Windows Tips and Tricks
Password Managers

Why do you need a password manager? See if any of these apply to you:
You write your password down on a scrap of paper or in a notebook. Then you can't find it. And when you have to change it you scribble over the old password and then can't read your handwriting, is that and S or an s, a Z or a 2?
You use the same password repeatedly because it is easy to remember.
Your keep your passwords simple so they are easy to remember.

A password manager provides several services. It stores your passwords so you can always find them. You only need to remember one password. When adding a new password, it will suggest complex passwords with uppercase, lowercase, numbers and special characters. And depending on your settings it will automatically fill in passwords for you, so you don't care if the password is "cR!2ehtMjz579bx".
There are two types of password managers, local and cloud. A local system is for those who only have one device and are nervous about using the cloud. A cloud system allows you to access your passwords from any device (computer, phone or tablet.)
There are many good password managers, both free and paid. Here are two highly regarded password managers, but do your own research to find the one that is right for you.

Local password manager.
KeePass 2. It stores your data on your computer. It is easy to use and has multiple versions available for computer, phone and other devices.
You can create folders to separate your passwords into groups such as E-mail or shopping. It has a search feature so, if you don't remember where you filed a password, it will find it for you.
It will suggest passwords of varying complexity based on what the requirements are for the site you will log in to.
If you choose, it will autofill passwords and usernames.
When creating a new account it will offer to use a default username such as your e-mail.
Because it is stored locally it will only be available on the device where the database is stored.
The disadvantage of a local program is that if something happens to your computer such as theft or drive failure, you will no longer have a password list. However, you are going to back it up regularly, aren't you? You can also print out a list and keep it somewhere secure in case of disaster.
Keepass is a free program that you can download. (Available from Ninite.com)

Cloud password manager.
LastPass which has both a free and a paid version. For most people it will work fine with the free version, but you can check out the extra features available in the paid version.
It has all the features of KeePass. Additionally, because it is a cloud service, it is available on all your devices and keeps them all in sync. Passwords can be modified, added or deleted on any device and the changes will be instantly available on any of your other devices.
For those of you who are nervous about the cloud, remember, companies like this have a lot of highly paid security people. How many highly paid security people does your computer have?
Because it is a cloud service you can use it from any device, even one that is not yours, if you remember your username and password. This is very useful if you are on a trip without your computer and need a password or are trying to recover from a lost or damaged device (remember the fire two years ago?).

Browsers
Browsers will offer to save passwords as you create the. This is cloud based but it is less secure because anyone with your email address and password will be able to log in and see your passwords. If they have access to your computer, they may not need any information to see all of the passwords you have stored there.
They can be convenient because they will automatically fill in your username and password. They can be dangerous because they will automatically fill in your password and username.

Security
Whatever password storage system you use be sure to have a strong password. It may be inconvenient, but it is the only password you need to remember. So, make a password with different elements (mAv72!rg9Df1%) or use a passphrase of 20 characters or more such as myfavoritegrandchildisbilly (sorry Susie, nothing personal). Difficult to type but easy to remember. No matter what, don't use password, qwerty, 12345678, 111111 or anything that is easy to guess or crack. Don't use individual words that are in the dictionary because hackers use a dictionary search when trying to crack passwords. Don't use your birthday or your pet's name. To see the most common passwords of 2019 go to https://techviral.net/common-passwords-might-surprise/
Don't use autofill for any sensitive sites such as your bank, brokerage company, credit cards or other financial accounts, Medicare or anything else where having your information compromised will be detrimental. If you are not using autofill you can open your password manager and copy and paste your password for these types of sites.