Cyber Fraud – brief report

This has been compiled from a training session at the SLCC branch meeting held on 23rd June and given by Laura Cowie and Grahame Mace, cyber protect officers with Devon and Cornwall Police.

This was a mainly slide presentation with voice over – I do not have access to the slides at present.

The session focused on how many gadgets most people have at home, which record their actions, their whereabouts, what they are searching for on Google, their voices, even thoughts. These gadgets ranged from the computer, the phone we all use daily, apps on the phone and computer, smart gadgets such as Alexa, heating systems, door bells, TV's, ovens, microwaves, fridge/freezers, even a smart toaster! So these items tell big brother all about you, where you are and what you are doing all the time. The more 'smart' gadgets you have, the more is known and tracked about you. This all comes in through the internet.

Passwords – there is one, a default, apparently in the router that we all have installed in our homes to access the internet. Did anyone know that? And, that you should change it once the router is installed as this is the first point of access to cyber thieves. (Google this and it will tell you how to change this password).
Most of us use easy to crack passwords, the ones with a capital letter, a number and a symbol and all of 8 digits long – apparently easy to crack. The longer the password and the more complicated, the better. Saving them on your computer with password protect is good; writing them down so they are handy, not good.

APPs – It is easy to download apps onto both phones, tablets and computers. It is just as easy to click through the questions asked online saying 'agree' to everything that has been asked, in order to get to the downloaded app as quickly as possible. Take some time to go to settings and check out your apps and what information they are recording – you can then change these settings to suit you and how much you wish any particular app to know about you. Eg. Why does my M & S app need access to my camera? Changed that now.

Phishing – these types of emails are winning hands down at the moment, clearing out people's bank accounts and making a great deal of money for the cyber thief. Do not believe that you have a tax rebate; HMRC will never tell you that on an email. Others I have noted include, not paying the TV licence (it's a DD), not taxing the car, (also a DD), friends asking for help financially???? You have won a prize!!! – how lovely, be wary how you claim it because it probably does not exist.
Two things to do before taking any actions on an email that may be fraudulent. 1) check the email address the email has come from – check very carefully as it could be just one letter or number that is slightly different – a 0 instead of an O, or a q instead of a g.
2) phone the person the email has supposedly come from and ask if they sent it.
Mostly that is a 'no'.

You can report all phishing emails by forwarding them on to report@phishing.gov.uk
Please do this as the more that are sent in, the more likely it is that something is done nationally.

As Councillors, do you think it is a sensible idea to hold a community meeting, sometime in the future once Covid allows, inviting Laura and Grahame to do a presentation?
There may be more to add to this, as I have asked for a fact sheet to be emailed to my council address.

Compiled by Penny Clapham BA(Hons) PSLCC
Clerk to Bampton Town Council, Kenn Parish Council and Colebrooke Parish Council
29th June 2021