THE LONDON BOROUGH
www.bromley.gov.uk

# TRADING STANDARDS ALERT!

# Phone scams

Alert 1.8

29 April 2021

Bromley Trading Standards have received a number of reports of **telephone scams** affecting Bromley residents.

As a result of these phone calls people, including some of the most vulnerable in our community, have lost money and suffered considerable upset and worry, having been targeted by scammers.

Some scam phone calls are automated with a recorded message, which usually requests you 'Press 1' to speak with an agent or team member, whilst others are made by a professional sounding caller, who appears to know some of your personal details.

If you are not expecting the call from the organisation they claim to be from and are not *absolutely sure* who is calling you, **HANG UP straight away.**

## How you can protect yourself:

**Don't reveal your personal details –** Never give out personal or financial information over the phone, even if the caller claims to be from your bank or the Police. This includes your bank account details, your PIN, your date of birth, your email address or your mother's maiden name.

**Hang up –** If you feel harassed or intimidated, or if the caller talks over you without giving you a chance to speak, end the call. It may feel rude to hang up on someone, but you have the right not to be pressurised into anything.

**Ring the organisation –** If you're unsure whether the caller is genuine, you can always ring the company or bank they claim to be from. Make sure you find the number yourself, perhaps from a previous statement or letter and don't use the one provided by the caller.

**Don't be rushed –** Scammers could try to rush you into providing your personal details. They may say they have time-limited offer or claim your bank account is at risk if you don't give them the information they need right away.

## Phone scams – landline or mobile:

### Bank scams:

Someone calling claiming to be from *your* bank, telling you that there is a problem with your bank card or account. The caller will often sound professional and try to convince you that your card has been cloned (copied) or that your money is at risk.

They may ask for your account and card details, your PIN number and could offer to send a courier to collect your card. They could suggest that you transfer your money to a 'safe' account to protect it.

Your bank would NOT ask you to do this – it's a scam.

### Computer repair or internet speed scams:

The caller may say they are from a well-known organisation for example Microsoft, BT or Virgin Media.

They say that there are problems with your computer or your internet connection and offer to repair it, (likely for a fee).

They could say they need access to your computer or other device and ask you to download software, which could be spyware and may be used to get your personal details stored on your computer.

Legitimate companies would not contact their customers this way

### Amazon scam:

Usually a recorded message stating that you have been charged for an Amazon Prime subscription.

To cancel the subscription you are asked to 'press 1' - if you do so , you will be put through to a scammer who will request personal information and may ask you to download software onto your computer to facilitate your refund.

Amazon will never ask for personal information or remote access to your computer or other device. You can read more from Amazon here

### National Insurance number scam:

A recorded message claiming that the persons National Insurance number will be terminated or has been compromised.

Find out more on the Action Fraud website

Don't be tempted to press 1 or call them back if they leave a number in the message.

### HMRC scams:

Usually a recorded message, the speaker will tell you that there is an issue with an unpaid tax bill or that you could be due a refund. You are asked to press a number to speak with an agent. The calls can be threatening and worrying.

Don't be tempted to press 1 or call them back if they leave a number in the message. HMRC would not contact you in this way.

### Investment & Pensions scam:

You could be contacted by someone with an amazing 'investment opportunity' or the opportunity to access your pension cash early.

Find out more about this scam on the Action Fraud website

Make your own enquiries and look at the Financial Conduct Authority website.

### Loft insulation:

A call from a company claiming that building regulations have changed and made it illegal to have rock wool or fibre glass insulation in your loft or that the insulation may cause damp and mould issues.

They may pressure you into making an appointment for them to inspect your loft – which could result in unnecessary works being carried out.

### Home appliance insurance:

These bogus callers claim that you already have a policy with them and offer to renew it for a cheaper price. If you do already have an appliance warranty, you could be caught by this.

Or they may keep calling with 'better' deals or even say you owe money for a policy you apparently signed up to years ago.

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

**Suspicious text messages:** forward suspicious text messages 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.

**Report suspicious emails**: if you have received any email that you're not sure about, you can report it to the Suspicious Email Reporting Service by forwarding the email to - report@phishing.gov.uk

**Remember not to** respond, click on any links or open attachments in emails or text messages

**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 visit www.Bromley.gov.uk/scams  where you can also sign up to receive the Alerts! direct to you.