# Havering Cyber Crime Summary
# October 2025

## Executive Summary

| | |
|---|---|
| Number of offences | 136 |
| Total loss | £827,975.47 |
| Average per victim | £6,088.05 |

## Top 5

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

| Fraud Type | Amount of Offences | Amount Lost |
|---|---|---|
| NFIB1H - Other Advance Fee Frauds | 21 | £80,998.19 |
| NFIB3A - Online Shopping and Auctions | 20 | £28,421.10 |
| NFIB3D - Other Consumer Non Investment Fraud | 15 | £23,496.31 |
| NFIB2E - Other Financial Investment | 9 | £107,106.24 |
| NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP) | 9 | £9,380.49 |

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

| Fraud Type | Amount Lost | Amount of Offences |
|---|---|---|
| NFIB5D - Mandate Fraud | £209,685.17 | 4 |
| NFIB1D - Dating Scam | £110,200.00 | 4 |
| NFIB2E - Other Financial Investment | £107,106.24 | 9 |
| NFIB19 - Fraud by Abuse of Position of Trust | £100,000.00 | 1 |
| NFIB1H - Other Advance Fee Frauds | £80,998.19 | 21 |

# 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.

# Havering Cyber Crime Summary
# October 2025

## Romance and Dating Fraud

**Dating online is now one of the most popular ways for new couples to meet, with millions of people finding new relationships, romance and love this way. Unfortunately, amongst the genuine profiles are fake profiles set up by fraudsters. They are after your money, not your love. They are masters of manipulation, playing on your good nature and emotions to ultimately steal your money.**

Criminals will build a relationship with online members, quickly asking to move communication off the dating website. This is so they can continue their contact with you, even if their profile is later identified by the site as fraudulent and subsequently deleted.

Fraudsters are often very flattering, appearing really interested in you within a short space of time. However, they will use a range of excuses as to why they can't meet in person, such as they are stuck overseas, have a family emergency or have an issue with their business. They then start asking for money to help with their problems, assuring you they will pay it back as soon as they can. The fraudster may claim to be desperate to meet you as soon as this obstacle is overcome. This is all a scam and their true intention is to take as much money from you as they can.

## How to Protect Yourself

- Stay on site.
- Keep all communication on the dating website you are using. Don't be convinced by profile 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 **https://www.tineye.com** or **https://reverse.photos**
- Do your own research on the person – are they members of any other social networking sites? Can you confirm what they are telling you about themselves, such as where they work or where they live?
- Never send money to someone you have not met in person and be extremely wary of giving money to someone you have recently started a relationship with.
- Be wary of anyone asking you to receive money on their behalf and transfer it on. They may be using you to launder money.
- Talk to family and friends for advice, even if the other party is asking you to keep the relationship secret.
- Watch our video on Romance Fraud at **www.met.police.uk/littlemedia**

**REMEMBER** - Stay on site! Never send money to someone you have not met in person, or receive/ transfer money on their behalf.

**CAUTION** - Be wary of continuing the relationship away from the dating website you initially made contact on.

**THINK** - Why are they so quick to declare their love for me? How do I know they are telling me the truth?

## 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.

# Havering Cyber Crime Summary
# October 2025

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?

## 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**

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

- **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.

# Havering Cyber Crime Summary
# October 2025

## Where to Report a Scam:

**If you think you have been scammed, contact your bank first by calling 159**

How it Works; 159 works in the same way as 101 for the police or 111 for the NHS. It's the number you can trust to get you through to your bank safely and securely every time. So if you think someone is trying to scam you into handing over money or personal details – stop, hang up and call 159 to speak directly to your bank.

Always report; scams, fraud and cyber-crime to Action Fraud, either online at **www.actionfraud.police.uk** **or by telephone on 0300 123 2040.**

Subscribe to the "**Which**" Scam Alert Service where you can receive free updates on current scams being used. Copy this link into your search engine **https://act.which.co.uk/** and locate "Scam Alerts newsletter" to register your details. **Which** will then provide practical advice to keep you one step ahead of fraudsters.

**Get advice** and report it to Trading Standards through the Citizens Advice consumer service on 0808 223 1133 or online advice at **www.adviceguide.org.uk**

**The Citizens Advice consumer service** provides free, confidential and impartial advice on consumer issues. It is important that all complaints are referred to the Citizens Advice consumer service as they maintain a national database of complaints that provides an invaluable source of information and intelligence to the trading standards community

Details of all consumer enquiries, dealt with by the Citizens Advice consumer helpline, are made available to Trading Standards

**Report a text message you think is a scam** - most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**. If you forward a text to **7726**, your provider can investigate the origin of the text and arrange to block or ban the sender, if it's found to be malicious.

**Report an email you think is a scam -** If you have received an email which you're not quite sure about, forward it to **report@phishing.gov.uk**

**If you've been scammed through the post -** Royal Mail investigates postal scams. If you've received something in the post you think is a scam, send it to **'Freepost Scam Mail'.** Include the envelope it came in and a completed scam mail report. You can download a scam mail report from Royal Mail or call them and ask for a form and pre-paid envelope

**If the scam involves financial services -** If the scam involves cryptocurrency, investments, insurance or pensions, report it to the **Financial Conduct Authority - 0800 111 6768**

**Friends Against Scams** is a National Trading Standards Scams Team initiative, which aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams.

Online learning available
**https://www.friendsagainstscams.org.uk/training/friends-elearning**