Scam Information from Suffolk Trading Standards

If you need advice or want to report a scam or rogue trader call the Citizens Advice Consumer Service on **0808 223 1133** or contact Action Fraud on **0300 123 2040** or online at www.actionfraud.police.uk.

Scams phone calls

Impersonation scams occur when the victim is persuaded to make a payment to a criminal claiming to be from a trusted organisation. This could include the police, a bank, a utility company, or a Government department such as HMRC.

Report all scam calls via the Citizens Advice Consumer Service on **0808 223 1133.**

Call from a fake Police Officer

Trading Standards has been made aware of an incident where a Suffolk resident was contacted by someone purporting to be the Police.

In the first report the Suffolk resident received a call from a gentleman explaining that he was calling from Martlesham Police Station, and that all the lady's money had been stolen from her bank account. He went on to explain that he was investigating and he required some information from her bank card.

The caller asked for the numbers on her card, including the security code on the back. This was not provided, but only because the resident was unable to read the numbers.

Courier Scam

Courier fraud occurs when a fraudster contacts victims by telephone purporting to be a police officer or bank official. To substantiate this claim, the caller might be able to confirm some easily obtainable basic details about the victim such as their full name and address.

The caller may also offer a telephone number for the victim to telephone or ask the victim to call the number on the back of their bank card to check that they are genuine. In these circumstances, either the number offered will not be genuine or, where a genuine number is suggested, the fraudster will stay on the line and pass the victim to a different individual.

Your bank or the police will never call you to ask you to verify your personal details or PIN by phone or offer to pick up your card by courier.

If you receive a similar call **HANG UP!**

If you need to call your bank back to check, wait five minutes; fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to call your bank.

Your debit or credit card is yours – don't let a stranger take it off you. You should only ever have to hand it over at your bank. If it is cancelled, you should destroy it yourself.

Spot the signs

- Someone claiming to be from your bank or local police force calls you to tell you about fraudulent activity but is asking you for personal information or even your PIN to verify who you are.

- They are offering you to call back so you can be sure they're genuine, but when you try to return the call there's no dial tone.
- They try to offer you peace of mind by having somebody pick up the card for you to save you the trouble of having to go to your bank or local police station.

Fake Trading Standards Officer Scam

A Suffolk resident received a telephone call from an individual, purporting to be from Trading Standards. The conman advised the resident that they were calling as an item they had sold on Facebook Marketplace was stolen, and that he was investigating the matter. The resident was fully aware that what they had sold was not stolen and so did not engage further. It is a criminal offence to impersonate a trading standards officer and can carry a prison sentence of up to 10 years.

All Trading Standards officers carry identification and can be verified by calling the national consumer helpline on 0808 223 1133. As with any telephone call that you receive out of the blue, be vigilant and take a moment to stop and think, especially if you receive a request over the phone or by e-mail to make a payment from someone claiming to be from a trusted organisation. If you are in any doubt, contact the company or organisation directly using an email or phone number from their official website.

Scam energy saving calls

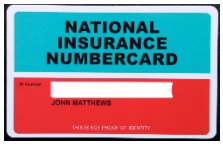
Possible scams include calls offering a "free boiler service" or calls offering a free loft insulation survey,

The advice from Trading Standards is never agree to anything, including a home visit, when approached by a cold caller on the phone, at your door or via email. Do your research first, and find out if it is a product or service that you want or require.

You may be entitled to a grant to help you with the cost of energy improvements on your home, but don't trust a cold caller who advises you that you are.

In Suffolk you can contact **Suffolk Energy Action locally on 0345 0371234** or **Simple Action Energy on 0800 444202.** Both will be able to clarify the current grants available, and what you may be eligible for. More information can be found here: https://www.simpleenergyadvice.org.uk/

Automated phone call scams



There have been reports of automated calls claiming to be from the Inland Revenue, with the caller stating that failure to appear at the Magistrates Court will result in the suspension of your National Insurance Number. You are encouraged to call a number to "resolve" the issue.

This is a scam. Do not telephone the number provided, or provide anyone with your personal details, including your bank or credit card information. HMRC is aware of these automated phone call scams. To help their investigations you should report full details of the scam by email to: phishing@hmrc.gov.uk, including the date of the call, the phone number used and the content of the call.

Amazon Scam

There is currently a scam involving Amazon. A lady calls and says that there has been a mistake and they need to refund your Amazon prime subscription. They ask you to put in a code to authorise the refund, for example 3450. They then appear to have control of your bank account and start transferring money out.

Scam Emails

Scam emails can come from a well-known company or Government agency such as HMRC, TV Licencing or DVLA.

if you receive a scam email:

- Do not click on any links in the scam email.
- Do not reply to the email or contact the senders in any way.
- If you have clicked on a link in the email, do not supply any information on the website that may open.
- Do not open any attachments that arrive with the email.

If you have received a suspicious email forward it to **report@phishing.gov.uk**. You could also report to the genuine company being impersonated).

DPD email scam

There have been reports of a scam using the DPD name inviting recipients by email to select a link to reschedule delivery of a parcel. Recipients are asked to give their bank details. Links in suspicious emails should not be opened and all Scam emails should be forwarded to **report@phishing.gov.uk** to guarantee malicious sites are closed down to protect others.

How you can protect yourself:

- If you are unsure whether the email or text is genuine, then don't use the link. Instead, visit the DPD website by entering the official web address directly into your browser's address bar, or search for it and follow the search results.
- Remember, your bank will never ask you to transfer money to another account or contact you out of the blue to ask for your PIN or full password.
- If you have received an email which you're unsure about, you can report it by forwarding it to report@phishing.gov.uk
- You can report suspicious text messages by forwarding them to **7726**.

Royal Mail email scam

Recipients receive an email purporting to be from Royal Mail. The message informs the recipient that they have missed a delivery from HM Court & Tribunals Service and gives a link to reschedule the delivery.

- DO NOT CLICK ON THE LINK! It is a phishing email designed to steal your personal information.
- Forward scam emails to the National Cyber Security Centre at report@phishing.gov.uk

Postal Delivery Service (PDS) scam

If you receive a missed delivery Parcel Delivery Service (PDS) card (or an email/Facebook message, do NOT share), do not phone the given number as you will be charged for a premium rate call.

Report to Royal Mail Fraud (**020 7239 6655).**

Scam Text Messages

Scam HMRC Text

Beware of fake HMRC text messages that state you are entitled to a grant, a tax refund or a rebate. These texts have been sent by criminals who have created fake websites. The websites that the text links to has been created to look similar to the government website, with the same branding, layout and font choices. The fake website informs users that they will need to provide their card details in order to claim the grant or refund. DO NOT CLICK ON THE LINK. If you think you have provided scammers with your financial details, contact your bank immediately.

HMRC will never send notifications of a tax rebate or ask you to disclose personal or payment information by text message.

If you receive what you think is a fake message, forward the text message, including phone number or company name, to **7726**. It won't cost you anything and it means your phone provider can investigate the sender. If you think you might have responded to a text message scam and provided your bank account details, contact your bank immediately.

Report all scams to Trading Standards via Citizens Advice Consumer Service on **0808 223 1133.**

Doorstep scams

Nottingham Knockers

These individuals claim that they have just come out of prison, and are on a youth offending scheme, attempting to mend their ways. They then try to sell the householder everyday household products at very high prices. Trading Standards always advise residents to refrain from buying at the doorstep and not to buckle to pressure from salespeople offering supposedly one-off 'buy it now' low prices.

These Nottingham Knockers work in gangs across the country and they are NOT involved in any officially recognised offender rehabilitation programme. Many do not possess Pedlar's Certificates, which are issued by police. If you are approached at the door, please refuse to buy.

Report all doorstep callers to us via **Citizens Advice Consumer Service on 0808 223 1133.**

Fish and Meat selling scams

Suffolk Trading Standards' advice is do not purchase any meat or fish from a cold caller.

If you are approached, do not deal with them and report to Trading Standards (0808 223 11330).

These traders travel nationally, cold calling consumers' homes selling the meat and fish. This is often misdescribed, mislabelled or unlabelled, overpriced and sometimes underweight. They usually use Transit-style vans which may not be refrigerated.

Facebook scams offering vouchers, promotions or competitions

Scammers set up a Facebook page offering vouchers or similar from a major supermarket or company. The page has been set up by scammers for 'like-farming', using your interaction to harvest personal data.

Before liking a page, especially if it is a large company, check if it has a blue tick. This means the page has been verified by Facebook. You can also look at the page transparency to see when it was created.

If you come across a fake page on Facebook, report it by going to the page and tap *** from the top right and select "Give feedback or report this Page". Select "Scams and Fake Pages". Fake promotions or competitions on Facebook typically urge users to either engage with a Facebook post (e.g. share and comment) to win a prize or click a link to claim a prize or possibly both. Trading Standards recommends that you never interact with this type of Facebook posts.

Loan Shark Scams

Beware of any requests for your details or money. Loan sharks may ask for copies of your passport or pictures of your house, the street and your house number. Never send money or give card details, online account details or copies of personal documents to anyone you don't know or trust. If you suspect someone may be a loan shark or they are acting inappropriately, you can report them anonymously to www.stoploansharks.co.uk or by calling the Stop Loan Sharks Helpline on **0300 555 2222**. Alternatively, you can email the team reportaloanshark@stoploansharks.gov.uk or access support via live chat on the website Monday to Friday between 9am-5pm. The Stop Loan Sharks App is free to download on both iOS and Android devices from the Apple App Store and Google Play Store.

Thinking of buying a pet online?

Capitalising on the rise in people getting pets due to the national lockdown caused by coronavirus, criminals have been posting fake adverts on social media, online marketplaces and specific pet-selling platforms. Unsuspecting victims will be asked to pay a deposit for the animal without seeing it in person first, with many criminals using the restrictions caused by the pandemic as a reason why they cannot see the animal. After the initial payment is made, more and more funds will be requested to cover additional costs such as insurance, vaccinations and even delivery of the pet.

How can you protect yourself from falling victim to pet fraud?

- **Do your research**: If you're making a purchase from a website or person you don't know and trust, carry out some research first. Look up reviews of the website or person you're buying from. If you're purchasing an item from an online marketplace, you can view the seller's feedback history before going ahead with the purchase.
- **Trust your instinct**: If you're unable to physically view the animal in person, ask for a video call. If you're buying a young animal, make sure you're able to see the mother and rest of the litter. Any responsible seller will understand why you want to view the animal in person. If the

seller declines, challenge them on why. If you have any suspicions, do not pay any money until you're certain it's genuine.

- **Choose your payment method wisely**: Avoid paying by bank transfer as that offers you little protection if you become a victim of fraud. Use a payment method, such as a credit card if you have one, that offers buyer protection in case anything goes wrong.

Brexit Scams

Britain's departure from the EU will provide criminals with an opportunity to target you with fraud and scams. These may include:

- Tricking you into purchasing European Health Insurance Cards from unofficial websites
- Fake HMRC websites urging businesses trading with the EU to register for a "UK trade number"
- Unsolicited calls/emails encouraging you to make new investments

Stay ahead of the criminals by always taking a moment to stop and challenge any requests for your personal/financial information or money. Remember they are experts at tricking you into believing they are from trusted organisations using urgent language and even easily obtainable personal information. You can protect yourself by seeking advice directly from the gov.uk website below and contacting organisations directly using a known email or phone number. If you're planning on making any investments, check the Financial Conduct Authority's register for regulated firms, individuals and bodies. Additionally, HMRC will never ask you for your personal or payment information via emails or text messages. https://www.gov.uk/transition

When things go wrong

Anyone can fall victim to fraud. If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at www.actionfraud.police.uk or by calling **0300 123 2040**. Action Fraud is the UK's national fraud crime reporting centre. It gathers intelligence on scams and passes it onto the National Fraud Intelligence Bureau for analysis by the police.

If you've given your bank details over the phone or handed your card to a courier, call your bank straight away to cancel the card.

For information on call blocking devices you may wish to look at advice by Which? available here: https://www.which.co.uk/.../how-to-block-nuisance-calls

Ofcom also has a comprehensive guide which explains the different types of nuisance call and message and includes advice on what action you can take to protect yourself and who you can complain to: https://www.ofcom.org.uk/.../protecting-yourself-from.

Further advice on all types of crime can be found at: http://www.suffolk.police.uk/advice/crime-prevention-z and http://www.ourwatch.org.uk/crime-prevention