**Chairman’s Report, December 2017**

**Welcome to yet** another packed newsletter, which provides advice on how not to be scammed, especially over Christmas. The festive period is a time for giving and receiving and showing good will to all, but it is also a time when we may inadvertently let our guard down and be more susceptible to being caught out. It is also a time when many of us have additional items and gifts in our homes or we go away.

Make sure your home is secure over Christmas and into the New Year. Please remember:

**Deterring would-be criminals is one of the most effective forms of crime prevention.**

Fit a motion sensor floodlight or outdoor Christmas lights to illuminate your home.

**Windows and doors.** A common mistake is to feed extension cables through partially open windows. Criminals know to look for this vulnerability. Government statistics show that 30% of burglaries happen through windows.

**Dispose of gift packaging carefully.** Refuse collections over the holiday period are often at different times. Put your rubbish out just before the collection; fold boxes so you don’t advertise your new possessions to thieves!

**Protect your Identity.** Shred receipts and personal paperwork.

**Keep your curtains and window blinds closed at night.** Make sure valuable items are out of sight. When going out for the evening use light timers to suggest you are at home.

**Away over Christmas?** Cancel any deliveries; ask a neighbour to park on your driveway; use light timers; don’t leave descriptive messages on your phone answering machine (“We’re away skiing for the Christmas holidays” etc).

**Secure garages and sheds.** Don’t hide keys outside your home; give the key to a family member or a neighbour; use alarms if fitted.

Please keep an eye out for your neighbours and if you believe you are witnessing a crime in progress please ring 999 and ask for the police.

Please stay safe and have a Merry Christmas and a Happy New Year

Chairman David Ayres

Contact email: david.ayres5@btopenworld.com
Mobile Telephone: 0779 6546 904
The 12 Online Frauds of Christmas

In the countdown to Christmas millions of people living across the UK will go online to buy presents for friends and family, search for holidays, book tickets for a big gig or send an electronic Christmas card.

What many do not realise is the hidden threat we now face from criminals online. They are targeting internet shoppers with scams which, on the surface promise to save them time and money, but in reality only deliver festive heartache and misery. Tens of thousands of people sadly fell victim to an online fraud in the weeks leading up to last Christmas and even more are at risk of suffering the same fate this year – being left hundreds, and sometimes even thousands of pounds out of pocket with no presents to give on the big day and their electronic devices corrupted with a computer virus.

To make life as difficult as possible for the cyber fraudsters, the major national police and cyber-crime agencies are supporting ‘The 12 Online Frauds of Christmas’ campaign. The aim is to raise awareness of the major internet threats and to give top tips on how to surf and shop safely, so that everyone gets to enjoy a very merry Christmas.

And if you do unfortunately fall victim to an online fraud, please report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk.

Online Shopping Fraud

This December, around 50% of UK citizens are expected to use the internet to buy more than half of their Christmas presents. Buyers need to be aware that fraudsters take advantage of this massive demand by creating bogus websites to advertise counterfeit goods and services that are often poor quality, unsafe, or are items that will never be delivered.

**Top tips to protect yourself**

- If possible use online retailers/brands you are aware of and trust. For major brands always go to the official website to find a list of authorised sellers.
- Check the delivery, insurance, warranty and returns policy.
- Be especially careful when purchasing expensive items.
- Make sure you have adequate anti-virus software that will enable your computer to flag any untrustworthy sites.

Christmas e-cards

An increasing number of Christmas cards are being sent via email. Many are genuine, but cyber-criminals are creating their own versions, which you should not open. The email may contain a virus (malware) that will embed itself on your electronic device – all without your knowledge – and then collect personal data, financial information, passwords and usernames which can then be used to commit fraud.

**Top tips to protect yourself**

- If you receive an anonymous e-card, better to play it safe and delete the email as it could be infected.
- Use a reputable anti-virus product on your electronic device, making sure it is regularly updated and always turned on.
- If you believe your electronic device has been infected, switch it off and disconnect from the internet to prevent further information being stolen. For advice on free malware removal tools go to www.cyberstreetwise.com. Also contact your bank and change passwords and usernames.
Auction Sites

Auction sites, such as eBay or Gumtree, are a popular way to buy Christmas presents. Whilst the majority of items on sale are genuine, there may also be some that are either counterfeit or do not even exist. Fraudsters use the festive period as an opportunity to 'sell' popular items such as smartphones, gadgets and ‘designer’ clothing at low prices on auction sites. Please take care before making a purchase. In reality, the chances are that the goods do not exist or what you receive will be a pale imitation of the legitimate version.

**Top tips to protect yourself**

- If it looks too good to be true, it probably is.
- Always use recommended methods of payment.
- Research the seller before you bid. If available, check their feedback but be mindful this can also be falsified.
- Be cautious when buying from sellers abroad or private individuals. If you are in any doubt, back out of the sale.
- If you are collecting what you have bought, take someone with you or let someone know where you are going.

Holiday Fraud

Over the festive period many people take a few days away, often in search of sunshine or snow. Most will go online to find a good offer. However, it is important to be aware of fraudsters advertising fake holidays on websites or social media. These often come in the form of cheap 'too good to miss' package trips, bargain-booking offers for villas and ski chalets or calls and texts offering tempting last-minute deals.

**Top tips to protect yourself**

- Always pay with a credit card.
- Use companies that are ABTA or ATOL protected. Verify this protected status by contacting the Civil Aviation Authority (www.caa.co.uk).
- Research the internet and consider the reviews of the company/person you wish to use before booking your trip.

Loan and Investment Scams

There is always an increase in online loan applications at Christmas as people seek to cover the extra costs. Fraudsters will exploit this opportunity by intercepting applications to legitimate lenders or by creating their own bogus company websites. You may also be tempted to put your money into an investment scheme which promises high returns and low, or no risk.

**Top tips to protect yourself**

- Authentic loan providers will not ask for an advance fee. If they ask for an advance fee just say no.
- Research companies online before making any financial commitment. Read the terms and conditions.
- If the loan or investment opportunity seems too good to be true, it probably is.
- Never set up a loan or an investment which starts with a cold-call. Always better to just hang-up.
- Go to www.fca.org.uk for a list of unauthorised firms and top tips on how to avoid dodgy investments.

Mobile Payments

Many people use mobile devices, especially smartphones, to make purchases. Data is usually stored in the phone’s memory and may be compromised if the device is 'hacked' or stolen.

**Top tips to protect yourself**

- Do not save passwords or personal/financial data onto your mobile device unless it is absolutely necessary and make sure the phone is passcode protected.
- If stolen, most mobile devices have the software to wipe all data from their memory remotely. Learn how this works (Google the question: 'How to wipe data from my phone?')
- Do not leave your Bluetooth switched on, as cyber-criminals can hack into your device unnoticed. Always install antivirus software and check the security features.
What background would you expect to find in a PCSO? Probably not a career in finance in London’s Square Mile, and 10 years in financial services in New York; but that is what Steve Windsor was doing before he joined the Dorset PCSO organisation a little over a year ago.

He and his family also moved to Dorset from Essex on their return from the USA, so his experience of different lives and communities has stood him in good stead in dealing with the daily challenges that face a PCSO.

As Steve is the most recent addition to the Ferndown NPT, we spoke about the process of recruitment and training for PCSOs.

The question of motivation was easy: in common with his Police and PCSO colleagues, Steve was attracted by the chance to serve the public and to work for a safer community. After many years in offices, there was also great appeal in the PCSO’s role on the front-line, providing a visible and reassuring presence on the streets.

‘I’d also add that I knew from one of my family, who works with the Dorset Police, that it is an excellent organisation, one I’d be happy to work for.’ It’s not easy to get in, and Steve went through several stages of interviews, but said, ‘it’s what you’d expect when selecting people for the role. It took several months, but I felt confident with the process.’

Steve joined a class of 16 for intense basic training at Police HQ, Winthrift. Only two of his group failed to graduate, which illustrates the effectiveness of the interview and selection process.

The training is based on the syllabus for a police constable, and during the Induction phase, PCSOs generally train alongside their student Police Officer colleagues.

The training begins with two weeks of induction and three weeks of community involvement and safer neighbourhood training, including community placements with partner organisations. At the conclusion of this phase, a de-brief day takes place where the students give presentations. Each student is also required to complete a project based on their community placement.

For Steve, the practical exercises involved scenarios such as neighbourhood disputes, parking and traffic infringements and complaints, all common problems encountered ‘on the beat’. He was impressed by the demands and the high quality of the training. ‘It was very intense,’ he said, ‘and the practical training was very life-like.’

At the end of the first five weeks, PCSOs have four more weeks of training specific to their role, which included further community placements.

Steve spent a week with the Bournemouth Churches Housing Association, focused on homeless people and rough-sleepers in the Triangle area of the town. This was followed by a week at a residential home for troubled children. His fellow trainees were placed with organisations such as those for the disabled, the elderly, modern slavery, vulnerable women. ‘It was an eye-opener for all of us,’ he said, ‘but vital training for our role as PCSOs.’

With this extensive classroom and practical training completed, Steve was allocated to the Ferndown NPT and spent his first eight weeks shadowing an experienced PCSO, in his case, Kate Hann. Thus fully trained, approved and qualified, Steve took his place on the team.

‘It’s a great job,’ he said. ’With shift-working and frequent calls to be available, it’s not a 9-to-5 job, but that suits me: mostly outdoors, meeting and helping people and doing my bit to keep Ferndown the pleasant, friendly and safe place that we enjoy.’

The essence of the role is to be seen, to communicate, and to be available for matters small and large. ‘We take a victim-first approach to the work, and give high priority to community engagement and being a reassuring presence.’

With the regular police committed to serious crime, the PCSO is able to fill the ‘bobby on the beat’ role that many remember and value.

Steve agreed, but with the caveat that the PCSO isn’t a bobby. ’But that has advantages,’ he added, ‘our limited role ensures that we are much less likely than the regular police to be called away for other tasks.’

What sort of incidents does Steve deal with? Predictably, the list doesn’t change: rogue traders, scam phone calls, opportunist theft, especially of garden sheds, traffic and parking problems.

Fortunately he finds relatively few incidents of anti-social behaviour and was pleased when the Ferndown Youth Centre re-opened recently.

And his Christmas message? Predictably it remains the same as in previous years: ‘Lock the shed’!
Rogue Trader Fined
A rogue trader in the South West who defrauded 21 people out of £108,000 has been jailed for 3 years and 2 months.

The rogue trader targeted older and vulnerable people by cold calling and advertising in local publications giving the impression of being genuine and respectable, using local telephone numbers that diverted to his mobile phone.

In all 21 cases the victims were given a quote, the work then started and as it progressed the trader would find 'extra' work needed. Expert witnesses who looked at the work reported that the real value of the work was often a fraction of the sum charged, while in some cases the work was never carried out at all. No cancellation rights were given to the victims; the sparse paperwork given did not include an address; and the telephone number was unobtainable, so the victims had no means of contacting the trader.

Your Rights
If you pay or agree to pay over £42 for any services or goods that are sold to you in your home, then you have 14 days to cancel the agreement. If you cancel, any monies that you have paid should be returned to you. The trader must give you a written notice of your cancellation rights when you agree the contract.

Display a ‘We Do Not Deal with Uninvited Doorstep Traders’ door sticker available from libraries across Dorset or by calling the Citizens Advice consumer helpline on 03454 040506.

HMRC Scam
Dorset Police has been made aware of emails, text messages and telephone calls being received from people purporting to be from the HMRC. These bogus callers encourage you to provide bank account or personal information in exchange for ‘tax advice’ or a bogus refund.

On some occasions they have informed the caller that HMRC is filing a lawsuit against them and that they must make immediate payment or police will be sent to their home. This is a scam. It has been widely reported and seems to be targeting elderly and vulnerable people.

Please don’t offer these people any personal details. If you have received an email, text message or telephone call that you believe to be fake, please contact Action Fraud on 0300 123 2040 or online at www.actionfraud.police.uk.

Modelling Jobs - A New Scam
The National Fraud Intelligence Bureau (NFIB) and Action Fraud have recently noticed that fraudsters have been setting up fake adverts on social media (including Facebook, Instagram and WhatsApp) and job browsing websites to dupe people into believing they are recruiting for prospective models.

Once victims show interest in the job, the fraudsters contact potential victims on the false premise of a modelling career and subsequently advise the victims to come in for a test shoot.

The fraud can then potentially be carried out in two ways:

First, the fraudsters can pressurise the victims in sending an up-front fee to book a slot for the test shoot. Once they have received the up-front fee, the victim will never hear from the fraudsters again.

The second possible method is that the fraudsters will take the advance fee that the victim sends for a photo shoot and arrange a photo shoot with the victim.

After the photo shoot, the fraudsters will contact the victim and convince them that their shoot was successful and offer them a job as a model. The victim will then be asked to sign a contract and pay another up-front fee, usually to secure the modelling contract.

Fraudsters are also creating fake adverts for supposed modelling opportunities for children. Fraudsters will inform parents or guardians that a potential career in modelling awaits their child. This tactic convinces the parent or guardian to sign up their child and send an advance fee. The jobs do not exist.

The fraudsters will also convince the victim that in order to become a model, they will need to have a portfolio. The fraudsters will recommend a number of packages and stress that if a package is not paid for in advance, the process of becoming a model cannot continue.

Over a two-year period (September 2015-August 2017), an average of 28 reports of advance fee modelling frauds have been received per month by the NFIB. In August 2017, 49 Action Fraud reports of this fraud type were received and may continue to rise. The total loss in August 2017 alone was over £71,000.

Tips for staying safe

• Carry out your own research prior to paying any type of advance or upfront fee.
• Be wary if you are asked to pay for a portfolio, as many legitimate agencies will cover that cost.
• Don’t give your bank account details or sensitive information to anyone without carrying out your own research on the relevant agency.

A Bank’s Advice on Staying Fraud Smart

• We’ll never ask you for your PIN, password, PINsentry codes or Mobile PINsentry codes. If someone contacts you asking for them, do not respond.
• On PINs and passcodes, when choosing a passcode, pick something that’s easy for you to remember, but hard for anyone else to guess. So avoid anything identifiable, like your birthday. You should also stay away from obvious sequences like ‘1234’ or ‘abed’.
• The strongest memorable words are at least 6 characters long, and are unique and random.
• One way to create a strong password is to take a phrase that’s memorable to you, like ‘I started school at Lincoln Secondary School in 2004’. Then use the initial of each word like this: ‘IssaLSSi#2004’.

Simples!
**Ticketing Fraud**

Creating wonderful memories is a part of the magic of Christmas and what better present to give than tickets to a rock concert or a sporting event? However, there are many bogus websites offering fake tickets. A tried and trusted formula for fraudsters is to offer cheap deals for tickets to events that have already sold out. In reality the tickets do not exist and anyone who tries to buy one will end up losing their money.

**Top tips to protect yourself**
- Only look at tickets from reputable websites that are secure (look for the padlock symbol on the website address). Before buying do an internet search for reviews on the event to see if anyone has fallen victim to a ticketing scam.
- Avoid entering your bank or credit card details on public or shared computers.
- Make sure you have good, up-to-date anti-virus software on all your electronic devices.

**Donating to Charity**

The festive period is traditionally a time when charities seek donations. Most collections and appeals are legitimate but be aware that fraudsters are looking to steal donations. One of the most common ways of doing this is online.

**Top tips to protect yourself**
- Visit the charity’s website by typing the address into your browser rather than clicking on a hyperlink shown in an email.
- Before you donate, check the website you are on is secure – the web address should begin with https:// (the ‘s’ stands for ‘secure’) and look for the padlock symbol.
- Do not respond to requests to donate through a money transfer company such as Western Union or MoneyGram.
- If you are still worried, a legitimate charity will advise you on other ways to give on their website or via a phone call.

**Mobile Malware and Malicious Apps**

Many people will be getting smartphones or tablets for Christmas. Cyber-criminals are constantly developing new ways to infect these devices through malicious apps or through infected websites. Although most malware is found on the Android operating system, there have also been recent cases of strains being developed for Apple’s iOS.

**Top tips to protect yourself**
- Make sure you have the latest version of software installed for increased protection.
- Only download apps from official app stores like Google Play and Apple Store. Always check reviews and ratings before downloading a new app.
- Install anti-virus software and keep it up to date.
- Do not click on links in emails from unknown sources or visit suspicious websites on your new devices.

**Social Media Scams**

Most of the adverts placed on networking sites such as Facebook and Twitter are genuine. However fraudsters are also advertising giveaways and offers in the hope that people will click on these bogus adverts and be redirected to a website full of scams. Cyber-criminals may also be on the hunt for personal details which can be used to steal people’s identities and commit fraudulent transactions.

**Top tips to protect yourself**
- Do not have too much personal information on social media accounts which could allow your bank accounts to be compromised.
- Be wary of installing add-ons to your internet browser as some can be used to extract personal and financial information from your search history.
- If you click on a social media advert do the necessary checks before buying anything from the website you land on.
Money Transfers

An authentic online seller will ask you to pay by card on a secure payment page, or occasionally by cheque. However tempted you are because ‘it’s the last one in stock’ or it’s ‘two days before Christmas’, never transfer money directly into the seller’s bank account. As well as at Christmas time, there are many situations where you may be asked to transfer money to other people and there are a number of respectable services you can use. But be aware fraudsters are also looking to cash-in by persuading people to transfer money for products and services that do not exist.

**Top tips to protect yourself**

- Never send a money transfer for online purchases.
- Never send money in advance to obtain a loan, or credit card, or ’processing fees’ on lottery or prize winnings.
- Never give your banking details to people you don’t know.

Dating and Romance Fraud

Many people will be making a New Year’s resolution to find their ideal partner, possibly by signing up to an online dating website. This can be a great way to find true love but you also need to be on the lookout for fraudsters – trying to win your affection and then asking for money to pay for them to visit you or help out with a family problem. Do not listen to promises of repayment. It is always better to sever contact and look elsewhere.

**Top tips to protect yourself**

- Guard your privacy when chatting online and be selective with the information you provide about yourself.
- Never send money or give credit card or online account details to anyone you do not know and trust.
- Trust your instincts, if something feels wrong take steps to protect yourself.

Know your consumer rights!

The run up to Christmas is a busy time for shopping, but do we all know our rights?

Anything you buy must be:

- of satisfactory quality
- fit for its intended purpose
- as described

If the goods are faulty you are limited initially to the first 30 days after you bought them to ask for a refund. So, if you can, make sure any presents you buy are examined within 30 days.

Once 30 days have passed you can only ask for the goods to be repaired or replaced. But this must be done at no cost to you, within a reasonable time and without causing you significant inconvenience. After just one attempt at repair or replacement, you can ask for a refund if the goods are still not satisfactory.

If repair or replacement is not possible, then you can choose whether to keep the goods or return them. If you keep the goods, you can claim a reduction in price. If you return them you are normally entitled to a full refund, less a reasonable amount to take account of any use you’ve had, if it’s more than six months since you bought them.

For digital content, for example, computer programs, smartphone apps, e-books, CDs, DVDs, etc, your rights are roughly the same as for ordinary goods. But you do not get the initial 30 days to reject faulty digital content alone, and get a refund, unless the digital content is supplied as an inherent part of physical goods, such as computer systems, smartphones and washing machines.

For pre-shopping advice, advice about a consumer problem, or to report something to trading standards call:

Citizens Advice Consumer Helpline: 03454 04 05 06
or visit citizensadvice.org.uk/consumer

…and finally,

Your Neighbourhood Watch Committee
Wishes You and Your Family
A Safe and Happy Christmas

…and don’t forget to lock the garden shed!
Can You Help?

Our Neighbourhood Watch is valued by the community and it works well. It depends on volunteers to undertake the relatively minor responsibilities that sustain it. We need more helpers to replace those who move, fall ill or retire from active service.

Would you please consider helping as a Distributor?

You’ll be supported by your local Sector Coordinator. It involves just two things:

- **Deliver** a few copies of the Newsletter to houses on your road, close to your home. Takes about 30 minutes, four times a year.
- **Collect** the £1 annual subscriptions from the same group of your neighbours. Done just once a year, at the same time as delivering the Spring Newsletter.

We need Distributors in all areas. Please help us to help your community.

Phone David Ayres, NHW Chairman, 07796-546904
or email at: david.ayres5@btinternet.com