

SCAMS BULLETIN

The purpose of this scams bulletin is to enable Isle of Wight residents to be aware, and therefore guard against, the types of scams currently being reported to the Trading Standards service.

Trading Standards will collate information on scams to provide information and intelligence to the public and other agencies but will not normally intervene unless the victim is **very vulnerable and has been financially abused**.

We will also seek to take enforcement action in the civil and criminal courts where it is appropriate in order to punish the offenders.

If you are worried about scams please contact:

**Citizens Advice Consumer Helpline on
08454 04 05 06
or online using the
[Online consumer complaint form](#)**

HANDLING: This bulletin may be distributed to the public

SCAMS BULLETIN

Auction Sites Scam

Auction Sites are a popular and convenient way of buying presents. Whilst the majority of sellers are genuine, there are some criminals who use auction sites to offer counterfeit goods or those that do not exist. Scammers use Christmas as an opportunity to advertise popular items such as smartphones, tablets, gadgets and designer goods. They display a low price to catch your attention. However, in reality the goods are not real, and once you have made your bid or payment, you will receive nothing in return. The Scammer will 'hide' behind a fake website or email address and the chance of catching up with them to claim your money back is slim.

Real life case study

Mr J was looking on an auction site for a laptop. He noticed one being advertised at a low price. He thought the price seemed too good to be true, so contacted the seller by email to enquire further. The seller responded and said he wanted a quick sale for cash. Mr J offered to purchase the goods at the agreed price. The seller then responded and said that he was currently on holiday and could not post the goods, but if Mr J made an upfront payment, he would arrange a meeting point where his friend could deliver the laptop. At this point, Mr J sensed a scam and pulled out of the deal.

How to protect yourself

- Always use a recommended method of payment for the site, rather than making direct payments to the seller
- Research the seller before you bid
- Check the sellers customer feedback but bear in mind this can be falsified
- Be cautious when dealing with sellers abroad or private individuals
- If you are going to pick up purchases in person, take someone with you and let people know where you are going
- If in doubt DO NOT PURCHASE

Citizens Advice Consumer Helpline on
08454 04 05 06

Or online using the

[Online consumer complaint form](#)

HANDLING: This bulletin may be distributed to the public

SCAMS BULLETIN

Charity Donation Scams

Most collection and appeals are legitimate but, unfortunately scammers can exploit people's charitable nature and steal money which the donor thinks is going to help a charity. Do not stop donating money to your good cause of choice. Instead take a few simple precautions to protect yourself, and your charity, against online fraud.

- Visit the charity's own website by typing the address into the browser yourself, rather than clicking on a link in an email.
- Before you donate any money, check the website is secure. There should be a padlock symbol in the browser window frame when you attempt to log in or register.
- If you receive unsolicited emails from charities you have never heard of or have no association with, do not respond and do not click on any links. It is best to delete them.
- Do not respond to requests that ask you to donate through a money transfer company. This is a tactic commonly used by scammers as it makes the payment hard to trace.
- Ensure the charity is genuine before divulging personal information or payment methods.
- When supporting disaster relief abroad, consider donating through the Disasters Emergency Committee.
- If you do not want to make an online donation check with a legitimate charity if they accept other ways to pay.
- If you think you have given your payment details to a bogus charity, contact your bank or credit card company immediately.

Charity bag collection scam

Trading Standards have continued to receive complaints about charity bags that are delivered or left outside a person's property. The wording on the bag invariably asks the resident to fill it with unwanted clothes or household items, which will then be used abroad or sold to support a charity. However, the bags may have been delivered by bogus commercial companies who will profit from the donations.

Don't be put off making donations to genuine charities but remember to carry out a few simple checks first of all. Do not rely on the contact details on the bag as this may be fake. Instead look up the official telephone number or website address to make sure your donation is going to the genuine place. If in doubt, throw the bag away.

For further advice or to report a scam contact the Citizens Advice Consumer Helpline on 08454 04 05 06 Or online using the [Online consumer complaint form](#)

HANDLING: This bulletin may be distributed to the public

SCAMS BULLETIN

Computer Scams

The Trading Standards Service warns residents to be alert to the following scams when working on their computers. In particular when browsing the internet or receiving emails.

Ransom 'spam'

This scam operates, where an email is sent, appearing to be from a genuine financial institution. However, the email contains an attachment that looks legitimate but is malware that encrypts computer files.

If the attachment is opened, a displayed countdown timer appears and demands payment, or a ransom, to decrypt the files. This may be in the region of £500.

Once the payment is made, no work is carried out and it is not possible to restore any encrypted files.

Police warning scam

A similar scam operates where a 'warning' appears on a computer containing a police logo and a message that an illegal site has been entered and internet access will be blocked until a fine is paid. They then asked for an up-front payment of £100 to remove the block, which should be made through a money transfer business.

If payment is made, the money will be lost.

Tips to protect yourself

- Do not respond to or open attachments from unknown sources
- Do not click on links in emails from unknown sources
- Make sure you have suitable anti-virus software protection installed
- Don't reply to any unwanted email
- If in doubt, delete the email without opening it

Isle of Wight Council Trading Standards Service has continued to receive calls from worried consumers who have been approached by fraudsters, attempting to scam them out of large amounts of money. The fraudsters will dupe victims into revealing their bank details, and are using ever more sophisticated and cunning tactics to access this information. NEVER give out you bank details to a caller. If you think you have been a victim of a scam, contact your bank immediately.

For further advice or to report a scam contact the Citizens Advice Consumer Helpline on 08454 04 05 06 Or online using the [Online consumer complaint form](#)

HANDLING: This bulletin may be distributed to the public

SCAMS BULLETIN

Inheritance Scams

Isle of Wight Trading Standards Service has continued to receive complaints about inheritance scams.

The scammer, who claims to be a lawyer or government official, will send a letter alleging a person sharing your family name has died and left behind a vast amount of money. They will say as no relatives have been identified the money can be released to you, due to your surname. They will ask for a fee to release the money. Once paid, you will not hear from them again.

Real life case study

Mrs P received a letter from a business based in Spain, alleging that someone with the same surname as her had died, leaving an unclaimed inheritance of £5million in a bank account. The business explained that unless a beneficiary was found, the money would be paid to the government. Mrs P was advised that as she shared the surname, the business could release the money. They suggested that 80% of the money would be split, with the final 20% paid to a charity. They asked Mrs P to contact them to discuss this proposition further. Mrs P recognised this offer as a scam and sent the letter to Trading Standards for information.

'PayPal' Scam

Real life case study

Mrs S received an email from an address that contained PayPal. It was advising that someone had tried to gain access to her account. The email was asking her to update her contact and payment details. Mrs S, who does not consider herself to be vulnerable, said at first glance she thought this was genuine, but noticed the English used in the subject line was poor – “We are detected that someone try to get access to your account”. This prompted her to contact the official helpline for PayPal who confirmed this was a scam.

Citizens Advice Consumer Helpline on

08454 04 05 06

Or online using the

Online consumer complaint form

HANDLING: This bulletin may be distributed to the public