Some simple steps to protect ourselves online (from waynedenner.com)

USE YOUR SCREEN LOCK

Most, if not all Smartphones offer some form of screen lock which automatically locks the device after a certain time period. Most of us have the option of using a pattern pass code, entering a pin code, using finger ID or facial recognition. Always be careful when choosing a pin code or pattern and ensure these can't be easily guessed.

#2 USE A PASSWORD MANAGER

Yes, I know it seems extreme but we really are all trying (and failing) to remember too many passwords. We all keep way too much personal information on our devices, especially our smartphone – so using a password manager, for example 'lastpass' which has a feature which allowing you to create 'secure notes'. These are kept within the app and only accessible by logging into the app to retrieve these. Software is available that can encrypt files or folders so that a code must be entered before a file can be viewed or copied.

#3 RECOGNISE & ONLY USE TRUSTED APPS & WEBSITES

With the increase of malware and apps/sites which might look like popular, genuine or official – it's important to be aware of the signs of false sites and apps and vigilant when downloading new apps. Pay attention to the permissions which the app might be asking for when you are installing it. Google play store offers 'verified by play protect' so look for apps which display this.

#4 WATCH THOSE LINKS!

When you're browsing online on your phone or device be ultra careful about what links you click on. Look out for links you may receive on Messenger, WhatsApp or email – directing you to websites asking for personal information such as your pin code, bank account number or password. Make sure you always look at the URL and make sure the 'http' has an 's' at the end. This ensures that the URL you are about to click on is secure but remember cyber criminals may not have got wise to this. Mis-spelling of domain names etc are also common.

#5 TURN OFF GEOTAGGING!

Many popular apps and social media platforms use geotagging. There are also other 3rd party apps which can pull in this data and use it to pinpoint a user's location movements or perhaps where they are right at this moment.

Photos for example are geotagged in the photo's metadata (called EXIF) and will have the location in which it was taken. You can turn the geotagging off on your images by going into settings -> privacy -> camera and turning off the individual app.

Take care online in 2020!