THE LONDON BOROUGH
www.bromley.gov.uk

TRADING STANDARDS ALERT!

Newsletter

Alert 2.0
2nd June 2021

Welcome to TS Alert! Newsletter. Since we launched the Alert! in February this year we have issued 8 specific Alerts! to warn readers about emerging scams including romance, Covid vaccines, Royal Mail delivery texts and Census 2021. These scams are still very much in circulation and the scammers continue to target residents with their plausible and sophisticated methods.

In this newsletter we're highlighting scams relating to gardening work, social media, insulation, text messages, gift cards and holidays.

But first, the news that The London Borough of Bromley is now a Friends Against Scams Organisation.

Friends Against Scams is a National Trading Standards Scams Team initiative which aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams. More information can be found on the Friends Against Scams website

Bromley's trading standards team have pledged to:
raise awareness of scams within the Bromley workforce to benefit our clients and residents & continue raise awareness of scams with Bromley residents, community groups and partner organisations.

Councillor Angela Page has signed up as a SCAMbassador and has pledged to raise the profile of scams in her new role as Portfolio holder for Public Protection.

If you would like to receive Trading Standards Alert! direct to your inbox please visit www.bromley.gov.uk/scams and complete the online form.

Doorstep scams - Gardening:

With the weather improving be wary of 'tradesmen' knocking on your door or delivering flyers/leaflets offering to carry out work on your garden, particularly your trees, hedges and bushes.

Such work often comes with the risk of poor workmanship, being overpriced and not being completed. Substantial amounts of money are often requested up front and agreed amounts are increased throughout the works including additional amounts for rubbish removal.

Always do your research, preferably get recommendations and obtain 3 quotes **before** having any work done on your property. Don't be rushed!

More information can be found at www.bromley.gov.uk/scams

If you or someone you know has been or is likely to be tricked into handing over money for unnecessary property repairs or garden work, then call the Rapid Response team on 07903 852090. In appropriate cases, officers from the team will attend and investigate.

This Rapid Response Service is for Bromley residents only; if you live outside the borough, please contact your local Trading Standards Department through your local council.

Social Media scams:

Social media scams are cleverly designed to ***appear*** as genuine friend requests, competitions, quizzes, promotions or money-off vouchers and often include a link to enter your personal details.

Clicking on these links can send your personal information to third parties and may trigger the share feature, automatically sharing the 'too good to miss' opportunity with your contacts which could make your family and friends more likely to fall for the scam if the endorsement comes from someone they know and trust.

Which? have top tips for spotting a Social Media scam which you can view on their website

It's important to ensure that your personal information remains confidential on social media and Get Safe Online guides you to advice provided by the social media platforms on how to manage the security and privacy settings on your accounts https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

Loft insulation scams:

Residents have reported being cold called and told that the foam insulation installed in their loft was causing problems and would need to be removed. The bogus caller stated he was 'authorised to check the installation' and said he suspected that there might be dangerous chemicals or damp/condensation issues.

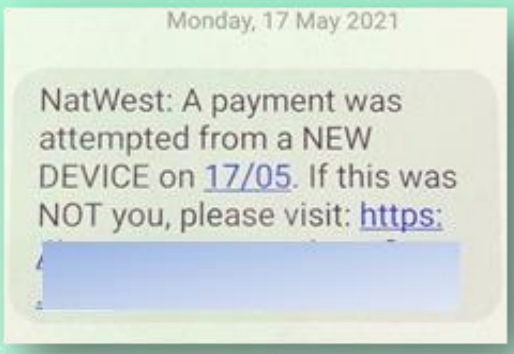
The caller pressured the concerned residents into booking a survey, which was later cancelled by a family member.

If you are contacted 'out of the blue' - Hang Up immediately and make some enquires yourself if you are concerned.

Text scams, like most other scams, are variations on a theme, with a common aim to gain your personal details, your money and possibly download malware (a virus) onto your devices. Here are some of those currently circulating:

Banks

Messages purporting to be from HSBC bank – both recently received by *Bromley's trading standards officers!*



Census 2021

These scam texts threaten the recipient with a £1000 fine for not completing the Census or filling it in incorrectly.

The ONS have confirmed that you will NEVER be contacted by text in relation to the Census and you will never be issued with a fine by text, phone call, email or social media.

Covid-19

Some text messages (and phone calls) claim to be from the Government, your GP surgery, the NHS or the World Health Organisation.

They might be to offer a test for the virus, a vaccine or inform you that you have been in contact with someone who has tested positive for the virus.

Ofcom have more information here

Pay Pal text scam

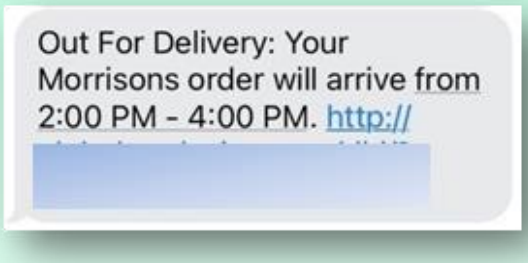
Text messages are being sent claiming to be from PayPal informing the recipient that someone has logged into their account.

Check by logging into your account with PayPal – not via a link provided in the text message.

Supermarket delivery

Fake text messages stating 'your supermarket order is out for delivery' with a link to a bogus webpage to 'track your order and view your delivery note'.

This is similar to the Royal Mail, DPD and Hermes delivery scam text messages



We are proud to be supporting Friends Against Scams - make sure you are scam aware, by completing the online awareness session at www.FriendsAgainstScams.org.uk/elearning/bromley

Gift card scams

Residents have reported being asked to pay with **gift cards** for overdue tax bills and to 'help a friend in need'. Others have been asked by scammers to pay utility bills or debts.

Victims have been told to purchase gift cards, e.g. iTunes or GooglePlay from local convenience or electrical stores or supermarkets and read the 16-digit code on the back of the card to the fraudster.

The fraudster then sells the codes on or purchases high-value products, at the expense of the victim.

Many are unaware of how gift card schemes work i.e. you purchase goods or services from the business issuing the card usually via their website.

Reputable organisations would never ask for payment by gift card or vouchers.

If you are contacted and asked to pay by gift card – **Hang Up** immediately. Contact the organisation via a trusted number or phone and speak with your 'friend in need'.

Holiday scams

With travel restrictions easing many are keen to take a break, both in the UK and abroad.

Before making any bookings make sure you do lots of research into your accommodation, the package or flights to ensure it's genuine.

Criminals often set up fake websites offering 'cheap travel deals' which are used to obtain your money and personal information. Websites may look like that of genuine organisations but subtle changes in the URL (website address) can indicate that it's fraudulent.

Always make payments within the organisations website system and avoid paying by bank transfer.

Check here for advice on spotting and preventing a holiday scam by Take Five - Stop Fraud

If you are booking event tickets you are also advised to make checks, buy tickets from the venue's box office, official promoter or agent, or a well-known and reputable ticket site. Action Fraud has more info here

Top 10 Tips to share

- Hang up – do not have conversation with anyone you don't know or trust
- Don't click on links or open attachments – in emails or in text messages
- Don't ring back a number provided to you in a message or text – select one from previous letters or from the organisation's website
- Be wary even if you think you recognise the number calling – scammers can make their number look like a genuine number – 'spoofing'
- Don't allow anyone remote access to your computer, phone or iPad
- Check who is at the door before opening if possible & don't do business on the doorstep – as family or friends for recommendations
- Don't reply to postal 'wins' e.g. prize draws/lotteries, or clairvoyants or buy 'health' supplements/products from catalogues received in the post
- Be wary if anyone asks for payment by Gift cards (e.g. Amazon, Google Play) or money transfer e.g. Western Union
- Do your research – websites, reviews, organisations like Financial Conduct Authority (see below)
- Keep personal and financial information private - Don't give out passwords or PINs to ANYONE (including your bank or the Police)

Suspicious text messages: forward to your service provider on **7726.**

You'll then receive an automated reply message asking you to enter the phone number from which the spam/scam text was sent and press send.

This free-of-charge short code enables your provider to investigate the origin of the text and take action, if found to be malicious.

Suspicious emails: report to the Suspicious Email Reporting Service by forwarding the email to - report@phishing.gov.uk

Other useful resources:

The Met Police have some useful short videos and booklets on many different scams including phone scams. You can view them here www.Met.police.uk/littlemedia

If you have shared any personal data, contact the ICO (Information Commissioners Office) www.ico.org.uk to understand what another person or company can do with these details.

CIFAS are an agency that deal with Fraud Prevention. If your details have been shared or compromised, they may be able to assist in stopping any further fraudulent action or credit taken out in your name. You can find details for them here: www.cifas.org.uk

If you think you have been involved in a scam, provided your personal or financial information, or allowed someone access to your computer:

- **Contact your bank as soon as possible, especially if you have lost money or given your bank details.**
- Tell someone you trust so they can help you to get the help you need
- Call Citizens Advice if you need advice and guidance **0808 223 1133**
- Report to Action Fraud on 0300 123 2040 or www.actionfraud.police.uk
- Consider changing your passwords and having your devices checked by a professional if you think the scammer may have had access to your computer, mobile phone, tablet etc.

Please share with family, friends, neighbours, colleagues & clients

Read it. Share it. Prevent it

REPORT

Protect others by reporting incidents.

If you or anyone you know have been affected by fraud or any scam report it to Action Fraud by calling 0300 123 2040 or visiting www.actionfraud.police.uk

If you have given out your bank details, contact your bank as soon as possible.

You can also visit www.Bromley.gov.uk/scams