

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 July 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



- Action Fraud: Regional Cyber Summary
- Action Fraud: Regional Fraud Summary
- Engagement Events

Contents

Looking Forward




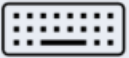









- Horizon Scanning
- What's Happening Next

North East Cyber Crime July Summary

**SLIGHT INCREASE THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR**



Total Cyber Reports (compared to July 2024)		 177 (+2.9%)
	Hacking -Social Media and Email	 136 (-2.9%)
	Hacking - Personal	 27 (+92.9%)
	Computer Virus/ Malware	 10 (+233%)
	Hacking Extortion	 4 (-69.2%)
	Denial of Service Attack	 0 (-200%)

Social Media: How to use it safely

Social media is a great way to stay in touch with family, friends and keep up to date on the latest news. However, it's important to know how to manage the security and privacy settings on your accounts, so that your personal information remains inaccessible to anyone but you

Scammers will make fake accounts and/or hack real accounts to use them to commit a range of fraudulent activities. Many sites have a process to verify accounts, such as verified badges for Instagram and Facebook. This can help to identify real accounts against fake accounts pretending to be a well-known person.

Online gaming for families and individuals











It is important to safeguard yourself and your personal data when playing games online. Online games can be played using various devices so keeping them secure can help prevent you falling victim to a criminal.

Guidance for practitioners supporting victims of technology-facilitated domestic abuse

Technology-facilitated abuse relates to the use of technology to facilitate domestic abuse offences, such as incidents of control, coercion, threatening behaviour, violence or abuse. The NCSC offers bespoke guidance to support practitioners working with victims of technology-facilitated domestic abuse, stalking and harassment.

North East Fraud July Summary

Total Fraud Reports (compared to July 2024)	 947 (+32.3%)
--	---

TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
	Advance Fee Frauds	 208 (+197%)
	Online Shopping and Auctions	 150 (-4.5%)
	Other Consumer Fraud	 97 (+61.7%)
	Investment Fraud	 83 (+112.8%)
	Cheque, Plastic Card and Online Bank Accounts	 44 (-18.5%)

£2.5 Million loss
this month (-26.9%)

INCREASED THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR



Contract Termination Experts

There have been more reports this month regarding victim's being charged when trying to cancel subscriptions. Last month, we highlighted a company called 'Termination Experts' requesting money for carrying out a service never requested. Victims were told they owed money for cancelling subscriptions to Netflix, Amazon Prime and gym subscriptions after never using their service. This month, victims report being charged whilst cancelling Microsoft subscriptions.

Winter Fuel Payments Messages

This month's increase in 'Advance Fee Frauds' is driven by the number of reports of fraudulent text messages about winter fuel payments. 48 victims reported receiving messages claiming to be from the DWP asking the recipient to click on a link to apply for their winter fuel allowance and enter personal and bank details. Victims report how credible the website looked. It asked their full name, mobile number, email address and full bank details (name on card, long card number, expiry date and security number on the back). The spoofed site said a £1 payment was needed to verify their bank details and would be refunded. Instead, transactions appeared in the victims' accounts for unknown purchases.

Bank Impersonation calls

There have been lots of reports this month from victims who have received fake calls from their banks. They have been asked to provide one time passcodes in order to prevent alleged fraudulent payments going out of their accounts. Once the code is provided, the pending transaction to the fraudster takes place. This is increasing as criminals try to bypass security measures put in place by financial institutions.

ENGAGEMENT EVENTS

Below is just some of what the team have been up to this month...

This month the team have been to Citizens Advice- Gateshead and delivered Fraud Awareness sessions to staff. The Department for Work and Pensions customers and staff at Darlington took part in a Fraud Awareness workshop.

Newcastle Building Society Darlington invited us to their monthly customer fraud session and got involved themselves with some staff CPD afterwards.

The team have started visiting Bread and Butter Thing Hubs where members of the community pick up food parcels.

We have recorded a podcast for Darlington Extra, watch out for our episode on Spotify.

Fraud Roadshows with Barclay's local specialists and other agencies have taken us to the Dolphin Centre in Darlington, Hartlepool Community Hub, Nissan and The Galleries in Washington this month.

Tynedale Lions took part in a Fraud Foundation workshop.



Get Charged For Cancelling Your **Subscription Plan**



MONTHLY



ONE OFF PAYMENT TO A
CRIMINAL

MOST POPULAR

- Most companies will not charge you for cancelling your subscription unless stated in your initial contract.
- You do not need a third party to cancel your subscription, use the legitimate website for the company and you will find instructions on how to cancel.
- If you find yourself on a website asking for your details to cancel on your behalf do not fill them in. There are websites that are collecting this data about you which they then use to say they have cancelled on your behalf with a demand to pay a fee.
- This is then followed up by further demands for payments and fees added on for non payment. This sometimes then leads to 'debt collection' letters to try and scare you into paying the money.
- Do not pay these demands when you have not used these services.



Subscribed ▾

Find out more:
gov.uk/stopthinkfraud



STOP! Turn on 2-step verification **THINK FRAUD**

**DO NOT SHARE TWO
STEP VERIFICATION
CODES OR ONE TIME
PASSWORDS.**

**THEY ARE IN PLACE
TO PROTECT YOUR
ACCOUNTS AND ARE
NOT TO BE SHARED
WITH ANYONE, NO
MATTER HOW
TRUSTED.**

Turn on 2-step verification (2SV) and double
the protection on your most important accounts,
especially your email and social media.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
❑❑❑ actionfraud.police.uk ❑❑❑

STOP!
THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

Don't get taken for a ride



Criminals are using social media to advertise 'cancelled' driving tests for sale. Facebook groups are being used to market the 'cancelled' driving tests and once the victim makes the payment no test is booked then they are blocked and deleted from the group.

What can you do to avoid this?

- Do not take recommendations from strangers or online forums. Ask friends going through the process.
- Act with extra caution and do not book driving tests using social media.

The Driver and Vehicle Standards Agency (DVSA) does not run, approve, or endorse any cancellation finder apps or services. GOV.UK is the only official driving test booking service.

Student guide to

FRAUD

If you would like a PDF version of our 'student guide to FRAUD' visit our website [2905 NEROCU-Student-fraud-booklet.pdf](https://www.nerocu.org.uk/2905-Student-fraud-booklet.pdf) or contact one of the team.

We will be visiting Colleges and Universities across the region over the coming months to speak with students and staff.



Student guide to

FRAUD

What are the top 'Fraud Types' to look out for as a student?

1. Investment Fraud :

Criminals will target students looking to make quick-wins with available cash through cryptocurrency or schemes with a promise of high return investment. They are targeted through social media and online where many investment schemes operate.

2. Employment Fraud :

Students looking for job opportunities can be targeted by Fraudulent adverts aimed at stealing personal information or money. Students might be asked for an upfront payment for a fake consultation or extra help finding a job.

3. Accommodation Fraud :

Criminals often target students looking for university accommodation. Fraudsters ask students to pay fees in advance without seeing a property first, and as a result they lose money as well as somewhere to live.

4. Online Shopping Fraud :

Often criminals will create fake websites or replicate legitimate online stores to get people to provide their personal and financial information for a purchase that isn't real. This can lead to those details being used for criminal activity.

5. Ticket Fraud :

Fraudsters will use opportunities, like highly in-demand events, to target students by selling fake tickets. Students looking for cheap deals for freshers' events can also be targets.



Three suspects arrested after targeted Investment Fraud strike in Newcastle.

The trio of men, 28, 30 and 62, have been arrested as part of a continued clampdown around investment fraud.

On Tuesday 5th August officers from the North East Regional Organised Crime Unit (NEROCU), supported by Northumbria Police, carried out strikes on addresses on Greenside Close, Wallsend and Pinegarth, Ponteland.

The targeted police operation saw an early morning wake-up call for the suspected Fraudsters who are believed to be linked to a wide-scale scam operation across the UK.

Searches of the properties resulted in the discovery of a large quantity of cash estimated at over £3k, a quantity of Cannabis and a huge haul of expensive alcohol seized.

The trio were arrested on suspicion of Fraud and money laundering offences. They have since been released on police bail while enquiries continue.



Durham Police Cyber Crime Team

🤔 struggling with the ever changing digital world and at a loss for how to keep your children safe online?

Join us online for an informative 30 minute session designed to help parents navigate the challenges of raising children in today's digital world. We will cover topics such as online safety, screen time management, and fostering healthy tech habits. 💻 📱 👍

💎 Don't miss this opportunity to learn valuable tips and strategies to support your child's digital well-being. Register now to secure your spot!

Dates & Times:

14th August, 16:00 - 16:30

18th August, 12:00 - 12:30

21st August, 13:00 - 13:30

2nd September 10:00 – 10:30

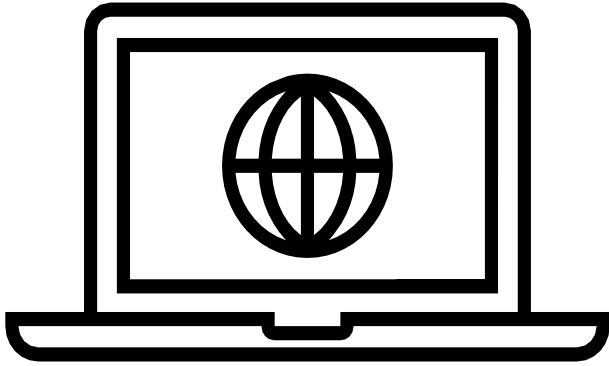
4th September 4:30 – 5:00

Sign up here 👉 [Click to get your webinar tickets from Eventbrite](#)

Links to attendees will be sent out the day before each event. Please check your junk mail.

Horizon Scanning

Monitoring Threats



Poundland, New Look, River Island and other popular high street stores have announced they are in financial difficulty and some stores have announced closures. This could lead to fake websites being created and advertised as 'closing down sales' as we have seen in the past when companies have gone into administration.



What can you do to protect yourself from fake websites:

- Always use a credit card for large purchases over £100, they offer more protection through section 75 of the consumer credit act.
 - Check you are using genuine website domain addresses when shopping online.
- Check for a padlock in the address bar, this means it is likely a secure website and offers more protection.
- Double check the website before entering any details or making a purchase, take a few minutes to browse for anything suspicious.

What's Happening Next?



Criminals use a variety of websites and social media platforms to advertise properties, often at attractive costs and in desirable locations. The offers will appear professional and genuine, accompanied by the expected photos, reviews and contact information.

Due to high demand for accommodation, the criminal will apply pressure and students will often be asked pre-viewing, to pay upfront fees in order to secure the property, however once the person pays the fees they find that they have been scammed and the person advertising the property does not own it and they are left with no accommodation and have had their money stolen.

What can you do to protect yourself?

- Try to view the property in person if this is possible.
- Check any websites contact details and geographical addresses.
- Reverse image search accommodation photos.
- Discuss with family and friends before going ahead with a payment .



What can we do for you?

If you think any groups that you attend or run could benefit from the services we offer, please get in touch at reccc@nersou.police.uk



Advice
Stalls and
Events



A link between
yourselves and
NEROCU



Monthly
Newsletter



Staff
CPD/Inputs/
Workshops



 For more
information
search 'nerccu
police'



Scan to visit our website



BUILDING RESILIENCE AGAINST FRAUD

How to report



Police

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

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



Emails

Forward Fraudulent emails to
report@phishing.gov.uk



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.



Phone Numbers

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

Handling Instructions

Distribution List
NEROCU
North East Police Forces

Copyright © NEROCU 2025 Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this document, it is provided in good faith on the basis that NEROCU and it's staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to NEROCU. Should you or your police force hold information, which corroborates, enhances, or matches or contradicts or casts doubt upon any content published in this document, please contact NEROCU. Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

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	Megan Turner – 3P Officer Claire Hardy– Economic Threat Desk Analyst Nicola Lord –Cyber Threat Desk Analyst
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.