

ONLINE SHOPPING AND AUCTION SITES

Online shopping can save you time, effort and money. Millions of people use websites such as eBay and AutoTrader to buy new or second hand goods for competitive prices. These sites give you the opportunity to purchase a huge choice of goods from all over the world. However, among the genuine buyers and sellers on these sites, there are criminals who use the anonymity of the internet to offer goods for sale they do not have, or are fake.

In the majority of transactions, the buyer and seller never meet. Which means when making a purchase or sale on a website, you are reliant on the security measures of the site.



Fraudsters will advertise an item for sale, frequently at a bargain price compared to other listings of a similar type. They may have pictures of the item so it appears to be a genuine sale.

A favoured tactic is to encourage buyers to move away from the website to complete the transaction, and the criminal may offer a further discount if you do so. Many websites offer users the opportunity to pay via a recognised, secure third party payment service, such as PayPal, Android Pay or Apple Pay. Read the website's advice and stick to it. Fraudsters might be insistent you pay via bank transfer instead. By communicating and paying away from the website, contrary to their policies, you risk losing any protection you had.

Criminals may also email or contact you if you have 'bid' on an item but not been successful in winning the auction. They will claim that the winning bidder pulled out or didn't have the funds and offer you the chance to buy the item. Once you agree, they will either provide bank details or even insist payment is made via a third party payment service for mutual protection. Once you agree, they 'arrange' this. You then receive a very legitimate looking email which appears to be from the website or a third party payment service directing you how to make the payment. Some are very sophisticated, even having 'Live Chat' functions that you can use to speak to a sales advisor! Unfortunately, you will again be communicating to the fraudster, so beware!



In both these scenarios, once the payment is made, the 'seller' won't send the item. They'll either not reply to you or make excuses as to why they haven't sent the goods.

If they do send the item, they'll send counterfeit goods instead of the genuine items advertised. Again, you may struggle to receive any compensation or resolution to this problem from the legitimate website, as it could be against their policies.

Fraudsters also use e-commerce websites to pose as 'buyers.' If you have an item for sale, they may contact you and arrange to purchase this. It is common for criminals to fake a confirmation that payment has been made. Before posting any item, log in to your account via your normal method (not a link on the email received) and check that you have received the money.

You must also be careful what address you send items to. Fraudsters may ask you to send items to a different address. They may claim they need it sent to their work address or to a friend or family member. If you send the item to an address other than the one registered on the user account, you may not be provided any protection from the website or payment service.

TYPES OF FRAUD

How to protect yourself

- ⚠ Stay on the website!
- ⚠ Be wary of offers that look too good to be true.
- ⚠ Read the consumer advice on any website you are using to make a purchase. Use the recommended payment method, or you may not be refunded for any losses to fraud.
- ⚠ Research the seller/buyer and any of their bidding history.
- ⚠ Don't be convinced by pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like www.tineye.com or <https://reverse.photos/>
- ⚠ Be suspicious of any requests to pay by bank transfer or virtual currency instead of the websites recommended payment methods.
- ⚠ Never buy a vehicle without seeing it in person. Ask to see the relevant documentation for the vehicle to ensure the seller has ownership.

⚠ If you are selling online, be wary of any emails stating funds have been sent. Always log in to your account via your normal route (not via link in email) to check.

⚠ Watch the Metropolitan Police's video on Online Shopping Fraud at www.met.police.uk/littlemedia.

REMEMBER

Stay on site.

CAUTION

Be wary of paying by bank transfer or virtual currency.

THINK

**Why is this item so cheap?
Is it a scam?**
