

# Hillingdon Cyber Crime Summary

## December 2022

### Executive Summary

Number of offences	132
Total loss	£374,409.93
Average per victim	£2,836.44

### Top 5

The top 5 by **volume** (number of reports) type of fraud is as follows:

Fraud Type	Amount of Offences	Amount Lost
NFIB3A - Online Shopping and Auctions	25	£40,739.37
NFIB1H - Other Advance Fee Frauds	15	£10,610.00
NFIB3D - Other Consumer Non Investment Fraud	12	£113,991.68
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	12	£32,273.48
NFIB3F - Ticket Fraud	7	£15,331.57

The top 5 by **amount** reported lost:

Fraud Type	Amount Lost	Amount of Offences
NFIB3D - Other Consumer Non Investment Fraud	£113,991.68	12
NFIB2E - Other Financial Investment	£60,727.81	5
NFIB3A - Online Shopping and Auctions	£40,739.37	25
Push Payment	£36,791.50	6
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£32,273.48	12

### Fraud Advice

#### Other Consumer Non Investment Fraud

Sometimes businesses use deceptive business practices that can cause their victims to suffer financial losses.

The victims believe they are participating in a legal and valid business transaction when they are actually being defrauded. Fraud against consumers is often related to false promises or inaccurate claims made to consumers, as well as practices that directly cheat consumers out of their money.

#### How to protect yourself

- Research the company before purchasing goods or services.
- Use Companies House to find out how long they have been trading.
- Ensure you use trusted, reviewed companies.
- Avoid using direct bank transfers when purchasing items online, instead use a credit card.

# Hillingdon Cyber Crime Summary

## December 2022

### Investment Fraud

Investing in stocks and shares or any other commodity can be a successful way of making money. However, it can also lead to people losing their entire life savings. Fraudsters will persuade you to invest in all kinds of products. They will offer you high rates of return, particularly over longer periods of time, which often do not exist.

Common products that will be offered include binary options, virtual currency, carbon credits, wine, rare metals, gemstones, land and alternative energy. Often, initial investments will yield small returns as an incentive to invest further funds. However, larger investments or cashing out will be met with excuses or a penalty charge. Eventually contact with the fraudster will be impossible and all funds and bogus returns lost.

Fraudsters are organised and they may have details of previous investments you have made or shares you have purchased. Knowing this information does not mean they are genuine.

Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

It is relatively easy to register a company with Companies House. This does not confirm or endorse that they can provide genuine investments. Indeed, emerging investment markets may be unregulated, making these open to abuse.

Companies may be registered at prestigious addresses, for example Canary Wharf or Mayfair. This does not mean they operate from there. It is an accepted business practice to rent such a virtual office to enhance a business's status. However, fraudsters are also aware of this and exploit it. The fraudster may put pressure on you by offering a 'once in a lifetime opportunity' or claim the deal has to be done quickly to maximise profit.

In addition - be wary of companies that offer to 'recover' any funds you have lost to any sort of investment scam. They may be linked to the company who initially defrauded you in the first place and may be targeting you again. This is known as 'Recovery Fraud'.

### How to protect yourself

- There are no get rich quick schemes. If it sounds too good to be true, it probably is.
- Genuine investment companies will not cold call you. Be extremely wary of anyone who does.
- Research both what you have been offered, and the investment company. Speak to Trading Standards if you have concerns.
- Before investing, check the Financial Conduct Authority register to see if the firm or individual you are dealing with is authorised (<https://register.fca.org.uk/>)
- Check the FCA Warning List of firms to avoid.

**REMEMBER** - Don't be pressured into making a quick decision.

**CAUTION** - Seek independent financial advice before committing to any investment.

**THINK** - Why would a legitimate investment company call me out of the blue?

# Hillingdon Cyber Crime Summary

## December 2022

### 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.

### How to protect yourself

- Stay on site!
- 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](http://www.tineye.com) or <https://reverse.photos/>



# Hillingdon Cyber Crime Summary

## December 2022

- 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 our video on Online Shopping Fraud at [www.met.police.uk/littlemedia](http://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?

### Remember:

Your bank, the police, or tax office will **never** ask you to attend your bank, withdraw, transfer or pay money over the phone or send couriers to collect your card or cash. Nor would they ask you to buy goods or vouchers.

**This is a scam.**

1. **Hang up** (Never give details or money following a cold call)
2. **Take 5** (Seek a second opinion, tell someone what has happened)
3. **Verify** (if concerned, contact the company via a pre-confirmed method)

All of our videos and electronic leaflets can be found on the following link;  
[www.met.police.uk/littlemedia](http://www.met.police.uk/littlemedia)

Free cyber advice can be found <https://www.ncsc.gov.uk/cyberaware/home>

Always report, Scams fraud and cyber crime to Action Fraud, either online at [www.actionfraud.police.uk](http://www.actionfraud.police.uk) or by telephone on 0300 123 2040.

### STOP

Taking a moment to stop and think before parting with your money or information could keep you safe.

### CHALLENGE

Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

### PROTECT

Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.