

Colin's Blog 28.4.2017



It has been many years since I last danced around a Maypole. Since then, many people have tried to lead me a dance, some succeeded, and I have often been going around in ever decreasing circles, trying to make sense of the world, or should I say, many of the people around me!

So, May Day is fast approaching, and I can't help thinking about, the other form of May day, which is often used at times of distress. One could be forgiven for wanting to shout '**MAY DAY!**' every time you hear the news, or pick up a newspaper!

As a Gemini, born on the 29th May, it is of course, my favourite month, and I look around me, and see new life, and new beginnings across the wide spectrum of nature.

As you know, as I prepare to retire (for the last time), May, more than ever is an important month for me, and will mean that my life will begin again, at the young age of seventy! A time to appreciate what has gone before, and rise to life's challenges in the future!

Fittingly, my next challenge, is to be part of the team running the Rotary table at the Ongar Community Day between 10am – 3pm, on Monday 1st. May, in the Budworth Hall, Ongar, next to the Ongar Neighbourhood Watch stall. (Who said men can't multitask?) Whoops, I think it was Sheila, my long suffering, yet understanding, wife!

Last weekend, we were staying with friends in Suffolk. Some of you may remember, Bob and Lyn Higgs and family. Bob was village policeman in Fyfield when I was based at Moreton. Feeling confident, we entered a village quiz, and I'm pleased to say our team came second, or to be honest, that's second from last, but at least we didn't come away with the booby prize!

I have just returned from spending the morning in the Harvey Centre, Harlow, where, together with members of the new Harlow Neighbourhood Watch committee, we managed to recruit in excess of fifty new Neighbourhood Watch members. A good mornings work, with an excellent result. Well done to the hard working, and enthusiastic committee!

So, it's back to work, deciphering the Burglary Hotspots, before I send them out!

MENTAL HEALTH AWARENESS WEEK 8th – 14th May 2017

<https://www.mentalhealth.org.uk/campaigns/mental-health-awareness-week>

In the past, too many mental health issues have been unnoticed, ignored or swept under the carpet. Years ago, sufferers were put away, into special units or asylums

away from the eyes of the public. I suppose one could say, that for many people, 'Out of Sight, was Out of Mind.'

I myself, suffered a work related, nervous breakdown in 1988, and the scars of such an experience, never go away.

It is refreshing to hear of the Royal family's involvement with '**HEADS TOGETHER.**'

Led by the Duke and Duchess of Cambridge and Prince Harry, Heads Together unites eight mental health charities, including Mind. We're very proud to be part of the team.

The campaign aims to change the national conversation on mental health, raising awareness and funds for mental health causes, including Mind and the network of local Minds.

Money raised by Heads Together will support the development of innovative projects that bring together the skills and expertise of the Heads Together charity partners, to get more help to more people.

Apparently, the title is currently being challenged by a commercial company, who claim that 'Heads Together,' is their brand name.

In my opinion, far too much pressure is put upon our children and young people these days, starting with the pressure of SATs in primary and preparatory schools, through to senior schools, and expectations, can, in my view, often, cut short or curtail, the time spent on childhood activities, yet alone, putting parents and teachers under undue pressure.

Whilst talking about pressure, one of the worst forms of pressure, is of course 'Peer Pressure,' often involving Cyber bullying, illustrated recently on East Enders.'

Social Media has it's uses, which sadly, are often overshadowed by its 'abuses.'

Many parents seem to be giving in to their childrens demands, to spend even more time on X Boxes, Play Stations, Smartphones, Computers, Tablets or other gadgets, without considering the side effects, or knock-on effects of them spending too much time on them. I know that some parents allow this, for a quiet life, but perhaps, they do not realise the possible consequences, which can affect their childrens behaviour patterns or attitudes.

Fraudsters are emptying bank accounts by diverting calls and text messages

Fraudsters are stealing large sums of money from victim's bank accounts by taking control of their mobile phones and intercepting calls / texts messages sent by banks.

Fraudsters are once again gathering as much information as possible on victims and using a method we have warned the public about in the past called **SIM splitting**, to gain access to people's bank accounts.

A recent This is Money investigation found that one victim from London lost **£22,300** when fraudsters raided their Santander accounts using this method. Another two victims had **£19,500** drained from their Santander accounts after criminals intercepted the bank's text messages.

How this fraud works?

Step 1: Fraudsters initially harvest as much as they can about an individual. This includes; intercepting their post, searching public information on social media/search engines, tricking them into installing **malware**, or buying information from Organised Crime Groups.

Step 2: Armed with this information, the fraudsters will call the victim's mobile phone provider and tell them that the handset has been lost, stolen or damaged. Provided they can answer basic security questions, the old SIM is cancelled and a new one is activated. The fraudster may also ask for all calls/texts to be diverted to a new phone.

Step 3: The first the victim will know of a problem is when their mobile stops working. This can seem innocent at first and some people may just think it is a signal problem.

Step 4: Fraudsters then hack into victim's online banking and open a parallel business account. Since the new business account is already in an existing customer's name, there are fewer security checks.

Step 5: The fraudsters then start to transfer money to accounts in their control. The banks will either call or text to confirm that payments being sent are genuine. The fraudsters will pretend to be the victim and insist that payments are pushed through.

How to protect yourself against this type of fraud

- Always make sure you have suitable anti-virus software installed and keep it up to date.
- Always consider what you are downloading – do not open files or click on links from unknown sources.
- If you discover a virus on your computer, disconnect from the internet immediately and ask a specialist for advice.
- When creating a password, try not to use the same password for more than one account. This will prevent further accounts being taken over if one has been compromised.
- Create a strong password by choosing three random words. Numbers and symbols can still be used if needed.

- Try not to post information on social media such as your birth date, your first pet, or school as these are normally included in security questions to reset your password.

Most of the information fraudsters need to steal your identity can be found on Facebook

I have warned my readers, many times before, about the dangers of Social Media.

Fraudsters need just three pieces of personal information to steal your identity, most of which can be found on your Facebook profile.

All it takes is your name, date of birth and address for fraudsters to steal your identity and access your bank accounts, take out loans or take out mobile phones in your name.

Recent YouGov research from **Equifax** has revealed that a high proportion of social media users risk identity theft by giving fraudsters easy access to this type of personal information.

- The survey found that almost 30% of adults with a social media account include their full name and date of birth on their profile pages.
- **Finding out your age and where you live**
- Even if you don't publically show your age on your Facebook profile, fraudsters can still work out your age from people wishing you well on your timeline. Once they have your date of birth, they can find out where you live too.
- You should review your privacy settings and ensure you are not revealing too much. If you need some guidance, this complete guide, will help you keep control of your Facebook account:-
<http://www.trustedreviews.com/opinions/facebook-privacy-settings-protecting-what-you-care-about>
- John Marsden, head of ID and fraud at Equifax, said: "People must act now to protect their finances for the long term. More adults in the UK are engaging with social media than ever before, especially on their smartphones, and a high number are readily sharing their personal information on these platforms."

- “Fraudsters get hold of this type of information so they can impersonate an individual, either by setting up accounts in their name or accessing existing accounts and stealing from them. The extent of damage can run to thousands of pounds’ worth of debt being racked up in your name. My advice to consumers is to be social savvy; avoid unnecessarily sharing personal details and risking your identity on platforms that can so easily be exploited. It’s always nice to receive well wishes on your birthday – but is it worth the risk?”
Report fraud and cybercrime to Action Fraud and receive a police crime reference number.

Copy and Paste into your web browser: -

http://www.actionfraud.police.uk/report_fraud

ActionFraud

Report Fraud & Internet Crime

0300 123 2040



KEEP ALERT, KEEP SECURE, KEEP SAFE, AND ENJOY THE BANK HOLIDAY WEEKEND!

Colin