Passwords

This information is presented as general purpose suggestions and the effects may differ on each device or based upon specific updates done to each device. The County of York assumes no liability to unintended results this may have on your specific device and will not assist in any issues that may arise from implementing these tips. This is not an all-inclusive list of all software options available, simply a partial list of some options for the reader to further research for what might work best for them.

Words of Advice

In today's electronic world, more and more information is being stored on the cloud or in the Internet. The only barrier between a hacker and your money or information is a password. This makes it absolutely critical to use secure passwords that you routinely change and do not reuse between locations. Unfortunately, it is beyond your control that a hacker may compromise a website / cloud service and obtain your username and password. Their next step is to try many other systems (banks, Facebook, etc.) with those same credentials. Since it takes most companies several months to realize they were hacked, the criminals will be long gone with your money and information by the time you realize you should change it. Luckily it usually takes the criminals some time to try all their stolen accounts against all these websites, so routinely changing it will also add a layer of protection. Better yet, don't reuse passwords (a password manager such as Keypasscan help with this).

Not all websites or systems are as critical as others. I would recommend your strongest passwords to be used for your email account and your banking website. The reason for this is not that your emails are necessarily sensitive, but many websites allow you to reset your forgotten credentials by emailing you. If the hacker has access to your email they can usually simply "reset" your other passwords to obtain access to them.

Bad Passwords

To understand how to make a good password it is often helpful to know what passwords to things to avoid at ALL COSTS. Below is a list of tips to avoid common mistakes.

1. Have the word "password" in any form as part of your password (Password, PaSsWoRd, Pa$$w0rd, etc.)
2. Using names (James, Charlie, etc.)
3. Using birthdates, phone numbers, house numbers, license plates
4. Avoid all dictionary words by themselves (unless part of a phrase/sentence)
5. Hard to remember passwords, unless using a password manager (ia5pl/yCzxFh9ozB/iw0, x0PKPXVup96+M3hX/557, etc.)

Keeping Passwords Secure

You can have the best password ever created but it you don't follow the human errors below it will most likely be worthless.

1. Never share your password, with anyone, ever…
2. Make every password unique, don't reuse passwords
3. Never let others watch while you type your password (also known as shoulder surfing)
4. Log out of websites and computers when done
5. Store your password securely (see "Managing Passwords")

Creating Good Passwords

Below are a list of strategies to create new secure passwords, many can be used with other strategies on the list.

1. The longer the password is the better. Try to keep all passwords at least 8 in length and for sensitive items 15 or more is ideal. This can be achieved by using sentences or phrases are your password or part of it. Spaces are considered symbols and allowed in almost all password systems. For example "When I leave work at 5 I want to sleep for 12 hours!" If you have difficulty typing fast or accurately you can make a password from the first letters, numbers, and punctuation so it would be "WIlwa5Iwtsf12h!".
2. Always try to have a complex password, meaning 3-4 of the following: Upper case, lower case, numbers, and symbols.
3. Use deliberate misspellings or mispronunciations such as "chawkolit" instead of "chocolate"
4. Substitute some letters for numbers and symbols (A=@, E=3, S=$, l=1, i=!, o=0). Avoid substituting out all common letters since many dictionary words with these substitutions are well known (use Air1in3, but don't use P@$$w0rd).
5. Create a very complex random password with a password manager. If you don't plan to use a password manager avoid this since these will be next to impossible to remember.

Using Better Password Security (Multi-factor Authentication)

The normal username and password combination is "something you know". With multi-factor authentication you are adding "something you have" or "something you are". Something you have is usually a cell phone that is registered specifically to your account, since most people always have their cell phones with them. "Something you are" is usually biometrics like a fingerprint or facial recognition. For any secure account (such as banking) or associated email account (see Overview section) I highly recommended using multi-factor authentication. Usually these are provided free of charge from banking website and email websites like Gmail.

Managing Passwords

Password managers can usually be installed on computers, tablets, or cell phones and generally require one master password to access the system. Once you provide the master password you view or update all associated passwords. Many will generate extremely complex passwords for you or tell you the strength of your passwords. If you do have one password compromised you can search for anywhere you might have reused that password (ideally you shouldn't be doing this though). The biggest drawback of this method is you MUST remember the master password, if you forget it, then you lose everything (all of your eggs in one basket). The other consideration is in your store it locally you need to make regular backups (in case of a hard drive failure) or store it in the cloud (and associated potential security risks involved in this). Below is a list of commonly used password managers available for free.

1. KeePass https://keepass.info/
2. LastPass https://www.lastpass.com/business-password-manager
3. Dashlane https://www.dashlane.com/

Reference: https://it.ucsf.edu/policies/bad-passwords