KeePass Installation and Usage
Go to http://keepass.info, click on Downloads
Download the latest version 2 “Installer”
If you also want to run Keepass from a USB stick, also download version 2 “Portable”
(Lower on this page are links to Keepass apps for Android and iOS apps)

Install Keepass on your computer from the downloaded installer, Add a Desktop icon if you want, then open KeePass

Create a new database to store all your passwords - File > New
Enter the master password. The database will be encrypted with this password. It should be long and with mixed characters upper lower case and numeric at least.
Do not use “Windows user account” or “Keyfile” options
MAKE SURE YOU REMEMBER IT otherwise your database will not be accessible.
Enter a file name and select location for your database

First set up your Groups - use default groups or make your own groups
Then start adding entries - Select a group then Edit > Add Entry
Enter some title for it, a username, an URL, username, password, and any other info
You can just use an entry to store information, such as bank account details, you don’t have to use the username password fields.

Save and back up the database
Click onto the 'Save' toolbar button. Make a backup copy of your database file on two USB disks

Getting username/password into a web site login page (or any other program)
Using Copy/Paste - right click on the entry.
You have several options now. You can for example copy the username of the entry, then paste it into any other program of your choice. The same works for copying passwords.

On many web sites you can use **Autotype** instead of copy/paste. To turn on Autotype for an entry:

- Double click on a database entry
- Choose the *Auto-Type* tab
- Tick *Enable auto-type for this entry* AND *Two-channel auto-type obfuscation*
- Click OK the Save the Database

To use Autotype (Note that autotype does not work on all web sites):

- Open the web site where you want to login, place the cursor in the username field
- Switch to KeePass, Right click on the entry in KeePass and choose *Perform auto-type*

Adding Images of Important Documents to KeePass
For example, to add your passport details:

- Make an image of your passport (photo or scan)
- Open *KeePass* and add a new entry called *Passport*
- Add the passport number and expiry date, etc. to the *Notes* section
- Click the *Advanced* tab, in the *File Attachments* section click *Attach,* then click *Attach File(s)…*
- Locate the image of your passport in the file open window that appears, then click *Open*
- Save your database

The image is now added to your KeePass database. To view the image click on the image name either in the Advanced tab, or at the bottom of the entry summary.

Securing your KeePass
You can change a number of settings that will make Keepass safer to use, including preventing keylogging malware from grabbing your master password.

Set Secure Desktop
Click *Tools / Options, then* click the *Security* tab then look at the *Options* section, tick *Enter master key on secure desktop* – this will make your desktop background fade whenever you type in your master password and prevent any other program eavesdropping. Click OK, then save the database

Key Transformation delay
If a hacker obtained your password database and had access to a supercomputer it is possible to eventually crack your master password. To effectively stop this ever happening, you can slow down your database's response to password attempts – the default setting is one second.
File / Database Settings > Security tab then click *"1 second delay"* to see how many attempts to crack your password could be made in one second on your computer without this setting.
If you change this setting, save your database. If you set this value too high it will increase the time to open your database.

Securing your database while open
Your passwords are vulnerable while KeePass has your database open – if you leave your computer with KeePass open, someone else can look at your passwords, print your database, or export your database to their own CSV or text file. Or they could find a password on your clipboard. To reduce the possibility of this:

- Click *Tools / Options* then click the *Security* tab
- Tick *Lock workspace after KeePass inactivity* and enter a number of seconds (suggest 300)
- Tick *Clipboard auto-clear time (seconds)* and enter a number of seconds (suggest 20)
- Click the *Policy* tab
- **Untick** the option *Export – no key repeat* – then your master password is required to be entered again to export your data
- **Untick** the option *Print – no key repeat* – then your master password is required to be entered again to print your data
- Click OK, then save your database
- Close KeePass and reopen it for your Policy changes to take effect.

Installing Keepass application on a USB stick

- Copy your KeePass database to your USB stick
- Make a new folder on your USB stick called Application (or whatever), open that folder
- Open the downloaded Keepass zip file, select all files > Copy
- Paste the files in the Application folder on your USB stick
- To run KeePass on any computer, plug in the USB stick, open the Application folder then double click on KeePass.exe
- File > Open your database that is on the USB stick
- Change the security settings as above.

Note: Keepass by default remembers the last database opened and will reopen that when restarted. To open a different database, just use File > open like any other program.

KeePass Help & Tutorials are available on the keepass.info site

KeePass Mobile device apps
Android: KeePass2Android
https://play.google.com/store/apps/details?id=keepass2android.keepass2android

iOS: PassDrop 2
https://itunes.apple.com/app/id1206056096