Many victims have had their computers hacked, emails compromised, passwords changed and have even been locked out of their user accounts. They have had machines infected with spyware, keystroke loggers, Trojans and more. So the point I want you to take away from this article is whether you are a security professional, student, or just a surfer, technology can be used both for and against you.

Why am I creating an article on passwords?

User credentials are the gateway to accessing personal and professional information, be it sensitive or otherwise, bank accounts, online shopping, individual identities, are both profitable and open to abuse by an unscrupulous individuals. So it is important to use more than one password, understand how to create simpler passphrases, and to use free tools that can help in both the creation of and the storage of passwords.

Think about it this way. If you separated from someone, and they refused to give you there key back, then you simply change the locks to stop them gaining access to your home, whilst you're out. This is no exception, you are simply changing the locks to your digital doorway.

People are human and they have trouble remembering 1 or 2 passwords especially multiple passwords, even more so if the passwords have upper and lowercase letters, numbers, and special characters. Like most people you have more to do than try to remember 50 different passwords.

So what do you do? The simplest option is use the same password for everything. That's solves that problem, you use your email address for the username and you one need to remember that one password. Fantastic, however! You have one small problem,

- If you use the same password for everything, and you have 30 accounts for example, and, the same password was used for all accounts then you would have to change the password 29 other times should the password be compromised.

- Another alternative would be to create 30 unique passwords and then write down all 30 passwords in a note book. Yes "That'll work". ***But!*** If the book is stolen that you have written down the passwords in then the thief has your passwords.

- OK save them all to a text file, then you only need one password, which is the one to login to your computer.
    - Again you have almost the same problem as the note book scenario.
    - another issue is if your machine is infected with spyware for example, and it records screen shots, as soon as you open the text file then screen recording will snap the image of the open text file and the bad guy can see all your passwords

- Complicated isn't it? So! What is the best solution? Use technology, and let that do the hard work. ***The best option is to use a tool that can allow secure storage of the passwords, and that can be locked up.***

A tool like Keepass, or, you can use a tool like Safehouse, in that you create a secure vault and store all documents that you want to protect.

When it comes down to creating a password there are many variables that can and need to be considered

- Such as size (length).
- Character usage (upper and lower case letters, No! and specialise characters).
- Change duration (change every so many days or weeks).
- Recovery if the password is lost, forgotten, or a machine is stolen with passwords on.

You must also consider usernames. This is a common aspect that is forgotten or not considered. A common question that I have been asked when I worked as an IT Trainer was “can usernames have numbers or special characters”. The short answer is some can.

So if you have a U$3rName and N3Wp@s$w0rD combination then then you are further hardening your login credentials. This combined with length and frequent changing makes it harder for an email account for example to be compromised. Especially if you have been a victim of a stalker that will do anything to control what you can and can’t do whilst trying to humiliate you in the worst way possible.

Some of the common answers that I have had when I asked users why they only use one or two passwords for all their accounts?

- They have trouble continually creating new and complex passwords! (After all, what do ***“you”***! define has long and complex. 6, 7, 8 or more characters, and or the inclusion or exclusion of letters, numbers, etc.)
- They cannot remember so many passwords! After all there is more to do than to remember passwords.
- It is just too much hassle.
- They have had to keep resetting their accounts as they have forgotten the password.
- They get the wrong passwords with the wrong accounts.
- They are worried about locking their account up and locking themselves out.

To give a point on the above comments I have and do on a weekly basis, with certain accounts purposely tick the “forgotten my password” box and reset it weekly. This serves two purposes

1. I don’t have to worry about when it was last reset?
2. I can confirm that to access my account with the same credentials, has only another 6 days.

This action gives me piece of mind and it is a habit that I have got in to, and is very normal, I also with some accounts have my mobile phone as an additional tool that is part of added security with regards to changing passwords.

So in this article I will show a couple of freely available tools that can both create and store all this important information and you only ever need to remember one single password and the free software will do everything else for you.

The password combined with a username is a way of proving to an application, website, a login screen, or a computer that you are who you claim to be. When logging in to an account such as your eBay, amazon, or Facebook account you require two separate elements one is your username and

one is your password. By combining these two elements together you are confirming that you are the correct individual to be logging into your account.

What is a password?

The password is a combination of upper case letters, lower case letters, numbers, and special characters $@£*!, that is one part of the verification process and that you are the account holder.

A password should be a combination of three of the four character set, but for a password to be a good password it must be both complex and long. The combination of both length and complexity, as well as the password not being a word found in a dictionary, is not related to family ties, is not a pet's name, and that it is not a duplicate of an existing password should be both hard to guess and hard to crack.

What do I mean hard to guess and hard to crack?

Let's say that I have a password with N0tT1ngH4M$hIr3 in!!! The problem is I have used a password that relates to where I live. However! Just because you have discovered the password of Nottingham does not mean that it would be easy to crack, simply because I could change the variation. For example

- I could use both upper and lower case letters.
- I could have inserted special characters.
- It could be combined with a place of significance such as Sherwood Forest Nottingham.

You know some of the password had Nottingham in it, but, is the password just Nottingham or is it Nottinghamshire, is it Gedling Nottingham, Gedling Nottinghamshire? Hopefully you get the idea?

If a password is to be strong ***"IT MUST"*** be a both complex and long, as well as changed regularly. The length of a password is just as important as is the complexity. Many people use the same password for all of their online accounts examples include:

- Online banking!
- Facebook!
- Twitter!
- Slide share!
- Instagram!
- LinkedIn!
- Etc.

They may even use the same password for logging on to the computer!

They may make a memorable reminder so that it helps them if they use two or maybe three password variants. These memorable reminds may be sticky notes under keyboards, post it notes on a monitor, it may be a text file, or the windows built in sticky notes. The problem here is that many times rather than just a memorable note, the user will write down the password, and in that instance you may as well not have a password in the first place.

- For example they may have a reminder note that states "where I went on holiday". That is great until they show all their friends and co-workers there holiday pictures from Corfu. How hard would that password be to guess?

- Other examples that I have seen “Dogs name” and everyone knows the dog’s name as that is your best friend?

- Another example “car” that is not hard to guess you simply try the make, model, or registration, and the latter is the most common.

- So what I will do latter in this article is to show you how to create a reminder that gives no clue at all, and could be pasted on a wall without anyone else knowing what the reminder means.

So Let’s return to the example of the Nottingham password again! How many variations can one person use for the password of Nottingham? Well lets analyse, the word has 10 letters in total. Now let’s look at the variations. You have 26 letters that is 26 possible uppercase letters that is 26 possible lowercase letters, you have from 1 through 0 on keyboard and then you have the special characters. Now that has been pointed out I will ask again how many variations you can have. A lot.

- You can use numbers only.
    - N0ttingham.
    - Nott1ngham.
    - Nottingh4m.
- Now let’s include the use of numbers and special characters.
    - N0tt!ngham.
    - NoTT1ng$m.
    - N0tT1nGh4m.
- You have just increased the cracking process.

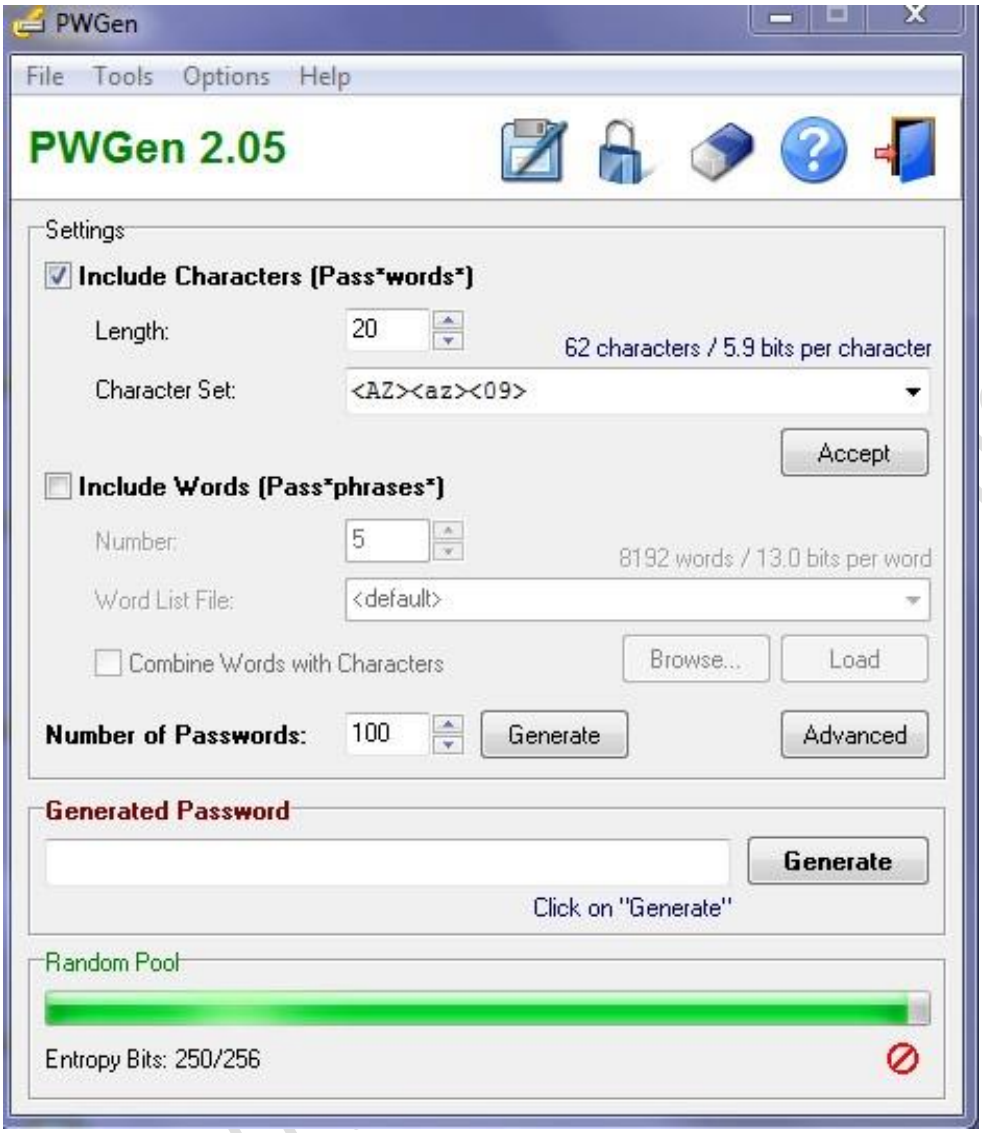
If you are going to use password reminders, ensure that you understand the reminder, but no one else will. For example $$ you know what that means, but no one else will. What you should never do, and I have seen this example used, is, to use a reminder such a “DOB and Start date” has it won’t take long to identify your password.

Now that I have got the reminders and what not to use out of the way. We will look at several ways to help you create multiple login credentials that are both complex and unique that you can save in a secure a manner, and that only you will have access to, whilst you only need to remember one password and technology will do the rest for you.

The first tool that we will look at in this article is a password generator. A password generator is exactly that. You give it a number, and a set of parameters such as change a tick box here or there, click the generate button and you have a unique and complex password.

The password generator called PWGen can be accessed via the “S O U R C E F O R G E. N E T” website or you can simply Google for password generators. To help get you started I have included the website address for PWGen. http://pwgen-win.sourceforge.net/

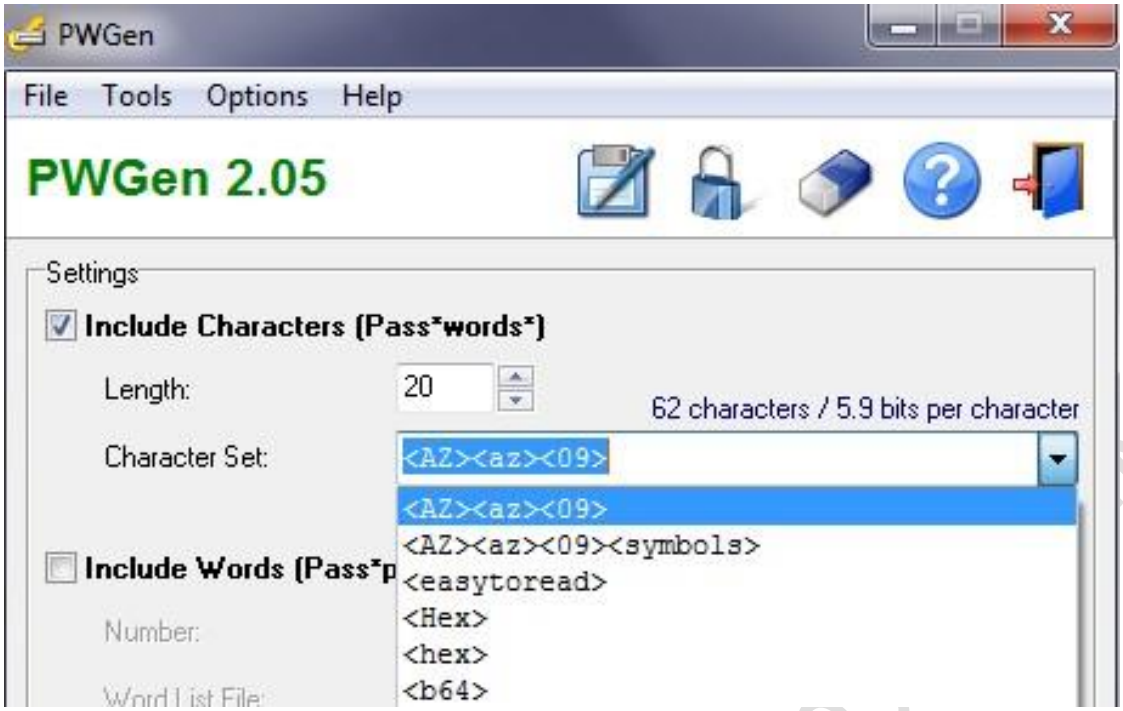
To give you an idea about what PWGen I have included some images of the interface, and some points on how to use the tool. For a free tool it is updated regularly, and is accessible through open source which means that it to the date of this article it is still free.



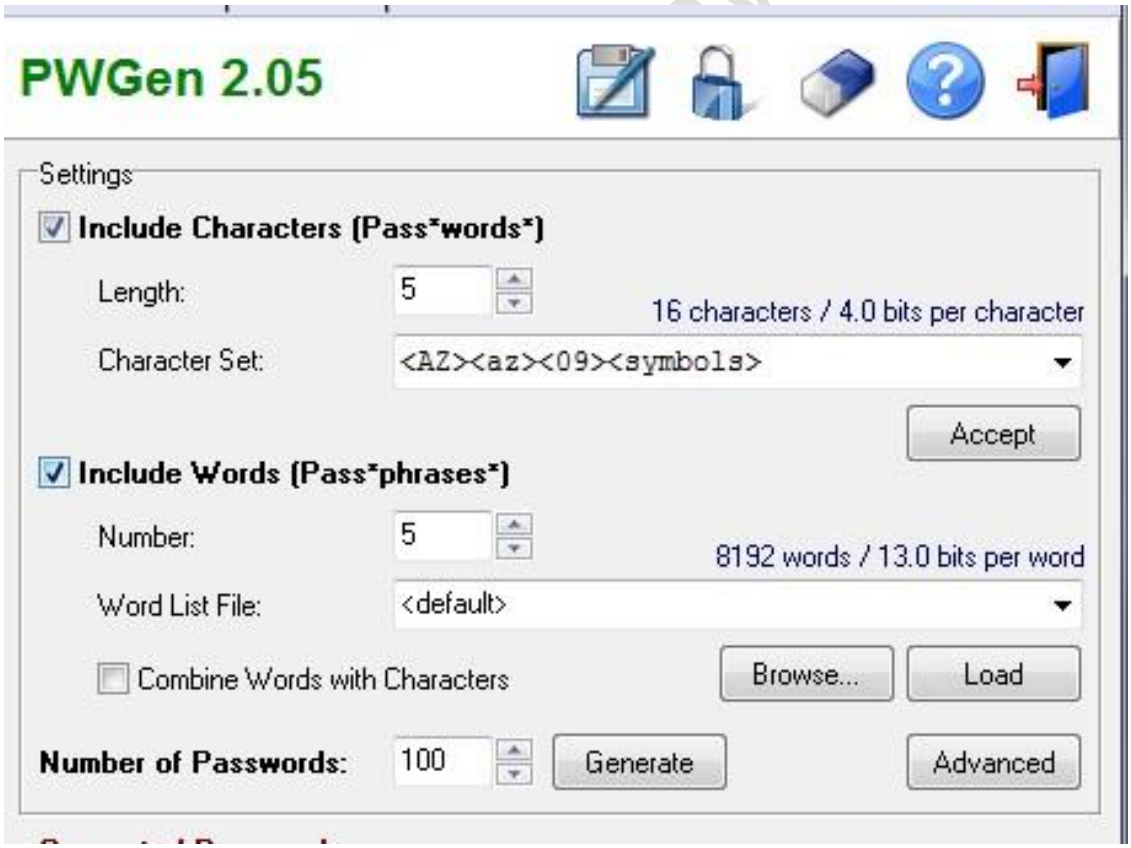
In the top part of the interface, the settings, you will see a tick box next to the word include characters. Beneath that is the word length, and at the side of that is a box that can change the number of characters, the change can increase or decrease the number of characters that is used in the password. This allows the individual to assign a password length for example in the screen print the number is 20 that means that the password length will be 20, **that is 20 characters!**

- **Not 20 letters!**
- **Not 20 numbers!**
- **Not 20 special characters!**

That will be a combination of 20 characters that will include numbers, upper and lower case letters and special characters.



As you can see in the image above you can change the character set via the drop down. As you can see this allows you to create a password in varying ways.



If you place a tick in the “include words pass phrase”, what you have is a combination of both characters that include numbers letters and special characters as well as the inclusion of a pass phrase. A pass phrase is a word, which combines several characters, which are joined to create an easy to remember password. I will show you pass phrase shortly and all will become clear.

Take for example “Mary had a little lamb its fleece was white as snow” how can this be a password or passphrase. How the passphrase works, you would take the M in Mary, H out of had, L in little, take the F out of fleece the W out of white and S out of to snow.

What you are left with is “M H L F W S” I agree it is no help at all, but bear with me!!! NOW let’s say that you decide to use M H and L only. From the three letters, you can combine those three letters, by including numbers, additional letters and special to create a passphrase

Now you have the same nursery rhyme, but as your new passphrase:

Example: M4Ry_ H4D- A- L!!tl3_ L4m13

As you can see Mary now has a little lamb, but what you have is a “pass phrase” not a password. The passphrase is now easier to remember. You can now use MHL as your password reminder after all you will understand what MHL means. Will anyone else?

In this Example M4Ry_ H4D- A- L!!tl3_ L4m13 you have 27 characters that include UPPER and lower case letters, special characters, Numbers, including several hyphens and underscores that will replace the use of the space bar.

By combining numbers, letters, special characters, using nursery rhymes, places, sites of interest, etc. you can quickly make unique, easy to remember and complex passphrases, and you can also make passwords that are not used over and over.

We have talked about creating passwords and passphrases, let’s look at the use of a password storage tool. There are many out on the internet if you do google a search tools include:

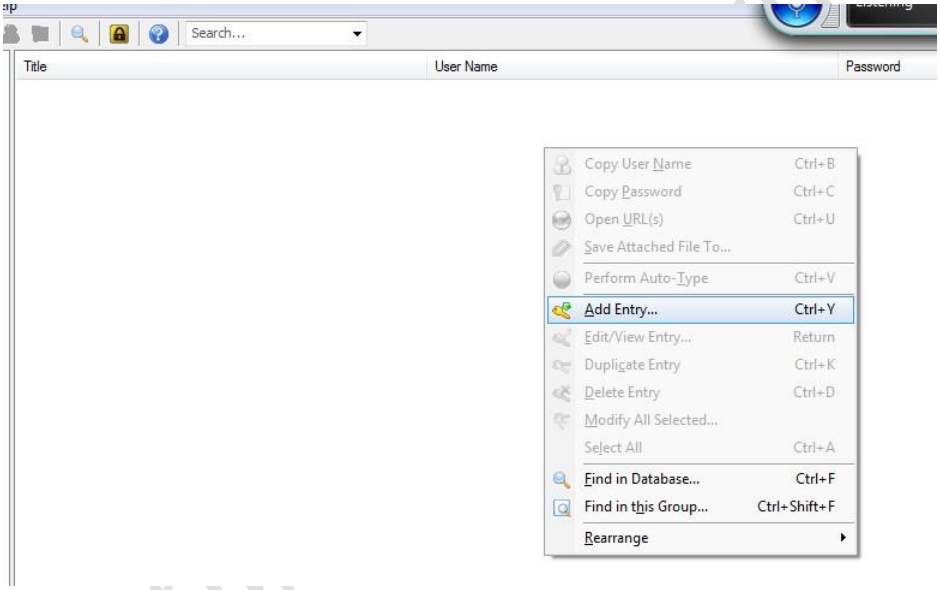
- Password Safe http://passwordsafe.sourceforge.net/
- Browser Based Safe http://www.passwordsafe.com/
- Last Pass https://lastpass.com/
- Password Box https://www.passwordbox.com/

Do not forget many browsers can remember passwords that are used, but, I prefer to use a third party application that I can save to a thumb drive, or, external storage device. My tool of choice is Keepass. The tool can remember usernames, passwords, website address, dates and times for you, and you can also make notes, that can also be locked safely and securely away, even if multiple users shares the same laptop or computer.

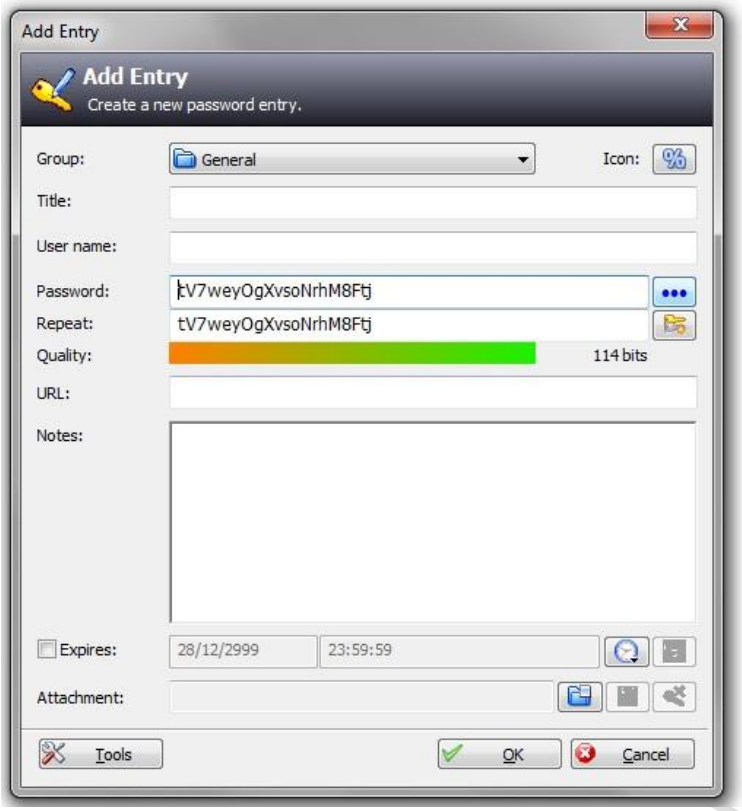
- Keepass http://keepass.info/

In the following screen prints we will look at Keepass. In addition to remembering usernames, passwords, websites, dates and times, and notes, the tool can also set and create attachments, and expiration dates. So this is a multi-purpose tool. Best of all it is a free tool that can be downloaded.

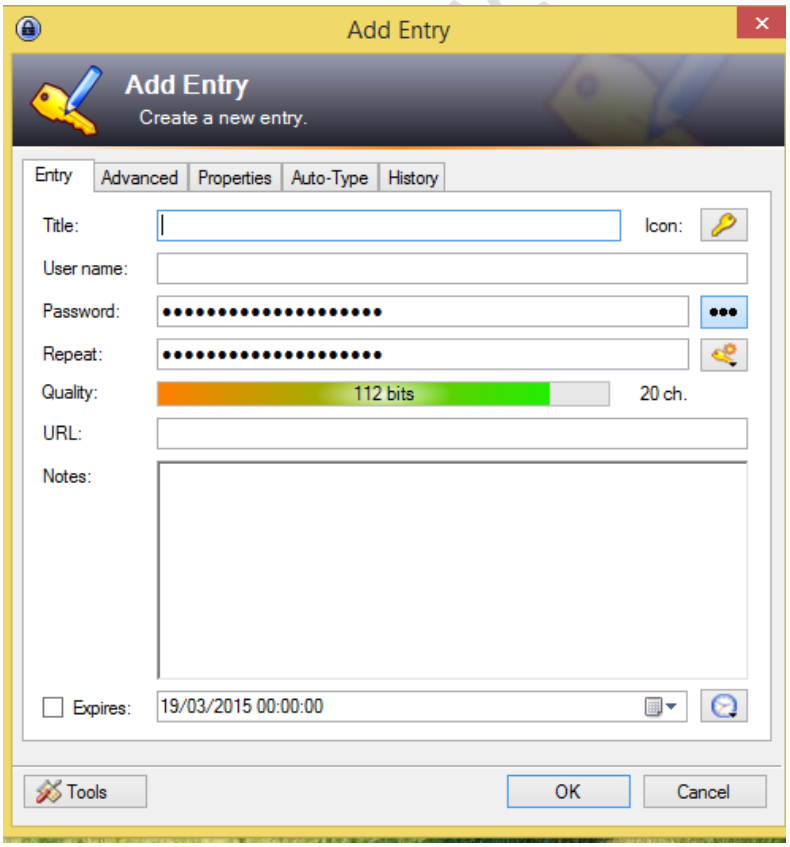
To add a new entry, right click anywhere in the right hand window



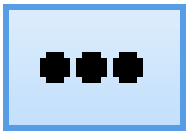
Click the add entry option



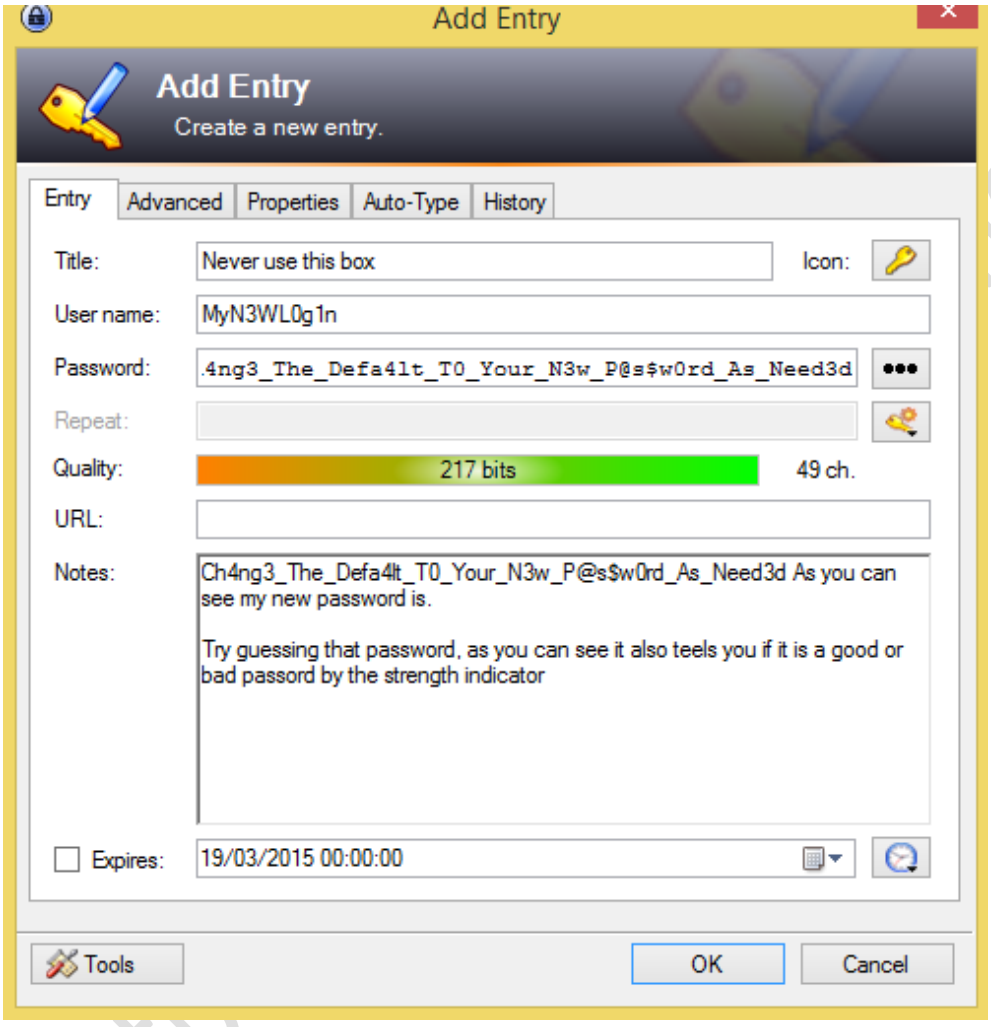
By default the password is blocked by black dots, but for this article I have changed them so that you can see the characters, when a new entry is created a new password will be generated automatically by Keepass. You can change this password if you like but as a general FYI the auto generated passwords are acceptable. We will create a new entry, simply click on the Edit menu, Add New, you will get the interface as below:



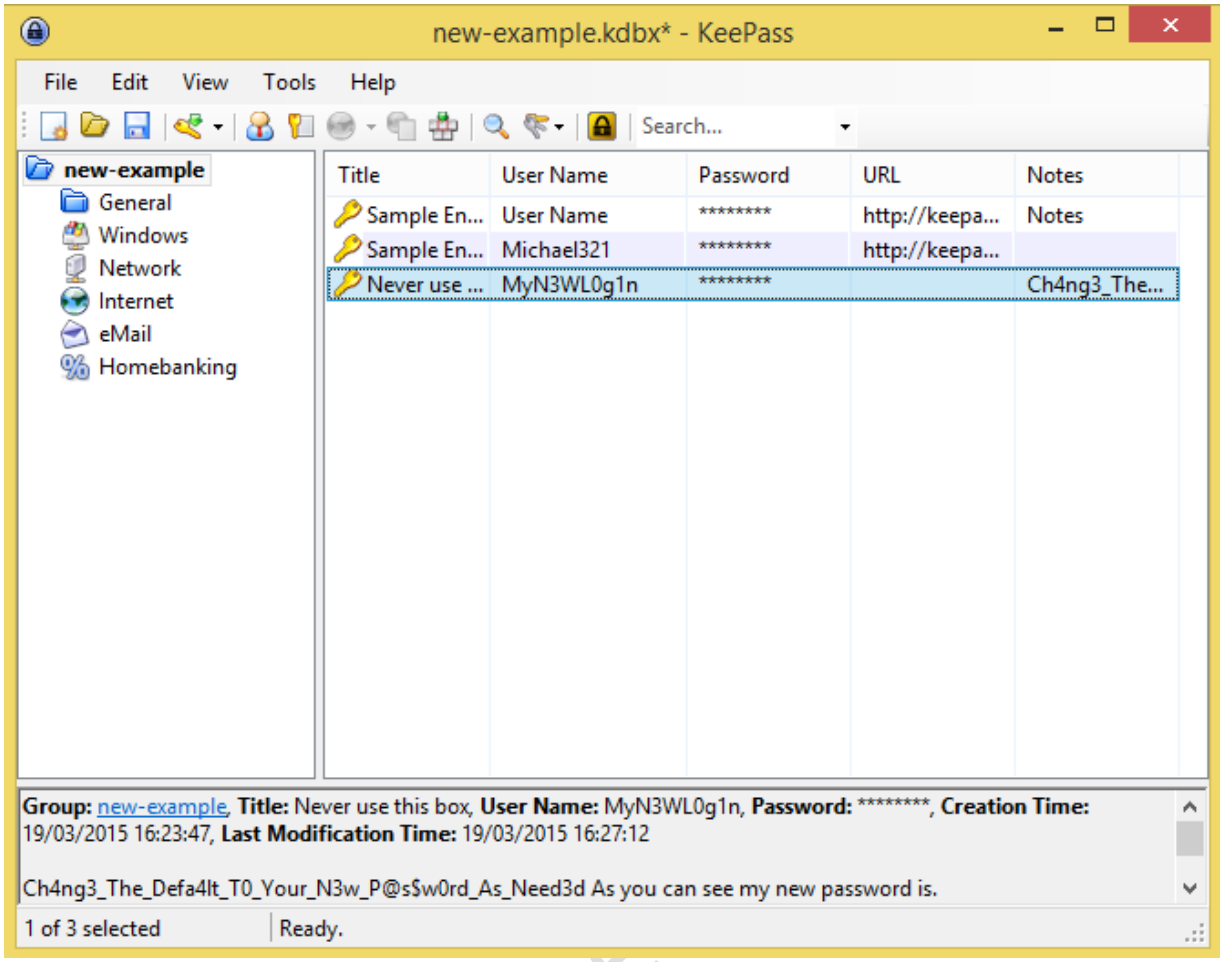
The first decision to make is to create a new password alternatively keep the one that was generated, to see the password simply click on the ellipse



Now just fill in the boxes and click OK

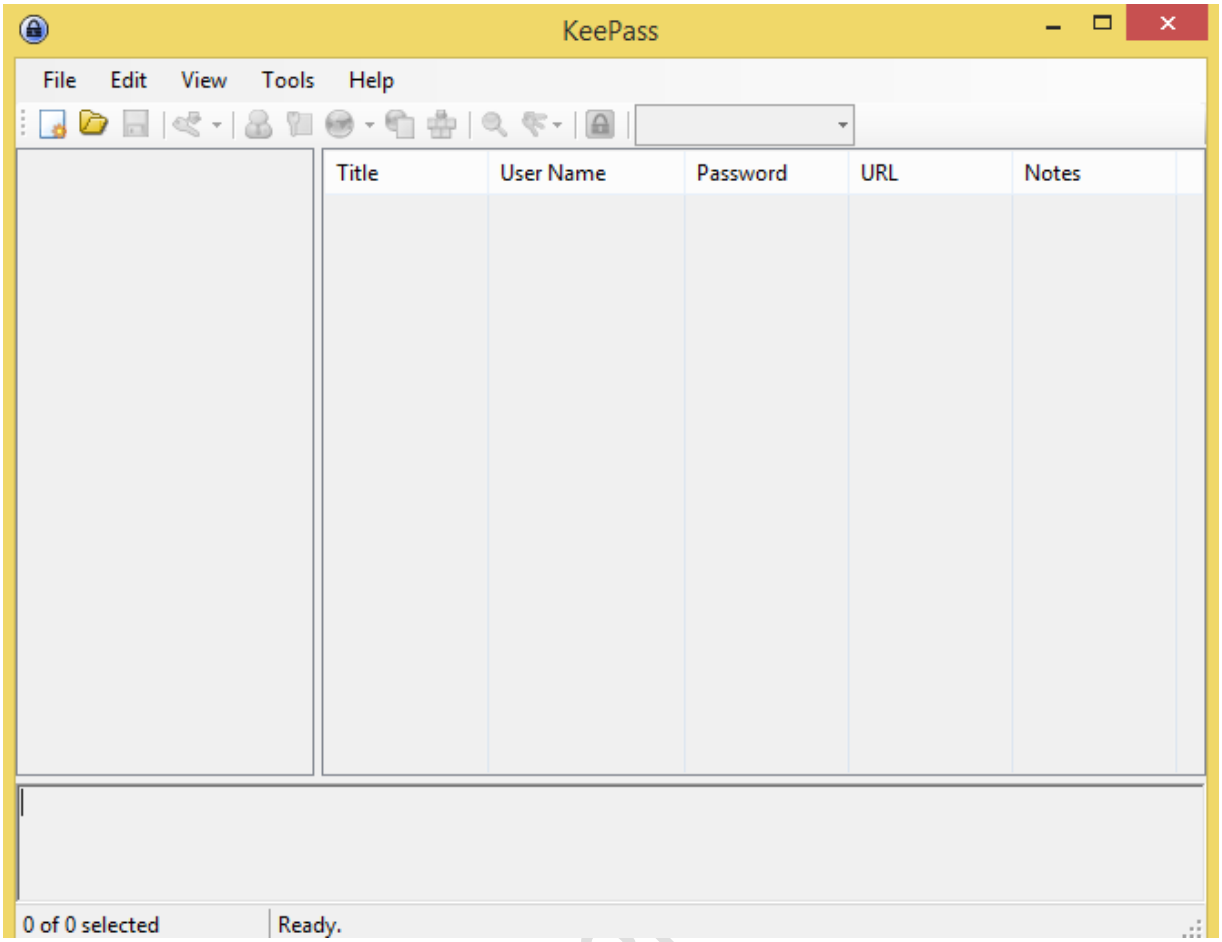


As you can see from the screen print above I have created an example username and password combination. The first thing you should notice is the password strength in the first screen is a different bit length to that in the second image. Note the greater the bit strength the stronger the password. The changes I made as you can see have increased the strength, thus it has an increased length and complexity. By simply clicking OK this will now add the entry two the new database.



As you can see from the screen print above the example entry is now finished. I would encourage you to go on to the Internet to do a Google search for Keepass, or password storage tools you can find free and paid commercial software, but this is a free trusted tool that is kept up to date alternatively click on the link provided http://www.keepass.info

Now all you need to do is remember one password the one that unlocks Keepass ***"I MUST"*** point out that if you forget the master password then you ***"WILL"*** lose access to all passwords, as a wrong password will simply open a blank database. So make sure you "***do not forget"*** the master password.



Now you only need to remember the master password, Keepass will do everything else for you. I would like to thank you for taking the time to read this article and I hope that you found this interesting.

If you have any comments, or, if you would like to have a specific article or require help please feel free to get in touch. You can find me at http://www.leehaynes.me.uk

Thanks

Lee