KeePass - to improve your process

Before proceeding with the article, please take this quick password safety test.

Password Safety Test – Score one point for every YES answer.:

1. Do you write your passwords down? (**YES** / NO)
2. Do you ever re-use a password on multiple systems or websites? (**YES** / NO)
3. Are your passwords shorter than 8 characters? (**YES** / NO)
4. Do you use dictionary words as your password or part of your password? (**YES** / NO)
5. Do you ever use family or pet names as your password? (**YES** / NO)
6. If you lift up your keyboard right now, will you find one or more passwords? (**YES** / NO)

Scoring:

If you answered the above questions with **YES** more than 5 times, then your use of passwords are extremely insecure and you may be in danger, you may be in serious trouble, keep reading and find out what you can do to fix this.

If you answered **YES** more than 3 times then you passwords are insecure and could lead to trouble for you, keep reading and find out what you can do to fix this.

If you answered **YES** at least once, then keep reading. You are not doing bad, but you could use some help.

KeePass is a free open-source password manager and safe which helps you keep track of all of your passwords. KeePass will help you be more secure in your use of passwords.

Too Many Passwords:

Prior to using KeePass I would need to remember dozens of passwords for all of the different websites and systems that I regularly use, along with the password for the systems that you rarely use. These passwords usually ended up on sticky notes on the side of my monitor or under my keyboard.

Re-using passwords:

It is very common for someone to use the same password again and again at every website they signup at. This alone is a security risk, for instance if you sign up with PayPal with one username and password combination, then you sign up some online store to buy something. If you were to

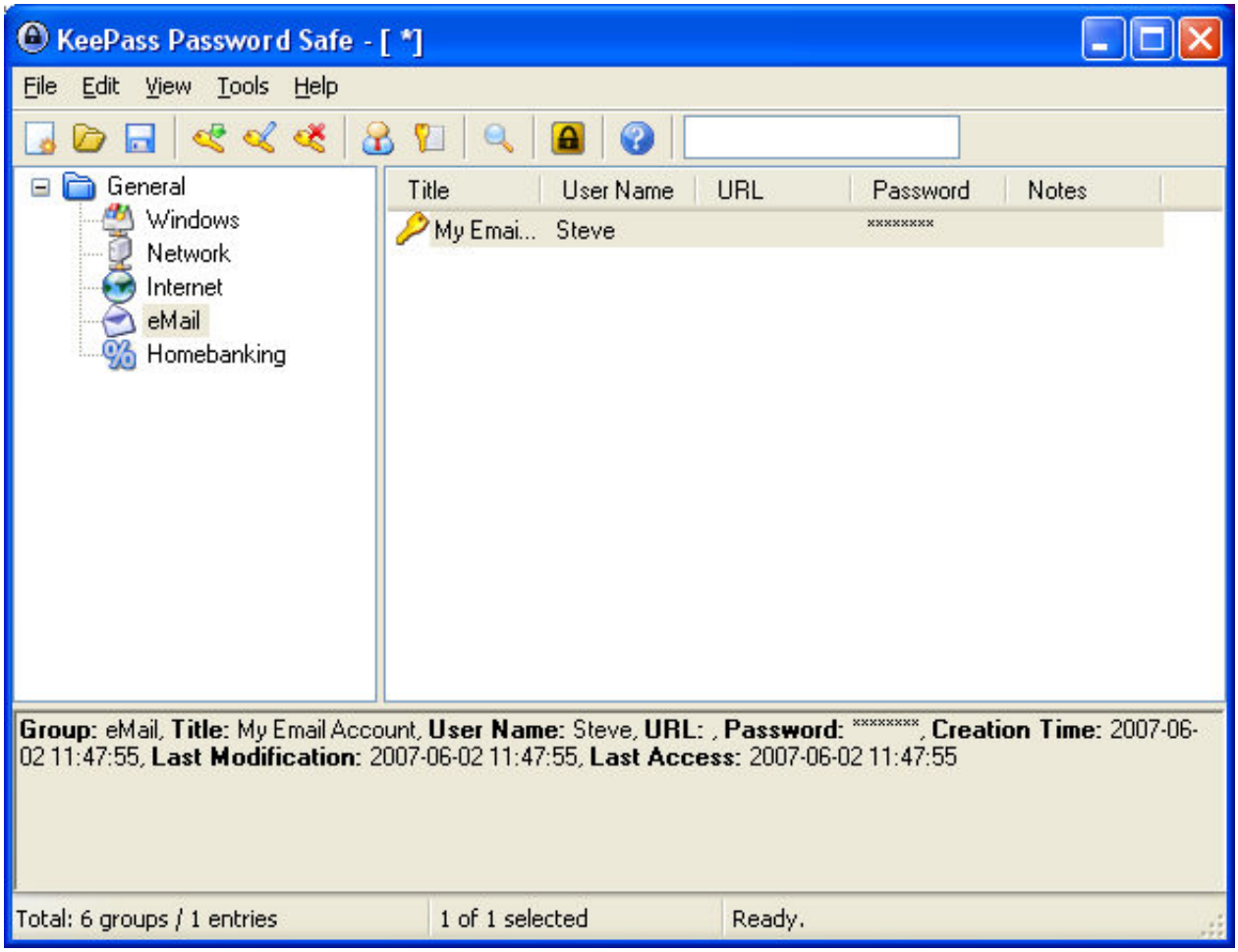
use the same password, then the company with the online store would know your PayPal password. Even worse than that, if one website with your password on it was hacked, and the password list was stolen, then those hackers would have access to a password that matched your PayPal account.

Forgetting your passwords:

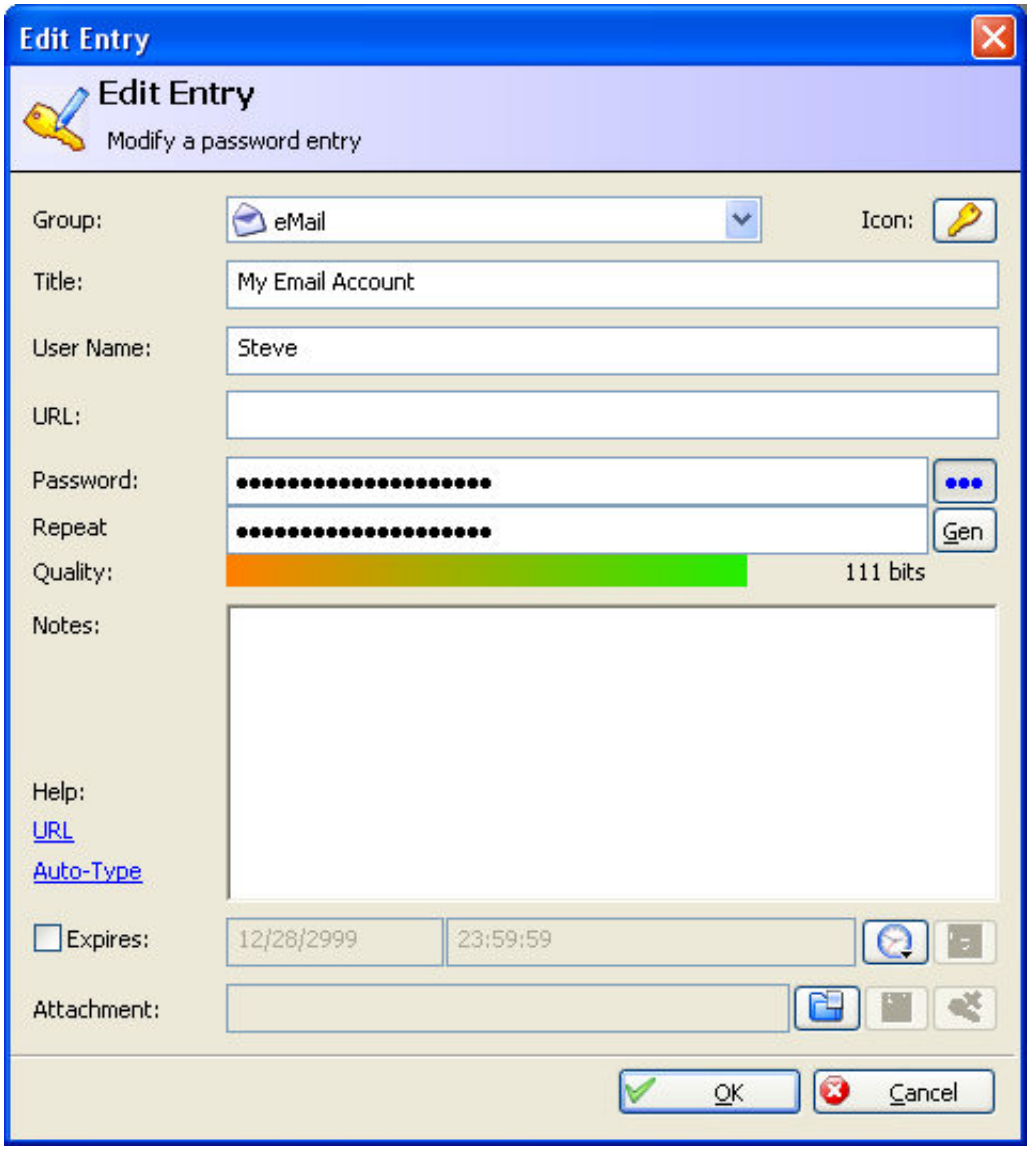
Have you ever gone on vacation for a couple weeks, then when returning home or to work, you realized that you had forgotten one of your commonly used passwords. Have you ever attempted to configure you email account on a new computer and realized that you entered your email account when you set up your old computer, and haven't typed it since, and have no idea what that password is. KeePass can help with this.

KeePass is a tool that I have been using for a while now. When I first started using it, I wasn't too sure if it would work for me, but it turned out great. This article outlines the cool things that I have discovered while using KeePass. This is not a paid advertisement of any kind, just my opinion and nothing more.

The main KeePass page is shown below. You can build a hierarchy of passwords and organize them into groups or folders. You can also search on a term if you forget which group your password is in.



All it takes to get started is to pick the category that you want to add a password to, then click to add an entry. The screen below will be shown. Passwords are generally hidden with ******* since you don't have a reason to see the password, you just need to copy it to the clipboard and paste it into a page.



Another common problem that is fixed by KeePass, is the generation of strong passwords. Strong passwords are passwords that would not be easily guessed by someone trying to break into your account. The challenge is creating strong passwords that you can easily remember. KeePass eliminates the need to remember any passwords, beyond the one password required to get into your KeePass system.

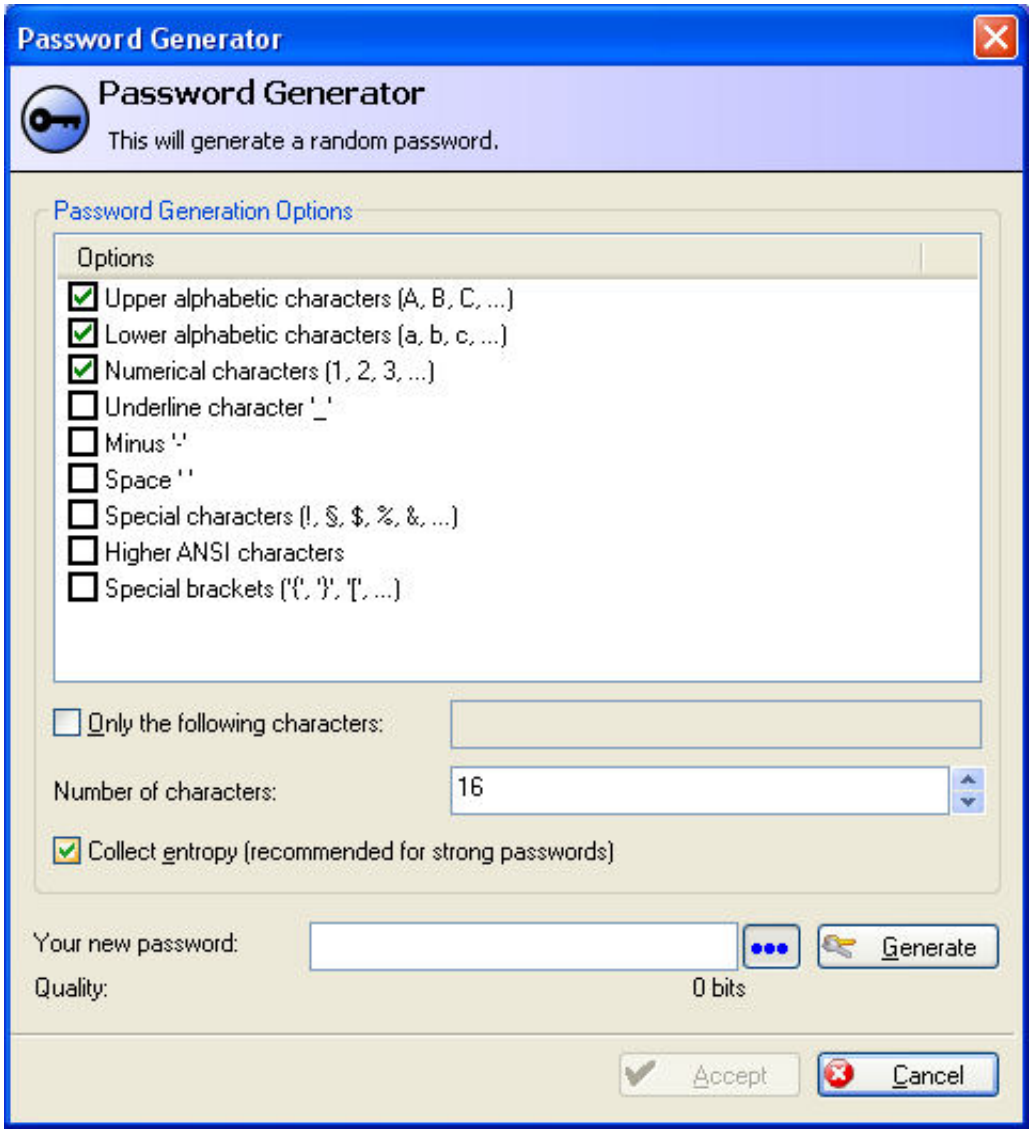
Rules of thumb when choosing passwords:

- Avoid using dictionary words.
- Never use your account name as its password.

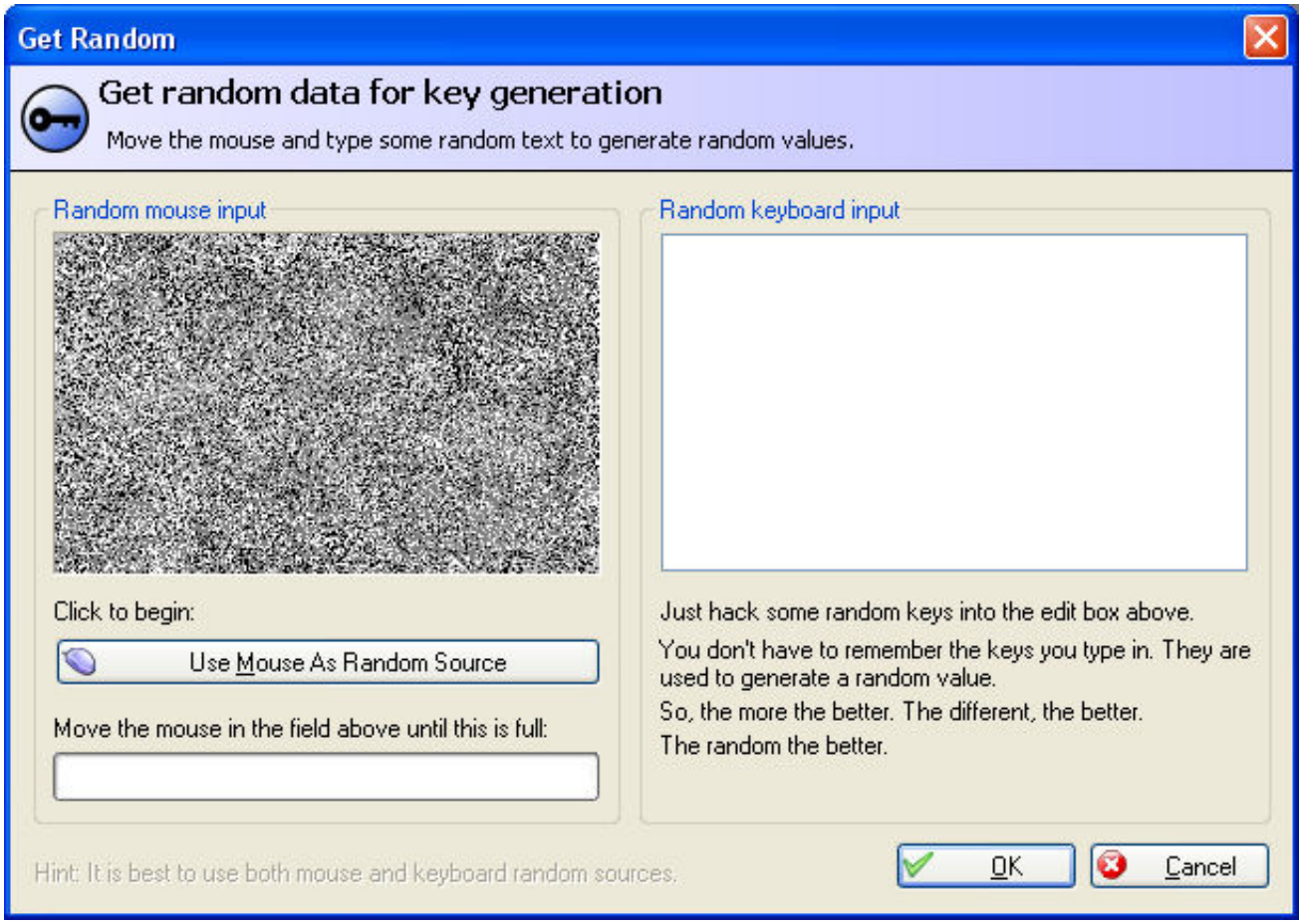
- Use different passwords for each machine.
- Don't use common misspellings of dictionary words (including replacing "i" with "1").
- Don’t use your first or last name in any form.
- Don’t use your spouse's or child's name.
- Don’t use your pet’s name.
- Don’t use a password shorter than 8 characters.
- Don’t use any “method” for creating passwords.

There are many other rules around choosing passwords, but to keep it simple the longer and more random the password, the more secure it will be.

The chart below shows the cracking time based on the length of the password.



KeePass provides tools for generating passwords for you, completely at random, using your keyboard and mouse for random input on the password.



Here are some examples of passwords generated by KeePass:

XUkaojtVwlMxHAZi

9YIlMRz1edPcieagLLpFipnJs8VJ4JUoyGk6Ay01

8A3FpRnkyv08oMS3CVhj6qRX3YFffRcST6ZpCYbw

After looking at these passwords you might think “How can I ever remember a password like that”. The simple answer is that you won’t, but you don’t need to. Just have KeePass store the password for you, then when you need it, copy it to the clipboard and paste it into the password field.

AutoType:

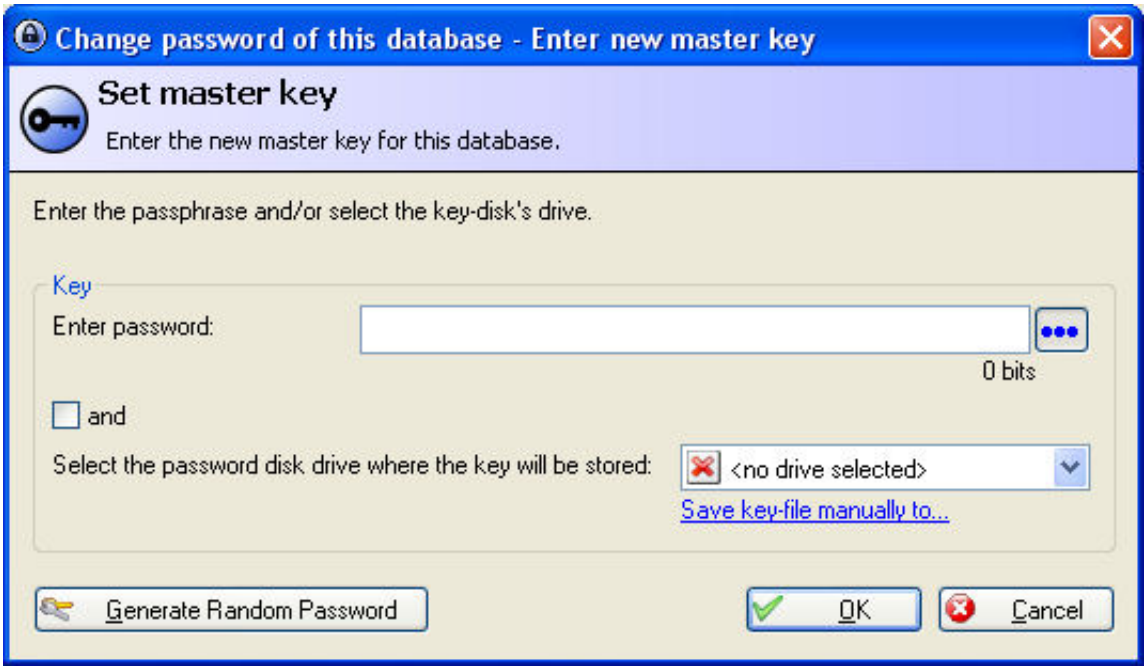
KeePass has a nice feature called autotype. With this you can define the sequence that you passwords should be entered with usernames. For instance an AutoType sequence of {USERNAME}{TAB}{PASSWORD}{ENTER} would send your username, hit tab to go to the next

field, then enter your password and hit enter to submit the form. This is very useful for forms that require multiple lines of input to log in.

With KeePass you set the master password for the whole password safe. Once this has been set, you need to enter this password every time that you start KeePass. If KeePass is minimized to an icon, you need to enter this password to restore it.

So what passwords do I need to remember?

You will only need to remember one password, the password used to use the KeePass program. You can choose this password, keep in mind that you will be typing this password often as you use the system.



Click here to see a video on KeePass and how it applies to LEAN Process.