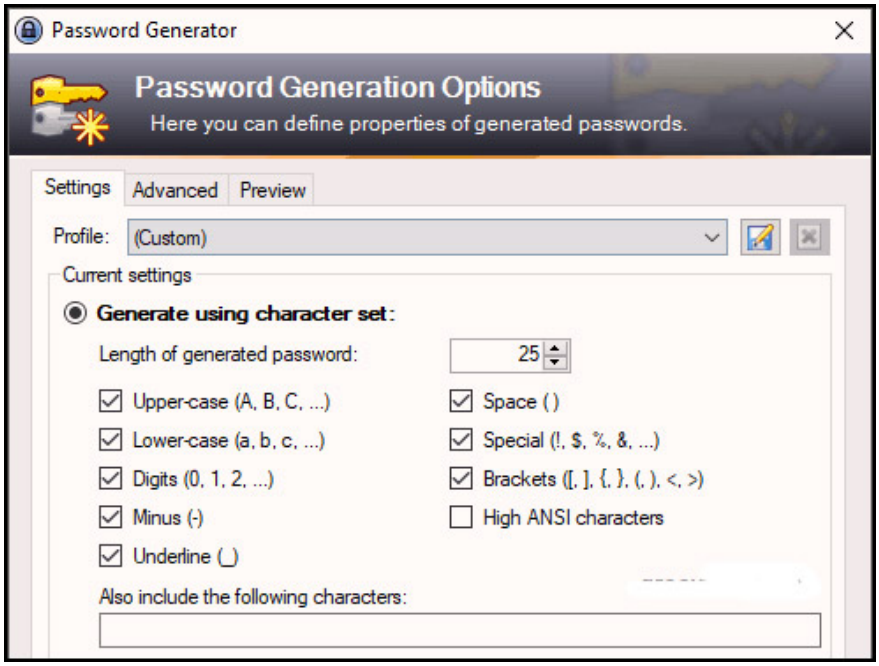
So when you click on the small key icon on the main database interface (in the toolbar), a box like the one above will display. But it will be empty. You need to fill this box. The **Title** section will be the name of the website, software, or whatever. **User Name** by your choice. **The URL** will be the name of the website or software service.

Now the password. For security reasons, passwords are hidden with dots. If you click on the button with three dots on the right hand side, the password will display itself. Press this button again to hide the password.

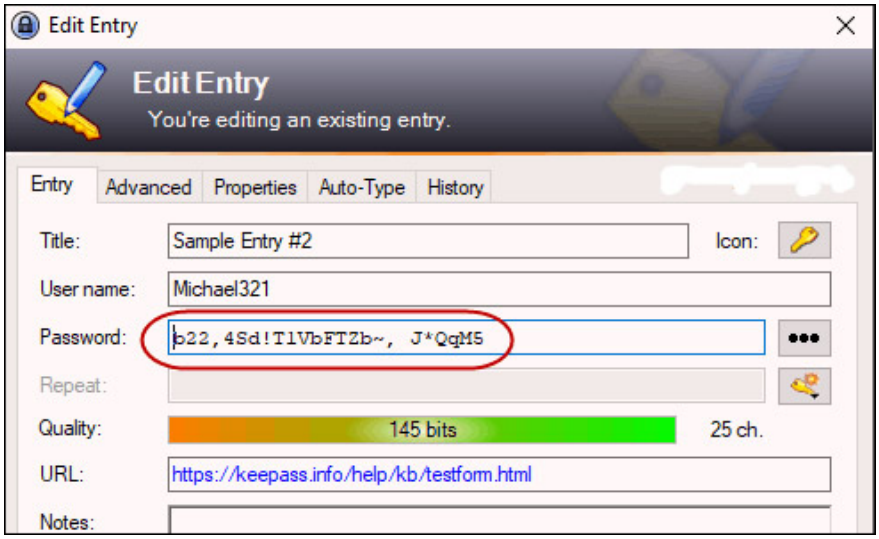
To create a password, click the key icon below the three dots button and you will receive this menu. Select '**Password Generator**'.



You just need to care about the first part. Choose your password length (minimum 25 characters). Then select the character you want in the password.



Now click **OK** at the bottom and you will see that your box has already been filled with a new password. Click the three dots button to see it.



Click **OK** to save the password and close the box.

Log in

When you want to log in somewhere, right-click the entry in KeePass and select **Copy Username** . Then, click the username box on the website and **CTRL + V** to paste the username into (or **CMD + V** on the Mac). Then, right-click the entry again and select **Copy Password** and repeat the process in the password box.

You have to act quickly because after 12 seconds, KeePass will delete information from the clipboard for security reasons. You can shorten or extend this time in KeePass options. In the options, you can also make KeePass log out of the database after a certain amount of time. This will be useful in an office environment.

With the simple installation and use of KeePass, there is no reason not to use this password manager. Prevent the risk of being attacked and start using a password that cannot be hacked. show today. Good luck!

See more:

1. Instructions for entering passwords from the browser to KeePass
2. Instructions for installing KeePass Password Safe on Ubuntu
3. 5 best password management apps for iOS