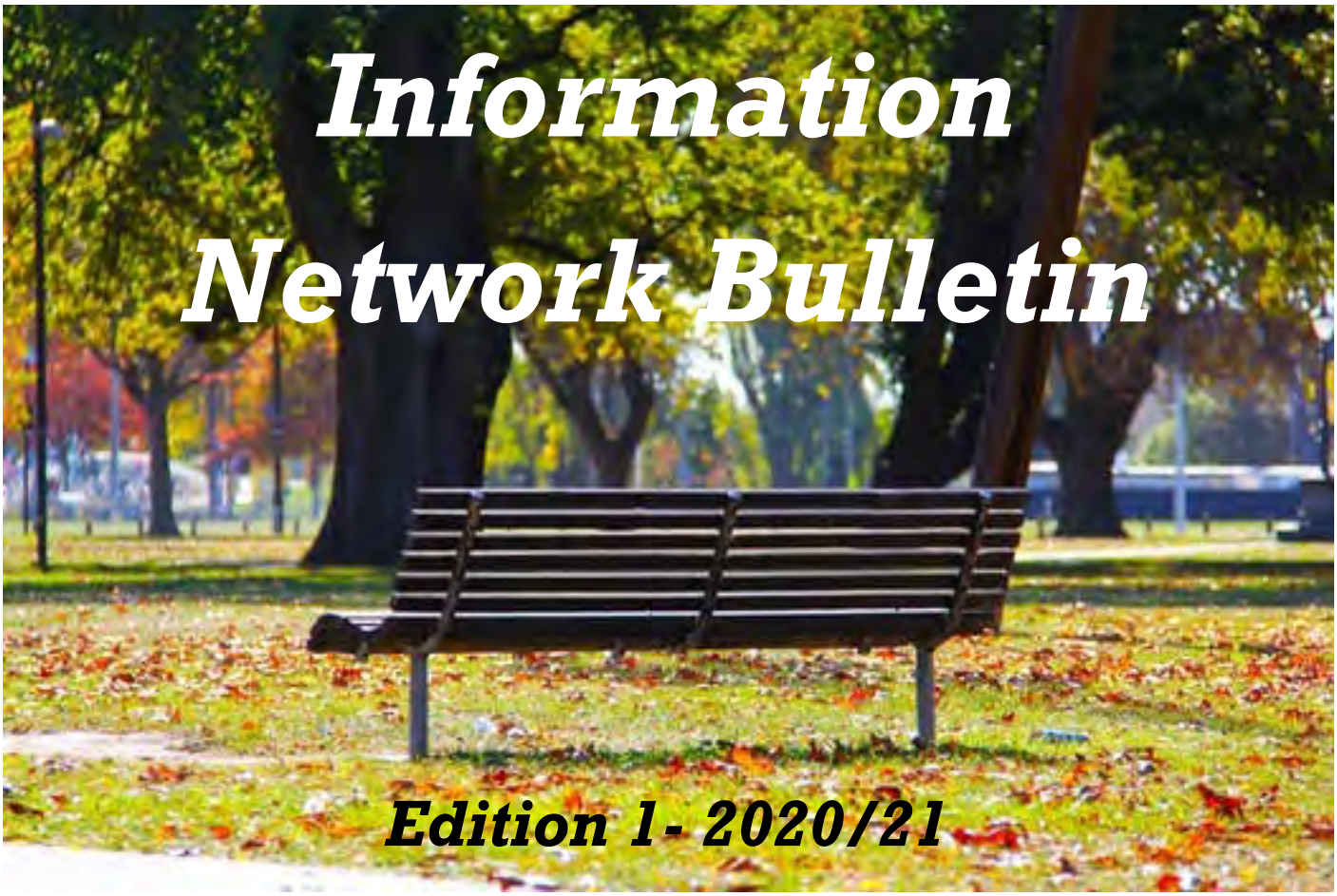

Information Network Bulletin

Edition 1- 2020/21

Welcome to the latest edition of the Information Network Bulletin brought to you by Croydon Council's Trading Standards team.
In addition to general news from the team, it includes details of some of the latest scams and fraud alerts which we have become aware of in recent months.

We hope that you find it useful.

Friends Against Scams

During the COVID-19 pandemic there has been a marked increase in scams. These are happening online, via text, email and fake websites and also by cold calling on the telephone. There have been a wide variety of scams reported ranging from HMRC scams, to fake and dangerous Personal Protective Equipment being sold, to fake charities being set up.

Friends Against Scams is run by the National Trading Standards Scams Team. Their aim is to protect and prevent people from becoming victim of scams by empowering people to take a stand against scams. The site contains a wealth of information on the types of scams about and how to protect yourself from them. This is the link to their website: www.friendsagainstscams.org.uk

They also have a free online training tool and have advice on how to raise awareness in your community. The direct link to the free training can be found here:

https://www.friendsagainstscams.org.uk/training/friends-elearning

Please remember to report to Action Fraud 0300 123 2040 or Citizens Advice Consumer Helpline 0808 223 1133 if you have actually been the victim of a scam.

Coronavirus : scams

Croydon Trading Standards wants to continue to raise awareness of scams this summer. Empowering the public to protect themselves and others from scams is more important than ever .
The coronavirus crisis means more people are facing issues - from employment and debt, to housing and health - resulting in more people being in vulnerable situations. Added to this, the overall heightened uncertainty and anxiety caused by the pandemic is making everyone more vulnerable and more likely to fall victim to a scam.
Scams are crimes that can happen to anyone and we can all take a stand to help stop them. There are actions we can all take to report them, share stories and raise awareness of scams to safeguard ourselves and others.

Recognising a scam

New scams to look out for include:

- advertising face masks or medical equipment at high prices
- emails or texts pretending to be from the government
- emails offering life insurance against coronavirus
- people knocking at your door and asking for money for charity

If you see emails or texts about coronavirus from someone you don't know, or from an unusual email address, don't click on any links or buy anything.
Don't give money or personal details to anyone you don't know or trust – for example someone who knocks on the door and offers to help

It might be a scam if:

- it seems too good to be true – for example, a holiday that's much cheaper than you'd expect
- someone you don't know contacts you unexpectedly
- you suspect you're not dealing with a real company – for example, if there's no postal address
- you've been asked to transfer money quickly
- you've been asked to pay in an unusual way – for example, by iTunes vouchers or through a transfer service like MoneyGram or Western Union
- you've been asked to give away personal information like passwords or PINs
- you haven't had written confirmation of what's been agreed

If you've been scammed, you need to:

- protect yourself from further risks
- check if you can get your money back
- report the scam

Reporting a scam

- Don't feel embarrassed about reporting a scam – scammers are clever and scams can happen to anyone.
- Reporting a scam helps track down and stop scammers. This prevents other people from being scammed.

Seek advice contact Citizens Advice consumer helpline: **0808 223 1133**

Report all types of scams to Action Fraud. They can give you a crime reference number, which can be helpful if you need to tell your bank you've been scammed.
It's quickest to report a scam to Action Fraud online at https://www.actionfraud.police.uk/ but you can also report the scam by phone.
Action Fraud Telephone: 0300 123 2040 (Monday to Friday, 8am to 8pm)

HMRC Scams

Tax Office scams continue to plague Croydon residents, either claiming that you owe HMRC money or that you are due to receive a tax rebate. Two typical examples are outlined here.

Recently a Croydon resident found an intimidating voicemail left on his mobile phone. The caller claimed that a lawsuit had been taken out against the resident, who owed money.

Frightened by this, the gentleman rang the number back and asked the person who answered who there were and where they were calling from? They told him they were from HMRC, the tax office, and then asked the gentleman what his name was. At this, he challenged them by stating that HMRC do not telephone people. They quickly hung up.

Clearly, the aim of the scammers had been to frighten the gentleman with the allegation of the law-suit for the money that they claimed he owed to HMRC and then to get him to make payment to them over the phone.

Another resident received a text message claiming to be from HMRC, which read:

HMRC: You have a pending tax rebate 01/05/2020. To calculate your claim click here: http://govrebateuk.co.uk

The link took him to a website which resembled a genuine webpage, but he could see that it was not a secure one, there was no padlock next to the web address. The page asked the viewer to input personal and bank card details, allegedly to calculate the tax rebate due and then pay it directly onto your bank card. At this time, when many persons are suffering financial hardship the scammers were looking to lure victims in with the promise of an instant tax rebate, when in all likelihood they would have used the bank card details to clear out the gentleman's bank account.

Fortunately, in both of these cases, the persons targeted by the scammers remembered that HMRC only communicate via letter. So they knew that both the voicemail and the text message were from scammers.

As well as reporting these scams to Trading Standards, they also alerted HMRC and Action Fraud.

To report scams to HMRC go to:
https://www.gov.uk/report-suspicious-emails-websites-phishing/report-hmrc-phishing-emails-texts-and-phone-call-scams

All scams should also be reported to Action Fraud, go to: https://www.actionfraud.police.uk/

Covid19 Bogus offer: TV Licence

Action Fraud have received reports concerning bogus offers, purporting to be from TV Licensing claim that the recipient's direct debit has failed and that they need to pay to avoid prosecution. Recipients are told that they are eligible for a "COVID19 Personalized Offer" of six months free. The messages contain links to genuine-looking websites that are designed to steal personal and financial information.

Always question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text.

Here's where you can get the latest information on coronavirus-related scams and how to protect yourself: http://actionfraud.police.uk/covid19

Double Your Money? Get Rich Quick? Too good to be true!

The COVID lockdown has resulted in many people having to live on a reduced income. Unfortunately, this also means that they may be more susceptible to investment scams or opportunities to increase their savings quickly.

One Croydon resident recently reported being the victim of an investment scam on YouTube.
The gentleman who usually worked in the building trade, was on a much reduced income as the firm he worked for had closed.

Whilst looking on YouTube he found a video of what appeared to be a live show talking about technology. Part of the presentation invited was about a bitcoin investment that would give you double your investment back.

The video had been edited to include known persons speaking about crypto currency and technology, so that they appeared to be part of the presentation and gave it the semblance of being genuine.
Viewers were told to send their bitcoin to a specified bitcoin wallet, with the promise of them receiving double their investment back.

Being short of money the gentleman sent his bitcoin off and within minutes realised that he had been scammed. As he put it, his lack of money had caused him to lose his head for five minutes and that had cost him all the money he had. He no longer even had the money to pay his rent.

Lured by the promise of doubling his money the resident made the transaction, only to lose a significant amount of money; as have many others.

Remember:

- In these difficult economic times treat any investment promising high returns with extreme caution.
- Do not rush to invest, take time to carry out thorough checks
- If it sounds too good to be true, it probably is!

If you have been the victim of a scam, please report it to Action Fraud by telephone 0300 123 2040, or via their website https://www.actionfraud.police.uk

Too Much Charity Mail?

It is known that some people find themselves overwhelmed by contact from charities – some who they will have never knowingly signed up to receive information from. The pressure to give and be charitable can cause unnecessary stress and hardship for those receiving this type of marketing.

In July 2017 a service was launched by the Fundraising Regulator which allows people to end direct marketing contact from charities. The service does not stop contact from all charities but subscribers can:

- Identify specific charities which they want to stop all communication with
- Select the form of contact they want to stop; email, phone, letter

The Fundraising Preference Service is an official service that lets you stop charities contacting you. Please visit http://public.fundraisingpreference.org.uk/ for more information.

Using their website, you can end contact with up to 3 charities at a time. If you prefer, you can call their help-line on 0300 3033 517, where you can end contact with up to 20 charities at a time. You can stop charities contacting you by email, telephone, post and/or SMS (text message). You can also end contact with charities on behalf of someone else, if you have their authority to do so.

Subscription Traps

Croydon trading standards often receive details of complaints where consumers have signed up to a 'free' trial of goods but to their surprise they then find out that card payments are subsequently taken from their bank account. This 'subscription trap' often applies to products such as slimming pills, health foods, pharmaceuticals, & anti-aging products. The website www.getsafeonline.org. has some tips to avoid being scammed in this way:

The risks

- Taking advantage of a free or low-cost offer, only to find that it ends up costing you hundreds or even thousands of pounds.
- Not being able to cancel an agreement or stop payments being taken from your account.

Avoiding subscription traps

- Read the small print (terms & conditions) carefully before entering into any agreement or making a purchase, however long this may take.
- Make sure the terms & conditions box has not been pre-ticked.
- If you make a purchase of this kind that gives you a limited timescale to cancel the agreement, make sure you do so before the due date if you want to cancel it.
- Never provide bank details to companies without doing some prior research beforehand.
- Keep a copy of any advertisement (print it or take a screenshot) that you reply to, and to keep a note of the webpage.
- Remember that you will have more chance of cancelling agreements or obtaining a refund if the company is UK-based. Even those with UK addresses are often just fulfilment companies who are contracted to send out the goods. The companies themselves often have no physical presence in the UK.
- Check your bank/payment card statements regularly for unexpected payments.

If you are the victim of a subscription trap

- Make every effort to contact the company concerned to cancel the agreement.
- Contact your bank to cancel future payments.
- Ascertain with your bank whether a new card is needed.
- Request reimbursement from the supplier if the advertisement did not explain the charges, but be aware that without a copy, your claim may fail. If the website has changed in the meantime, try accessing your internet browser's cache or the internet archive.
- Refer a complaint about the bank to the Financial Ombudsman Service If the bank refuses to stop the charges or reimburse charges that have been made, consider referring the issue to the Financial Ombudsman
- Contact your local Trading Standards.
- Report it to Action Fraud, the UK's national fraud reporting centre by calling **0300 123 20 40** or by visiting **www.actionfraud.police.uk**.

Croydon *Plus*

SAVINGS & LOANS FOR PEOPLE
IN CROYDON, MERTON & SUTTON

CroydonPlus was originally established in 1999 as Croydon Savers Credit Union Ltd (Croydon Employees Credit Union) as a Credit Union for Croydon Council staff. In 2004 we expanded our membership, savings and loans services to anyone living or working in Croydon and in 2010 changed our name to Croydon Merton & Sutton Credit Union to reflect our expansion into Merton and Sutton. In February 2016 we changed our name to CroydonPlus to mark the beginning of a sustained process of modernisation for current and new members, as we respond to the opportunities and challenges of financial services in the digital age.

As we have grown, our purpose has remained the same: to provide local people with an accessible, secure and ethical way of saving and borrowing money.

This year marks our 21st Birthday and we are extremely proud that we have been able to continue to provide a safe, ethical and affordable way of helping our members manage their money for such a long time. Michael Wilson, CEO at CroydonPlus commented "21 years wow - to think that we have been helping people with their finances for that long? We are proud to have reached this milestone. It feels amazing to be a part of an organisation that truly places the community at the heart of what we do"

At CroydonPlus, we know that financial worries can often be cause for concern for many and not having a savings pot when an emergency happens can be a worry. We are committed to helping our members with financial solutions for all of life's unexpected situations.

For more information on our products and services, please visit our website at www.croydonplus.co.uk

Personal Loan
fairbanking
for your financial well-being
Personal Loan

Covid-19 and your pension

Scammers are continuing to target pension pots of all sizes during the coronavirus outbreak. Before making a decision on your pension, read below to find out how to protect yourself from scams.

The coronavirus pandemic has impacted on all kinds of companies to a varying degree, including those listed on the stock market. As a result, markets have been volatile and are likely to remain so for a while. This can have an impact on pensions, and lead to an increase in scams.

If you're facing financial difficulties because of coronavirus, you may be tempted to cash in some of your pension. This isn't usually possible before the age of 55, except in cases of ill-health or where you have a protected retirement age that is below 55.

Read this easy-to-read guide(link is external) to find out how the Government and regulators are working together to support savers and protect pensions during covid-19.

The warning signs

Scam offers often include:

- free pension reviews
- higher returns – guarantees they can get you better returns on your pension savings
- help to release cash from your pension even though you're under 55 (an offer to release funds before age 55 is highly likely to be a scam)
- high-pressure sales tactics – the scammers may try to pressure you with 'time-limited offers' or even send a courier to your door to wait while you sign documents
- unusual investments – which tend to be unregulated and high risk, and may be difficult to sell if you need access to your money
- complicated structures where it isn't clear where your money will end up
- arrangements where there are several parties involved (some of which may be based overseas) all taking a fee, which means the total amount deducted from your pension is significant
- long-term pension investments – which mean it could be several years before you realise something is wrong

4 simple steps to protect yourself from pension scams

Step 1 – reject unexpected offers
If you're contacted out of the blue about a pension opportunity, chances are it's high risk or a scam.

If you get a cold call about your pension, the safest thing to do is to hang up - it's illegal and probably a scam. Report pension cold calls to the Information Commissioner's Office (ICO)(link is external).

Be wary if you're contacted about any financial product or opportunity and they mention using your pension.

If you get unsolicited offers via email or text, you should simply ignore them. Fortunately, most people do reject unsolicited offers – our research suggests that 95% of unexpected pension offers are rejected.

Be wary of offers of free pension reviews. Professional advice on pensions is not free – a free offer out of the blue (from a company you have not dealt with before) is probably a scam.

And don't be talked into something by someone you know. They could be getting scammed, so check everything yourself.

Continued next page

Covid-19 and your pension (cont.)

Step 2 – check who you're dealing with
Check our Financial Services Register to make sure that anyone offering you advice or other financial services is FCA authorised, and they are permitted to provide those services regarding pensions. If you need any help checking, call our Consumer Helpline on 0800 111 6768.

Check they are not a clone – a common scam is to pretend to be a genuine FCA-authorised firm (called a 'clone firm'). Always use the contact details on our Register, not the details the firm gives you.

Check the FCA Register
If you use an unauthorised firm, you won't have access to the Financial Ombudsman Service or the Financial Services Compensation Scheme so you're unlikely to get your money back if things go wrong.

If you use an authorised firm, access to the Financial Ombudsman Service and FSCS protection will depend on the investment you are making and the service the firm is providing.

Check to see if they are registered with Companies House (www.gov.uk/government/organisations/companies-house) and the directors' names. Search the company name and the directors' names online to see if others have posted any concerns.

Check the FCA Warning List – use our tool to check the risks of a potential pension or investment opportunity. You can also search to see if the firm is known to be operating without our authorisation.

Step 3 – don't be rushed or pressured
Take your time to make all the checks you need – even if this means turning down an 'amazing deal'. Be wary of promised returns that sound too good to be true and don't be rushed or pressured into making a decision.

Step 4 – get impartial information or advice
You should seriously consider seeking financial guidance or advice before changing your pension arrangements.

- The Pensions Advisory Service (www.pensionsadvisoryservice.org.uk) provides free independent and impartial information and guidance.
- If you're over 50 and have a defined contribution pension, Pension Wise (www.pensionwise.gov.uk) offers pre-booked appointments to talk through your retirement options.
- You can also use a financial adviser to help you make the best decision for your own personal circumstances. If you do opt for an adviser, make sure they are regulated by the FCA and never take investment advice from the company that contacted you, as this may be part of the scam. Find out more about getting financial advice (www.moneyadviceservice.org).

If you suspect a scam, report it

- Report to the FCA – you can report an unauthorised firm or scam to us by contacting our Consumer Helpline on 0800 111 6768 or using our reporting form.
- Report to Action Fraud (www.actionfraud.police.uk) or by calling 0300 123 2040.
- If you've agreed to transfer your pension and now suspect a scam, contact your pension provider straight away. They may be able to stop a transfer that hasn't taken place yet. If you are unsure of what to do contact the Pensions Advisory Service for help.
- If you have already invested in a scam, fraudsters are likely to target you again or sell your details to other criminals. The follow-up scam may be completely separate or related to the previous fraud, such as an offer to get your money back or to buy back the investment after you pay a fee.

Buying & Selling Vehicles

As the economy starts to open up after the COVID-19 lockdown period more people will begin to think about either buying or seller a used car. Croydon trading standards wants to remind people of the main issues that they should consider when entering into a transaction so that they do not lose out financially.

Safe Buying

- Pay for the vehicle when you physically collect it from the seller. Never send money abroad, part with any money (including a deposit) for a vehicle you have not seen and inspected, or to a 'payment protection' service.
- If the vehicle is being offered at a much cheaper price, it could be the sign of a scam. Always check the market value by getting a valuation or comparing the price on Auto Trader or similar sites.
- Perform a Google image search to check if photos have been copied from other websites. This could help to save you from being defrauded by buying a non-existent vehicle.
- Physically check the vehicle (preferably in daylight) and its documentation – V5C document (also known as the 'logbook', service history and MOT certificates – before handing over any money.
- Check the mileage appearing on the milometer matches its service history and old MOT certificates. On analogue milometers (found on some older vehicles) ensure the numbered barrels line up. Check the general condition matches age and supposed mileage.
- Check – or have an expert check – that the vehicle is not a 'cut and shut' (two or more vehicles welded together).
- Check that the V5C is authentic, with a DVLA watermark. Check the serial number in the top right-hand corner – if it falls into the following range it could be stolen and the police should be informed: BG8229501 to BG9999030, and BI2305501 to BI2800000.
- View the vehicle at the seller's home and check the address is the same as the one listed on the registration document (V5C). Ensure that the seller is the recorded keeper, otherwise they may not be legally entitled to sell the vehicle.
- Check that the Vehicle Identification Number (VIN) is the same as that on the V5C. This number is commonly found on the chassis, on the windscreen or on the floor by the driver's seat. Check that this has not been tampered with.
- Get a car history check to find out whether the vehicle has been recorded as stolen, written off, scrapped or is subject to outstanding finance. You can check online to find out what information the Driver and Vehicle Licensing Agency (DVLA) holds about a vehicle. Other organisations including Auto Trader offer car history checks.
- If buying from a dealer or vehicle supermarket, check up front that the advertised price is the total price and that you will not be charged 'admin fees' or other additional costs.

Continued next page

Buying & Selling Vehicles (cont.)

Safe Selling

- Make sure any test driver has a valid driving licence and suitable insurance cover. You could be liable for any accidents they may have.
- To avoid buyers being left alone (and potentially driving away) with your vehicle, keep hold of their keys at all times and avoid leaving them in the ignition.
- Never hand over the vehicle keys or documentation until your bank has confirmed the full value of the vehicle has cleared into your bank account.
- Never send money abroad.
- Never pay a large deposit.
- Don't be pressured into releasing your vehicle – a genuine buyer will not mind waiting until the draft has cleared.
- Be careful about how you take payment:
- Cash – ask for the cash to be handed to you in a bank, where the notes can be checked for forgeries and paid in immediately.
- Cheques – never let the buyer take your vehicle until the funds have cleared in your bank account.
- Bank drafts – are not as good as cash, so treat them in the way you would a personal cheque.
- Online bank transfer is one of the safest ways to pay as it avoids handling large amounts of cash and the problems associated with cheques.
- Obscure the number plates in the photo(s) you use to advertise your car. If a potential buyer asks why, explain how plates can be cloned for use on other vehicles for more serious crimes.

And as with all kinds of online transactions, always observe the following precautions:

- Do not reply to, or click on links contained in, unsolicited or spam emails from companies or individuals you do not recognise.
- Make absolutely sure the correct website address appears in the address bar, as it is easy for fraudsters to use similar spellings or other details to fool you into visiting a fake site.
- Before entering payment card details on a website, ensure that the link is secure, in three ways:
    - There should be a padlock symbol in the browser window frame, which appears when you attempt to log in or register. Be sure that the padlock is not on the page itself ... this will probably indicate a fraudulent site.
    - The web address should begin with 'https://'. The 's' stands for 'secure'.
- Double check all details of your purchase before confirming payment.
- Some websites will redirect you to a third-party payment service (such as WorldPay). Ensure that these sites are secure before you make your payment.
- Choose safe passwords and do not reveal them to anybody, however trustworthy you think they may be.
- Always log out of websites into which you have logged in or registered details. Simply closing your browser is not enough to ensure privacy.
- Keep receipts.
- Remember that paying by credit card offers greater protection than with other methods in terms of fraud, guarantees and non-delivery.
- Check credit card and bank statements carefully after shopping to ensure that the correct amount has been debited, and also that no fraud has taken place as a result of the transaction.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

Ensure that if you are using a wireless network, it is secure and encrypted.

(Continued next page)

Buying & Selling Vehicles (cont.)

If you suspect anything

- If you receive an email which you believe to be from a fraudster, do not respond, but forward it to the abuse department of the sender's email provider and use your email software to block further emails from the sender.
- If you receive a text message asking you to phone a premium rate number, contact the free Phone-paid Services Authority (PSA) helpline on **0300 30 300 20**. Alternatively, you can make a complaint to Phone-paid Services Authority or check a premium rate number.

Report it!
If you think you have been a victim of vehicle fraud:
Report it to Action Fraud, the UK's national fraud reporting centre by calling 0300 123 20 40 or by visiting www.actionfraud.police.uk

Key Fraud Protection Advice

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you hoping you'll let your guard down for just a moment.

They can contact you by phone, email, text, on social media, or in person. They will try to trick you into parting with your money, personal information, or buying goods or services that don't exist.

If you are approached unexpectedly remember to:

- Stop: Taking a moment to think before parting with your money or information could keep you safe.
- Challenge: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- Protect: Contact your bank immediately if you think you've fallen victim to a scam and report it to Action Fraud.
- The police, or your bank, will never ask you to withdraw money or transfer it to a different account. They will also never ask you to reveal your full banking password or PIN.
- Do not click on links or attachments in unexpected or suspicious texts or emails.
- Confirm requests are genuine by using a known number or email address to contact organisations directly.
- To keep yourself secure online, ensure you are using the latest software, apps and operating systems on your phones, tablets and laptops. Update these regularly or set your devices to automatically update so you don't have to worry.

Was this bulletin helpful?

Contact Trading Standards to request a free door sticker advising cold callers that they are not welcome. If you are a victim of scam mail, contact us to receive a free copy of our toolkit on how to avoid falling victim and how to stop the letters.

Additionally, please let us know what you think of this bulletin and what Trading Standards topics you would like to see covered in future editions.

Contact Trading Standards: Tel: **020 8407 1311**
Email: **trading.standards@croydon.gov.uk**

Citizens Advice Consumer Service: Tel: **03454 04 05 06**
Web: **www.citizensadvice.org.uk**