Islington U3A

Logging into Web Sites

USERNAMES

Logging into web sites requires, at least, a username and a password. Your username is usually your email address. If you use the email address that came with your broadband provider, you might lose this address when you realize your broadband is too expensive and you change provider! If you use this address to log on to sites, all your logons will need to be changed. It is better to use an independent email address that is permanent and does not rely on your provider.

You can have as many email addresses as you like, for example gmail, Microsoft, Mail.com, etc. I think it is best to have three different, independent email addresses.

- One for personal use for family, and friends.
- One for important web sites that need your personal data like credit card numbers, bank details, health data, etc.
- One for sites where security is not so important. Some sites ask for an email address before they let you have information. If you use social media sites, like Facebook, keep this separate from the previous addresses.

PASSWORDS

Perhaps you could get away with simpler passwords where you just need to log into a site to see some information, **but**, **anywhere where you give any personal details, you must have a good password.** Poor passwords can be cracked relatively easily. The internet bad guys have dictionaries, lists of common passwords, dogs' names, etc, etc. Poor passwords can be cracked in seconds.

A good randomly generated password made up of a mixture of, say, 20 capital letters, small letters, numbers and symbols could take forever to crack. If the bad guys can't get in easily, they will give up and go to the next target. Only government, banks and large organisations deserve greater efforts on their part.

If you google "password generator", you can generate passwords as strong as you like. You can define what you want as some web sites will only accept letters and numbers but not symbols.

Islington U3A

REMEMBERING PASSWORDS

If you only have a few passwords, then just write them on a piece of paper.

If more than a few, keep them in a Word document that you have passworded so that only you can open it. You can print a hard copy, or, better still, **keep another copy somewhere else, just in case.** For example, on a USB drive that can be kept in a drawer. One advantage of having a Word file is that you can copy and paste the username and password into the web site login page. I find it very easy to make a mistake manually typing a long and complicated password. (See Note 1)

Browsers will offer to save your passwords but there are serious doubts about their security. Granted, you don't need to download and install extra software but you are locked into that browser. Also, some browsers' passwords can be seen without a master password to protect them. Anyone with local or remote access can see them.

Windows 10 and Apple's Keychain on iOS platforms require a master password before entering passwords into web sites. Firefox is also ok, as long as you activate the master password requirement in Options. Use Chrome at your peril.

There are many Password Managers on the internet that can be very useful. They look after your passwords and enter them into login pages where appropriate. They require a master password before you can start logging on.

If you google "free password manager reviews" you can read about them and take your choice. If you don't like one you can always ditch it and try another.

Roboform is a password manager I have used without problem for many years. It has lots of helpful support pages for guidance.
To have a look, click here ROBOFORM

Important Note If a site like a bank says it will lock you out after three or so errors, do not try for a third time, no matter how sure you are that you are correct. Unlocking your account can be very tedious. They may even need to post a new password. After two wrong attempts, just click on the "Forgot Password" button and follow the instructions. This is the quickest way to maintain access.