East Division

Neighbourhood Watch Newsletter

Issue 5 March 2016

Fraud

The focus of this newsletter is telephone, postal and internet fraud, known as scams. We have received feedback regarding the length of the previous newsletters, so we have made this one shorter. I shall use the messaging service to update you regarding individual Association news.

Thank you to our volunteers who continue to support us in sending messages, contacting NHW co-ordinators and scheme members, and compiling the newsletter.

Alexandra Harrington - Volunteer and Watch Liaison Officer. East Division. Kent Police.
Karen Uzzell-Childs - Volunteer and newsletter author.

Why are people still getting scammed?

It is an unfortunate fact that so many of us are still being scammed by criminals, whether it is via the phone, post or email. In particular the most vulnerable members of our society are being hardest hit, because of their inability to understand they are being scammed, and to seek help to stop it happening in the future. There is a lot of information out there about scams so we have tried to cover the most relevant things for you. The best way to stop it happening to you or someone you know is to find out how criminals attempt to defraud us and report anything suspicious to the relevant authorities.

TELEPHONE SCAMS

Examples of common types of telephone scams:

Computer helplines, telephone services (landline), Personal Protection Insurance (PPI), prize draws, banking services, advertising, energy, local Government, accident claims.

How to avoid telephone scams

- Don't give out your telephone number. Tick the boxes on forms you complete to say that you do not wish to be contacted. Pay particular attention to on line forms as the no contact information is not always obvious.

- Register with the Telephone Preference Service (which is free) on 0845 070 0707 or to get further advice on 0845 703 4599 or via their website www.tpsonline.org.uk.

- Check the call blocking facilities available from your own telephone provider. Many phone companies have services available, although some may incur an additional charge. For example: BT customers have BT Call Minder which allows messages to go straight to voicemail and can be retrieved later, or the receiver can choose to answer it when the caller leaves their name. It also identifies up to 3 callers who have dialled and hung up without leaving a message (assuming they have not withheld their number). BT will also be launching a new service later this year to divert nuisance calls within its network before they ring on customers' phones.

- If you are told to call a number back, for example your bank or utility company, first check the number on your card or a recent statement. Do not call the number back but go into a branch to question the call. Previously, fraudulent callers were using 0800 or 0300 numbers, however, now they are purchasing and using local land line numbers to get those with caller ID to answer the telephone as it is a local call number displayed. We have been notified that this is happening in East Kent, in particular in Thanet and Dover.

Examples of recent telephone scams reported in Kent

1. A report of scam phone calls from people claiming to work for the telecommunication service, BT. The caller asks for an upfront fee of £300 to opt-out of scam telephone calls and tries to gain the resident's confidence by quoting the last four digits of their credit card. The caller then asks for the beginning of their credit card number to complete the transaction. In this case, it is likely that this person may be using the identity of an existing company employee to scam residents.

2. Reports of a company telephoning Canterbury residents claiming they are required to check their electrics meet suitable standards under new government regulations. The resident contacted their energy supplier who confirmed this work is not necessary. This bogus company is misleading residents into accepting unnecessary work.

3. Some older people have received telephone calls from a caller who purports to be from the local doctor's surgery and is asking for an appointment to discuss the person's mobility needs. During the appointment the person is persuaded to buy mobility aids which are either unnecessary or inappropriate and always expensive. If you receive a call like this, please check with your GP's surgery first before agreeing to a visit. This fraud has already been circulated to all GP surgeries and the Clinical Commissioning Groups by the NHS.

4. Reports about phone calls from people claiming to be from a Government Loyalty Scheme. The caller stated the resident was entitled to £8,000 for being a good citizen. The caller instructed the resident to go to the Post Office with their passport and mobile phone and to pay a fee of £210 in order to be awarded the £8,000. The telephone number the scam caller used was 0207 1935 354.

5. A call from someone claiming to be working for the National Accident Helpline or Association – number: 10151-324-1003, asking if the respondent has had an accident recently. The caller then tries to gain more personal information so they can write to you with more details about your "accident".

6. A call from a man stating that he could block all nuisance calls from India. Caller asked for the expiry date of respondent's Visa card, telling them it was a certain date and saying he had the information from their telephone supplier. When the respondent questioned him about the supplier, he became persistent in asking for the Visa Card number. The phone number was 0203 129 1533.

   If you receive a call similar to any of the above, please report it to Kent County Council Trading Standards via the Citizens Advice consumer service on 03454 04 05 06.

A quick note on avoiding mobile phone scams

- Do not reply to any suspicious texts, nor should you text 'STOP', unless you are confident you know where the message has come from. Scammers will often use this to find out if the number is still active and it may then be sold on to other cold calling companies.
- Be careful who you give your mobile number out to.
- Do not list your mobile number on social media or even sites you believe are secure.
- Check the small print on forms in regards to a company's privacy policies.
- To make a complaint contact the Information Commissioner's Office, www.ico.org.uk

- If you bank online do not respond to texts supposedly coming from your bank, check with the bank in person or on a recognised land line number

POSTAL SCAMS

Examples of common types of mail scams:

Competitions you have never entered, inheritance, lotteries, investment and financial offers, debt collection, catalogues and brochures, chain letters with dire warnings if recipients do not reply.

How to avoid postal scams

- Do not reply to any letters that you are unsure about, instead contact Trading Standards or Citizens Advice. Contact banks, utility companies etc. via the contact details you have from recent statements, check contact details in the phone book, websites or visit local branches.

- Never send cash, disclose personal details or buy goods to claim a prize. There is never a 'prize' to win; these companies just want people to send money.

- Watch out for secret 'get rich quick' schemes and inheritance notifications. If something sounds too good to be true, it is. Always seek professional legal and financial advice. Contact the Financial Conduct Authority www.fca.org.uk or telephone 0800 111 6768 (freephone) or 0300 500 8082 from the UK.

- Ignore so-called psychics and clairvoyants who may claim to have seen something in your future and ask for money to disclose what it is. They may also be working with criminals behind fake prize draw letters, encouraging you to keep on sending money and discouraging you from talking about it with family or friends. Think Jessica is a charity that raises awareness of this growing problem and supports victims and their families. www.thinkjessica.com

  > Quote from the site: "Those who respond end up having their details put on what criminals call "suckers lists". Fraudsters sell these lists to other scammers all over the world. This can result in victims being delivered 100+ scam letters a day and plagued by international phone calls. Millions of victims have a condition which Think Jessica is trying to get recognised as Jessica Scam Syndrome (JSS). People with JSS have been "brainwashed" by criminals who are having an easy and assisted passage into their homes, minds and bank accounts."

  Recently there have been national agreements for Royal Mail staff to work with partner agencies to identify those who may be at risk so that appropriate interventions can be put in place.

- To reduce junk mail register with the Mail Preference Service. Tel. 0845 703 4599 or register via their website www.mpsonline.org.uk

- To stop receiving all unaddressed letters and leaflets delivered by Royal Mail contact: Freepost RSTR-YCYS-TGLJ, Royal Mail Door to Door Opt Outs, Kingsmead House, Oxpens Road, Oxford, OX1 1AA, or register via the website www.royalmail.com/personal/help-and-support/how-do-I-stop-receiving-any-leaflets-or-unaddressed-promotional-material

Examples of recent postal scams in Kent

1. As previously mentioned in telephone scams, some Kent residents have also been receiving letters claiming to be from the telecommunication service, BT. The letter asks for an upfront fee of £300 to opt-out of scam telephone calls. The Telephone Preference Service is a free service that helps to reduce unsolicited sales and marketing telephone calls.
2. The story below hit the national headlines in 2015 and raised deep concerns about how charities were contacting vulnerable people, via mail and phone calls, requesting cash donations.

A 92-year-old poppy seller who took her own life felt "distressed and overwhelmed" by the huge number of requests for donations she received from charities, a report has concluded. Olive Cooke, who died in the Avon gorge in Bristol, may have received almost 3,000 mailings from charities in a year, the report from the Fundraising Standards Board (FRSB) says. About a quarter of the charities that had Olive Cooke's details on file passed them on to other organisations. After the death of Olive Cooke questions rose about charities' tactics after regulator's report said Olive Cooke, 92, was overwhelmed by approaches before her suicide."

Source: www.theguardian.com/society/2016/jan/20/poppy-seller-who-killed-herself-got-up-to-3000-charity-mailings-a-year

Since the death of Olive Cooke the FRSB has published seventeen recommendations to control the way charities contact current and potential donors. These include:

- Limit the frequency of charity approaches per year
- Clarify that charities cannot call people that are registered on the Telephone Preference Service (TPS), unless the individual has given clear permission to receive calls.
- Expand current guidance for communicating with older supporters and those in vulnerable circumstance

Source: www.frsb.org.uk/interim-investigation-report-published

Email Fraud (electronic mail - phishing)

In 2015 over 96,000 people reported phishing email to Action Fraud.

Examples of email scams:

1. Emails supposedly from a bank telling you there is a problem with the account; hard luck stories; requests for a money transfer (especially outside of the EU); lottery scams; email telling you to open an attachment (could be a computer virus); investment opportunities; romantic emails asking for financial assistance
2. PayPal scam emails: In research conducted by Which Magazine, 59% of people surveyed had received a scam email claiming to be from PayPal. Often the email will ask for passwords, bank information or credit card details. PayPal will never ask such information from its customers or ask you to download and install any software. Forward any suspicious emails to spoof@paypal.com PayPal say the safest way to confirm the email's validity is to log in to your PayPal account where any of the activity reported in the email will be available to view. Do not use the links in the email received to visit the PayPal website. Instead, enter www.paypal.com into your browser to log in to your account.

If you have received a scam email

- Do not click on any links or attachments in the email if you are unsure of its source. These may contain a virus. Forward this to Action Fraud without opening it.

- Do not reply to the email or contact the sender in any way. If it is purportedly from a bank, either phone them directly or go into the branch.

- If you have clicked on a link in the email, do not supply any information on the website that may open; this could be a fake page made to look like a legitimate company's own website.

- If you think you may have compromised the safety of your bank details and/or have lost money due to fraudulent misuse of your cards, you should immediately contact your bank. It may also be possible to forward the scam email to the relevant department at your bank via their website so they can investigate and warn customers about fake emails.

How to spot a fake email (known as phishing):

- The sender's email address doesn't tally with the trusted organisation's website address.
- The email does not use your proper name, but uses a non-specific greeting like "dear customer"
- A sense of urgency; for example the threat that unless you act immediately your account may be closed or frozen
- A request for personal information such as user name, password or bank details. Also remember your bank would never ask for your pin number
- The entire text of the email is contained within an image rather than the usual text format
- You get a message from a friend but it has no personal pleasantries/messages in it
- The content contains grammar and spelling mistakes

For more information on hoax emails go to: www.hoax-slayer.com

Examples of recent email scams in Kent

1. A resident recently received an email claiming to be from Royal Mail. It said that a parcel addressed to them has been seized by HM Revenue & Customs and invited them to go on to the following site: roy-mail185@lincoln.websitewelcome.com

2. Bogus Blue Badge websites charging £49 for a badge. The websites will ask for your personal information and will not have the authority to issue you a Blue Badge. The official Blue Badge costs £10; you can find more information and apply for or renew your Blue Badge by visiting the Kent County Council website. You can contact Kent County Council's Blue Badge Team on 03000 416262 or bluebadgeteam@kent.gov.uk.

Use long passwords (such as a line from a poem or a song lyric) and do not use passwords that are easy for hackers to crack e.g. ones that contain family names, house numbers and dates of birth as much of this information is available on line already. There is a site that hackers use that contains in excess of 150,000 commonly used passwords and they will use this "hash generator" site to try to hack into your computer once they have minimal details. Don't make an assumption that on line providers will keep your passwords safe; the recent talktalk scandal demonstrated that it is relatively easy for hackers to obtain information.

Social Media

If you or members of your family use social media, take time to review what details are on the sites you use, including the photographs that have been uploaded. These sites contain a large volume of personal data and this is used by criminals to apply their various frauds/cons.

For more information on this visit the Dedicated Card and Payment Crime Unit (DCPCU) website:

www.theukcardsassociation.org.uk/what_we_do/dcpcu.asp

The DCPCU is a special police unit which consists of police officers, drawn from the City of London Police and the Metropolitan Police Service, who work alongside industry fraud investigators. It was created in response to a rapid growth in payment card crime between 1999 and 2001, which experts attributed to the growth of organised crime in this area. The main objective of the DCPCU is to investigate, target, arrest and seek the successful prosecution of offenders responsible for organised cheque and payment card crimes.

For updates on current scams in the Kent area go to:

www.kent.police.uk/advice/property_security/fraud/Fraud.html

For advice and to report issues to Kent Trading Standards: www.kent.gov.uk/business/trading-standards
Call 03454 04 05 06 (Monday to Friday, 9am - 5pm)

Text phone 18001 03454 04 05 06 (Calls are answered by Citizens Advice Consumer Helpline)
www.adviceguide.org.uk

www.met.police.uk/fraudalert - This will give you a link to the third edition of the Metropolitan Police's Little Book of Big Scams. Also available in audio edition online

For more general help and advice the agencies and companies below may be able to help.

- Age UK Advice: 0800 169 2081 www.ageuk.org.uk
- OFCOM: 0300 123 3333 www.ofcom.org.uk
- www.thinkjessica.com
- Mailing Preference Service: www.mpsonline.org.uk
- www.actionfraud.police.uk tel. 0300 123 2024
- www.hoax-slayer.com
- Regularly check your credit file through any of the three credit reference agencies: Call Credit Expert, Equifax or Experian. All can be found on line and in the phone book.
- www.gov.uk/consumer-protection-rights
- www.frsb.org.uk (Fund Raising Standards Board) Tel. 0333 321 8803
- www.moneysavingexpert.com For independent advice
- https://ico.org.uk (Information Commissioner's Office)
- www.fca.org.uk For financial advice on investments

Remember, you can take a number of precautions to prevent yourself or someone close to you from becoming a victim of scams. If you or someone you know is caught out, then the quicker you act and report what has happened, the more chance there is that the damage can be limited and any money lost may be recovered.

Alexandra Harrington

Karen Uzzell-Childs