Computer-Ease

Complete Computer Solutions

www.CVWare.com

Custom Programming IT Services Network Management Websites Computers

Keeping Track of those passwords

Using a **Password Manager** is a great way to safely and securely keep ALL of your passwords in one place, making it easy to find and use when you need them. It can also be an excellent way to update, keep track of old passwords, keep security questions, and much more.

The latest push at password management is to have an online password manager, and while these do have some advantages, personally I prefer to have a local, safe password manager that is NOT in the cloud. In the cloud you never know who is attempting to hack your account, plus some systems can be compromised from 'behind' if they are not properly encrypted and maintained. Add to this the cost of most services and how they work, and I will take a local password manager every time!

KeePass is an excellent password manager, which keeps passwords in a local, encrypted database, has an amazing set of features and is free! Every computer that I have installed or setup in the last five years should have a KeePass link on their desktop or loaded on their machine. You may need to update it, but it should already be loaded for you to take a look at it.

You will also discover that KeePass is not only an excellent password manager, but it also has many other excellent features. For example, you could save bank statements, sensitive documents, store information about your credit cards, pin numbers etc. all in KeePass. And because the KeePass database is encrypted and secure, all of this information is safe.

KeePass organization is simple and easy to use. All data is stored in a Group / List Entry structure, which is easily searchable, and can be easily modified as well.

KeePass uses a single Master password to access this secure area, so you need to make sure you have a good, strong password, and that you never lose it. Once you have logged in to KeePass, use is as easy as finding the location you want to log into, clicking on the URL and then using the username and password data to login.

KeePass also has the ability to even choose multiple "MasterPassword login" methods. As an example you could require a certain file (or set of files) to be at a certain location on your hard drive to login in KeePass, making it even more secure. (And if you want even better security, there are MORE methods to 'lock it all down'.)

Simply stated, KeePass is an open source, well maintained software which is safe, secure and will help you manage all of your password needs. (and it works on ALL computers and phones too!)

Writing about all the features that KeePass has is an entire subject in itself, but I will describe some of the best features below. (I have written a KeePass tutorial for anyone wanting more instruction on it – please just let me know.)

Groups:
KeePass uses Groups to organize the data, and it comes already setup with some common groups you may like and use. (General, Windows, Network, Internet, email and Home Banking) Or if you prefer, you can easily change / add / delete groups exactly how you would like them.

Entries:
An Entry is where data is kept in KeePass, and this is where you will enter and find your data. Each Entry is typically one location to work with.

A basic Entry contains: website URL (or location), your account / username and then the password to login to that location. Typically you will only have one login here and the current password for that login. Using this Entry, and three clicks, KeePass will log you in to that location.

Each Entry also has an area for notes, and you can keep copies of your older passwords here as well. (And you should always keep old passwords, for several reasons, 1) to be able to know what passwords you have used, and 2) some locations require the last password you can remember if you have to recover your account!)

There are also several additional types of data that can be utilized in each Entry, and these are defined in different Tabs in the main Entry Dialog. The General Tab is where the Title, Location, User name, Password and Notes are located and where you will be most of the time. This General tab also has a place for the internet location (URL), as well as showing you how strong your password is. (The Quality field.) Everything you 'need' is on this one tab.

The Notes field can contain any notes, old passwords, security questions, pin #'s etc. Additionally, if you go to the Advanced Tab you will find another area where you can do much much more.

Typical Use:
Normal use of KeePass is basically three steps once you have logged in to KeePass.
1) Find the Entry you want to use (ie use the Search Field)
2) Double click on the URL of the entry. This will open the URL in your web browser
3) You then would either:
   a) Copy and Paste your username and password into the web page
      or
   b) Right Click on the username and then choose Perform Auto-type

There can be a little more that has to be done on some websites for Auto-Type to be used, and some websites will attempt to block any 'auto type' functions, However Auto-Type is a great feature and can save some steps where you can use it. (And Auto-Type is configurable, so many times we can work around a website's issues too.)

Advanced Tab:
On the Advanced tab there are two sections, String Fields and File Attachments. String fields are a "Name / Value" pair that you create to contain any information that you want to save. This could be a pin number, or security questions, special phone numbers, or much more.

The second area, File Attachments, is where you can add any digital file and it will be kept safe. Some examples of sensitive information you might want to save here include: bank statements, ins policies, health information, special documents, etc. The file is attached and the name is shown and you can open the file directly from here or save it out to open / print etc.

Searching:
Every field on the General tab is searchable, and so from the main KeePass screen you can search for any information contained on the General Tab. Title, User Name, password, URL or Notes can all be searched, which provides a super fast method of finding your data!

Recycle Bin:
KeePass has its very own Recycle Bin, so data that you delete when in KeePass does not leave the secure area. All deleted entries are placed in this secure Recycle Bin, until you delete the Entry in the Recycle Bin and then it is gone forever.

Security:
I wont get deep into security here, and will just say that KeePass utilizes SHA-256 encryption which is one of the highest security protocols there is and it is one of the strongest and safest encryption schemes that is available today. (You do still need to create a GOOD strong Master password for KeePass – and make sure to never lose it!)

Simply stated, KeePass is an open source, well maintained software which is regularly audited by various private and public security commissions and agencies. The strength of this open-source method is that the code can be viewed by security experts, any problems identified and discussed for the best fix possible.

Saving to the Cloud:
One of the beauties of KeePass is how secure it is. While the KeePass database resides locally on your computer, it is so secure that you could put the KeePass database into a DropBox location and use it. While I will always say that local is typically far safer than “the cloud”, keeping your KeePass database safely backed up and secure is critical, and even if someone were to get a hold of it, there is little they could do to crack it.

Because all of your passwords and sensitive data is in KeePass, you need to make sure you keep it backed up, especially when you add or modify the database. Keeping KeePass automatically backed up is a great idea, and DropBox or a service like that, will help with automating that process.

Sharing:
KeePass can even be shared among people. KeePass has the ability to understand if multiple people are using it on a network and it will react (ie let you know) if someone changed data at the same time and will usually save the data properly. In instances that there is an issue saving, you are presented with possible resolutions to choose from.

Additionally, we can use KeePass in many situations where we want to pass data to another person, or have the data on a USB stick and we don't have to worry about that data being compromised should the stick be lost or stolen. The database is typically small, and so it can easily be emailed or saved to a stick as well.

If you need / want to have someone hold a copy of your passwords for security or in case something happens to you, this is a great tool to use for that as well. As an example, I have clients that have their KeePass database in their DropBox data with their children having access, and then the Master Password for KeePass is stored in their Trust documents – This presents an extremely secure method to "hand your passwords" to someone for safe keeping, but not letting them use them until they have the Master Password.

And KeePass can have multiple and different databases as well. So you could have a database for work, a different one for home, and could make as many databases as you need. (one for family, or one to just hold special papers, etc).

With today's requirement of being proactive in security and the handling of passwords being of upmost importance, I urge everyone to start using a good password manager! And KeePass is an amazing solution to help you handle both passwords as well as your sensitive data.

In the next article we have more about staying safer on-line, a large topic with many pieces, but some we have already covered and are already on our way to understanding being safer.

And you can read about these issues and more at: www.cvware.com/articles.html

This article in PDF is at: www.cvware.com/articles/KeePass-Password-Manager.pdf