Home, Computer and internet security – additional measures

This document covers some optional measures you can take in addition to the 'behaviours' discussed in the first document. These measures cover several important areas and are worth the effort to experiment with even if you eventually decide not to use them. It is useful to know what is available in any case. Other solutions are available – just check carefully.

- This document covers my personal suggestions and these are not 'endorsed' by the U3A in any way they are provided 'as is' for you to decide what is appropriate to you
  - It has been prompted by the alarming increase in scams and ransomware etc.
  - Many people use them on a wide range of devices and computers
- It is your responsibility to carefully check these suggestions and only implement those you feel confident to try. However they can be added, experimented with and removed without causing any problems
- Sources are included for additional reading before you try them
- Some basic instructions are included to help you get started
- There are many more things one could do, but each additional security measure tends to make the internet more difficult to use because the security has to STOP stuff working since it is very hard to tell if a software action is actually good or bad
- Another point to bear in mind is that good software is not free. It costs a lot of money to develop the software and run the services. However, some very good software is free because it is supported by a company or a wealthy individual or a group who just want to do it and offer good, safe software to the public. So in the following pages;
  - Ublock Origin is free and supported by the originator Raymond Hill
  - Keepass is free and supported by donations
  - SIGNAL is free and developed and supported by its originator and donations I think
  - FREEDOME is a paid for service
  - The Linux operating system is also free/supported by donations and its original developer Linus Torvalds. It is worth noting that Android is a development of Linux and in fact so is Apple OSx. Most digital TVs, routers and a huge proportion of the internet also depend on the Linux operating system
- It is hoped this information is useful and helps you improve awareness and the security of your computer
- These are suggestions, they may differ from yours or you may be very happy with your own protections – none of this is mandatory!

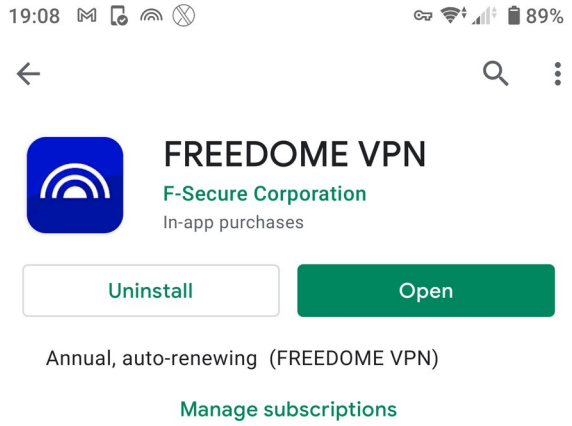
Mobile phones and tablets – Adding a VPN

For greater privacy, turn off your bluetooth, wifi location and data when you are not using them and never use open wifi hot spots – just use your phones data it is far safer

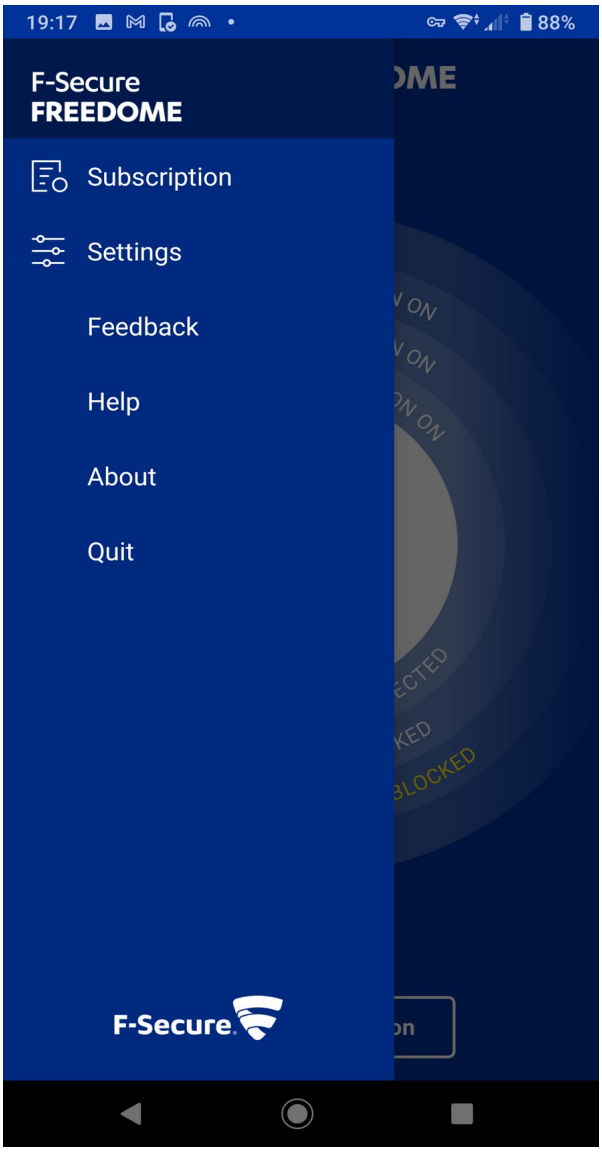
- Never do any banking or financial transactions when you are connected to any ‘hot-spots, airport, cafe, Hotel wifi etc. These are snooped by hackers and criminals
- Better still is to install a VPN – Virtual Private Network. This is a software application on your computer, phone or tablet. It encrypts all data travelling between your device and the exit point of the VPN. BUT you must use a secure and trusted VPN or you cannot trust the exit point
- The safest and simplest found so far is the FREEDOME VPN from a Finnish company called **f-secure.** They have been established for many years, have an excellent reputation and are well respected. Here is their website:

  https://www.f-secure.com/en/home
- This software also blocks you visiting known bad websites, it checks all of your applications and whenever they update. It also blocks websites tracking where you visit.
- It works by encrypting the data mainly any phone data, your email and browsing, then it is transported to secure servers run by f-secure, decrypted, checked and only then allowed into the internet.
- This means your data cannot be intercepted by hackers and criminals over any wifi
- It does not slow down your device
- It can just be left ON and it just works over your data connection too protecting you from known harmful websites
- It offers a month free trial period (I don’t think you have commit to purchase for the trial – it just times out after a month). It costs about £22 per year and it also runs on all your devices that are on one account (say a gmail account) so if you have paid for it, it will run on any tablet or phone you have on that account.
- It is also available for Apple and Windows computers but at additional cost to the account on your mobile device
- In the settings you can add your TRUSTED wifi networks so that you can control any home devices (like a Firestick or Chromecast etc.)
  - NEVER trust hotel, airport, cafe, wifi - these are what FREEDOME protects you from
  - If you cant connect to an open wifi when FREEDOME is running, don’t turn off FREEDOME - use your data service
- In settings you can also disable FREEDOME for other SPECIFIC applications on the device that wont work over a VPN. BBC iPlayer is one for instance because it is geographically

restricted and a VPN can exit in any country. Be very careful which applications you allow to bypass FREEDOME – since its protecting you



Above - The app in the play store



You can turn it on/off here and clicking the 3 lines opens the settings page (left) where you can add trusted wifi networks

Left shows , click the settings

This is a very good – essential App to add to your phone/tablet and well worth the annual cost

The internet – browser – adding one helpful security tool

Together with email, this is your main connection to the internet for email, banking and shopping and it is therefore a primary target for scammers and hackers as are all the web-sites.

- Google chrome, Apple Safari, Microsoft Edge, Mozilla firefox
  - These are all good browsers, the companies try to keep them secure but they do all have weaknesses that can be and are exploited all the time
- These browsers permit the addition of small software programs called ADD-ONS or EXTENSIONS. Some of these are very good and offer valuable additional protection to your browser. You must be very careful what you do add as not all are tested, safe, supported and maintained
- The main one you could add for good additional protection with a MINIMAL impact on usability is **Ublock Origin**

Ublock Origin

This is a small 'tool' that runs all the time in the browser. It has rules that try to identify and block bad web sites, bad web page actions and things that track you. It may sometimes stop a web site working fully but you can turn it off for the site you are on and it remembers.

It is fast and comprehensive and it is maintained. It is respected and recommended by many security experts. It is not likely to interfere with any anti-virus suite you may have installed and it offers valuable additional protection that many anti-virus systems don't. If it should interfere, you can disable it for the site you are on and it remembers specifically any site.

Find the setup/configuration/preferences section for

Mozilla Firefox — Add-Ons and click find more add-ons then search for Ublock origin
they do change the layout of the ADD-ONS system occasionally and confusingly once installed they are then called 'extensions'. However it should not be too hard to find the correct ADD-ON

Google Chrome — Go to the three dots on the right and select Tools/extensions
at bottom of the panel Open web store and search for Ublock Origin

Search for **ublock origin**

Make sure the developer is **Raymond Hill** (gorhill)

Add it to your browser (allow it to work in private windows – if it asks)

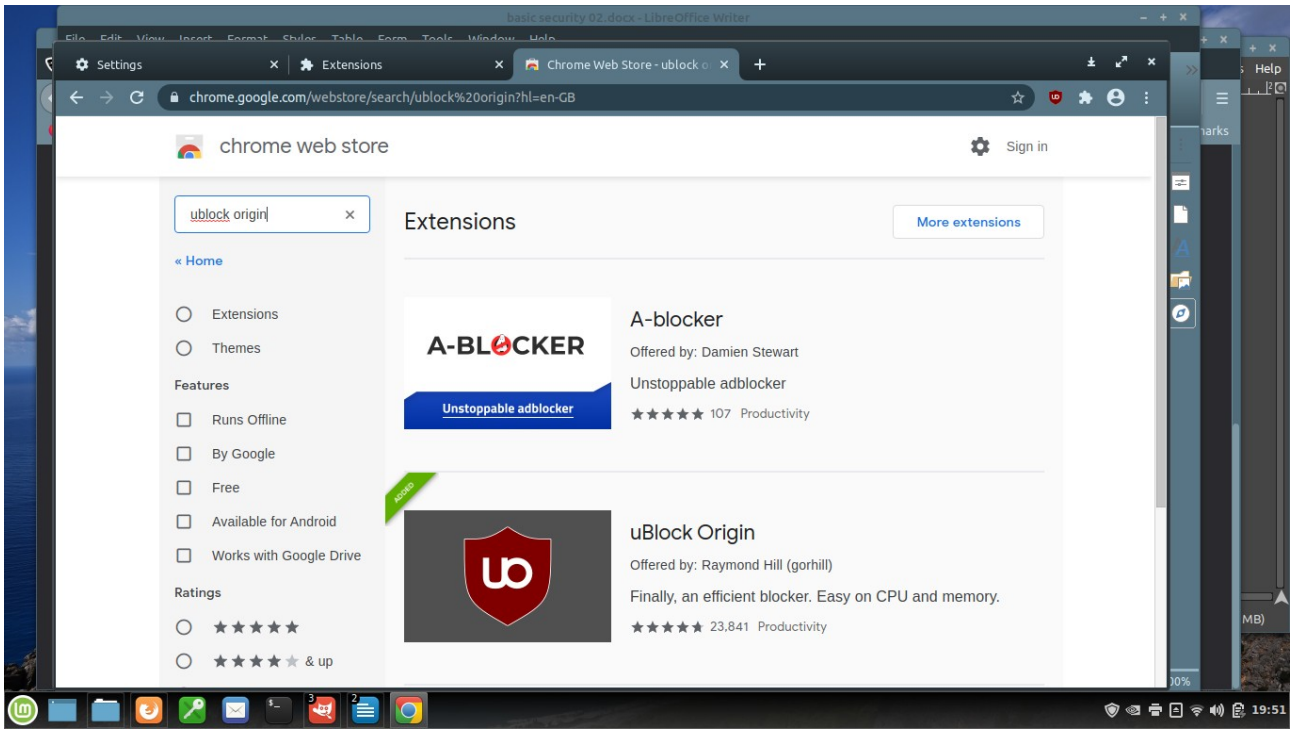
You can read more about it on the developers website – here

https://ublockorigin.com/

An extract from the above site

> In January 2017, *uBlock Origin* was added to the repositories for *Debian 9*, and *Ubuntu (16.04)*, and the uBlock Origin extension was awarded the prestigious IoT honor of “Pick of the Month” by *Mozilla*.
>
> As of 2021, *uBlock Origin* continues to be maintained and actively developed by founder and lead developer Raymond Hill.
>
> The *uBlock Origin* extension remains an industry leading, open-source, cross-platform browser extension with software developed specifically for multiple platform use, and as of 2021, uBlock Origin’s extension is available for several of the most widely used browsers, including: *Chrome*, *Chromium*, *Edge*, *Opera*, *Firefox* and all *Safari* releases prior to 13.
>
> The *uBlock Origin* project still specifically refuses donations at this time, and instead advises all of its clients, users and supporters to donate to block list maintainers.

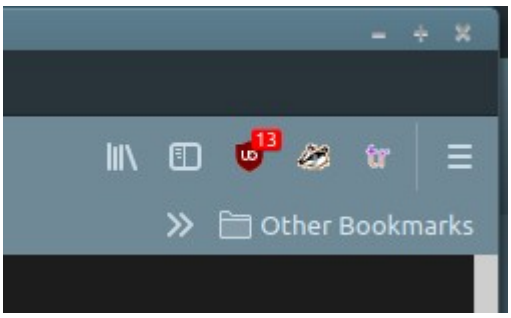
In Chrome – it looks like this with the red shield and Firefox will be similar



If you click on the Ublock Origin icon, it will give you additional information.

MAKE SURE it is **Ublock Origin by Raymond Hill (Gorhill)**

Once installed, it will add a small red shield to the browsers top line on the right like this.



The number shows how many functions on this website page are being blocked

Web sites use many functions and link out to all sorts of places (sometimes hundreds). It will be a mix of required functions and loads of adverts, tracking activity and perhaps much worse. Ublock Origin will help protect you from it.

Adverts are usually supplied to websites from ‘advert servers’ that are often not well maintained and many have malware (bad virus software) – often you don’t even have to click on an advert for your computer to get infected, your browser just has to receive it. Ublock Origin helps protect your browser from these problems.

If you click on the shield a panel pops up and you can disable Ublock Origin for the site you are on by pressing the blue button and it will remember that for when you next visit that page/site

Like this

Passwords

These are a modern scourge – but they are the most common and important method to access an account. Criminals and hackers attack websites and extract millions of users email addresses and passwords. They then use computer programs to try these combinations on all other sites to see if duplicate or simple passwords have been used. This is done on an industrial scale. Your only protection is a unique and complex password and being careful.

- Don't forget – your house / computer is available to the planet and so are all the web sites you visit – therefore our devices and website are targets of hackers and criminals
- YOU MUST HAVE A SEPARATE PASSWORD FOR EVERY ACCOUNT
- NEVER RE-USE A PASSWORD ANYWHERE
- THEY MUST ALL BE at least 12 (more is better) characters with a mix of upper, lower case, numbers and 1 or 2 of the basic symbols (like # * & $ % @ etc.)
- THEY MUST BE RANDOM no names, words, numbers used as letters etc.
- To manage this you <u>should</u> use a good password manager, but a spreadsheet or word document with a password is ok. BUT it wont generate high quality passwords for you
    - it must not be 'on the internet'/cloud or whatever
    - you must store all your (correct) web site addresses (the login page) and corresponding usernames and passwords in the password manager (or spreadsheet / document)
    - storing the login page address of each web site (called the URL) in the manager means it will only ever take you to the <u>correct address</u> and therefore avoid the l1oydsbank trap

<u>A secure, tested audited password manager</u>

- This would be one called <u>Keepass</u> – it does not connect to the internet
- It will take some practice to use, it is deliberately not 'automatic' to improve reliability and security. To automate means having to be dependent on the computer and browser in use and that makes it much more complex and less secure. It uses a simple copy and paste method for that reason – you have to copy/paste between Keepass and the browser – not difficult
- IT WILL GENERATE and manage unique, complex passwords for you
- It is available for Apple, Linux, Windows and Android and your password store will work with all the computer systems even a phone/tablet with a USB On-The-Go lead
- Its a small (only 4.3Mb and smaller than a word document) simple program that stores all your websites and passwords in a small encrypted file and it is better to put this on a removable USB pen specifically for your passwords

- This means you only need to remember ONE complicated password for Keepass and you never need to remember any others – so they can all be complicated!
- You can also store your bank cards, PINs and other security info etc. in it
- You can organise it however you like
- It will open your browser and take you directly to the login page of the web site you select
- In some cases it can 'auto-type' (enter) the username and password for you but some sites ask for the username first, then present a new page for the password. So I always just copy the username then the password.
- Keepass will scrub the copy/paste memory after 30 seconds or so – never leaving anything on the computer
- Put your password store on a small USB pen, always have a backup copy of this pen, always keep them both up to date, store the spare in a safe place. This is important because if your computer fails, or you got a ransomware virus that encrypted your drive, you would still have all your passwords safely on the pen(s)

How to get Keepass

https://keepass.info/

Above is the main website page

https://keepass.info/ratings.html

Above covers the awards, auditing by the EU and security services that recommend/specify it

https://keepass.info/download.html

On the downloads page above you can get the Windows version.

Here there is also the Windows portable version in a zip file. Its best to get this one as well and put it on your secure pen. You can un-zip it onto the pen and it is useful if you are somewhere where you don't have it on a computer or no internet to download the keepass program. The portable version just runs from the pen. Also on the downloads section are other versions so for:

LINUX the best one is **KeePassXC**– this is probably in the linux software store anyway

Also from https://keepassxc.org/

MAC Osx the best one is **KeePassXC**

Also from https://keepassxc.org/

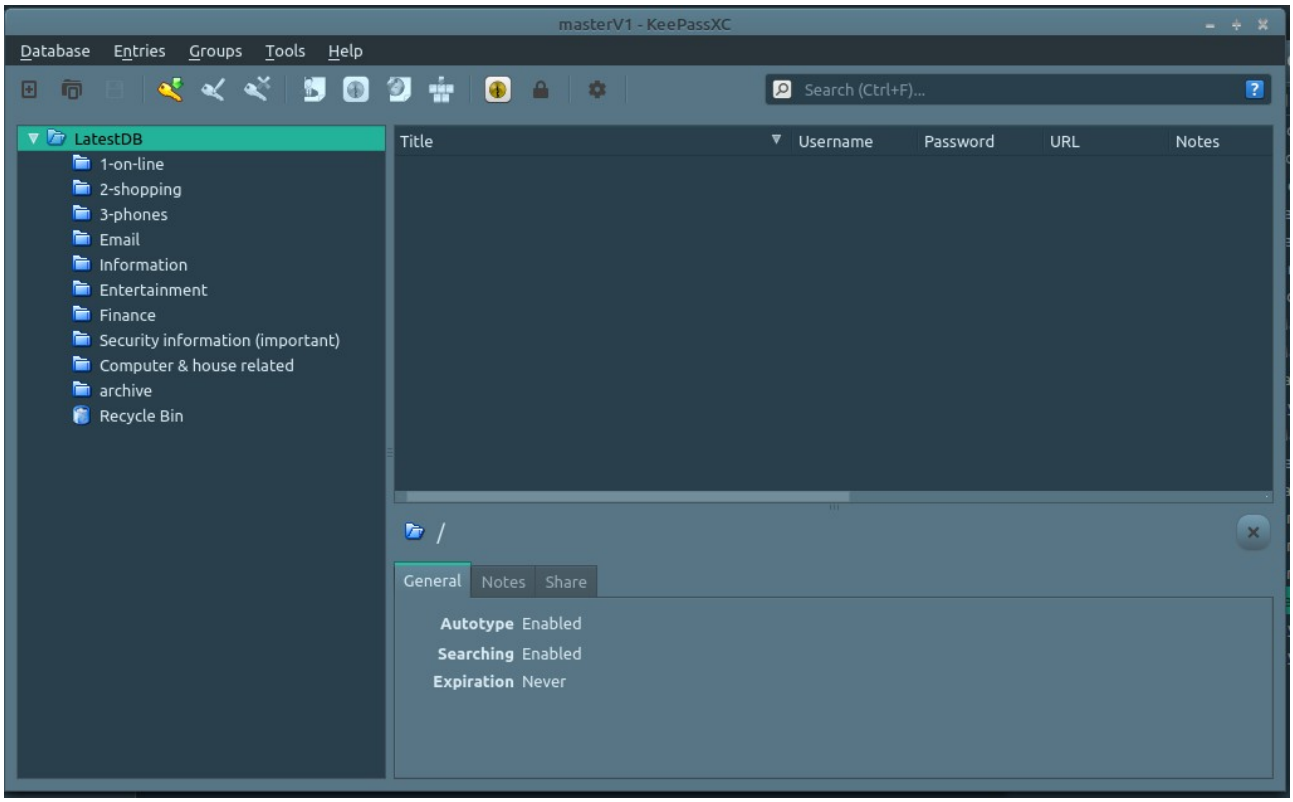
ANDROID the best one is **KeePass2** (in the play store)

Only install the off-line version

iPHONE – I don't know if Keepass is available in the App Store

Using Keepass

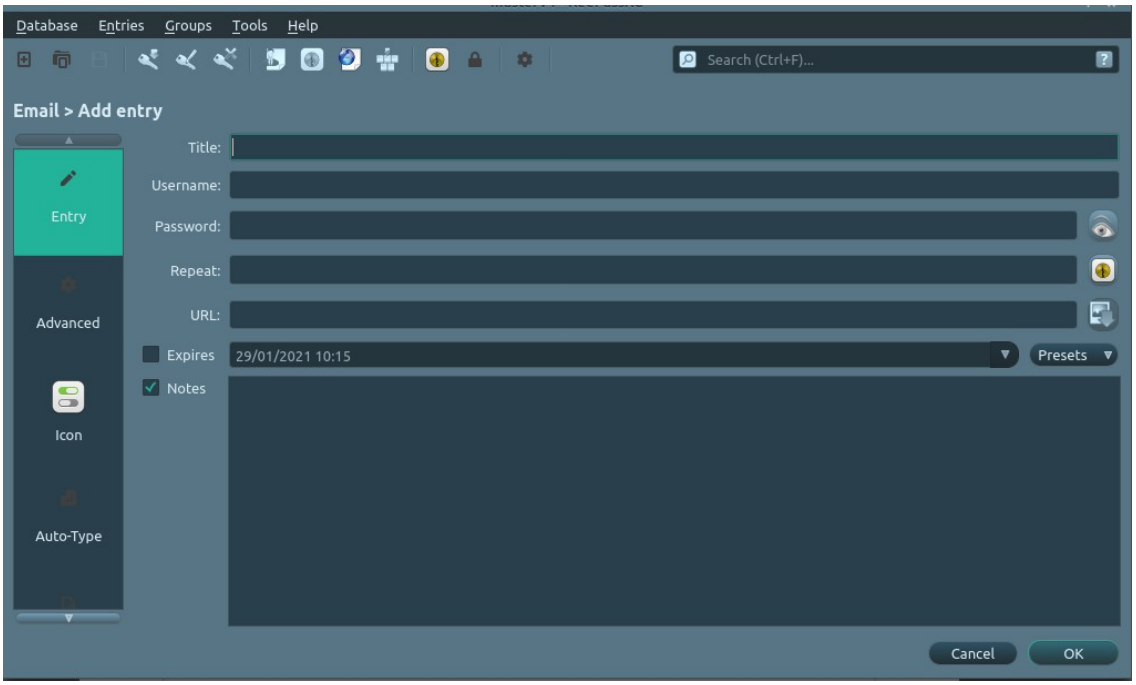
Once you have started a new password database file and given it a password, you see something like the screen shown below. The categories (folders) on the left are examples – you could make your own.



These will all read your password database wherever you store it (on your USB pen is best) and it will work on all operating systems.

- To add a new website – click the yellow key (new entry), this gives a new entry form. On the right hand side is an ‘eye’ symbol – this will display a password. Under that is a ‘key hole’ symbol (looks like a cats eye) – this is the password generator and rules
- Enter a name for the entry
- Enter your username for this site (usually your email address)
- Enter your existing password or generate a new one – you can change the generation rules, length (number of characters), and complexity. You should see the yellow ‘key hole (cats eye), click this to change the length and complexity and accept. You could avoid using symbol characters in some of your passwords (so just numbers, upper and lower) but then you should select a 20 character length – but it is easier to enter on a phone/tablet
- If you are going to change an existing password, you must go through the procedure on that website and make sure you copy the new one generated by Keepass and test it

- Make sure you go to the websites login page with your browser, copy the browser address line and paste it into the URL section in the Keepass entry
- In the notes section you can add notes, card PIN and Bank account numbers etc. anything you like, it all gets encrypted safely into the small store file
- SAVE your entry



Above – the new entry screen

Using Keepass to visit a site

Plug in your USB pen if you store the password file on one

Open Keepass, select your password file (it does remember the last files location) then enter your Keepass password.

You should see all your saved websites or folders with them organised. On the web site you want to visit - click the entry (left mouse to highlight/select) then click the right mouse button and a pop-up shows a menu.

The main ones to use are – in bold:

- **open URL**
  - this makes your browser open and go straight to the website address you saved in the entry which should be the login page for that site
- **copy username**
  - copies username into the copy buffer
  - go to the browser (a tab on your screen) and paste into the websites username field

- **copy password**
  - copies password into the copy buffer
  - go to the browser (a tab on your screen) and paste into the websites password field
- Auto-type
  - This can type your username and password into the website for you but it cant always work because of the way websites are designed – it is therefore better to just use the above copy and paste method

All data in the copy/paste buffer is erased after about 30 seconds

Secure, safe and private text and phone calls

SIGNAL from Silent Whisper Systems is an encrypted and secure text and phone call service for general communications, although based in the USA, the owners/developers have provided a very secure and free service. See here for information https://www.signal.org/

Its in the Apple/Andriod app store

They also support versions for Windows, Apple and Linux computers available on the above website

Signal uses end-to-end encryption, does not retain logs, has no spying on messages it is free and has no adverts. Get rid of Whats-app and its much better than phone text messages (but it does require you mobile phone data to be enabled)

More advanced things

email

- If you use an email program (outlook/thunderbird etc.) – and some on-line email systems also support this - you can make ‘filter rules’ so that any email that arrives that is not in your address book will not be shown in the INBOX but placed into another folder (say called SUSPECT). This helps remind you that emails in here might not be from people you normally communicate with
- You can configure your email software to not display images. These ‘images’ can be company banners within the email or a single hidden element (a pixel). These are used to track you and detect when the email is opened – at least they collect statistics at worse they know the email account is a real and used one – block images stops this
- You can usually disable links so clicking a link in an email wont open your browser (just in case you forget!). This is a good safety tip
- Always use the SPAM filter and mark any and all junk email as junk. This trains your spam filter and helps it correctly identify junk