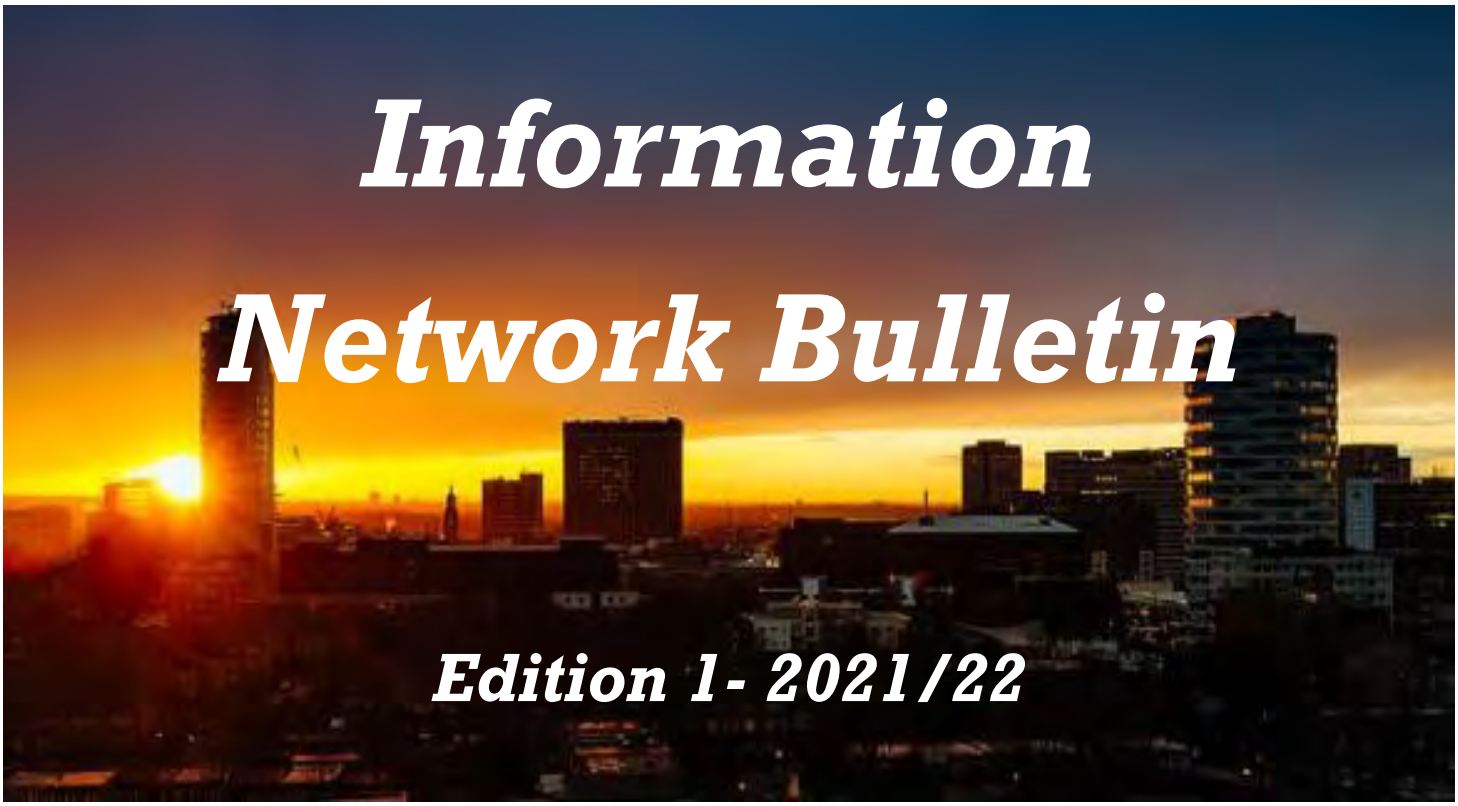

Welcome to the latest edition of the Information Network Bulletin brought to you by Croydon Council's Trading Standards team.
In addition to general news from the team, it includes details of some of the latest scams and fraud alerts which we have become aware of in recent months.

We hope that you find it useful.

Croydon Resident falls victim to PayPay scam

A Croydon resident recently posted their unwanted iPhone for sale on an online platform.

She received a number of enquiries about the phone, including one from a gentleman who offered her £240.00 for the phone. They agreed on this price and he advised that he wished to make the payment through his PayPal, which she also agreed to, being a secure payment method.

The resident received an email, apparently from PayPal, advising that they had received the money from the purchaser. She checked this via the link in the email and it showed that the money was held.

The resident sent iPhone by recorded delivery and checked it had been received.

However, instead of receiving her £240.00, she received another email from PayPal, this time stating that the PayPal account was personal and that she would have to pay £150.00 to upgrade to unlock the money and receive the payment.

Now realising that something was very wrong she contacted the buyer, who confirmed that he had received the phone. When she asked him what this £150.00 payment was all about, he hung up and then blocked her number.

The resident then carefully studied the emails that she had received, apparently from PayPal, and realised that they were spoof emails made to appear to be from PayPal.

Croydon Trading Standards remind residents to be vigilant and to carefully check emails that receive.

There are numerous spoof websites in operation and spoof emails being sent out apparently from genuine businesses, government agencies, etc; but designed to scam you out of your money or steal your personal information.

If you receive a suspicious email, forward it to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk and their automated programme will immediately test the validity of the site.

Any sites found to be phishing scams will be removed immediately.

NEIGHBOURHOOD WATCH
CROYDON

Neighbourhood Watch Network is a charity registered in England & Wales, CIO no: 1173349

PROTECT YOUR POOCH

Dog theft is on the rise and we are urging the public to keep their dogs SECURE, IN SIGHT and SEARCHABLE, and to help make pet theft a SPECIFIC OFFENCE.

Keep them:

1. SECURE (pets are easily stolen from unsecured gardens if left unattended)

2. IN SIGHT (when out and about keep them close and practice good recall)

3. SEARCHABLE (to support quicker recovery if they go missing keep them microchipped, tagged and up to date photos)

AND HELP MAKE PET THEFT
A SPECIFIC OFFENCE

Find out more on all of the above and more at
ourwatch.org.uk/ProtectYourPooch

We hope you find this update helpful and interesting, please pass on to your watch/residents.

#FeelSafeStaySafe

Your Croydon Neighbourhood Watch Team

We are your Neighbourhood Watch, working to reduce crime in Croydon

#FeelSafeStaySafe

Community Fund Bringing Communities Together
Neighbourhood Watch CROYDON
CROYDON www.croydon.gov.uk | Delivering For Croydon

Caller ID Fraud

The UK telecoms regulator Ofcom is warning the public not to trust caller ID on their phones as it tries to help stop people becoming victims of fraud.

Ofcom states caller ID should not be used as a means of verifying a caller's identification.
Fraudsters are increasingly changing their caller ID to disguise their identity, known as number spoofing.

Ofcom describes number spoofing as people who deliberately change the telephone number and the name that is relayed as the Caller ID information.

For example, scammers call you and they 'spoof' the number of your bank or another organisation. If you query the call they say "check the number on the back of your bank card, it will be the same". This is because the scammers have been able to change the ID of their number so it appears as a genuine number for a bank, organisation or company, or another mobile number. They use software to do this and carefully written scripts to help convince you of their legitimacy. They then aim to get personal or banking information from you in order to commit fraud and financially gain from your mistake.

Our advice, if you receive a call, is to **hang up**. Leave the phone for a couple of minutes so the fraudsters call is ended and you can consider what was said to you.

Contact the bank or organisation directly using a number you would usually use, a number from a letter or their official website. You can then check the validity of the call.

A genuine organisation will understand why you ended the original call. If it was a 'spoofed' call then you would have avoided becoming a victim of fraud.

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.

Please report any suspicious or scam texts to 7726. This is a free-of-charge service. You copy and forward the content of the text to the number and then forward the content the number the text came from.

For further information and articles with examples of Caller ID Spoofing please visit the links below:

- https://www.bbc.co.uk/news/business-56934517
- https://www.which.co.uk/news/2019/10/whos-really-calling-you-an-investigation-into-the-worrying-rise-of-number-spoofing/

New National Insurance Number Fraud

A worrying new scam has recently come to light involving National Insurance numbers.

We all have these numbers to identify us on government systems, such as HM Revenue and Customs (HMRC) and the Department for Work and Pensions (DWP).

But hundreds of people have reported receiving an automated telephone call, during which tells them that their "National Insurance number has been compromised".

They are told to "press 1 on their handset to be connected to the caller", allegedly to fix the problem and obtain a new National Insurance number.

However, on doing this and connecting to the "caller", victims are then pressured into handing over personal details, which the fraudsters claim is to enable them to receive a new National Insurance number.

However, once they have your personal details, these criminals are able to commit fraud using your credentials and information.

Remember:

- Be vigilant and cautious of any automated calls you receive mentioning your National Insurance number becoming compromised.
- If you are contacted out the blue by someone asking for your personal or financial details, this could be a scam.
- Even confirming personal details, such as your email address, date of birth or mother's maiden name, can be used by criminals to commit fraud.
- If you have any doubts about what is being asked of you, hang up the phone.

If you have any concerns and want to contact National Insurance with queries use:

https://www.gov.uk/government/organisations/hm-revenue-customs/contact/national-insurance-numbers

Illicit Tobacco & Singles Cigarettes Sales

In September 2020, Croydon Council Trading Standards officers confiscated thousands of illegal cigarettes and tobacco products from shops suspected of selling counterfeit and illegal goods.

The seizures included non-duty paid foreign cigarettes which are also insufficiently and incorrectly labelled for the UK market, oral tobacco which is a banned product and suspected counterfeit hand rolling tobacco and cigarettes.

Illegal tobacco is sold cheaply. This encourages people to continue smoking, the prices are attractive to young people and children, and the packaging does not carry the relevant health warnings.

The oral tobaccos we have found being sold carry extreme health risks. The oral cancers that come from the use of such products contribute to horrific deformities and health problems to users.

If you know of anyone selling oral tobacco such as RMD, Kuber, Mirage, Black Naswar or Tulsi please let us know so we can remove the items from sale and protect the community.

Another issue which we have had reported is that of shops in Croydon selling single cigarettes. Selling a single cigarette or breaking a pack and selling the contents is illegal.

If a trader sells illegal tobacco, be it non-duty paid, counterfeit, oral or singles they are committing criminal offences.

If you suspect a trader is selling illegal tobacco, please use the reporting channels as described below to help us protect our community.

We are continuing our work on illegal tobacco this year and any information our community can give to help us fight this type of crime is appreciated.

Examples of oral tobacco:

The main way to report any issue to Trading Standards in the first instance is via the Citizens Advice Consumer Advice line on **0808 223 1133** or via their **'Chat Service'** or via an **online reporting form –** all found at https://www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/
If you want to anonymously report consumer crime, or a business that you are aware is trading illegally or unfairly to Trading Standards, you can do this via a number of means.

Via the **London Trading Standards online reporting form** found at: http://www.londontradingstandards.org.uk/contact/

You could also report via **Crime Stoppers on 0800 555 111** or via their online reporting tool at: https://crimestoppers-uk.org/ - this may take longer to reach us.

You can also contact Croydon Trading Standards directly at Trading.Standards@croydon.gov.uk but please be aware this will not be anonymous and you will receive an automated message giving you the details of the Consumer Advice Line.

CONSUMER SAFETY ALERT

Small high-powered magnetic products: risk of serious injury or fatality if magnets swallowed.

Swallowing two or more magnets can cause serious internal injuries.

Keep products with small or loose magnets away from young children.

Talk to older children about the dangers associated with putting magnets near or in their mouths or swallowing them.

Signs of magnet ingestion include stomach pain, vomiting, and fever.

Act fast if you suspect your child has swallowed a magnet. Take them to A&E straight away or call 999.

Office for Product Safety & Standards

Child Safety Week 7th – 13th June 2021

Croydon Trading Standards are supporting Child Safety Week 7th – 13th June 2021. This is an annual campaign run by the Child Accident Prevention Trust (CAPT) to raise awareness of the risks of child accidents and how they can be prevented. In 2021 the campaign is raising awareness of the number of children that are seriously burned and scalded each year.

Child Safety Week is back. CAPT's Safety in lockdown downloads and Social Media Posts for 2020 can be downloaded here #childsafetyweek #safetymakessense https://www.cbtrust.org.uk/child-safety-week

Anyone looking after children 24/7 right now deserves all the tea or coffee they can drink. Just remember to put your cuppa down in a safe spot out of reach of little hands that can grab as soon as your back is turned. You'll be winning against hot drink burns.

Breakfast, lunch, dinner, repeat … sound like your life at the moment? When you're exhausted it's easy to get distracted, so use the back rings of the cooker and turn pan handles in. It keeps danger out of reach of little hands that grab.

An easy win to avoid horrendous bath water scalds … get in the habit of putting the cold in first and top up with hot. You'll be saving your child from the risk of falling or climbing into a boiling bath.

Hair straighteners can get as hot as your iron and can still burn 15 mins after they are switched off

Your hot drink can scald a baby 15 minutes after it has been made

With so many appliances and devices on charge, make sure not to overload electricity sockets

What's the quickest route out of your house in a fire? Make sure you and

Awareness of hot drinks around children

A hot drink, even one that's been made for 15 minutes, can seriously scald a baby.

"Scalds from cups of tea and coffee are one of the commonest preventable injuries in crawling babies and toddlers that we see in the Paediatric Emergency Department. Most parents take safety in the home very seriously, for example fitting safety gates. But they do not always realise the danger caused by hot drinks left on dining tables, coffee tables or kitchen work-tops. Children can often reach further than their parents expect, so make sure 'out of reach' really is a safe place." Dr Rachel Jenner, Consultant Paediatrician Emergency Medicine, Royal Manchester Children's Hospital.

Hot drinks and young children don't mix:

- Hot drinks are the number one cause of serious scald injuries among babies and young children
- Parents don't realise how bad the injuries will be until after the event
- Young children are unpredictable, love exploring and reaching out
- They can't be relied on to do what they're told and they're too young to understand consequences

For more accident prevention advice from the Child Accident Prevention Trust go to www.capt.org.uk/safety-in-lockdown

Ticketing scams

As events, concerts, festivals and theatre shows begin to reopen, criminals will be on the look out to take advantage of people booking these events.
Criminals either set up fake websites or social media profiles to sell tickets that are either fraudulent or don't exist. Web sites may even look similar to the genuine organisation's one but subtle changes in the URL can indicate that it's fraudulent. Make sure you book tickets directly through official sellers who are members of the self-regulatory body STAR, as anything else could be a scam.

Always remember:

- Use the secure payment method recommended by reputable online retailers and auction sites.
- Always access the website you're purchasing from by typing it into your web browser and be wary of clicking on links in unsolicited emails or social media posts.
- Criminals are experts at impersonating people and trusted organisations so always make sure to research who you are buying tickets from and be wary of celebrity-endorsements in case it's a scam.

Be suspicious of any "too good to be true" offers or prices and always be wary of any requests to pay by bank transfer when buying tickets online or on social media.

Scams Awareness Fortnight

Croydon Trading Standards are promoting Citizens Advice Scams Awareness campaign. The aim is to create a network of confident, alert consumers who know what to do when they spot a scam.

We all need to be aware of scams all the time.

Protecting people against scams is more important than ever. Many people are facing issues as a result of the coronavirus pandemic - from employment and debt, to housing and health - meaning more people are in vulnerable situations. Scammers are taking advantage of this, so it's vital people have the knowledge and tools they need to protect themselves.

Recognising a scam

Coronavirus - be aware of new scams

It's important you're aware of the many new scams around at the moment because of coronavirus. 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

To find out more go to : https://www.citizensadvice.org.uk/about-us/our-work/our-campaigns/all-our-current-campaigns/scams-awareness-campaign-2021/advice-on-scams/

https://www.citizensadvice.org.uk/about-us/our-work/our-campaigns/all-our-current-campaigns/scams-awareness-campaign-2021/

Pension Fraud

Action Fraud has reported an increase in pension scam reports in the first quarter of 2021 when compared with the same quarter in 2020.

On Tuesday 20th April, Action Fraud launched a national awareness campaign to highlight the importance of people doing their research before making changes to their pension arrangements. Common pension scams include early pension release scams and pension review scams. In pension release scams, investors are often cold called, but contact can also be made via email, post, or from word of mouth. These scams work by investors being told that they can take cash from their pension even though they are under 55. The funds will then be transferred from the legitimate pension scheme into one set up by the scam which may be abroad.

The investor may then be loaned an amount with the company involved taking a fee, the amount of which is often unclear and will not include the tax the investor will have to pay for accessing the pension early. Any money left over will be invested in high risk products or is sometimes stolen.

Pension review scams work by contacting people offering a free pension review via email, text message, a phone call or sometimes from an online advert. Many of the companies offering these pension reviews are not authorised by the Financial Conduct Authority (FCA) but they may claim that they are.

The pension scam review works by trying to persuade you to move money from your pension scheme to a high risk scheme instead where your pension pot is invested in unusual investments which may be badly run or are a scam. Tempting offers to induce you to move your money may be made, such as cash or guaranteed returns.

Advice from the Financial Conduct Authority (FCA) is to report pension cold calls to the Information Commissioner's office (ICO). The Pensions Advisory Service can also offer assistance in advising you if you unsure whether you should report a matter or not.

* *

Garden Landscaping and the Law

With spring arriving, and COVID-19 restrictions beginning to ease, many people will be turning their attention to hard and soft landscaping projects in their gardens. But where large projects are undertaken by traders and these don't go to plan, consumers can sometimes be unsure of the forms of redress available to them.

Garden remodeling projects can contain aspects of supply of goods, provision of services or a combination of the supply of goods and services. Where the issue relates to goods only, such as a piece of garden furniture supplied in isolation, which does not conform to contract, this would be subject to a short term right to reject, allowing customers to seek a full refund.

After 30 days, the consumer's right to redress may be a repair or replacement for which the trader has one opportunity to fix the issue, and if after this process, the matter is still not settled, the consumer may be entitled to a full or partial refund.

Where services are not carried out with reasonable care and skill, and in a reasonable time period, consumers are entitled to a repeat performance at no extra cost. This repeat performance must be carried out in a reasonable time and with no significant inconvenience to the consumer.

Failing this, the consumer may be due a price reduction. Where a contract includes supply of goods such as plants, and services such as design planning, tree removal etc. and problems occur, such that the consumer cannot be put back into a position that they were in prior to the contract starting, then the consumer may be able to treat this as a breach of requirement for services as well as for goods so that they can choose either the route of service remedies or goods remedies.

There is also an ombudsman scheme (this is a voluntary scheme) that may be able to assist consumers and traders to resolve disputes – this is the Furniture and Home Improvement Ombudsman. Their website, www.fhio.org details the type of disputes that they can assist in resolving, via a conciliation approach to dispute resolution.

Croydon Healthy Homes

Home Owner in Croydon?
Gross Household income under £30k?

How about free renewable electricity or improving the thermal comfort of your home?

Don't miss out on up to £10k of government grant funding for

1. Free Solar PV panels or
2. Free Solid Wall Insulation or
3. Free Air Source Heat Pumps

www.warmerhomes.org.uk/lad-programme
or phone 0800 0385737

The grant funding is through government's Green Homes Grant Local Authority Delivery (LAD) funding. Croydon Council was part of a successful consortia bid led by Portsmouth City Council and energy specialists AgilityEco. £5k grant funding available for private sector landlords www.croydon.gov.uk/energyadvice

CROYDON www.croydon.gov.uk | Delivering for Croydon

The Money Advice Service warn of cruel scam

The Money and Advice Service is an organisation set up by the government to improve people's financial capabilities. The service provides free money guidance and debt advice online and by telephone.

The Service has recently issued a warning about scam WhatsApp messages claiming to be sent by them.

The messages received state that following a recent conversation with one of their debt advisers, it is likely that the recipient's application to have some of their debt written off will be approved.

The messages then continue by explaining that in order to have their debt reduced, the recipient must provide them with recent bank statements, payslips, ID and any letters from creditors; so that they can process the application.

This is a scam message and The Money Advice Service has confirmed that they will never send unsolicited WhatsApp messages. Personal details and documents provided in this scam will likely be used to impersonate the victim to set up new credit facilities and take over existing accounts.

Global Health Insurance Card (GHIC) scams

When travelling in the EU, people can access emergency and medical care with a Global Health Insurance Card (GHIC). This card has replaced the European Health Insurance Card (EHIC) however criminals are capitalising on this new card to commit fraud, asking victims for payment details when the GHIC is free. They are advertising these cards on fake websites that look like that of the NHS. The sites claim to either fast-track or manage your application process before charging you an up-front fee.

Always remember:

The GHIC, which replaces the European Health Insurance Card, is FREE to use and can only be obtained directly via the NHS website: https://www.nhs.uk/using-the-nhs/healthcare-abroad/apply-for-a-free-uk-global-health-insurance-card-ghic/

You also don't need to apply for a GHIC until your current EHIC expires.

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**