



# *Information Network Bulletin*

*Edition 4- 2021/22*

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.

## ***MORE ILLICIT TOBACCO SEIZED***

Croydon Council Trading Standards and HM Revenue and Customs teamed up with specialist detection dogs to track down and seize illegal tobacco worth over £175,000 from a storage unit in the borough recently.

Officers recovered 270,600 illegal cigarettes and 14.8 kilograms of hand-rolling tobacco from a storage facility during the joint operation with BWY Canine Ltd on Tuesday 22 February.

Since the end of September, Croydon's Trading Standards officers and HM Revenue and Customs have seized over 660,000 cigarettes and over 375 kilograms of hand-rolling tobacco worth over half a million pounds as part of an ongoing crackdown which is part of Operation CeCe, a national campaign which focuses on joint working between Trading Standards and HM Revenue and Customs.

If you have information about the sale of illegal tobacco in Croydon please report it via the Citizens Advice Consumer Advice line on 0808 223 1133 or email [trading.standards@croydon.gov.uk](mailto:trading.standards@croydon.gov.uk)



CHARITY COMMISSION  
FOR ENGLAND AND WALES

# Please give safely

# [www.gov.uk/checkcharity](http://www.gov.uk/checkcharity)

## Safe giving in support of Ukraine

In times of crisis, such as the situation in Ukraine, many people will be wanting to help in some way. Unfortunately, as we have seen with the COVID-19 pandemic, there will be scammers who will try and take advantage of this situation and of people's generosity, to try and obtain people's money and personal details.

Scammers will usually cold-call on the phone or use text messaging and often take you to fake websites or social media pages. Do not click on links that pop up on a social media feed or download attachments in any unsolicited emails, texts, or social media messages. A common method that scammers use is to get you to inadvertently download malware onto your device or take you to a fake website to steal your money and personal information. Forward any suspected scam emails to [report@phishing.gov.uk](mailto:report@phishing.gov.uk) and then delete it. Be cautious of fundraising pages on platforms that do not check the legitimacy of the fundraiser or that do not promise your money will be safe if the page is found to be fraudulent. Crowdfunding requests can also be used to scam people. You should check the charity's name and registration number at [www.gov.uk/checkcharity](http://www.gov.uk/checkcharity). Most charities with an annual income of £5,000 or more must be registered and you can use the advanced search function to find the charities working in specific regions and countries. You should look out for the Fundraising Badge on charity fundraising materials, this is the logo which shows that a charity has committed to fundraise in line with the Code of Fundraising Practice.



If you think you have been scammed, please contact your bank immediately, and make sure you do your research on the charity before committing your resources to them so you know how your money will be used.

## Post Office Parcel Scam

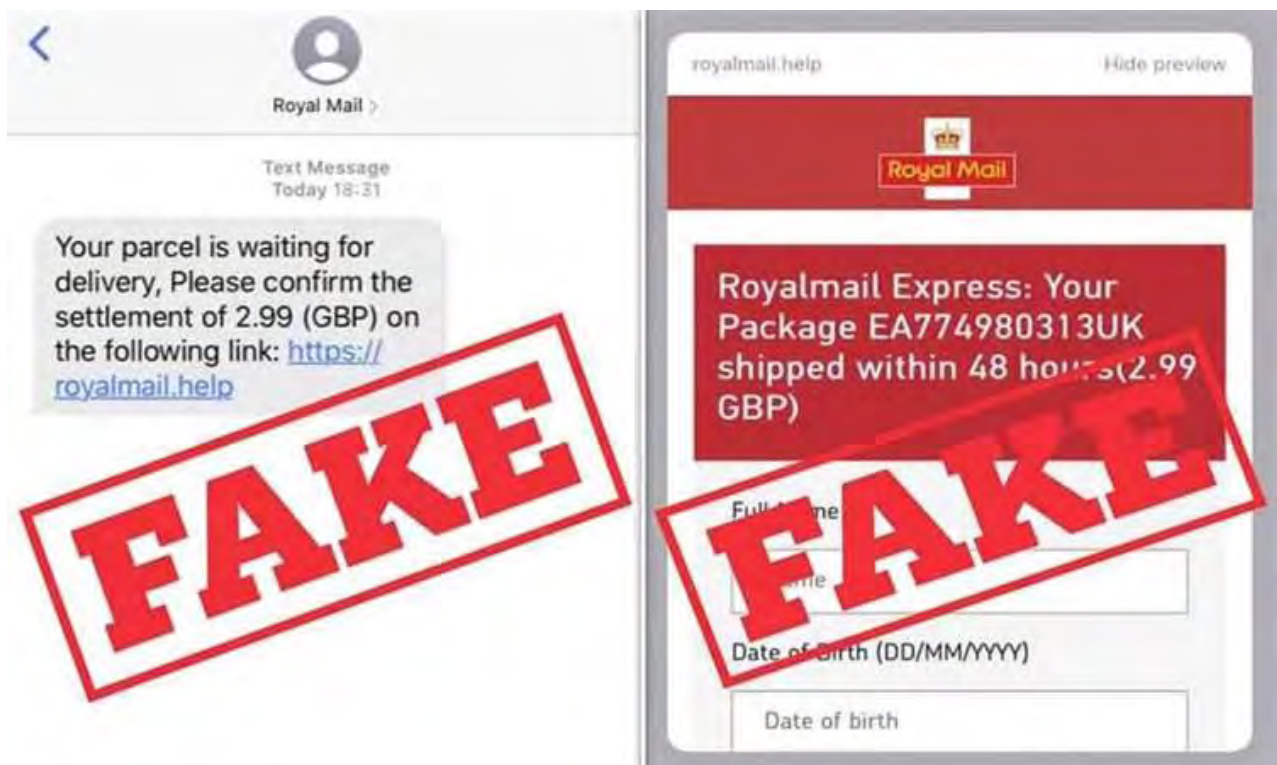
For some time now a variety of fake texts have been sent informing customers that a parcel delivery has failed and requiring them to follow a link to reschedule the delivery. These typically targeted the national parcel delivery firms.

However, a new version impersonating the Post Office uses a clone website which the Post Office warn is extremely convincing.

This new text asks recipients to follow the link in order to 'reschedule delivery', however the URLs take users through to a cloned website. It is important to check the website address as that is how to spot the scam URLs because they don't include the classic postoffice.co.uk domain.

Those unsuspecting consumers who click on the link in the text are taken to an 'extremely convincing' mock Post Office site. They will initially be asked to enter their postcode, before the scammers go on to request details like their full name, delivery address, email address and date of birth.

This vital information will then be relayed back to the scammers who can use it to create a profile with which to commit identity fraud. These fake identities are then used to make purchases, take out loans, hire agreements, etc, with the innocent consumer only discovering what has happened when they receive a demand for payment for something they know nothing about.



## Beware of Rogue Emergency Locksmiths

Please be aware there has been a rise in reports of emergency locksmiths charging excessive fees. This has been acknowledged as a national problem and not just limited to London.

Often when locked out the first thing people do is to Google a locksmith and in panic contact the one at the top of the search list. Unfortunately there are criminals who are preying on people at their most vulnerable moment and they pay for their adverts to be seen first, often hooking people in with seemingly low prices – however these are never what is actually charged.

These traders are criminals, and having completed what is often a relatively quick job, they then charge the victim an excessive amount, way over what was first quoted, effectively holding the keys to the new lock to ransom until it is paid. They bring a mobile payment device with them and people feel intimidated into paying, sometimes up to £300-400 for 10 minutes work and a substandard lock. In some cases they have also caused damage to property as some are not skilled or trained to do the work. They often drill out a lock that could have been dealt with without replacing the whole lock.

Try to ensure the companies or traders are legitimate by finding a locksmith registered with the Master Locksmith Association (MLA). Please head to their website for further information:

<https://www.locksmiths.co.uk/> - use the search feature to find a local registered locksmith

<https://www.locksmiths.co.uk/faq/how-to-spot-rogue-locksmith/> - visit this page for tips on how to avoid a rogue locksmith.

This 'how to spot a rogue locksmith' article lists the Red Flags to be aware of when looking for an emergency locksmith and will help you identify a potential rogue locksmith.

The top Red Flags as described by the MLA are listed below:

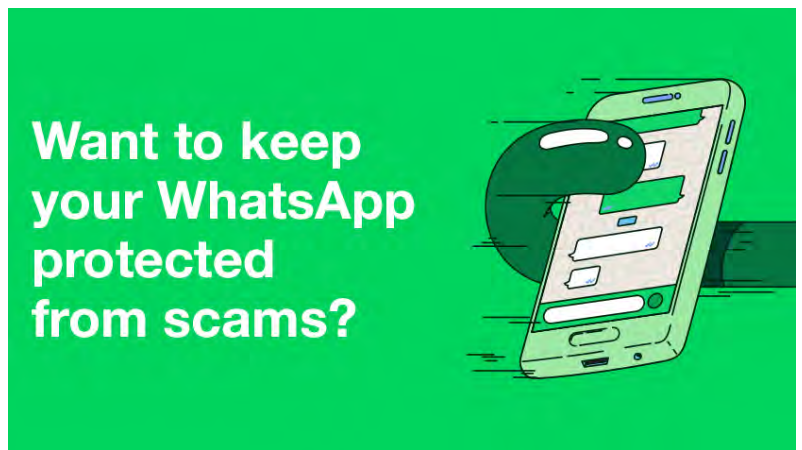
- Paid Google Adverts stating "from £39 / £49 / £59 – these are just prices to reel you in and are not representative of what they will charge.
- Claims of 3<sup>rd</sup> party approval / accreditation / certification
- Claims of Police approval – Police will NOT recommend any trader
- The use of subcontractors
- Being vague about the price
- Attempting to drill a lock immediately – it is usually a last resort for a genuine experienced locksmith.

Please remember to report to Action Fraud 0300 123 2040 if you have actually been the victim of a scam or call Citizens Advice Consumer Helpline 0808 223 1133 if you require advice on an issue you are having with a trader or wish to report a trader.

The image shows a Google search results page for the query 'locksmith'. At the top, there is a search bar with the text 'locksmith' and a search icon. Below the search bar, there are navigation options: 'All', 'Maps', 'Images', 'News', 'Shopping', and 'More'. The search results show 'About 43,100 results (0.48 seconds)'. A privacy reminder banner is visible, with a red flag icon and the text 'From £39 = Red Flag'. Below the banner, there is an advertisement for a locksmith service. The ad text includes 'Local Service From £39 Only' (highlighted with a red box), 'Feefo Gold Trusted Service Award 2018 Winner. No Callout Charge. Call Now! No Call Out Charge. Certified Locksmiths. Arrival within 20 minutes. Local Locksmith Near You.', and two columns of service details: 'Lock change/installation' and 'Reliable and Affordable'.

# WhatsApp launches 'STOP. THINK. CALL.' campaign to stamp out message-based scams

WhatsApp launched its STOP. THINK. CALL, campaign in partnership with the National Trading Standards' Friends Against Scams campaign, in late 2021. The campaign aims to help educate the public on how to protect themselves and their WhatsApp account from message-based scams.



Almost (59%) of the British public say they have received a message-based scam in the last year - or know someone who has. According to recent research, these types of scam messages have been sent both via SMS text message (46%), or WhatsApp (13%), and unfortunately appear to be increasingly common.

WhatsApp, and Friends Against Scams are calling on the British public to STOP. THINK. CALL. before they respond to a suspicious or unusual message.

**STOP:** Take Five before you respond. Make sure your WhatsApp two-step verification is switched on to protect your account; that you're happy with your privacy settings, and your six-digit pin is secure.

**THINK:** Does this request make sense? Are they asking you to share a PIN code which they have had sent to you? Are they asking for money? Remember that scammers prey on people's kindness, trust and willingness to help.

**CALL:** Verify that it really is your friend or family member by calling them directly, or asking them to share a voice note. Only when you're 100% sure the request is from someone you know and trust, should you consider it. If it turns out to be untrue, report it to Action Fraud at <https://www.actionfraud.police.uk/>

Citizens Advice Scams Action is encouraging anyone who is worried about being targeted to visit their site to get help with online scams.

<https://www.citizensadvice.org.uk/consumer/scams/get-help-with-online-scams/>

Friends Against Scams runs free online training sessions to empower people to take a stand against scams, helping identify different types of scams and providing directions on how to report them. The campaign also recruits 'SCAMBassadors', who are MPs, senior officials or someone who will use their influence to raise the profile of scams at a national level.

For more information and resources on how to stay safe online, visit:

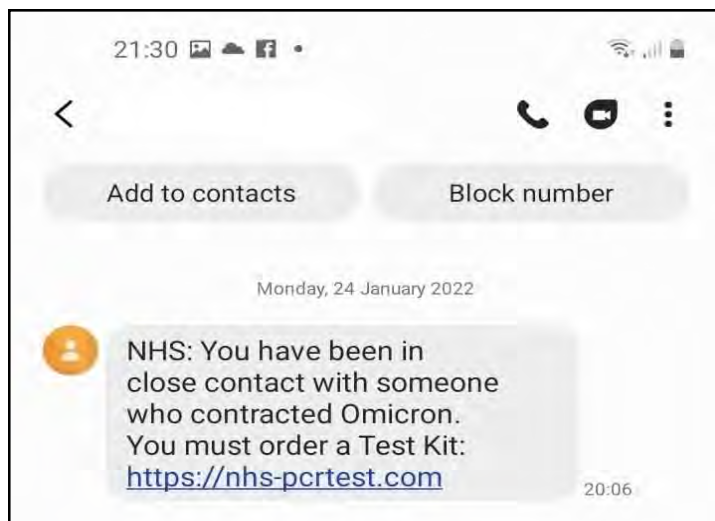
<https://www.friendsagainstscams.org.uk/stophinkcall>

## Scam alert: fake NHS Covid-19 PCR test text

A fake text message purporting to be from the NHS has been circulating, demanding that you 'order a PCR testing kit'. Here's what it says.

"You've been in close contact with someone who has been infected with Omicron Variant. You will need a Test Kit"

The message then directs you to a website to purchase a test kit.



These texts take you through to convincing clones of the NHS site. Following the instructions will eventually lead to a page requesting your bank card details in order to pay a 'delivery fee'.

The NHS would not contact you in this way or ask for your bank details. If you need to get a PCR test, visit the official GOV.UK site at <https://www.gov.uk/get-coronavirus-test>

If you think you may have given sensitive information to fraudsters, let your bank know what's happened immediately.

Many of us have been 'pinged' by the NHS Covid-19 app at some point over the last year, so you might be inclined to believe another communication stating that 'you have been in contact with someone who has COVID-19'.

This is yet another example of fraudsters seeking to panic you into following a URL leading to a fake website, known as 'smishing'.

### Reporting fake texts and websites

While the NHS does contact people via text in some cases, it would only ask you to order a test via the official GOV.UK site (<https://www.gov.uk/get-coronavirus-test>), while contact tracing only takes place in England via <https://contact-tracing.phe.gov.uk/>

You can also report the website in the text to the National Cyber Security Centre via [report@phishing.gov.uk](mailto:report@phishing.gov.uk)

## Energy Advice

Croydon Healthy Homes is Croydon Council's free energy advice service aimed at Croydon residents on low incomes, and those more vulnerable to the effects of living in a cold home (especially families with young children, older residents, and residents with pre-existing medical conditions). Please email [healthyhomes@croydon.gov.uk](mailto:healthyhomes@croydon.gov.uk) to apply for support. In your email, please include:

- your full name
- your full address, including postcode
- a daytime contact phone number
- your housing tenure (whether you are an owner occupier, rent from a private landlord, rent from Croydon Council, or rent from a Housing Association)
- the reasons you are looking for advice from Croydon Healthy Homes

If you are referring someone else please provide the details above for the resident, your contact details, and an explanation of your relationship to the resident you are referring. Please make sure you have their consent before emailing us.

## More Calls From Bogus Police Officers

The past two years have affected most of us in some way and left many in financially difficult positions. Undeterred, heartless scammers continue to seek out those most vulnerable in society, depriving them of what little money they have.

This scam begins with someone calling the victim, pretending to be either from the Government, the police, or similar. Through a series of carefully-planned tricks, these criminals convince the victim that they owe tax and must pay immediately, or that their bank account is about to be frozen because of some allegedly fraudulent activity so they must empty the account or lose the money. The fraudsters stay on the phone to the victim the entire time, to keep up the pressure and not allow the time to pause and reflect on what is going on and the call might not be genuine.

A similar incident was recently reported to Croydon Trading Standards by a person not familiar with the way HMRC and the Police operate.

The resident received a telephone call from a man claiming to be from HMRC, telling her that her national insurance number had been used to send laundered money abroad and that her bank account was about to be frozen. They asked her for the telephone number to a local Police Station so that they could liaise with them over this matter. Terrified, she gave them the number for Croydon Police Station.

Minutes later she received a call from the Croydon Police Station number, from a gentleman who identified himself as a Police officer, giving her his name and badge number. He advised her that they were about to freeze her bank account and advised her to go to a local shop and purchase as many gift cards as she could with the money in her account, as this would be the only way to stop it being frozen in her account.

The man stayed on the phone to her the whole time while she went out and bought ten gift cards each for £100. He then asked her to remove the labels and send him images of the cards. She did as instructed, not realising that as soon as she did the scammers stole the money from the cards that she had just bought.

Not content with the £1,000 that they had just stolen, the 'officer' then quizzed her as to any other money she might have access to. Fortunately, her husband rang her, interrupting the scam call and when she told him what was happening got her to end the call from the officer as it was a scam.

Please remember:

- Nobody from the government, law enforcement or utility company will ever tell you to pay them with cryptocurrency or gift cards.
- If there is a problem involving your bank account, you will not be advised to convert your money into gift cards or crypto currency in order to have access to your money.
- If someone does tell you this, it's a scam, every time.
- Any unexpected tweet, text, email, call, or social media message — particularly from someone you don't know — asking you to pay them in advance for something, including with cryptocurrency or gift cards, is a scam

Anyone who requires fraud support in the UK can visit Action Fraud via <https://www.actionfraud.police.uk/>

## Product Safety

Croydon Council trading standards service has carried out product safety inspections at retail outlets in 2021 and during the first quarter of 2022. These inspections have been carried out at a number of premises throughout the borough and have identified a range of unsafe and non-compliant products that have been removed from sale and destroyed. In some cases, product recalls have had to be initiated due to the nature of the problems identified.

Of recent concern, has been the range and number, of unsafe and non-compliant toys that are being sold to the public. To assist consumers in identifying safe and suitable toys for children please look out or consider the following points prior to making such a purchase:

- toys should either have the CE symbol or have the UKCA mark.
- look for the voluntary British Toy and Hobby Association's (BTHA) 'Lion Mark'.
- buy from traders who have a reputation for selling safe and reliable toys.
- be careful if you buy second hand toys. Only buy second hand toys that are CE/UKCA marked, contain any relevant warnings and instructions and check for any obvious faults.
- make sure toys are suitable for the age of the child. Small children should not be given toys with small parts, or toys where small parts detach as these are a potential choking hazard. Some toys will have a symbol present warning that the product is not suitable for children under 3 years of age.
- avoid toys with sharp edges, points or loose ribbons.
- avoid toys with loose pile fabric or hair which sheds easily – these are a choking hazard. Also avoid toys sold with items of food.
- if toys become damaged over time, and wish to be kept, ensure that the toys are repaired properly so that all hazards are removed such as sharp edges.



### 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](mailto:trading.standards@croydon.gov.uk)

Citizens Advice Consumer Service:

Tel: 0808 223 1133

Web: [www.citizensadvice.org.uk](http://www.citizensadvice.org.uk)