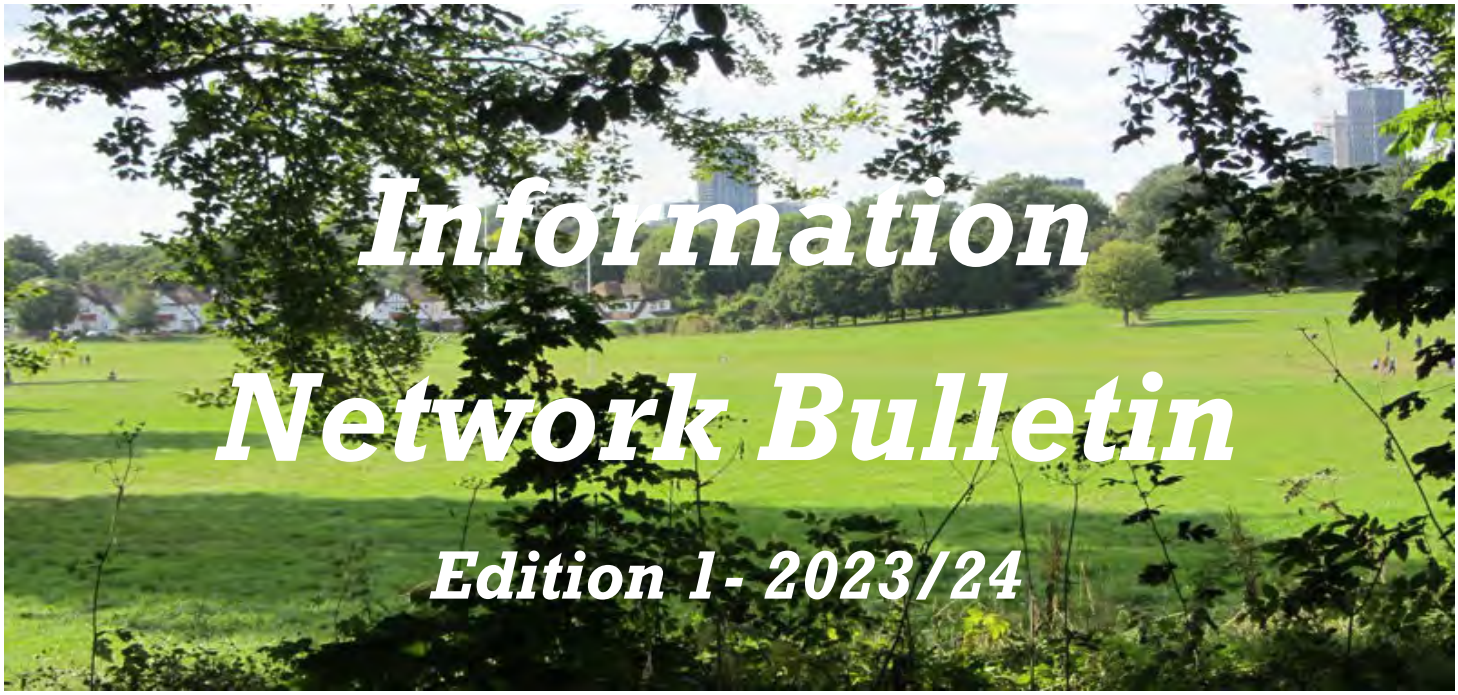

Information Network Bulletin

Edition 1- 2023/24

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.

Fake text messages and emails relating to cost of living and energy

The government is offering help for households but beware of criminals pretending to offer these support schemes.

These scam emails and text messages come in many different forms and promise financial gain. They are often official looking and pretend to be from the government or HMRC.

Examples include:

- fake cost of living related grants
- fake cost of living relief funds
- fake council tax reductions, rebates or refunds
- fake tax rebates from HMRC
- fake offers of assistance to help with universal credit applications

Look out for text messages and emails asking you to click on a link and check the official government website – do you need to apply for the support or is it paid automatically?

Did you know? You can easily report scam text messages and emails for free:

- **Text messages** - forward the text to 7726.
- **Emails** - forward the email to report@phishing.gov.uk.

Households across Great Britain will receive a £400 non-repayable discount off their electricity bills, via the government's Energy Bills Support Scheme. However, there is no need to apply for the scheme. **You will not be contacted by the Government or Ofgem asking you to share your bank details to claim this benefit.**

Find out more about the government support available - www.helpforhouseholds.campaign.gov.uk

Glastonbury Ruined for Croydon Residents

A Croydon resident recently reported having been scammed out of thousands of pounds for Hospitality tickets to Glastonbury.
The resident had purchased theatre tickets from a gentleman advertising his services on social media.
Having successfully purchased tickets for several more events, the gentleman offered Hospitality tickets to Glastonbury.
The package sounded great so the resident, together with some of their family and friends decided that they would purchase tickets and go to Glastonbury as a group. They all transferred their money into the resident's account and on this occasion, the gentleman asked that the payment for the tickets be made to his business account.
That was they last that they saw of their £14,000. The tickets did not arrive and their money was not refunded. Tickets purchased for other events did not arrive either. The gentleman stopped replying to messages and disappeared from social media.
These purchase scams trick online shoppers into thinking they're dealing with a legitimate contact or company when it's actually a scammer. Fraudsters can advertise on social media, genuine selling sites, create fake websites or hack sellers' accounts.

Purchase scams
These scams can happen when you find something online that you want to buy such as a holiday, flights, concert tickets or a games console. Once payment has been made, the seller disappears, leaving you with either no goods at all, or goods that are worth less or are significantly different to those advertised.

Selling scams
These scams can happen when selling items online. You may send the goods as agreed and never receive payment, or you may be tricked into returning an overpayment; for example if the scammer claims to have sent you a cheque for more than the price of the item you sold, they then ask you to transfer the excess payment back to them. The seller then loses the item they sold as they never get paid for it and the 'excess' money that they sent back to the purchaser.

How can you spot these scams?
These fraudsters are very clever and convincing, but there are sometimes warning signs that could help you identify them in the future.
- If an item that is advertised is priced lower than the recommended selling value – does it sound too good to be true?
- If the seller makes contacts you numerous times to push the sale through.
- If the buyer sends you, or claims to have sent you, more money than they needed to pay for the item, asking you to return the difference.
- If a seller you don't know and trust asks you to use 'PayPal Friends & Family' service or to pay for goods by bank transfer.

Social media platforms are frequently used to buy and sell locally, but be wary when buying an item that you can't see in person. The seller may be using a fake profile, or if they have a website, it may not show their own buyer and seller protection information. Buying this way is high risk.

How can you protect yourself?
Even if there are no warning signs, considering the following:
- If buying from a reputable buying website, stick to the advice and processes that they have in place for making the purchase. Never communicate outside the site.
- Avoid paying in cash or by direct money transfer, where you are able to pay with secure payment methods, such as PayPal or your credit card.
- If you're buying a large item such as a car, make sure you see it in person before making any payment.
- Be wary of accepting payment for goods by cheque.
- You should not send personal or financial details by email.

Vishing Phone Scams – New O2 Scam

Cold-call phone scams are becoming ever more sophisticated but there are ways to identify if the caller is a fraud.

The top vishing scams involve callers pretending to be from official organisations or businesses and are trying to get personal information from you or to hack into your accounts.

In the last few weeks there has been a huge increase in scammers targeting O2 customers with calls claiming to be from O2. They may already have some information about you, which will be used to take you through a 'security' process.

You'll receive a text from O2. The text tells you a one-time passcode has been requested and will arrive shortly. This genuine message will have been triggered by the scammer trying to log into your account on the O2 website. Ultimately, the scammer wants to access the account and change your password - potentially enabling them to attempt to take out contracts in your name.

The text message from O2 includes a warning stating 'if someone's calling you and asking for a code, please end the call because they do not work for O2'. While this should arouse your suspicions, the scammer will try to talk you around and claim their request is genuine. You then receive a follow-up text containing the code. If you read it out to the fraudster, they'll be able to use it to get into your account.

This may branch out into other phone providers so please be aware!

Most major communication networks have signed up to the **7726 service**, making it very easy to report scams texts/WhatsApp's or calls to your mobile.

To report a scam call number you just need to copy the number, put it into a text writing 'Call' before you put the number in and send it to 7726.

When you've done this, it alerts your mobile provider to investigate the number and potentially block it from the network, if it's found to be a nuisance.

Please also remember to block the number on your handset.

Scams Employment - Are you being used?

Whether applying for full time work, or a part time role perhaps reflecting age or parental responsibilities, employment websites - such as Indeed and LinkedIn - are very popular. They allow you, from the comfort of your home, to place your CV or personal details on internet job sites, so that potential employers can see them and, hopefully, offer you a job.

However, fraudsters are always lurking – and job scams are more common than you might think. Recent data from Ofcom shows that of 43 million adults who have encountered scams or fraud online, 30% have come across fake employment scams.

These scams may come in two forms – someone purporting to be from the business contacts you to acknowledge your application; or someone claiming to be from a recruitment agent contacts you to say they are considering you for another position.

In the former, the person may tell you that the job you are now being considered for is different to the one you applied for. In the latter, the job you are being offered probably does not exist. In either case, you will be invariably asked to divulge personal information including your bank details. You may be asked to pay initial application fees, with further payments for supposed travel or accommodation related to the promised employment.

So, if you are -

- contacted by someone claiming to be an employer's agent offering you a new job; or
- asked to fill out a questionnaire or to give them personal information about yourself over the phone; or
  asked to give money to them as an administration fee.
  think very carefully as you may become a potential victim of employment fraud.

Further advice can be obtained by emailing: trading.standards@croydon.gov.uk

To report a suspected crime, or if you have fallen victim to fraud or cyber-crime, contact Action Fraud via its website or by calling 0300 123 2040

Beware the lure of Crypto Currency Scams

These are a type of investment scam that fraudsters use to steal money from people hoping to make big returns by investing in digital currencies.

Crypto currency is accessible to everyone, with any budget, so anyone can fall victim to these scams.

How can you protect yourself from scams and fraud?

Crypto currency is not a regulated product, so your dealings are not protected by the Financial Ombudsman Service or the Financial Services Compensation Scheme if things go wrong.

- Even if you use a regulated firm when buying the crypto currency, your protection is limited if things go wrong.
- If you are considering investing, research the company first and consider getting inde pendent advice.
- Don't fall for high pressure sales pitches with limited timescales to invest and promises of too good to be true returns.
- Apparent celebrity endorsements don't mean it is not a scam and avoid offers on social media or via the telephone.
- Never allow anyone to set up a crypto currency wallet, upload your ID documents or manage investments remotely on your behalf.

Use FCA ScamSmart, an online tool to help identify whether your investment is a scam. Answer several questions and get a clear picture of the potential risks.
https://www.fca.org.uk/scamsmart

Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cyber crime in England, Wales and Northern Ireland.

The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB) who are responsible for assessment of the reports and to ensure that your fraud reports reach the right place.
www.actionfraud.police.uk – please take time to visit this website to learn all about the types of frauds and also how to prevent fraud.

The A-Z of Fraud pages explain the many different types of fraud and what to be aware of. The Prevention pages show what you can do to help yourself not fall victim to a fraud or scam. These are really useful resources that can help you navigate safely through the myriad of criminals trying to defraud people.

You can sign up for free to Action Fraud Alert to receive direct, verified, accurate information about scams and fraud in your area by email, recorded voice and text message.

Please go to www.actionfraudalert.co.uk to register.
You can find helpful resources such as leaflets that you may wish to read or use for local community groups at www.actionfraud.police.uk/resources

You can also report a fraud on the website via the reporting tools or call an advisor on 0300 123 2040.

Public embraces email reporting service created after spike in coronavirus-related scams

As part of the Cyber Aware campaign, the NCSC successfully launched its suspicious email reporting service (SERS), resulting dozens of malicious web campaigns shut down in its first day after spike in coronavirus phishing scams.

- More than 80 malicious web campaigns taken down in a day after 5,000 suspicious emails were flagged to new cyber service for investigation within a day of its launch
- The UK's National Cyber Security Centre experts had seen a growth in the use of fake corona-virus-related services in malicious emails tricking people into online harm
- The NCSC, a part of GCHQ, yesterday urged people to flag such campaigns to their new world-leading 'Suspicious Email Reporting Service' while launching Cyber Aware
- Campaign teaches six actionable steps to stay safe online as the country continues to rely more on technology while staying at home to protect the NHS and save lives

Security conscious Britons have been praised after they embraced a service launched yesterday to stop malicious email campaigns with more than 5,000 reports – leading to 83 scams being nullified.

The National Cyber Security Centre (NCSC) launched the pioneering '*Suspicious Email Reporting Service*' on Tuesday 21 April to make it easier than ever to flag suspicious emails – including those claiming to offer services related to coronavirus.

Empowering people to simply forward questionable emails to report@phishing.gov.uk meant that the service had already received 5,151 reports as of 1200 the day after launching.

By forwarding any dubious emails – including those claiming to offer support related to coronavirus – to report@phishing.gov.uk, the NCSC's automated programme will immediately test the validity of the site. Any sites found to be phishing scams will be removed immediately.

The service was launched yesterday alongside the new cross-governmental Cyber Aware campaign, which promotes recommended behaviours to stay as secure as possible online.

The Cyber Aware campaign will be delivered by the NCSC working alongside the Home Office, the Cabinet Office and the Department for Digital, Culture, Media and Sport (DCMS).

This Suspicious Email Reporting Service was co-developed with the City of London Police. As well as taking down malicious sites it will support UK policing by providing live time analysis of reports and identifying new patterns in online offending - helping them stop even more offenders in their tracks.

If people have lost money, they should tell their bank and report it as a crime to Action Fraud, but sending emails to report@phishing.gov.uk will offer an automated service to people who flag what they think to be a suspicious email.

Fake Loans

WARNING!

With costs rising around us, more people will be looking to take out a loan, but if you are looking for a loan, be sure to borrow from a legitimate company and be aware of criminals and their often too-good-to-be-true offers.

These scams offer guaranteed loans that require you to pay an upfront fee for the loan. Once the fee has been paid, you do not hear from the criminals again and the loan is never received.

Did you know? A money lender has to be authorised by the Financial Conduct Authority (FCA) to lend money legally. Those who aren't authorised by the FCA are known as loan sharks:

Check the FCA register - www.fca.org.uk/firms/financial-services-register

FCA FINANCIAL CONDUCT AUTHORITY

Report a loan shark - www.stoploansharks.co.uk

STOP LOAN SHARKS
Intervention . Support . Education

Croydon Trading Standards Need Test Purchasers

Trading Standards work with young people to monitor the sales of age-restricted products across Croydon. Part of this work involves a young person under strictly controlled conditions trying to buy knives, alcohol, fireworks and cigarettes & vapes from shops in the borough. We are looking for volunteers, aged between 14-16 years and 18-24 years to help us carry out test purchasing activities.

To find out more and sign up as a test purchaser contact Croydon Trading Standards by email at: trading.standards@croydon.gov.uk
or call us on 020 8407 1311

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: **0808 223 1133**
Web: **www.citizensadvice.org.uk**

Protect your Mobile Phone from Nuisance and Scam phone calls!

How does trueCall SIM work?

When a call arrives trueCall checks the caller's number. If it is a trusted caller then the phone rings as normal, but if it's an unrecognised caller, trueCall intercepts the call and plays them a message.

For example: "Hello -if you're a friend, family member or invited caller please press '1', if you are a cold caller please hang up and don't call again."

Most telemarketers hang up when they hear this message, and automated and silent calls can't get through. In trading standards trials this method proved to block over 95% of unwanted calls.

If you want to protect a vulnerable person then trueCall can completely block unrecognised callers. For example: "Hello -we only accept calls from friends and family members. If your call is important, please hang up and call Bob on 07752 XXX XXX or enter your code now."

This guarantees that whenever the phone rings it will be a trusted caller, and it allows other legitimate callers to get in touch via the carer, or by entering a code.

Key features

- **Works quietly in the background blocking unwanted calls**
- **No need to change your existing phone -works with smartphones and flip phones**
- **Invisible technology -there are no codes to learn or special buttons to press -the phone just rings less often!**
- **The level of protection can be adjusted to meet your needs**
- **trueCall allows you to monitor the calls received, manage the trusted caller list and adjust settings over the Internet**

Pricing

- **The trueCall SIM service is provided on a SIM card that replaces your existing card:**
- **Unlimited minutes and SMS messages per month to UK landline and mobile numbers**
- **If you already have a mobile phone, your existing phone number can be ported to the SIM card**
- **Service is provided by the EE network**
- **The pricing is set to be just a few pounds more per month than a regular monthly mobile phone contract fee from a reputable operator**
- **This is a rolling monthly contract, so you are not locked in**

Tariff	Monthly fee
Unlimited calls and SMS messages (UK), no data	£18.00
Unlimited calls and SMS messages (UK), 2Gb data	£20.50
Unlimited calls and SMS messages (UK), 4Gb data	£23.00
Unlimited calls and SMS messages (UK), 10Gb data	£31.00

+ one-off £25 activation fee with all options

What do our customers say?

"I feel safe answering my phone now as I know I don't have to worry about the person on the line being a scammer"

"The SIM card has been a great success. No scam calls!"

"I feel very safe with the card installed. It has been very effective"

trueCall Ltd, 2 Castle Yard, Richmond, Surrey TW10 6TF
0800 0 336 339 / SIM@trueCall.co.uk