

(Eventually to: Newsletter Editor for Newsletter, Chris Woodward  
newsletter@exmouthu3a.org.uk)

## REVIEW OF CYBER CRIME AWARENESS TALK

Budleigh Salterton Public Hall, 24 Feb 2020

The Hall was full. Lots of members and visitors, some from as far away as Honiton, braved the wind and the rain to learn how to protect themselves from Cyber crimes. Two excellent speakers were there to show them how!

Laura Cowie, of Devon and Cornwall Police, Digital Capabilities Unit, introduced herself as the first to occupy this new post and told us that the hierarchy led all the way up to GCHQ.

So what is Cyber crime? Crime facilitated by the internet. There are two main types – Cyber Enabled, which comprise mainly traditional crimes made easier by the internet, and newer crimes – Cyber Dependent – which depend on the existence of the internet and networks.

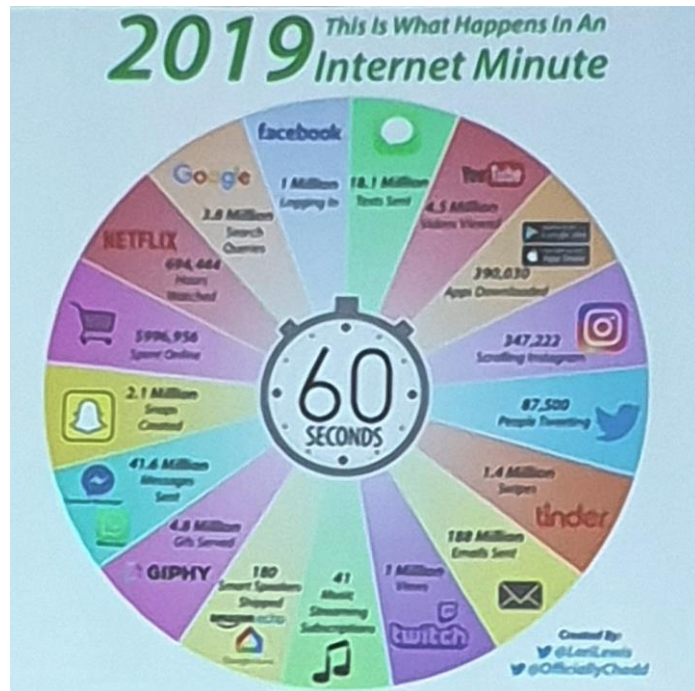
Characteristics include:

- Criminal need not be present at the scene
- Can commit multiple offences at the same time
- Often international
- Low risk, high reward.

To illustrate the scale of such crime, attention was drawn to examples of companies which had not looked after customer data, had it stolen and had been fined hundreds of thousands of pounds as a result.

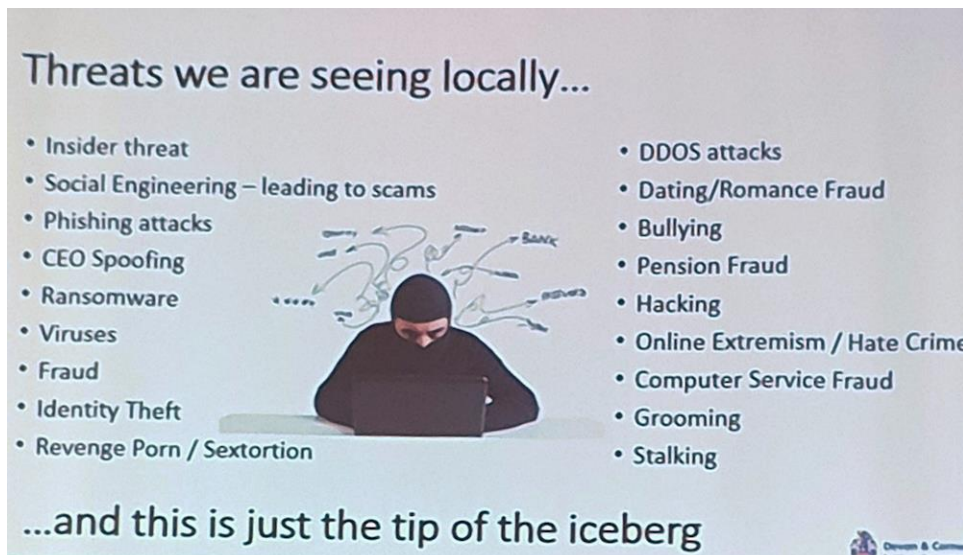
A pie chart was presented showing what happens on the internet in the space of just one minute. For example, Google has 3.8 million searches, Facebook has 1 million logons, Instagram has 87,000 scrolls and nearly

400,000 apps are downloaded! That's a lot of internet use in just 60 seconds.



Most people probably think that it's only their computer or phone that might be targeted. They'd be wrong. Home networks can have an increasing number of devices connected, such as doorbells, baby monitors, smart speakers, smart watches and smart meters. Before long we'll have connected significant numbers of fridges, washing machines, central heating controls and even cars. So we need to be aware that personal data can be associated with all of these and we need to be sufficiently aware that we don't let any of this leak unnecessarily. (There's a story, probably apochryphal, that someone was talking about their painful frozen shoulder within hearing of Amazon Alexa and a shoulder of lamb turned up in their internet shopping!)

Locally, in September 19, Devon and Cornwall police had 682 reports of Cyber Crime, including dating sites (someone gained your confidence and begged for money – it and they then disappeared of course), Scam phone calls, extortion (pretending to have compromising photographs and demanding money to keep them private) and general Banking Scams.



Perpetrators of Phone Scams will try to panic you into believing that you're owed money, or you owe money, or any other way of getting you to reveal your bank details. They're persistent and often appear legitimate. Don't be taken in and put the phone down. No reputable organisation will contact you by phone asking for your details and to move money. Just hang up.

Important ways to protect yourself online:

1. Use strong passwords and a lot of characters, include Caps, numbers and special characters. Here's an example that you'll never remember: **MfcwaSsj410wihf12m!** Well you might if you read **'My first car was SJ410 which I had for 12 months!'**
2. Install computer security software – virus protection, firewall. (There are free versions which are just as good as paid for ones.)
3. Download software updates.
4. Be vigilant and don't just trust that people are who they say they are!

Answers to questions can be summarised as follows:

Best not to accept strong passwords offered by sites. You don't know who already knows them – use your own.

What about Password Managers? Dubious as all your eggs are then in one basket.

Websites that ask for your permission to set 'cookies' (small text files which record details of your visit, pages looked at, perhaps your IP address which identifies your computer etc.)? Your choice, but you can accept which is easier, and then routinely delete your cookies. Your browser settings allow this eg. Delete/clear your browsing data/history.

And finally, let people know if you've been defrauded – Action Fraud, Police etc. The authorities can only act if they know what's happened.

### **Reporting fraud and cyber crime by phone**

You can report fraud by speaking directly to specialist Action Fraud advisers by phoning 0300 123 2040. They will also be able to give you help and advice about fraud.

We were left with this quotation: "There are two types of Organisation – Those that have been hacked and those that will be hacked."

-----

The second half of the talk was given by Janet Quinn of Devon, Somerset and Torbay Trading Standards. She deals with Doorstep callers, Rogue Traders, Food Safety and Weights and Measures. The format of her presentation consisted of answers to a predefined set of questions.



Q What should you do about doorstep callers or phone cold callers?

Send doorstep callers away. Preferably have a Trading Standards 'No Cold Callers' sign at your door. (These were available at the talk.) Ignoring these is an Offence.

Don't answer phone calls if you know they're scam callers. Use the Telephone Preference Service to try to stop such calls, but this needs to be renewed, say yearly. Ignore and put the phone down. Internet Providers will never call you about losing your service. (A personal story: Callers often claim to be from BT. I ask "Where are you calling from?" '15 Newgate St, London.' (Anyone can find the address of BT HQ online.) "What can you see out of your window?" They're stumped, mainly because they're not there. I've worked in Newgate St on many occasions. You can see St Paul's Cathedral!) Nor will your bank ask you to move money!

Q. Promises of money, lottery prizes, tax refunds etc.

Put the phone down. You don't get something for nothing and especially if you've never even bought a Spanish Lottery ticket!

Q. Card through your letterbox claiming, variously, that they have spare asphalt – do you want your drive resurfacing, noticed a roof tile missing, will prune trees etc. then call later. They may only have a mobile phone number and a van with no information/identification on the side – a real giveaway.

Don't accept. They may give you an estimated cost but this is meaningless. They often find 'extra work that needs doing' – it doesn't. Only a firm written Quote for itemised work is valid. If you really need work doing, get other quotes from reputable traders. Use Trading Standards Approved Traders lists.

Be aware of Cancellation rights. If traders are in your home and you agree to work, you have, by law, a 14 day cooling off period. They will try

to pressurise you to accept straight away, because they know this too. Hold your ground and say no.

**Q.** What about AirBnB and airlines which go into liquidation? You turn up at a cottage and find that the owner never lets their accommodation!

Don't ever pay direct. Only pay through AirBnB. They hold your money and only pay the owner after your stay. Pay by credit card if over £100. The Credit Card company is then liable. Take out travel insurance before you book.

**General:** Call blockers can help but use the Telephone Preference Service or set up blocking via your telephone company. Some call blockers are scams, especially those that charge.

Trading Standards work with the Police and recommend approaching the Citizens Advice Consumer Service. Sign up to Trading Standards Newsletter online. Current scams are listed.

-----

After useful, detailed and interesting talks by two excellent speakers, there was a lot to take in and it may seem overwhelming. The following seems to be a good summary:

We are not helpless in the face of all of these attempts to defraud us. Our main protection is to be vigilant but also suitably cynical and untrusting. The latter two go against our better nature, but criminals rely on our better nature to succeed! It's easy to be paranoid but better just to be careful and not fall for well known scams. Put the phone down and close the door!

Ian McLauchlin, U3A Committee Member, 24 Feb 2020