

# Havering Cyber Crime Summary

## August 2025

### Executive Summary

Number of offences	145
Total loss	£400,186.6
Average per victim	£2,759.90

### 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	20	£58,800.45
NFIB3D - Other Consumer Non Investment Fraud	16	£10,360.00
NFIB52C - Hacking - Social Media and Email	13	£0.00
NFIB1H - Other Advance Fee Frauds	12	£12,738.00
NFIB2E - Other Financial Investment	10	£136,539.83

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

Fraud Type	Amount Lost	Amount of Offences
NFIB2E - Other Financial Investment	£136,539.83	10
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£98,016.50	8
NFIB3A - Online Shopping and Auctions	£58,800.45	20
NFIB5D - Mandate Fraud	£30,924.00	2
Push Payment	£26,213.80	7

### Fraud Advice

#### Push Payment Fraud

Online banking makes managing money easier for the general public, however criminals are taking advantage of this ease of banking and using it to defraud the public.

Criminals can pretend to be from somewhere official, for example, your bank, or the tax office. They contact you via email, phone or social media, and then warn you of fake suspicious or criminal activity on your bank account. They state that they've set up a safe account for you to transfer your funds into. However, this is actually their account.

#### How to protect yourself

- Be suspicious of a call out of the blue from someone claiming to be from a position of authority.
- Take down the person's details (name, authority, department, branch etc.) and verify using independent source contact details.
- A genuine official from the Police, your bank, HMRC or any other trusted authority will NEVER call you to ask you to verify your personal banking details, PIN or password, or threaten you with arrest.
- Never transfer money into another account unless you are 100% certain of the owner of the account.
- Your bank will never set up a "safe" account for you.
- If you are a victim, contact your bank as soon as possible, as they may be able to help stop the transfer.
- Watch our video on Impersonation Fraud at [www.met.police.uk/littlemedia](http://www.met.police.uk/littlemedia).

# HaVering Cyber Crime Summary

## August 2025

**REMEMBER** – Your bank will never set up a “safe account”.

**CAUTION** – Unless you definitely know who the account belongs to, it might not be safe.

**THINK** – Who told me this account was safe? Have I checked their identity?

### Social Media & Email Hacking

**If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.**

You can improve your cyber security by taking six actions:

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices
6. Back up your data

**More information and cyber advice can be found here;**

**<https://www.ncsc.gov.uk/cyberaware/home>**

### 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.



**METROPOLITAN  
POLICE**



# Havering Cyber Crime Summary

## August 2025

### 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>

- **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.

### 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](http://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](http://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.

# Haivering Cyber Crime Summary

## August 2025

**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>



**METROPOLITAN  
POLICE**

