Scams, Cold Callers and Email Fraud

Why do people get conned?

Confidence tricksters defraud a person or group by gaining their confidence and trust. Confidence tricks exploit human characteristics such as honesty and naïveté. They are particularly effective against the most vulnerable in society, knowing these people are much less able or willing to report incidences of crime involving fraud. The advancements in technology and communication have benefited our lives immensely but sadly have also attracted criminals, keen to exploit vulnerabilities for financial gain. There are many different kinds of scams used by criminal gangs or individuals, some have been around for years but are still trapping victims. Scams are always evolving along with new technologies; the authorities are constantly tackling new types of fraud and ensuring the public are made aware of these. Hopefully this newsletter will provide you with enough information to feel safe and secure and also have the confidence to report incidents. There is a lot of information out there about scams so we have tried to cover the most relevant things for you.

The three main ways a fraudster will attempt to con you:

Phone/Post/Email

By Telephone

Over a third of scams are over the telephone. These fraudsters often use the names of well-known companies to commit their crime, as it provides a mask of legitimacy. Telephone scams are the second most common type of scam in the UK, but many more go unreported.

Examples of common types of telephone scams:

Computer helplines; telephone services (landline); Personal Protection Insurance (PPI); prize draws; banking Services; advertising; energy; local Government

How to avoid Telephone Scams

Don't give out your telephone number unnecessarily.

Tick the box to indicate that you don't want to be contacted with promotional material when signing contracts.

Register with the Telephone Preference Service (which is free) on 0845 070 0707 to reduce calls or via their website www.tpsonline.org.uk.

Marketing calls are legal, but not if you tell the business you don't want to receive them or you are registered with the Telephone Preference Service.

Go ex-directory.

Check the call blocking facilities available from your telephone provider.

Consider buying a call blocker device, such as trueCall devices, which can block 98% of nuisance phone calls. Available at www.truecall.co.uk and also with various other online retailers.

If you receive silent or abandoned calls, contact OFCOM on 0300 123 3333, (Monday to Friday from 9:00am to 5:00pm).

After the call, hang up the phone and wait five minutes, or use another phone to call the company back (double-checking their number first). If you haven't got another telephone to use, call someone you know first to make sure the telephone line has actually cleared. Scammers can keep your line open if they don't hang up, stopping you from calling the legitimate authorities to check the call. Call your bank or card issuer on their advertised number to report the fraud/scam attempt.

'Vishing' Scams

Figures released by Financial Fraud Action UK (FFA UK) show a significant rise in the number of people who have been targeted by phone scammers over the past year. The research, carried out on behalf of FFA UK by ICM, suggests that 58% of people have received suspect calls, a rise from 41% from the research conducted a year ago. The increase in scam calls is reflected in another survey, also published recently, which show a threefold rise in the amount of money lost to phone scammers. Over the last year, at least £23.9m of losses can be attributed to 'Vishing' (voice phishing) – up from £7m in the previous year. In response, a rare 'UK Banks Joint Declaration' has been issued. This has brought together banks, building societies, credit card companies, and the Association of Chief Police Officers, to clarify the warning signs of a phone scams. In particular they are urging customers to be very wary of using their phone immediately after receiving a call which could be a scam (see the advice above). Your bank will never ask you to check that the number showing on your telephone display matches their registered telephone number. The display cannot be trusted, as the number showing can be altered by the caller. To report a fraud and receive a police crime reference number, just call Action Fraud.

Some phone providers like BT and TalkTalk offer services including *Last Call Barring* and *Anonymous Caller Reject*, with their phone packages. TalkTalk offers these for free, once you have activated the relevant settings on your account, go to www.help2.talktalk.co.uk/last-caller-barring.

For advice from BT go to www.bt.custhelp.com, some customers may have to pay an additional charge for these services if not available to them as part of an existing package.

A quick note on mobile phones: There are three main types of spam message.

Legitimate marketing messages - These should include the name and contact details of the sender. You will usually have given consent for them to be sent, though possibly unknowingly. How to spot them: firms will identify themselves within the body of text or in the sent from number.

Premium messages - These are services you have agreed to but you may be unaware that by buying a service, or game, on your mobile you're receiving a regular, charged text. How to spot them: it will be from a four, five or six digit number and will bill you for receiving the message.

Spam texts - These usually message randomly generated numbers, advertising services such as accident 'ambulance chasers', PPI claims handlers or debt write-off firms. How to spot them: they usually come from an 11 digit mobile number and the company isn't identified.

How to avoid Voice/Text Scams

If you do not recognise the number and cannot confirm it is a legitimate company do not text STOP – this indicates that the number is active and may be sold on to other cold calling companies, you may also be charged for the text. If it is a legitimate company cold calling you can text STOP to their short code number to unsubscribe. Err on the side of caution, and delete the message if you are not sure.

Be careful who you give your mobile number out to.

When you are giving your number out write it down and pass it to the person, you do not know who is standing behind you listening to your number – ask the person to give the details back to you and shred them.

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 complaints contact the Information Commissioner's Office, www.ico.org.uk.

By Post

This often takes the form of prize draw letters for competitions which the recipient has never entered. To enable them to claim their prize, they are told to act immediately and asked to buy an item or pay a 'fee' to release the prize. These letters are often followed up by a telephone call urging the person to claim without delay.

Examples of other common types of mail scams:

Inheritance, lotteries, investment and financial, debt collection, catalogues and brochures.

How to avoid Postal Scams

Do not respond to any letters that you are unsure about, instead contact Trading Standards or Citizens Advice. If the letter claims to be from your bank/building society then contact them by phone on the legitimate number you will find on your bank card or statement. If you are still suspicious then go into your local branch.

Never send cash, disclose personal details or buy goods to claim a prize.

Watch out for secret 'get rich quick' schemes and inheritance notifications. If something sounds too good to be true, it usually is.

Always seek professional advice before signing up to any type of investment scheme including precious gems, carbon credits, solar panels, land, wine and property. Contact the FSA (Financial Services Authority). The FSA website is www.fsa.gov.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. The below insert is taken from the Think Jessica website www.thinkjessica.com;

> "Criminals worldwide are hunting down the most fragile members of our society by "working" from mailing lists which categorise people as being elderly or vulnerable in some way. Everyone is at risk but those listed as living alone, not having the internet or any way of being educated about scams or how to report them are their preferred targets. Those who respond end up having their details put on what criminals call "suckers lists". They 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."

Treat any unexpected letters with caution; you don't win prizes for competitions you have never entered.

To reduce junk mail register with the Mail Preference Service, this is a free service. Telephone 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/opt out.

By E-mail (electronic mail)

Just as we all get junk mail through the letterbox you will also find that every time you open your e-mail inbox to check your mail, there will probably be a few items of spam or junk mail. Most of this comes from companies or third parties we have used online. Criminals use this method to either trick us into believing the e-mail is from a genuine company (phishing), or will spin a tail that the sender is in trouble and needs financial assistance.

Examples of e-mail scams:

Hard luck stories, requests for a money transfer (especially from abroad), lottery scams, an e-mail telling you to open an attachment (could be a computer virus), investment opportunities and romantic e-mails asking for financial assistance.

If you have received a Scam E-mail

Do not click on any links in the e-mail if you are unsure of its source.

Do not reply to the e-mail or contact the senders in any way.

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

Do not open any attachments that arrive with the e-mail as these may contain a virus.

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 e-mail to the relevant department at your bank via their website, so they can investigate and warn customers about fake e-mails.

How to spot a Fake E-mail (known as phishing):

The sender's e-mail address doesn't tally with the trusted organisation's website address.

The e-mail is sent from a completely different address or a free web mail address.

The e-mail 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.

A prominent website link - these can be forged or seem very similar to the proper address, but even a single character's difference means a different website.

A request for personal information such as user name, password or bank details.

The e-mail contains spelling and grammatical errors.

You weren't expecting to get an e-mail from the company that appears to have sent it.

The entire text of the e-mail is contained within an image rather than the usual text format.

The image contains an embedded hyperlink to a bogus site.

How to spot a Fake Website:

Check the real URL (Universal Resource Locator – or website address to you and me) by positioning your mouse pointer over the provided link. You will then see true the website address to which you would be directed on the bottom line of your screen. In some programs this information might appear in a box alongside the URL over which you hover. If the true website address differs from the one that appears in the e-mail then there is a good chance that the sender is up to no good and it would be wise not to follow their link. Once a sender is identified as a likely scammer you can add them to your e-mail program's blocked list to send future messages to the junk mail folder. This tip is just one of many, provided on the Hoax-Slayer Website, which is provided free of charge to help us all become safer computer users. If you want to stay up-to-date with the information provided by their service, simply subscribe to their message page by visiting the website. From there you can register to receive regular advice messages, www.hoax-slayer.com.

Unsubscribing from mailing lists:

It is unlawful to send unsolicited direct marketing e mails or text messages to you, unless you have previously told them it's ok to do so.

If there is an existing customer relationship between you and the company, they can send you unsolicited messages about similar products and services, as long as you are given the option to refuse it.

Usually, e mails will have an option at the bottom of the e mail to enable you to unsubscribe from their mailing list.

New research conducted by Which Magazine has revealed the top five scams to be aware of this year.

1. Bank scam e-mail,

69% of people surveyed had received at least one scam e-mail. Usually the e-mail states there are problems with your account and will ask you to update your account details by replying to the e-mail or

clicking on a link. Never click on a link in an e-mail! Call your bank or go straight to your bank's official website.

2. PayPal scam e-mails,

59% of people surveyed had received a scam e-mail claiming to be from PayPal. Often the e-mail will ask for passwords, bank information or credit card details. PayPal will never ask such information from their customers, or ask you to download and install any software.

3. Tax rebate scam,

42% of people surveyed had received an e-mail claiming to be from HM Revenue & Customs (HMRC) promising a tax rebate which asked for account numbers and passwords to complete the payment. HMRC will never ask for any bank accounts details via e-mail.

4. Scam e-mails purporting to be from HMRC,

40% of people surveyed had received scam e-mails claiming to be from HMRC self-assessment form or that your tax notice has been issued. They might be asking to verify your identity by providing a copy of your passport or stating that you have made a mistake on your self-assessment form. Never respond to these e-mails and instead speak directly to HMRC.

5. Scam e-mails seeking money for services or help,

35% of people surveyed had received e-mails seeking money for services or help. This technique is always refined by the scammers and will often prey on the most vulnerable offering low investments and high return. If the e-mail looks like it has come from someone you know and are pleading for money, contact the person directly on alternative contact details.

Bogus Callers on our Doorsteps

What is a bogus caller?

Most people who call at your home will be genuine. However, occasionally people may turn up unannounced and try to trick their way into your home to steal valuables or money; sell you services or items you do not want or need or carry out unnecessary repairs to your home at inflated prices. They may work alone or in pairs, and could be male or female. They could pretend to be from the local council, say they work for a utility company, or use children to trick their way in to your home. In policing terms the offence is known as “burglary artifice or distraction burglary.”

If you have concerns about anyone calling at your home, DON’T OPEN THE DOOR.

Lock your back door and close windows before you answer the door.

Use a spy hole and chain to check who the caller is before you answer.

Ask to see the caller’s identification, even if they have made an appointment to see you, and call their company yourself (not on a number they provide) to check they are genuine.

Never leave the door open and unattended – close it until you return.

Ask the caller to return another time when someone can be with you.

Never agree to have a job carried out if you feel unsure or pressured into it – a genuine caller will not mind coming back at a more convenient time or giving you time to think about an offer.

Do not hand over large sums of money on demand – it may indicate to a rogue trader that you keep large amounts of cash at home.

Never accept an offer to be driven to withdraw money from your bank or building society from anyone you do not know or do not trust.

IF IN DOUBT KEEP THEM OUT

Checking the caller's identification:

Check the expiry date on the identification – is it still valid?

Look at the photograph – has anything been stuck over it, and does it match the person at the door?

Call the company by finding the number in the phone book, on a bill or call directory enquiries. Do not use the number the caller provides – if the ID card is not genuine then the number won't be either.

Ask the company to confirm they have sent someone out to you. They will ask you for information about the identification card, a description of the caller and possibly the date of birth or password of the caller.

Set up a password with your electricity, gas and water companies – each password should be unique but something you will remember.

When a representative calls at your home, they will give you this unique password to confirm they are legitimate.

If you write your passwords down, keep them out of sight but somewhere you can easily find them.

In April 2015 a man was charged with 25 offences after he posed as a bogus water board official and gained entry into homes in Dover, Ashford, Swale and Shepway. The victims were vulnerable members of your communities and need your help to protect them from such criminality. In these situations good descriptions of the offenders, including detail about accents/conversations and any vehicle details that you can note are extremely helpful. Private CCTV images are also useful to assist in case building as they show evidence of behaviour in particular locations.

Be a ScamSmart investor (Source: scamsmart.fca.org)

Investment fraud is often sophisticated and very difficult to spot. Fraudsters can be articulate and appear financially knowledgeable. They have credible websites, testimonials and materials that can be hard to distinguish from the real thing.

Get the tools to spot investment scams:

Reject cold calls

Check the FCA Warning List

Get impartial advice

People offering high risk investments or scams, will often cold call. The firms that the Financial Conduct Authority (FCA) regulates are very unlikely to contact you in this way about investment opportunities. If you're called about an investment opportunity, the safest thing to do is hang up. There are ways that callers can pretend they are not cold calling you. They may refer to a brochure or an e-mail that they have sent you. That's why it is important you know the other tell-tale signs that suggest the investment opportunity is likely to be very risky or a scam.

Callers may do one or more of the following:

Make contact unexpectedly about an investment opportunity. This can be a cold call, e-mail, or follow up call after you receive a promotional brochure out of the blue.

Apply pressure on you to invest in a time-limited offer, for example, offer you a bonus or discount if you invest before a set date, or say that the opportunity is only available for a short period of time.

Downplay the risks to your money, for example talking about how you will own actual assets you may sell yourself if the investment doesn't work as expected, or using legal jargon to suggest the investment is very safe.

Promise tempting returns that sound too good to be true, for example, offer much better interest rates than those offered elsewhere.

Call you repeatedly and stay on the phone a long time.

Say that they are only making the offer available to you, or even ask you to not tell anyone else about the opportunity.

If you recognise any of these, you have every reason to be suspicious. Use the FCA Warning List to check any investment opportunities you're currently interested or involved in.

If you have already or are thinking about transferring your pension, the FCA strongly recommend that you do not send any more money. Find out more about pension scams on The Pensions Regulator website.

Not all investment opportunities offered out of the blue will be very risky or scams, but you should be very wary, especially if they are unusual investments. An investment offered to you in this way is unlikely to suit your specific needs and could be a very bad idea or a scam. It is generally best to seek out your own investment opportunities, either through research or with the benefit of impartial advice from a financial adviser.

The most effective way to stop fraudsters is to report anything suspicious to the relevant authorities and to get help for yourself or someone you know who has been affected.

For updates on current scams in the Kent area go to: www.kent.police.uk/advice/property

For advice and to report issues to Kent Trading Standards: www.kent.gov.uk/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.citizensadvice.org.uk

The Samaritans: 08457 90 90 90 (24 hours a day, 365 days a year) or E mail jo@samaritans.org.

Age UK Advice: 0800 169 65 65 www.ageuk.org.uk

OFCOM: 0300 123 3333 www.ofcom.org.uk

Think Jessica: www.thinkjessica.com

Mailing Preference Service www.mpsonline.org.uk

Action Fraud: 0300 123 2024 www.actionfraud.police.uk

NHW: 0116 2293118 Monday – Friday 0900 – 1700 hours www.ourwatch.org.uk

www.hoax-slayer.com

Office of Fair Trading (OFT): 08457 224499 to report incidents of prize-draw scams www.oft.gov.uk

www.charity-commission.gov.uk - if you have any doubts about door-to-door charity collectors you can check that the charity is registered.

www.moneysavingexpert.com/phones/no-more-junk.