

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 August 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




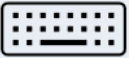









- Horizon Scanning
- What's Happening Next

North East Cyber Crime August Summary

**INCREASED THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR**



Total Cyber Reports (compared to August 2024)		 154 (+16.7%)
 Hacking -Social Media and Email		 125 (+25%)
 Hacking - Personal		 18 (+12.5%)
 Hacking - Extortion		 8 (+14.3%)
 Computer Virus/ Malware		 2 (-77.8%)
 Hacking - Server		 1 (+100%)

NCSC: Free Cyber Action Plan

The NCSC have a free cyber action plan which can help you identify any areas where you might need to improve your personal cyber security.

The aim is to provide individual guidance and learn how to secure your devices, safeguard personal data, and stay secure online.

The action plan can be completed on the NCSC website here -
[Cyber security advice for you & your family - NCSC.GOV.UK](#)

Jaguar Land Rover Cyber Attack












There has been a news of a cyber incident impacting Jaguar Land Rover. The cyber attack, which first came to light on 1st September, forced the manufacturer to shut down its computer systems and close production lines worldwide. Jaguar Land Rover is thought to have lost at least £50m so far as a result of the stoppage but experts say the most serious damage is being done to its network of suppliers, many of whom are small and medium sized businesses. It is suggested that the hackers may have taken data. A statement from the NCSC regarding the incident can be accessed here - [NCSC statement: Incident impacting Jaguar Land Rover - NCSC.GOV.UK](#)

North East Fraud August Summary

£3.9 Million loss
this month (+77%)

INCREASED THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR



Total Fraud Reports (compared to August 2024)		 788 (+25.3%)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
	Advance Fee Frauds	 133 (+98.5%)
	Online Shopping and Auctions	 126 (+7.7%)
	Other Consumer Fraud	 78 (+52.9%)
	Investment Fraud	 65 (+103.1%)
	Cheque, Plastic Card and Online Bank Accounts	 39 (-9.3%)

Cash Codes



Some banks have introduced the facility to withdraw cash from ATMs without your bank card, fraudsters are taking advantage of this.

Cash codes give you the ability to withdraw cash without your bank card by generating a code through your Banking App, this can also be used to help out a stranded family member who has lost their purse/wallet for example by directing them to an ATM and providing them with the code so that they can withdraw the money to get home which is a great idea.

Fraudsters are targeting victims in the North East claiming to be from their bank to highlight suspicious activity. Victims were informed new cards would be sent to them but in the meantime, they could access instant cash until the card arrived by using the cash code function. The Fraudsters explained they would get everything set up and as part of this the victim would have to supply the cash code from their banking app to them to test that it was working, the victim's supplied the fraudsters with the code which was then used to steal the victims' money.

Your bank will never request this information. If you receive an unexpected call, hang up and call 159 from a separate line, if possible, to verify the call.

Cold Calling Rogue Tradesmen

There has been an increase this month in the number of rogue traders cold calling at properties across the North East. Mostly offering for gardening work or roofing repairs. A total of £29,400 has been stolen from elderly victims with an average age of 80. In one instance, the victim paid using a card payment machine but did not see the amount entered by the fraudster as the display was blocked.

ENGAGEMENT EVENTS

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

This month the team have delivered Fraud Awareness sessions to The Withcraft Arts and Crafts Group, Middlesbrough Soroptomists, Citizen's Advice Gateshead, Band Tees Valley Music Services and Deaflink British Sign Language Group.

Fresher's Events have been ongoing throughout the month at Prior Pursglove College, Middlesbrough College, Northumbria University and Stockton Riverside College with further freshers happening throughout the rest of September.

The team attended the Fraud and Fakes Project ran by Pallion Action Group, Nissan Staff Wellbeing event and have attended various The Bread and Butter pop ups across the region to give Fraud Awareness advice to those who use the services.

Sunderland Fans club hosted an event at the Galleries Washington where the team attended and handed out leaflets and provided advice to members of the public.



International Students

are often targeted with Fraud claiming they face deportation/are part of an investigation, there are problems with their visa or stating they need to pay fees.

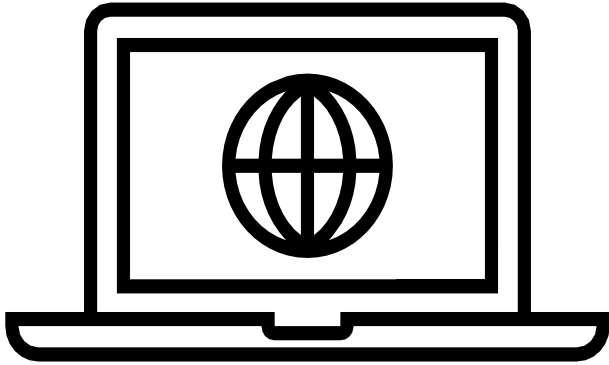
There have also been various tactics used to obtain money from the student or the students family in the form of fake kidnaps and ransom, sometimes even contacting the families of the student.

Please make your friends and family aware that they could be targeted and ask them to contact you directly if this happens, remind them not to send any money if they are suspicious.

The RECCC continue to work with Universities in the North East, speaking to staff and students to raise awareness and give advice on how to keep themselves safe.

Horizon Scanning

Monitoring Threats



Great North Run Medals

Thousands of Great North Run Medals were given out with an error where they showed Sunderland instead of Newcastle. They are being listed online from £35 to £5000 due to how unique they are. It is likely that criminals will look to exploit this. If buying a medal from social media or an auction site please be aware, it could be a scam.



Contact for personal details on social media

There has been an increase in reports from members of the public stating that they have been asked to verify themselves on Facebook by sending documentation such as a picture of their driving licence or passport and a selfie. Please also watch out for anyone sending or asking to be sent cash codes.

Be aware that if you are being asked to provide this, it is most likely a scam.

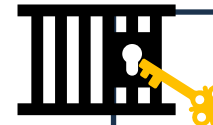


What is a 'Money Mule'?

What is a 'Money Mule'?

Criminals who have illicit funds often target people to launder their money. This was mainly students but recently there has been an increase in other age groups being approached. It can be via social media, texts, in person, online or via email, they may make an offer of a job to 'earn quick/easy cash'. However, they will request that money is passed through the persons bank account to 'clean it', this is illegal and classed as money laundering and could result in imprisonment.

As usual throughout September, October and November we are running our Fraud Roadshows, attending freshers along with other events to raise awareness amongst students who are often targeted and approached to be a 'money mule'.



**14 YEAR
PRISON
SENTENCE**

KNOW THE SIGNS :

- Job offers using social media or even job websites offering 'quick cash' or 'easy money'.
- Someone requesting to use your bank account/transfer money.
- Someone you do not know asking for your bank details.



Cost Of Living Fraud



What has been seen so far? :

As it has been announced energy bills are due to rise again for the autumn and winter, we expect to see an increase in cost-of-living type Frauds, where criminals are looking to exploit those in need of financial support. Last year there were Smishing texts with links requesting personal details to receive a £900 cost of living payment, with more expected to be seen within the coming months along with DWP and HMRC smishing texts likely to increase.

What can you do to protect yourself? :

- Do not click any links within texts or emails and try to use the legitimate website address.
- Always check it out first and do not enter any personal details.
- If in doubt, ignore it!
- If you do require financial help, contact your energy company to see what support they can offer.
- Be wary of anyone contacting you via text, phone call or email claiming to be from Ofgem or an energy company.

What's Happening Next?



Online Shopping Fraud remains the highest reported Fraud in the North East which means the region should be extra vigilant in the run up to Christmas which are the busiest months for people spending money online.

Christmas is approaching and people will be on the lookout for bargains.

There are upcoming shopping events such as Black Friday and Cyber Monday where people will be increasing their spending putting more people at risk of becoming a victim of Fraud as they seek the latest deals. With discounts being offered across lots of websites during this time it makes those 'too good to be true' deals look more believable.

Advice :

- Use a credit card where possible (especially for large purchases) as they provide more protection under Section 75 of the Consumer Credit Act.
- Read reviews of the website you are purchasing from, be wary of new websites that have only been online for a short time.
- Always type the web address into your browser and be wary of accessing links through unsolicited emails.
- If you're asked to make a bank transfer instead of using a secure payment system be extra cautious.



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@durham.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.