Waltham Forest Cyber Crime Summary August 2025

Executive Summary

Number of offences	165
Total loss	£790,052.00
Average per victim	£4,788.19

Top 5

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

Fraud Type	Amount of Offences	Amount Lost
NFIB52C - Hacking - Social Media and Email	23	£0.01
NFIB1H - Other Advance Fee Frauds	20	£912,77.87
NFIB3A - Online Shopping and Auctions	19	£8,901.64
NFIB3D - Other Consumer Non Investment Fraud	15	£26,846.66
NFIB3F - Ticket Fraud	10	£8,363.78

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

Fraud Type	Amount Lost	Amount of Offences
NFIB1D - Dating Scam	£468,794.00	6
NFIB2A - Share sales or Boiler Room Fraud	£100,000.00	1
NFIB1H - Other Advance Fee Frauds	£91,277.87	20
NFIB3D - Other Consumer Non Investment Fraud	£26,846.66	15
NFIB2E - Other Financial Investment	£21,038.56	8

Fraud Advice

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

Waltham Forest Cyber Crime Summary August 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?

Ticket Fraud

Getting tickets to see your favourite band, football team or theatre production can be extremely difficult as tickets sell out quickly. Criminals take advantage of this by offering tickets for sale that do not exist or are fake.

Most event tickets are sold via reputable websites operated by promoters, the event venue or other official agents. Many tickets are also offered for sale on secondary resale websites, place adverts on secondary resale sites or use social media to sell tickets they do not have.

Once a payment is made you will either not receive the tickets or the tickets you receive will be fake or non-transferrable. When you arrive at the venue you will not get in. Some tickets are non-transferrable and can only be used by the person who initially purchased them. In many cases unauthorised resale of these tickets is illegal.

Waltham Forest Cyber Crime Summary August 2025

How to Protect Yourself

- Buy tickets from the event promoter, venue box office, official agent or a reputable ticket exchange site or app.
- Be suspicious of requests to pay by bank transfer. Where possible use a credit card when making purchases over £100 and up to £30,000 as you receive protection under Section 75.
- Be wary of paying for tickets where you are told someone will meet you at the event with your tickets as they may not arrive.
- If the retailer is a member of the Society of Ticket Agents and Retailers (STAR) you are offered additional protection if something goes wrong. If a website shows their logo you can check they are really a member on www.star.org.uk
- For further information on buying tickets safely visit the STAR website.

REMEMBER – The site you are using could be fake.

CAUTION – Use your credit card to pay this could offer you additional protection.

THINK – How can I check the tickets are real?

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.

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.**

Waltham Forest Cyber Crime Summary August 2025

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