Colin's Blog

Special Edition

1ST July 2017

Welcome to 'Scams Awareness Month JULY 2017'

Citizens Advice and Trading Standards Services are leading activities throughout the month of July for Scams Awareness Month. The campaign is all about supporting partnerships nationally and locally to give consumers the skills and confidence to identify scams, share experiences and take action, by reporting suspicious activity**.** **Further information and advice can be found at: -**

https://www.citizensadvice.org.uk/about-us/campaigns/current_campaigns/scams-awareness-month/find-out-about-scams-awareness-month/

NEWS from ACTION FRAUD

Following a global ransomware incident which took place earlier this week, we're reminding businesses and individuals how they can protect themselves from ransomware and what they should do if they become a victim.

How to protect yourself: -

- Don't click on links, or open any attachments, you receive in **unsolicited emails or SMS messages**. The links may lead to malicious websites and any attachments could be infected with **malware**.
- Always install software updates as soon as they're available. Whether you're updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
- Install anti-virus software on your computer and mobile devices, and keep it updated. Bear in mind that ransomware can often be picked up by visiting disreputable sites including illegal movie streaming websites and some adult sites.

- Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It's important that the device you back up to isn't left connected to your computer as any malware infection could spread to that too.

If you think you may be a victim:

- **Report to us** by calling **0300 123 2040**.
- Don't pay extortion demands as this only feeds into criminals' hands and there's no guarantee that access to your files will be restored if you do pay.

City of London Police collaborate with Microsoft to tackle computer software service fraud

- Four arrested following two-year collaboration between **City of London Police** and Microsoft with officers from **North East Regional Special Operations Unit (NERSOU)** and Surrey and Sussex Police Cyber Crime Unit making the arrests.
- Worldwide losses to **computer software service fraud** thought to be in the hundreds of millions of pounds.
- Computer software service fraud is the third most frequently reported type of crime to us.

Earlier this week, four people were arrested as the result of two years of work from Microsoft and the City of London Police into the global problem of computer software service fraud.

In Woking, Surrey and Sussex Police Cyber Crime Unit arrested a 29-year-old man and a 31-year-old woman on suspicion of fraud. They have since been bailed.

In South Shields, a 37-year-old man and 35-year-old woman were arrested on suspicion of fraud by NERSOU officers. Both were later released pending further enquiries.

Microsoft collaboration with police

The arrests have come about as a result of work by the City of London Police and forensic and investigative services provided by Microsoft analysing tens of thousands of Action Fraud reports and working with other affected organisations, such as BT and TalkTalk, to attempt to trace the source of the problem. This analysis and enquiries undertaken by the City of London Police have shown that many of the calls originate in India and that the worldwide losses from victims are thought to be in the hundreds of millions of pounds.

The collaboration with Microsoft was formed against a background of ongoing

engagement with industry by the City of London Police to combat fraud in a diverse range of areas such as insurance and intellectual property.

For the financial year 2016/17, there were 34,504 computer software service fraud reports made to Action Fraud, the national fraud and cyber reporting centre, with attributed losses of £20,698,859. This accounts for 12% of all reports to Action Fraud, making it the third most reported fraud type. The average loss suffered by victims is £600 and the average age of victims is 62. Despite these losses the number of victims is thought to be much higher as analysis shows many fail to report.

How computer software service fraudsters work

Computer software service fraud involves the victim being contacted and told that there is a problem with their computer and that, for a fee, the issue can be resolved. No fix actually occurs. Once the fraudster has access to the victim's computer they can install software which could potentially be malicious. The victim is cold called the majority of times but recently there has been an increase in contact via a pop-up on the victim's computer which then prompts them to phone the suspect.

The victim is persuaded to grant remote access to their computer and provide payment details. The fraudster then uses a variety of methods to obtain access to the victim's bank account to extract large sums of money. The victim may also be contacted again later and are told they are due a refund and they are again asked for access to the account. The fraudster will use this opportunity to take more money.

The fraudster often claims to be calling from Microsoft, or other technology companies, in order to give them more credibility with the caller.

The two-year collaboration came about due to the growth in reports of this crime to Action Fraud and Microsoft.

Commander Dave Clark, City of London Police and National Co-ordinator for Economic Crime said: "These arrests are just the beginning of our work, making the best use of specialist skills and expertise from Microsoft, local police forces and international partners to tackle a crime that often targets the most vulnerable in our society.

Detective Superintendent Alan Veitch, of NERSOU, the North East Regional Special Operations Unit said: "We are determined to tackle online fraud, which we know affects many people across the UK.

"Tackling organised crime is a priority for us and we work together with other agencies to deal effectively with it by providing investigative and technical resources and doing all we can to safeguard victims."

Hugh Milward, Director, Corporate, External and Legal Affairs for Microsoft UK, said: “Realising that you’ve fallen victim to a scam is a horrible experience for anyone. Not just the loss of money but also the feeling that you’ve been tricked and that your personal information has been stolen. Unfortunately, the names of reputable companies, like Microsoft, are often used by criminals to lull victims into a false sense of security. That’s why we partnered with the National Fraud Intelligence Bureau to track these people down and bring them to justice. It’s a collaboration which can cohesively combat and investigate computer service fraud. Today’s arrests are just the start.

We’d also like to reassure all users of Microsoft software that we will never cold call you out of the blue or use tech support pop ups on websites, Scammers can be extremely convincing, but if you think you have been contacted by them, **please visit our website for guidance**: -

https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx

As identity fraud hits record levels survey reveals that people are still not protecting themselves

REPORT DATED: 27th June 2017

Action Fraud, the City of London Police, Cifas and Equifax launch Identity Fraud Campaign with the hashtag **#AreYouOneofThem**.

- YouGov Survey commissioned by Equifax reveals that people in the UK are aware that they need to improve their online safety but still aren’t doing so.
- Identity fraud is estimated to cost the UK **£5.4 billion** per year.
- **172,919** people reported identity fraud to Cifas in 2016 with the reporting figures steadily rising since 2008.

Today we have launched an identity fraud campaign with the City of London Police, Cifas and Equifax, asking members of the public to consider how careful they are with their personal and financial details. A recent ‘YouGov Survey’ commissioned by Equifax found that the UK population are failing to take basic steps like protecting passwords or installing anti-virus software to protect their identities from criminals.

Identity fraud has been growing steadily over the past 10 years according to the **2016 Annual Fraud Indicator** and it is estimated that the cost of identity fraud to the UK is £5.4billion. Figures recorded by Cifas show that identity fraud now represents over half of all fraud members, with 9 out of 10 perpetrated online. In 2016, 172,919 people reported identity fraud to Cifas.

“Throughout the week we are urging people to think about their online behaviour and look at our advice to find out what they can do to protect themselves from identity fraud”.

How to protect yourself from identity fraud:

- Set your privacy settings across all the social media channels you use. And just think twice before you share details – in particular your full date of birth, your address, contacts details – all this information can be useful to fraudsters!
- Password protect your devices. Keep your passwords complex by picking three random words, such as roverducklemon and add or split them with symbols, numbers and capitals:R0v3rDuckLemon!.
- Install anti-virus software on your laptop and any other personal devices and then keep it up to date. MoneySavingExpert have a recommended list of the best free anti-virus software: www.moneysavingexpert.com/shopping/free-anti-virus-software
- Take care on public wi-fi – fraudsters hack them or mimic them. If you’re using one, avoid accessing sensitive apps such as mobile banking.
- Download updates to your software when your device prompts you – they often add enhanced security features.

What to do if you're a victim:

- ACT FAST if you think you have been a victim of identity fraud
- If you receive any mail that seems suspicious or implies you have an account with the sender when you don’t, do not ignore it.
- Get a copy of your credit report as it is one of the first places you can spot if someone is misusing your personal information – before you suffer financial loss. Review every entry on your credit report and if you see an account or even a credit search from a company that you do not recognise, notify the credit reference agency. They all offer a free service to victims of fraud
- Individuals or businesses who have fallen victim to identity fraud should **report to us**.
- If you have information about those committing identity crime please tell independent charity Crimestoppers **anonymously online** or call on **0800 555 111**.
- If you have been a victim of fraud, you can contact **Victim Support for free**, confidential advice and support. Victim Support is the independent charity for victims and witnesses of crime in England and Wales.

Lisa Hardstaff, identity fraud expert at Equifax said: "How people manage and store their passwords for their online accounts is the first line of defence to keeping their personal information safe and secure from fraudsters. "The fact that just under a third use the same password for multiple accounts and slightly more admitted to writing them down, clearly demonstrates people are being complacent and are of the belief that their personal information won't be at risk. "The majority also thought that it is the over 60s that are most at risk of identity fraud, but the reality is that ID fraud is an indiscriminate crime that affects all ages in the UK irrespective of where they live or how much they earn. Everyone is vulnerable – so everyone needs to be vigilant."

Simon Dukes Chief Executive at Cifas said: "With nine out of ten identity frauds committed online, identity fraud continues to be a significant fraud threat. Our statistics show that all age groups are at risk, with younger people increasingly so, therefore we welcome this new campaign and urge everyone to take more responsibility in protecting their personal information and avoid making themselves an easy target for the identity fraudster.

"However, it isn't just members of the public that need to be mindful of the threat, the survey also reveals that 52% of people wouldn't be willing to share their personal details with organisations that have lost customer data. The fight against fraud is a collaborative effort. This finding should serve as a wake-up call to any organisation that handles personal data. The consequences of not taking data security seriously can directly impact an organisation's bottom-line as well its reputation."

The recent survey commissioned by Equifax has helped to reveal some of the public's attitudes towards protecting their identity.

The survey found:

- 55% of people surveyed access public Wi-Fi that is not password protected.
- 40% of people do not have antivirus software installed on their devices.
- 27% of people use the same password for multiple accounts.
- 32% admit that they are at risk to identity fraud because of their behaviour.
- 31% of people think the over 60s are the most at risk to fraud.

City of London Police, Commander Dave Clark, National Police Coordinator for Economic Crime said: "The recent survey results have highlighted that we need to do more to protect ourselves from fraudsters. There is a common misconception that only old people fall victim to fraud but reports show that every age and demographic is affected.

“There is no doubt that identity fraud is a growing problem and this is why we have launched our #AreYouOneofThem campaign . We want to draw people’s attention to identity fraud and to highlight the risks they face when sharing details online.

How to protect yourself from identity fraud:

- Set your privacy settings across all the social media channels you use. And just think twice before you share details – in particular your full date of birth, your address, contacts details – all this information can be useful to fraudsters!
- Password protect your devices. Keep your passwords complex by picking three random words, such as roverducklemon and add or split them with symbols, numbers and capitals:R0v3rDuckLemon!.
- Install anti-virus software on your laptop and any other personal devices and then keep it up to date. MoneySavingExpert have a recommended list of the best free anti-virus software: www.moneysavingexpert.com/shopping/free-anti-virus-software
- Take care on public wi-fi – fraudsters hack them or mimic them. If you’re using one, avoid accessing sensitive apps such as mobile banking.
- Download updates to your software when your device prompts you – they often add enhanced security features.

What to do if you're a victim

- **ACT FAST** if you think you have been a victim of identity fraud
- If you receive any mail that seems suspicious or implies you have an account with the sender when you don’t, do not ignore it.
- Get a copy of your credit report as it is one of the first places you can spot if someone is misusing your personal information – before you suffer financial loss. Review every entry on your credit report and if you see an account or even a credit search from a company that you do not recognise, notify the credit reference agency. They all offer a free service to victims of fraud
- Individuals or businesses who have fallen victim to identity fraud should **report to us**.

ActionFraud
Report Fraud & Internet Crime
0300 123 2040

- If you have information about those committing identity crime please tell independent charity Crimestoppers anonymously online: -

https://crimestoppers-uk.org/in-your-area/eastern/essex/

Alternatively, if you have been a victim of fraud, you can contact Victim Support for free: -https://www.victimsupport.org.uk/help-and-support/get-help/support-near-you/east-england/essexconfidential advice and support.

Victim Support is the independent charity for victims and witnesses of crime in England and Wales.

Every day I hear about more and more, new scams that blight our daily lives. If only the scumbags, who create and carry out these scams, put their thoughts and minds to legitimate schemes and projects, rather than resorting to crime, maybe the world would be a better place.

Scams can affect all of us at anytime, whether we are: young, middle-aged, elderly, vulnerable, indeed, no one is exempt from being a target to scammers, which is one reason why I came up with the 'Keep Triangle,' as a simple reminder to all of us to: -

Three rules, to remind us to take time to protect ourselves against scams, and many many other situations that we meet up with in our daily lives.

Since retiring last month, I don't seemed to have stopped, attending various meetings at the start of the week, organising a joint Rotary and Probus BBQ at the Hunters Meet on Thursday evening, a whole day at my grandchildrens sports day yesterday, grandparent duty until midnight last night, then, our Rotary Antique valuation day in Ongar today.

Together with colleagues from the new Harlow Neighbourhood Watch committee, I will be at a special event at the Harlow Museum and walled gardens, tomorrow afternoon, then running a joint information stall afternoon with Essex County Fire and Rescue, at the charity stall, adjacent to Barclays Bank and Costa Coffee on Epping Market on Monday morning. I certainly haven't had time to be bored!

Over the next few weeks, I hope to bring you more updates and information about scams, and any other topics which I feel are worthy of a mention. Meanwhile, take care and please continue to report crime or anything suspicious direct to Essex Police in the usual way. Thank you for your continued support. Colin