Monthly Threat Update
North East Economic & Cyber Crime

Welcome to the Monthly Threat Update (MTU) from NEROCU. This document provides an overview of Economic and Cyber crime trends within the North East and UK.

This document contains December 2025 data with a forward outlook.

Please contact the Regional Economic Crime Coordination Centre (RECCC) if you have any questions: RECCC@durham.police.uk

Reading Time 5-10 minutes.

Contents

Looking Back

Contents

Looking Forward

North East Cyber Crime December Summary

Personal data breaches.

A data breach occurs when information held by an organisation is stolen or accessed without authorisation. Criminals can then use this information when creating phishing messages so that they appear legitimate.
Even if your details are not stolen in the data breach, the criminals will exploit high profile breaches (whilst they are still fresh in people's minds) to try and trick people into clicking on scam messages.

NCSC Advice:

- Find out if you have been affected by contacting the organisation.
- Be alert to suspicious messages.
- If you receive a suspicious message including your password; change the password as soon as you can across all your accounts using that password.
- Check online accounts to confirm there has been no unauthorised activity.
- If you suspect an account of yours has been accessed, refer to the NCSC guidance on recovering a hacked account.

There are several online tools available to check if your data has appeared in data breaches such as:
https://haveibeenpwned.com

Ofcom investigates X over AI Grok tool.

In recent weeks Grok (the chat bot within the X platform) has been used to create non-consensual sexualised images. Users can upload photos of individuals and instruct the bot to remove their clothes or pose them in a sexualised way. Ofcom are investigating whether X has failed to take down illegal images including 'non-consensual intimate images' and child sexual imagery. In response to this, the UK government plans to bring in a law that criminalises the creation of such images.
If you are a victim of Grok or other non-consensual intimate images. report it to the Police. The creation and sharing of intimate and explicit images without consent including AI-generated deepfakes is illegal under the UK Online Safety Act 2023. It is also recommended to report it to the social media platform as they are legally required to remove the content under the Online Safety Act.

TikTok remove fake AI weight loss ads.

A weight loss drugs company pretending to be Boots has been removed from TikTok. The adverts showed a healthcare professional from Boots advertising the weight loss drug, but it was AI generated with no affiliation to the company Boots.
This use of AI is harmful and misleading to consumers who believe they are buying a drug from a reputable retailer. Taking medication sourced by unknown means carries serious risk to users' health with no guarantees what the drug contains.
Consumers should ensure they are viewing a verified account online. This is usually shown with a blue tick across mainstream social media accounts such as Tik Tok, Instagram and Facebook. Individuals can further scrutinise the advertisement by visiting the retailer's official website to verify if the products are for sale rather than following links provided in the advert on social media platforms.

Almost 1 billion attempts to access malicious sites blocked by new government cyber tool.

Almost one billion early-stage cyber attacks and attempts to access scam websites have been blocked by a new government cyber service in less than a year, according to new figures from GCHQ's National Cyber Security Centre (NCSC) and BT.
The Share and Defend Service – developed by experts at NCSC works to disrupt online crime by sharing near real-time data on known fraudulent and malicious websites with internet service providers, which can then prevent customers from clicking through.
Online content such as fake shops, phishing sites and malicious links (including from emails reported to the NCSC by the public) are being blocked automatically providing better protection at scale.
Individuals and organisations should remain alert to possible fraudulent or malicious websites. For guidance on how to spot scams, visit the NCSC website.

North East Fraud November Summary

Arthritis UK Fake Calls

Fraudsters have been making telephone calls purporting to be from Arthritis UK offering to help with the completion of benefits forms in return for a fee. This activity has not been carried out by or on behalf of Arthritis UK so please be vigilant.

Jellycat sales scams

Jellycat soft toys are in high demand and can sell for up to £50 each. Jellycats are collectible, with many fans hunting for rare, retired designs, especially early models or limited editions.

Scammers are advertising fake or non-existent toys for sale on social media sites such as Marketplace, priced to attract buyers. Some sellers appear legitimate, but their accounts have been cloned by fraudsters.

Some sellers are selling stolen items at lower costs as demand has driven an increase in thefts from retailers.

One victim's Paypal account flagged the sellers account for suspicious activity at the point of payment, but the seller convinced them that they were legitimate and to try another payment method.

Buyers are recommended to order through the legitimate website and never use another payment method if Paypal fails for suspicious activity.

Voice Recognition

A North East victim reported receiving a call from their banks Fraud department and was told a loan had been taken out in their name and in order to cancel it, they would have to apply for another loan. The victim was made to participate in scenarios where they believed they were recorded stating "I would like to make a payment of X amount". It is believed that the Fraudster then impersonated the victim and contacted the victims bank as a large sum of money was taken from their account.

National Insurance Scams

A trend is emerging Nationally where Fraudsters impersonating police officers have called victims stating their National Insurance number had been misused and were under investigation. In order to obtain a new number and halt the investigation, victims were told to purchase gift cards and send the reference numbers to the fake police officer via Whatsapp.

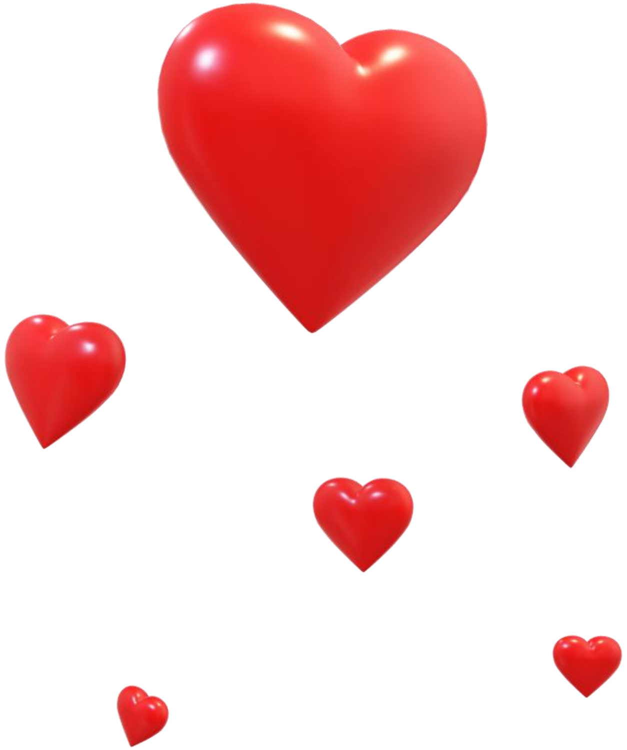
There have been 3 reports in the North East and all victims are from non-white British Ethnicities.

ROMANCE FRAUDSTERS

USE FAKE IDENTITIES TO FORM ONLINE RELATIONSHIPS AND MANIPULATE VICTIMS.

THEY EXPLOIT EMOTIONS WITH URGENT REQUESTS FOR MONEY.

PROTECT YOURSELF– NEVER SEND MONEY TO SOMEONE YOU HAVEN'T MET IN PERSON.



North East ROCU
Regional Organised Crime Unit Network

🛑 How to Spot the Signs of Romance Fraud

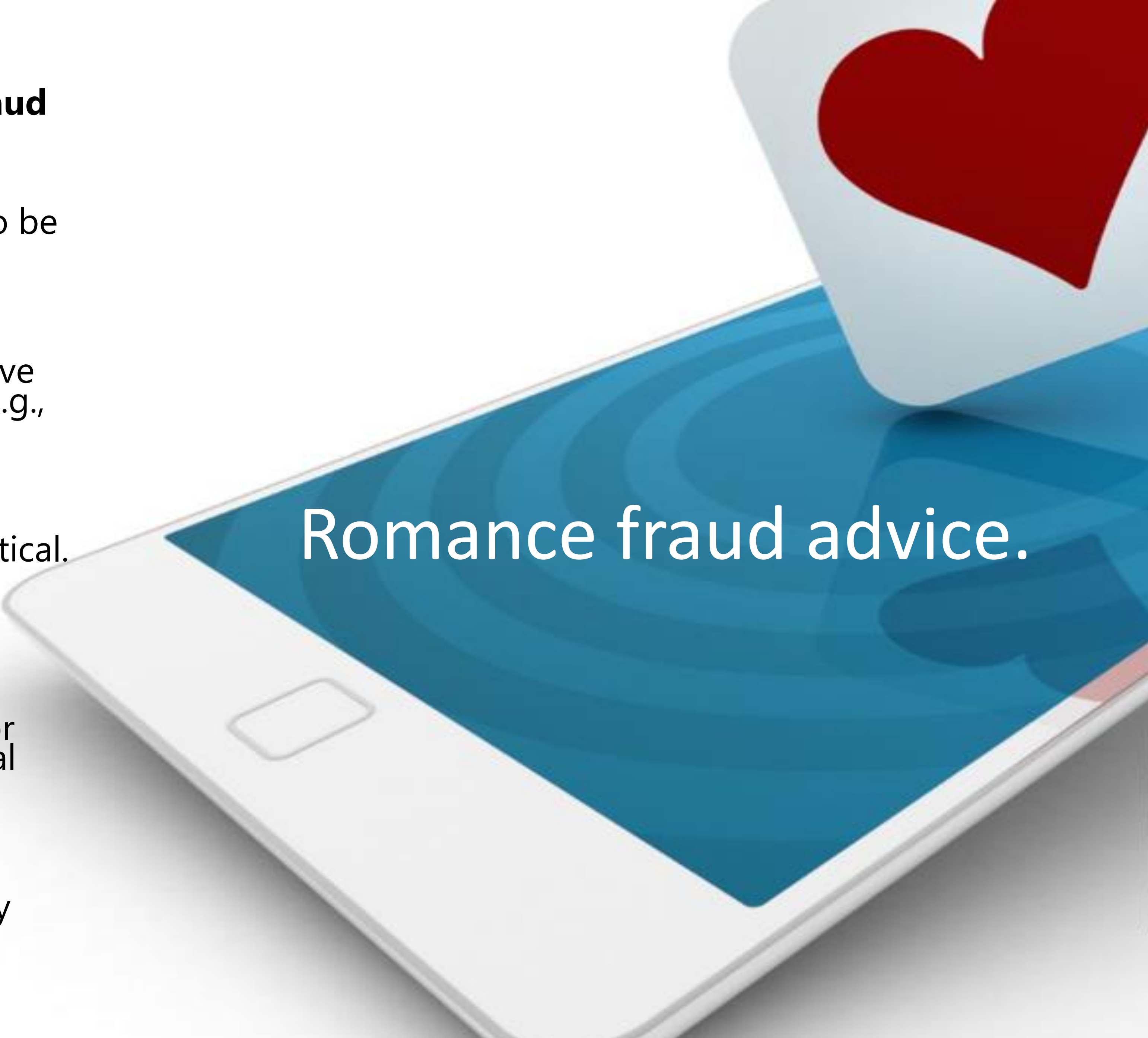
💭 **They move too fast**
You strike up a relationship online and they declare their love quickly. They often claim to be overseas due to military or medical work.

📵 **They avoid video calls or meeting**
They repeatedly make excuses and try to move conversations off the platform you met on (e.g., WhatsApp, Telegram).

💸 **They ask for money**
Requests are urgent, emotional, and time-critical. They may become defensive if you refuse to help.

📸 **Their pictures look "too perfect"**
Images may be stolen from actors, models, or influencers. A reverse image search can reveal where the photos were taken from.

🤐 **They push for secrecy**
They tell you not to speak to friends or family about your relationship, creating isolation.



Total amount lost to Romance Fraud in the North East 2025.

The figure on the right shows the total amount stolen from victims in the North East through Romance Fraud last year

(Data collected between 1/1/25 – 10/11/25)

£1,359,593

Report Fraud

Tell the Police about cyber crime and fraud

reportfraud.police.uk or call 0300 123 2040

Report Fraud has replaced Action Fraud, for use in England, Wales and Northern Ireland.

Anyone searching for how to report cyber crime or fraud, or trying to use Action Fraud, will be redirected to the new service, which can be reached directly online at reportfraud.police.uk or by calling 0300 123 2040.

Report Fraud will provide:

- A clear and simple reporting process to tell the police about cyber crime and fraud.
- Guidance on what to report and how that information is used
- Further support information for victims.

ENGAGEMENT EVENTS

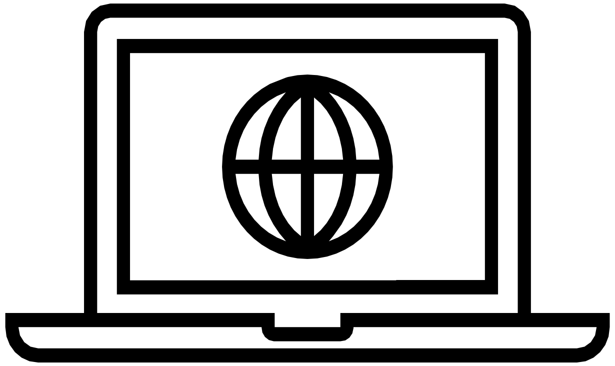
Below are just some of the events the team have attended this month…

- Northumbria University – offering support and advice to students regarding online financial abuse.
- Fraud Roadshow Stalls at all North-East branches of Nat-West and Barclays banks.
- Fraud Foundation – Skerne Park academy - Darlington
- Fraud Watch – Yarm Age UK, Cyber Focus.
- Fraud Foundation – Thriving Together NE, Blyth Rugby and Cricket club.
- Teesside University – student online safety and financial wellbeing sessions.

North East ROCU
Regional Organised Crime Unit Network

Horizon Scanning

Monitoring Threats



PPI Compensation for car owners ***update***

On 7 October, the UK's financial regulator, the Financial Conduct Authority (FCA), announced it's consulting on proposals for a mass redress scheme on unfair motor finance, with a predicted £8.2 billion to be paid out on an expected 14 million agreements.

While it's called a 'consultation', this is the regulator setting out its plans. Its focus is a simple system, where firms must pro-actively reach out, to include the maximum number of people. Barring legal challenge (and there is some talk that firms are trying to make it difficult), our guess is there'll be few major changes.

This consultation is (hopefully) at the final stage and the FCA has said that it'll announce the final redress scheme rules in early 2026. At the moment, motor finance complaints remained paused, meaning firms aren't required to respond to them. This pause is due to lift on 31 May 2026 – however once the redress scheme is launched, any revised timeframes will be set out by the scheme.

BOOKING A HOLIDAY?

Travel companies ramp up advertising campaigns for the turn of the year, recognising this period as a prime time for travel. With enticing deals and promotions, early January often becomes a major selling season for the industry. Some deals and holidays are not what they seem with fake companies selling non-existent flight and accommodation.

HOW TO PROTECT YOURSELF

- **Book with Trusted Sources:** Use ABTA/ATOL protected agents or well-known platforms
- **Secure Payments:** Pay by credit card for protection; avoid bank transfers, Western Union, or gift cards.
- **Verify Deals:** If it's incredibly cheap, it's likely a scam. Check reviews for legitimacy.
- **Check Website Security:** Look for "https" and the padlock icon in the URL bar.
- **Beware of Urgency:** Don't let pressure tactics rush you into paying.
- **Research the Company:** Look for physical addresses, contact details, and check if they are a legitimate member of travel schemes.

What's Happening Next?

World Cup USA

In June, the Football World Cup will take place in the USA. Be mindful when buying flights and tickets as fraudsters will use the opportunity to defraud sporting fans using social media.

Also in 2026, big name acts Ariana Grande, Metallica, Bon Jovi and Take That are touring and tickets demand is likely to be high.

To stay ahead of the scammers:

- **Only buy tickets from the venue's box office, the promoter, an official agent or a well-known and reputable ticket exchange site.**
- **Should you choose to buy tickets from an individual (for example on eBay or on a social media), never transfer the money directly into their bank account but use a secure payment site such as PayPal.**
- **Paying for your tickets by credit card will offer increased protection over other payments methods, such as debit card, cash, or money transfer services. Avoid making payments through bank transfer or money transfer services, as the payment may not be recoverable.**

FIFA WORLD CUP 2026

North East
RECCC
Regional Economic Crime Coordination Centre

North East
ROCU
Regional Organised Crime Unit Network

For more information search 'nerccu police'

BUILDING RESILIENCE AGAINST FRAUD

How to report

Police

All Fraud in the UK is reported to the police at Report Fraud by phone or online:
www.reportfraud.police.uk
0300 123 2040

Report Fraud is the central reporting point for all reports of fraud, your local police force will be informed by Report Fraud

Banks

Dial 159 (Stop Scams UK Anti-Fraud Hotline)
An automated line which Takes you through to your Bank's Fraud team .

For alternative ways of contacting your bank only use the contact details on your bank card or the official website.

Emails

Forward Fraudulent emails to
report@phishing.gov.uk

Phone Numbers

Forward phone numbers Sending you Fraudulent Messages or calls to **7726**

Handling Instructions

Distribution List
NEROCU
North East Police Forces

Provenance: Available upon request.

Protective Marking	**Official – Law Enforcement**
Version	**Final**
Purpose	**Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports and open source which have not been verified as true and accurate accounts.**
Owner	**NEROCU**
Authors	**Claire Hardy– Economic Threat Desk Analyst** **Nicola Lord –Cyber Threat Desk Analyst** **PC Brian Collins – Engagement Officer**
Reviewed By	**Sgt Emma O'Connor**

Handling Instructions
This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by NEROCU in confidence and may not be shared other than with the agreed readership/handling code without prior reference to NEROCU. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 2018.
The cover sheets must not be detached from the report to which they refer.