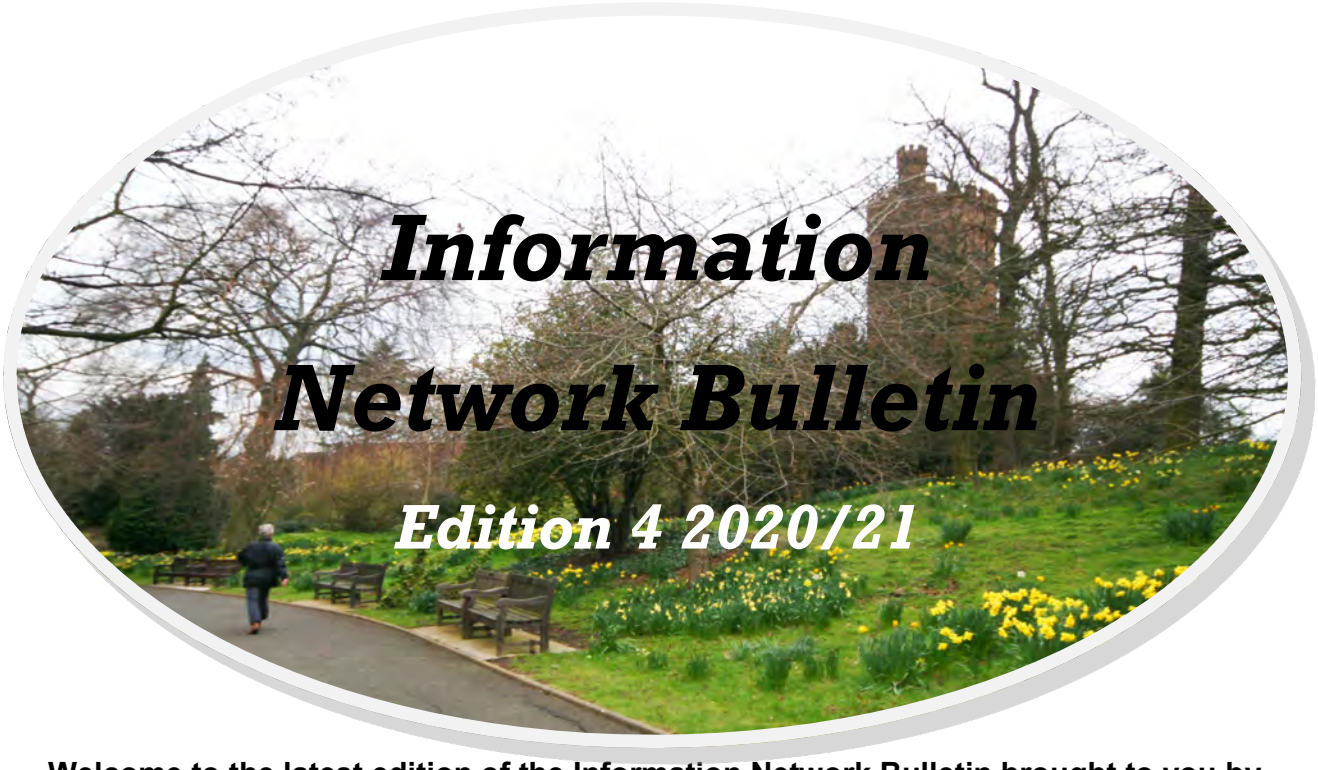


Information Network Bulletin

Edition 4 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.

Contactless Payments

During the COVID-19 pandemic the contactless payment limit was increased from £30 to £45 as the move towards cashless payments continued due to health fears over cash handling.

A recent Government announcement has been that the contactless limit will be further increased to £100 later this year, and the threshold limit will increase from £130 to £300, which is the limit of contactless payments which will then trigger the customer to have input their pin number.

Contactless payments work by using technology called Near Field Communication (NFC). A customer's card has a wireless chip containing the payment details and this can communicate by radio waves with a card reader when the card is waved near the reader. While this technology undoubtedly makes paying for goods and services faster and easier, there are risks to using this payment method. These include the NFC chip being wiped remotely either by error or maliciously, or having your financial information stolen or your card cloned, by the wireless signal being intercepted by fraudsters, although how much of a problem this is still unknown.

You can take steps to protect your contactless card by purchasing special sleeves or wallets so that they cannot be intercepted by fraudsters. These wallets are lined with aluminium which prevent the contactless card communicating with any card reader used by fraudsters. You should also check bank statements regularly and make sure you know the terms and conditions for the use of the card so you know who is liable in the event that an incorrect payment or security breach takes place.

It is also important to know that the majority of contactless card fraud takes place by fraudsters stealing or obtaining a customer's card either by pickpocketing or distraction techniques or if the card is lost.

Cryptocurrency Fraud

Action Fraud are **warning the public to be vigilant of unsolicited emails promoting cryptocurrency (Bitcoin) investment opportunities.**
They received over 750 reports during a single week in February 2021 about Bitcoin-related phishing emails that use fake celebrity endorsements to try and lure victims into investment scams. The links in the emails lead to fraudulent websites that are designed to steal your money, as well as personal and financial information.

How you can protect yourself:

Investment opportunities: Don't be rushed into making an investment. Remember, legitimate organisations will never pressure you into making a transaction on the spot.

Seek advice first: Speak with a trusted friend or family members, and seek independent professional advice before making significant financial decisions.

FCA register: Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money.

For more information about how to invest safely, please visit: https://www.fca.org.uk/scamsmart

Report suspicious emails: If you have received an email which you're not quite sure about, you can report it to the Suspicious Email Reporting Service by forwarding the email to - report@phishing.gov.uk
For more information about how to invest safely, please visit:

https://www.actionfraud.police.uk/a-z-of-fraud/cryptocurrency

Green Homes Grant Scheme

"Home owners and residential landlords who are considering applying for grants to make their homes more energy efficient are advised to be careful when dealing with businesses offering to do work under the Government's Green Home Grants Scheme. Under the scheme, home owners and residential landlords may apply for a grant of up to £10,000 towards the cost, for example, of insulating their home to reduce energy use or installing low-carbon heating to lower the amount of carbon dioxide the property produces. Full details of the scheme can be found at

https://www.gov.uk/guidance/apply-for-the-green-homes-grant-scheme

If the application is successful, a voucher for payment can be obtained to give to your chosen trader who must be a certified installer. However, Trading Standards are aware of issues not only with unscrupulous traders but employees of properly certified installers who are making false claims. Some home owners are being told that they can get the work done and then apply for a grant which will pay for the work done. What must happen is that a quote should first be obtained from a Trustmark registered person, an application made to the Scheme which - if successful - will issue a voucher which can then be redeemed when you are happy that the work has been done.

Dating Scams and Romance Fraud

In 2020, there were nearly 7,000 reports of so-called romance fraud. It cost victims almost £70m last year. And according to trade association UK Finance, there has been a 20% increase in bank transfers relating to romance fraud during the pandemic.

Dating or meeting new people online is very common place but amongst the genuine profiles there are many fraudulent profiles. The people behind them are not after love or company, they are after money. Due to the 'meeting' being online and rarely in person the fraudsters are able to disguise their real Identity and the true nature of their character.

Criminals build relationships very quickly and ask communication to move off the dating app so that the communication cannot be monitored. They use a range of excuses as to why you cannot meet in person such as they have a family emergency, they are stuck overseas, they have an issue with their business and quite quickly resort to asking for money to help them; relying on the emotional attachment they have formed with their victim. They often ask a lot of personal questions about you to build up a relationship but do not tell you much about themselves.

They often use very flattering pictures of someone else. One thing you can do is to check the photos by doing a reveres image search via Google Images, TinEye or other similar services. You may even find the images in use on other profiles or other websites.

How to protect yourself

- Keep all communication within the app or website. Say that you want to keep talking there – there is no reason not to. If they keep insisting on moving the communication to email or phone ask then ask yourself why?
- Check out the images they are using – can you find them elsewhere?
- Carry out research on them – are they on other social media?
- Can you confirm anything they have told you independently; like where they work, where they live? Often they keep details vague so make sure you ask questions you can verify.
- Ask yourself why they are so quick to declare their love or feelings for someone they have not met?
- Never send any money to anyone you have not met or agree to transfer money on their behalf.

Money lost to fraudsters is very hard to trace and get back. People often find themselves so ashamed at realising they have been scammed they do not want to tell anyone or report the fact they have been a victim of a romance fraud. If you have engaged in an online relationship, please ensure you talk to other people about this; friends, family, neighbours. After all, if it was genuine there would be no issue in doing so. They may spot clues something is not right that you have not seen due to being involved with the person.

For more information, please visit:
https://www.actionfraud.police.uk/a-z-of-fraud/romance-scams

Are your blinds safe?

Blind safety checklist

2021

Changes to standards for blinds in 2014 have led to improved product safety. New blinds with looped cords must have child safety devices installed at the point of manufacture or sold with the blind. However, blinds installed earlier may not have these features and millions of households could be affected. Our advice will help you make your home safer for your children and young visitors.

✔ Fit a tidy, tensioner or a cleat

Tidies and tensioners should be firmly fixed to an adjoining surface so that the cord or chain are permanently held tight. Cleats should be positioned out of children's reach on an adjacent surface, at least 1.5 metres from the floor. Cords should be fastened up in a figure of eight after every use of the blind, making sure all the spare cord is secured on the cleat.

✔ Move furniture away from windows

Children love to climb, so keep furniture clear of windows blinds. This includes cots, beds, highchairs and playpens.

For more advice, go to:
www.rospa.com/blindcords | www.capt.org.uk/blind-cords
www.tradingstandards.uk/campaigns | www.makeitsafe.org.uk

Over the next few weeks and months many people will be planning for holiday trips abroad. But for the unwary, fraudsters can cause huge financial losses and distress and inconvenience to consumers by advertising villas, flights and holidays that don't exist. Fraud can occur from

-paying for a fake ticket or for a ticket that never arrives

- fake websites and emails offering holidays that do not exist. The consumer pays a deposit and this money is never recovered

To prevent becoming a victim of travel fraud, be careful to research the travel/holiday company online.

You can look for online reviews, and check to see if they are a member of a recognised travel scheme which offers financial protection and a complaints service if things go wrong.

Take out adequate travel insurance ahead of the trip, and be careful when making any payment. Ensure that the payment link is secure by looking for a padlock symbol on the browser window frame when you attempt to log in or register. This symbol should not be on the page itself. Also make sure that the page starts with 'https://'. The 's' stands for 'secure'. This of course doesn't mean that the website you have visited is genuine – carefully check the wording of the website address for any spelling mistakes or unusual characters that don't look right. It's important to highlight, that when making payments you should use a secure payment site.

You should not use PayPal Friends and Family as this will not provide you any protection as using PayPal may otherwise do. You may be asked to pay via PayPal Friends and Family so that the seller doesn't have to pay PayPal charges. If you are thinking of renting a villa or apartment try and deal with the owner or agent directly. You can check review sites to see the feedback of other guests, and remember to obtain the full address of the property so that you can find it on Google maps to check its location and legitimacy.

Before making any payment, make sure that you have a contract setting out the terms and conditions for your holiday. Look for ABTA and ATOL protection – ATOL protection will be of use if you become stranded abroad if your travel business collapses. ATOL is a UK financial protection scheme and it protects most air package holidays sold by travel businesses that are licensed in the UK. You can check businesses which hold ATOLs or are members of an ATOL accredited body at the following address:
https://siteapps.caa.co.uk/check-an-atol/

You can check ATOL holders with the largest number of passengers on their licence at the following address:
https://siteapps.caa.co.uk/atol-reports/.

Each unique licence number is four to five digits long and may include a T at the start. Be aware that some websites fraudulently display ATOL logos to try and dupe consumers into having confidence in their website. Full details of the ATOL scheme can be viewed on the Civil Aviation Authority's website – its address is https://www.caa.co.uk/home/.

New Twist on Bank Account Scam

We recently received a report from a resident whose bank account had been cleaned out by scammers.

Our resident had received a telephone call from a gentleman claiming to be from her bank's Fraud Team. He seemed to already have a lot of her personal details and checked with her that these were correct, they all were.

He then got her to check that the number he was calling her from, that was displayed on her phone, was the same as the telephone number for the bank that was shown on the back of her bank card, it was. He also asked her to check some other details and when the call dropped, she rang the number back and heard the banks usual recorded message before the call was answered, so she was convinced that the call was genuine.

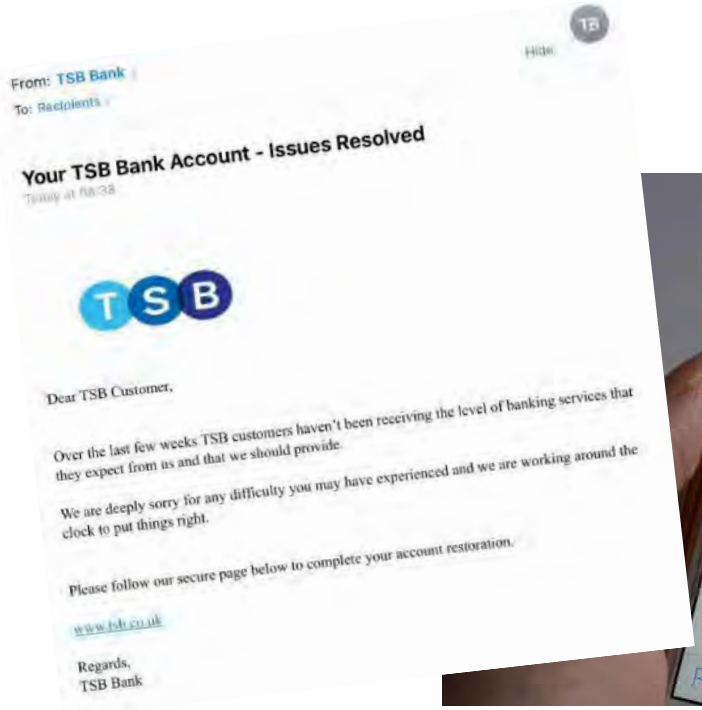
The caller advised the resident that there had been fraudulent transactions made on her account and that to protect her money they had created a new account for her to transfer her money into to keep it safe. They gave her the details of the new account and she transferred all her savings into it.

As they were talking, the call dropped out again. When the gentleman didn't call her back, she rang her bank using the number on the back of her card and explained what had happened, giving the new account details, etc.

It was then that our resident was advised that she had been scammed. The call hadn't been from the bank's fraud team and the new account that she had just transferred all her savings into was with a totally different bank. She was devastated.

Remember:

- Even with the COVID restrictions banks will not ask you to give your details over the telephone
- Nor will they ask you to make transfers or money withdrawals over the telephone
- If you receive a call from someone who says that there is a problem with your account, do not give them any of your details
- Go to your bank and speak directly with someone there, so that you know who you are dealing with
- If there is a problem they will be able to sort it out or contact their fraud team
- If there is no problem, then it was a scam and you will have been saved from losing all your money


From: TSB Bank

To: Recipients

Your TSB Bank Account - Issues Resolved

Dear TSB Customer,

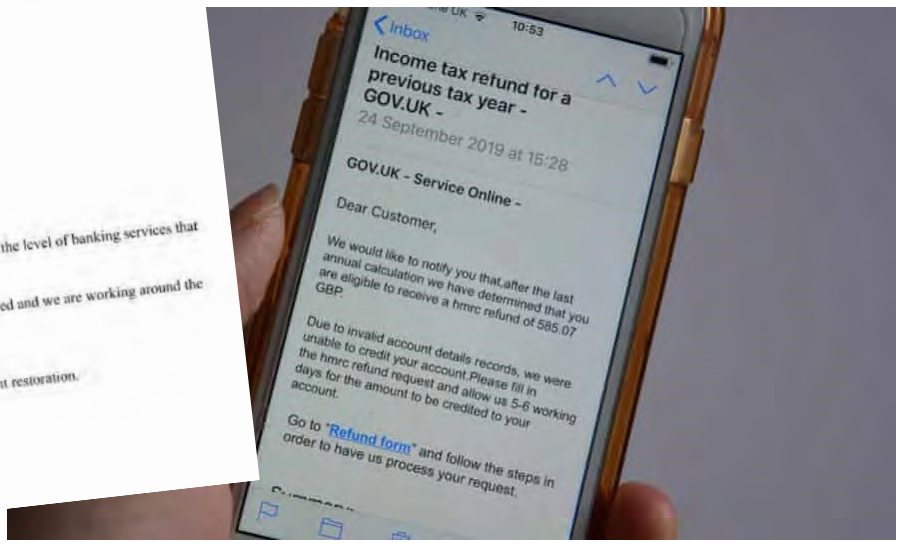
Over the last few weeks TSB customers haven't been receiving the level of banking services that they expect from us and that we should provide.

We are deeply sorry for any difficulty you may have experienced and we are working around the clock to put things right.

Please follow our secure page below to complete your account restoration.

www.tsb.co.uk

Regards,
TSB Bank



Button Batteries

The dangers of button batteries

We rely on button batteries to power everyday objects like car key fobs, remotes and children's toys.

Did you know that they can badly injure or even kill a child if they are swallowed and get stuck in the throat?

This is because the button battery reacts with saliva to create caustic soda – the chemical used to unblock drains. This can burn a hole in the throat and cause internal bleeding or even death. Larger lithium 'coin cell' batteries are the most dangerous.

It sounds scary, but there are simple ways to keep your child out of danger.

If your child swallows a button battery

Symptoms may not be obvious. Your child might be coughing, gagging or drooling, or pointing to their throat or tummy. Unclear symptoms mean it's important to be vigilant.

If you think your child has swallowed a battery, take them straight to the nearest A&E department or call 999 for an ambulance.

Do:

- take the battery packaging, toy or gadget – if you can – to help staff identify the battery
- trust your instincts and act fast, even if there are no symptoms

Don't:

- let your child eat or drink
- make your child be sick

How to stay safe

Store spare batteries securely

Store spare button batteries securely and out of children's reach. Don't leave them loose in drawers or on surfaces. Watch out when opening multi packs of button batteries incase they fall on the floor.

Know which toys and gadgets use button batteries

This includes everyday toys and gadgets, such as: robot bug or fish toys, fidget spinners with LED lights, slim remote controls, car key fobs, calculators, scales, gaming headsets, watches, hearing aids, nightlights and novelty items like singing santas.

Check your home

Have a look around your home, if you find things powered by button batteries where the battery compartment isn't secured by a screw, move them out of reach of small children. If it's faulty, get it fixed or get rid of it safely. You can also report faulty toys to your local Trading Standards.

Teach older children the dangers

Teach older children why button batteries are dangerous and why they shouldn't give them to young children.

Get rid of dead button batteries immediately

Children often find discarded button batteries lying around or under sofa cushions. 'Dead' button batteries can still have enough power to badly hurt a small child. When you remove one, store it securely and recycle it properly promptly.

Look out for fake Seresto dog and cat collars

Vets urged to help identify and report counterfeits

Bayer is making vets aware of a growing problem with counterfeit Seresto flea and tick collars. The company has released a video to help vets and consumers identify the illegal products.

The Seresto collar promises to protect pets from fleas and ticks for up to eight months, but Bayer says it has become a prime target for fraudsters. Fake products don't provide flea protection and could be harmful to the animal.

The company has launched a campaign to educate pet owners on where to buy the product safely. It says vets can play a key role in helping to stamp out the illegal products, by identifying and reporting the fake collars when they come across them in consultation with pet owners.

Tips to avoid buying fake Seresto products

- **Only buy from reputable retails**
- **Avoid buying from private sellers from online platforms**
- **UK Bayer address should be on the tin if bought in UK**
- **The whole front of the tin is completely printed and has Seresto logo embossed on the tin**
- **Real product have lot number and expiry date on tin and matching lot number on the collar itself**
- **The Bayer logo is stamped into the collar**
- **The collar has a ridge marker along the length of the collar**
- **Product has a safety data sheet inside the tin**
- **Fake product smells of Lemon or chemicals. The genuine product has not ordour.**

Find out more by watching the Bayer video to help vets and consumers identify fake collars:
https://mrcvs.co.uk/en/news-story.php?id=18659

HMRC tax fraud scam sees Britons threatened with arrest – key warning sign to look out for

HMRC scam phone calls are unfortunately circulating in a dangerous scam, where Britons are told they have undertaken tax fraud, and could be arrested if they fail to "press one".

HMRC, or HM Revenue and Customs, is a familiar name amongst millions of people who are required to deal with taxes each year. Due to the widespread use of the official service, the latest scam associated with HMRC has the potential to affect many, and is therefore particularly worrying. Several Britons have reported receiving a phone call which informs them there is supposed tax fraud associated with their name.

Individuals are then directed to 'press one' on their phone to speak to an adviser about the situation. If they fail to do so, the automated voice states, they may face a warrant for their immediate arrest.

Understandably, the prospect of criminal charges such as fraud is likely to be particularly frightening for Britons who come into contact with this call. However, the correspondence is simply a scam, designed to get people to part with their personal details.

When pressing one, it is likely people will be asked to hand over sensitive details, or even part with money in order to settle the supposed fraud against their name. This information can then be harvested by unscrupulous scammers who could go on to use the details to commit identity fraud.

The issue has become so severe in recent days that Cifas, a fraud prevention service in the UK, has also issued an alert to Britons about HMRC scams currently taking place. The organisation has warned about calls, emails and texts purporting to be from HMRC stating someone is due a tax refund or owes tax.

As HMRC outlines, suspicious emails can be forwarded to the Revenue for further investigation, and texts sent to 60599.

Latest courier fraud reports:

Victims have reported a particular tactic of being called by someone impersonating a police officer. The suspect uses the name Eric Shaw and gives over his badge number, in order to appear trustworthy to victims.
The suspect asks victims to move money to a “secure bank account” until the victims are sent a new national insurance number. In reality, their money is being transferred into an account under the criminal’s control.

What is courier fraud?

Courier fraud is when victims receive a phone call from a criminal, pretending to be a police officer or bank official. Typically, victims are told to withdraw a sum of money and someone is sent to their home address to collect it. Criminals may also convince the victim to transfer money to a ‘secure’ bank account, hand over their bank cards, or high value items, such as jewellery, watches and gold (coins or bullion).

How to protect yourself and your loved ones:

- Your bank or the police will never call you to ask you to verify your personal details or PIN by phone, or offer to pick up your bank card by courier. Hang up immediately if you receive a call like this.
- If you need to contact your bank back to check the call was legitimate, wait five minutes; fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to contact your bank.
- Your debit or credit card is yours: don’t let a stranger take it from you. You should only ever have to hand it over at your bank. If it’s cancelled or expired, you should destroy it yourself.

Spot the tell-tale signs:

- Someone claiming to be from your bank or local police force calls you to tell you about fraudulent activity, but is asking you for personal information, or even your PIN, to verify who you are.
- They’re offering to call you back so you can be sure they’re genuine, but when you try to return the call, there’s no dial tone.

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**