Advice and Guidance

Scams

HARTLEPOOL BOROUGH COUNCIL

TRADING STANDARDS SERVICE

Introduction

The purpose of this leaflet is to provide you with advice regarding scams and offer you:

- An insight into the different types of scams and the ways you can identify them.
- Tips to avoid becoming a victim of a scam.
- Advice should you feel you are a scam victim.

What are scams?

A scam is a dishonest scheme to con people out of their money. They come in many forms but the most common delivery methods include; telephone, letter, email and text message.

Scammers target everybody but vulnerable groups such as the elderly are more likely to respond. Statistics show that the average age of a scam victim is 75 years old and 53% of people aged over 65 state they have been targeted by scammers.

Research carried out by the National Trading Standards Scams Team indicates that UK consumers lose around £10 billion a year to scammers, however this figure is likely to be much higher as only 5% of incidents are thought to be reported.

Telephone Scams

In most instances the scammer will ‘Cold call’ you, i.e. you will receive the call unexpectedly or ‘out of the blue’. They will claim to be from an organisation that can help you in some way. Some of the common types of telephone scams are discussed on the following pages.

Banking Scams

The caller will claim to be from your bank and tell you that there is a problem with your account or bank card and that your money is at risk of being lost or stolen.

The caller will then ask you to confirm information about your account such as your name, date of birth, account numbers and pin number. They will then use this information to try and gain access to your account.

On other occasions they may send someone to your house to collect your bank card (such as a courier) or tell you to move your money to a ‘safe account’. In reality, this is a scam and your money will be lost.

Your bank will **NEVER** contact you in this way

Computer Scams

The caller will tell you that there is a problem with your computer. They will then guide you through a process which grants them remote access to your computer before installing a spyware virus. The virus will then search your computer for personal information such as banking details and passwords.

Alternatively, the caller may install a ransomware virus onto your computer which will block access to your files until you pay them a fee to remove it.

This type of scam may also be initiated by a sudden ‘pop up box’ on your computer screen whilst you are accessing the internet. It may advise you that you need to telephone a number and pay a fee to resolve the problem.

Council Tax and HMRC Tax Scams

The caller will claim to be from the Council or HMRC and tell you that you are due a tax return. They will ask you for your bank account details and then steal money from your account. Alternatively they may ask you to pay a processing fee before the tax return can be granted.

Councils and Government bodies will not contact you in this way.

Phantom Debt Scams

You will receive a phone call from someone claiming to be from a debt collection agency. They will state they are working under the instruction of a Court and demand payment of a non-existent debt. If you refuse to pay they will threaten to visit your home or say the police will come and arrest you.

What should I do if I suspect a telephone call is a scam?

- **NEVER** reveal personal or financial information to a cold caller, no matter who they claim to be.
- If you feel that a call may be a scam, end the call. Don’t let them talk over you or keep you on the line and don’t feel as though you are being rude by hanging up.
- Don’t be rushed into making a decision. Scammers make you feel as though you need to act fast to prevent you from realising what is really happening.

- Contact the organisation the caller is claiming to be from using a telephone number you have located yourself. For example, if the caller claims to be from your bank, use the number on the back of your bank card. **NEVER** call an organisation from a telephone number a caller gives you and if possible use an alternative phone to make the call.
- Buy a handset which has ‘Caller ID’ where you can see who is calling you. You should be aware that scammers use a tactic known as spoofing so their telephone number appears the same as a genuine organisation.

- Buy a telephone with nuisance call blocking technology which will prevent unwanted calls (including from scammers) from getting through to you. They are very effective and can be purchased from major electrical retailers and supermarkets.
- Add your telephone number to the Telephone Preference Service (TPS). The TPS is a free opt-out service for people who do not want to receive unsolicited sales and marketing

telephone calls. This option should reduce the number of cold calls you receive but may not necessarily block all of the scammers.

Postal Scams

Postal Scams are those which are sent by letter or catalogue. They are generally categorised into three different types.

Lottery and Prize Draws

The letter will congratulate you on winning a prize, but to claim it you will first need to call a premium rate number or pay an administration fee. In reality, the prize doesn't exist and will never arrive, instead, you will be told to pay more money before the fictional prize can be sent.

Psychics and Clairvoyants

The letter will advise that the sender has seen your 'lucky' future and they want to share the information with you. However, before they will do so you have to pay a fee. If you pay the fee they will send another letter asking for more money.

If you refuse their request they may then threaten you with an ‘evil curse’ or bad luck.

Mass Marketing Scams

The letter will tell you that you have won a prize but to claim it you need to order an item from their catalogue. If you place an order, you will receive the item, but the prize will never arrive. The items you will receive are often poor quality, misdescribed and vastly overpriced. Common items for sale include confectionary, health products and trinkets.

How can I tell if a letter is a scam?

If you are unsure about a letter you have received, postal scams have common characteristics - some of which are discussed below.

- You will receive the letter ‘out of the blue’.
- It will state you have won a prize for a competition you have not entered.
- You may be told to keep the letter a secret. This tactic is used to prevent a victim telling someone who may expose the scam.
- It may ask you to make a payment in advance to receive a prize or information.
- It may ask you to buy an item from their catalogue to claim a prize.
- It will give you a tight deadline to reply. This tactic is used to get a victim to respond without properly thinking it over.
- It may ask for personal details or passwords.
- The originating and return addresses may be from locations outside of the United Kingdom.

What should I do if I receive a letter which I believe may be a scam?

- Ask a friend or family member for a second opinion.
- Call Hartlepool Trading Standards who are happy to provide advice. Their number can be found at the back of this leaflet.
- Report it to Action Fraud who are the UK's national reporting centre for Fraud. Their number can be found at the back of this leaflet.
- Shred it and bin it. Ensure that you destroy personal information such as your address before putting it in the bin to prevent identity theft.
- Do not reply under any circumstances, not even with a negative reply as you may end up on a 'Suckers List'.

Email Scams

Emails are a cheap way for scammers to reach large numbers of people easily. They are generally, but not always, versions of the other scams mentioned on the previous pages. Like other types of scams, they have common characteristics - some of which are discussed below.

- The email will be received 'out of the blue' or was not expected from the organisation claiming to be the sender.
- The sender's email address is not the same as the organisation's website address.
- It is not addressed to you personally and a greeting such as 'Dear customer' is used instead, or it uses your email address as your name.
- It states that you will need to act fast or you will miss out.

- It asks you to send personal information such as bank details, usernames and passwords.
- It may appear unprofessionally written and/or contain spelling and grammatical mistakes.

- It contains a link to a website. Criminals set up fake websites which appear to be the same as a genuine organisation's but in reality they are there to harvest your information.
- It contains an attachment. The attachment may be described as an invoice or letter and be from an organisation you can trust. If you open the attachment it will contain a virus which will infect your computer.

What should I do if I receive a scam email?

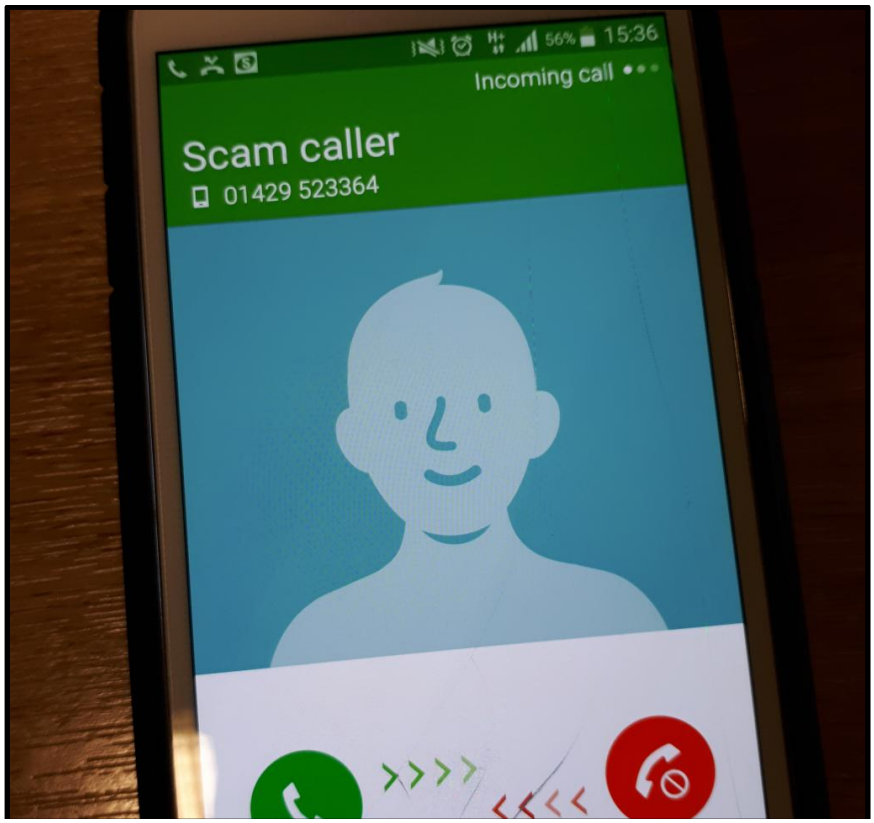
- If you know that the email is a scam upon receipt, do not open the email and delete it immediately.
- Do not reply to the email, even if your reply is negative. The scammer may still add your name to a target list if you respond negatively.

- Do not click on any of the links found in the email.
- If you have clicked on a link, do not enter any personal information on to the website. The scammers clone websites to make them look like the legitimate sites.
- Do not open any of the attachments that are present with the email. The attachment may contain a virus.

Text message (SMS) Scams

You will randomly receive a text message from someone claiming to be from a reputable organisation such as your bank or your network provider. The message will advise that your account needs verifying, updating or reactivating and ask you to follow a link to a website or call a telephone number in order to do so. Once you follow the link or call the number you will be asked to disclose personal and/or financial information.

In realty, you will be taken to a bogus website or to a scam call centre and the details you disclose will be used to steal your money and identity.



What should I do if I think I'm a victim of a scam?

If you believe that you may be a victim of a scam, it is important that you act in the best way possible.

- If you have provided your bank details, contact your bank **immediately** and inform them of the incident. By acting fast you may prevent your money being taken.
- If you have lost money or fear that you may be about to, again contact your bank immediately.
- After you have reported the incident to your bank, call the police using their non emergency telephone number (below)
- Tell a friend or family member. Remember you are not alone.
- Report the incident to Action Fraud on the telephone number found below.
- Call Trading Standards on the number below. An officer will be able to advise you on the best course of action.
- Above all do not feel ashamed or embarrassed. Criminals develop very sophisticated methods of scamming people and there are many other people from all different age groups who have also fallen victim.

Useful Telephone Numbers

Police Emergency:	**999**
Police Non Emergency:	**101**
Hartlepool Trading Standards:	**01429 523362**
Victim Care and Advice Service:	**0303 0401099**
Citizens Advice Bureau:	**01429 408401**
Citizens Advice Consumer Helpline:	**03454 040506**
Action Fraud:	**0300 123 2040**

Golden Rules

Remember the golden rules to protect yourself against scams.

- **Be suspicious at all times.**
- **Never give out personal or banking details to someone you do not know or trust.**
- **Never send or bank transfer money to someone you do not know or trust.**
- **Never let someone rush you into making a decision.**
- **Never telephone an organisation from a number provided by a cold caller.**
- **Never follow a link to an organisation in an email.**
- **Ask a friend or Trading Standards for a second opinion if you are unsure.**
- **If you feel as though you may be a victim, tell someone at the earliest opportunity.**
- **If it sounds too good to be true, it generally is!**