North East ROCU
Regional Organised Crime Unit Network

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 May 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.

North East RECCC Regional Economic Crime Coordination Centre

NERCCU North East Regional Cyber Crime Unit

Contents

Looking Back

Contents

Looking Forward

North East Cyber Crime May Summary

REDUCED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Cyber Reports (compared to May 2024)	**163 (-2.4%)**
Hacking -Social Media and Email	**109 (-16.2%)**
Hacking - Personal	**29 (+81.3%)**
Computer Virus/ Malware	**18 (+80%)**
Hacking Extortion	**7 (-22.2%)**
Hacking Server	**0 (100%)**

New warning issued this month warning the public to continue reporting phishing emails

As of April 2025, the total number of phishing scams reported to the Suspicious Email Reporting Service (SERS) reached over 41 million since its launch in April 2020. This has resulted in 217,000 scams being removed from across 393,395 websites pages by the National Cyber Security Centre.

You can report suspicious-looking emails or messages.

- Forward emails to report@phishing.gov.uk
- forward spam text messages to 7726

Recovering a hacked/compromised accounts

There is guidance available from the NCSC to help you recover accounts which have been compromised. Don't forget about accounts/apps you use for shopping / booking holidays or trips away.

If you have any old accounts that you no longer use or have removed an app which you won't use again – make sure these accounts are deleted as old accounts can lie vulnerable especially if they have a weak password or no 2 factor authentication applied. Simply deleting an app won't get rid of your account, you will need to go into the settings and confirm that you want to delete your account.

North East Fraud May Summary

£5.2 Million loss this month (+79%)

INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Fraud Reports (compared to May 2024)	**730 (+11.2%)**
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Online Shopping and Auctions	**147 (-10.9%)**
Advance Fee Frauds	**127 (+53%)**
Other Consumer Fraud	**70 (+22.8%)**
Investment Fraud	**57 (+83.9%)**
Cheque, Plastic Card and Online Bank Accounts	**41 (-6.8%)**

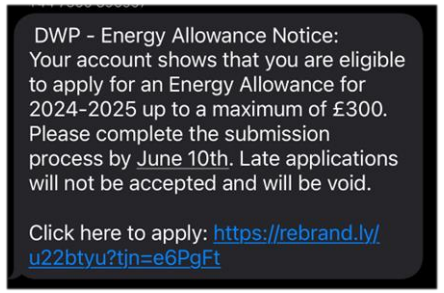
PPI Scam Calls
Victims report receiving calls from companies regarding PPI claims. After asking for personal and banking details, the fraudsters claim a courier will deliver a cheque for over £6000 but the victim would need to pay £100 onto a Paysafe card for the costs to be reimbursed later.

Job Scam Continue
As GCSE and sixth form students finish their exams, there will be an increase in the number of young people looking for summer work. Scam Adverts on social media have increased in circulation to target job seekers. 27 victims have reported losing a total of £63,591 in May 2025 from this increasingly frequent Fraud type. Adverts are vague offering online, remote task-based work rating Tik Tok videos, hotels and moving cryptocurrency.

Such scams are contributing to the increase in reporting for Advance Fee Frauds.

Amazon Impersonation Frauds
There has been an increase in the number of calls naming Amazon in the call script. 14 victims report receiving calls from their bank stating that there were mobile phones in their Amazon baskets and a code would be required to prevent the fraud.

DWP Energy Allowance
Fake text messages from the DWP regarding winter fuel allowance applications have been replaced with a generic message pushing residents to apply for an Energy Allowance urgently.



North East Fraud May – Continued

Third Party Websites for ESTA's

This month, victims have reported losing money and potential personal details after searching for and using websites they believed to be official to apply for Visas for the US. The websites are appearing at the top of search browsers and charge more than the actual cost and request a high level of personal passport and banking information likely for use in identity Fraud.
Similar reports regarding the DVLA website when applying for driving licences have been received.

International Students Targeted

North East University International students have had significant amounts of money taken after receiving calls from fraudsters.

One victim received a fake call from their home countries Embassy about fraudulent banking activity and the other was told they were in trouble with UK Immigration & Visa authority and implicated in a crime in linked to money laundering with threats of deportation. To prevent deportation the victim has paid bail in 6 payments over several months.

The victim was monitored during the time of the fraud over Skype and Teams and made to show screenshots of communications to prove they hadn't contacted anyone. They were also made to delete social media apps.

New MO - Phone Contract Scam Twist

One victim was targeted in a phone contract scam using a fake job offer for the MO.

After applying for a job on Indeed and being told they were successful without interview, they received a call from the new manager about taking receipt of their work phone.

They were told that a phone would be delivered and they must provide give the courier with the pin then deliver it back via the closest store to ensure the phone will be used for work purposes only. After following the instructions, there was no further contact.

The offender must have used the personal details supplied by the victim during the job application process to take out the contract in their name.

Impersonation Fraud

A police Impersonation Fraud targeting an elderly victim used an unusual MO when communication was moved to a Whatsapp video call. The picture on the call displayed the Action Fraud logo to attempt to add legitimacy to the Fraud.

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

ENGAGEMENT EVENTS

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

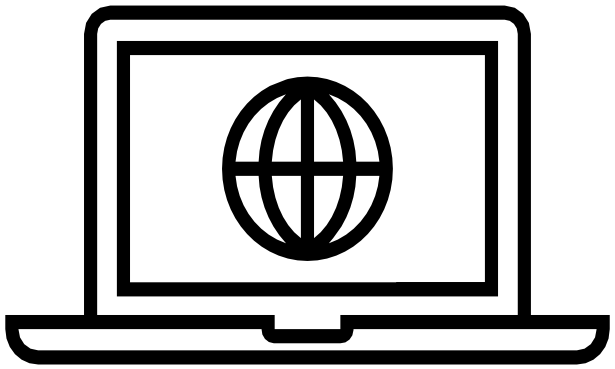
The team were invited back to the NHS health and wellbeing festival aimed to target staff at North Tees and Hartlepool Hospitals.

Citizens Advice across the region, The Voluntary Organisations North East Network and Cumbria, Northumberland, Tyne and Wear Trust have all received some staff CPD sessions in the from of Fraud Awareness Workshops.

Sessions have started in conjunction with Durham Digital Hubs to deliver Fraud Awareness sessions to staff across all 25 hubs.

Horizon Scanning

Monitoring Threats



Tik Tok job scams have been circulating. The text messages sent to victim's state there is a job earning thousands of pounds to watch and review TikTok videos. They are then asked to pay an amount of money to sign up and find out the ‘job’ does not exist. Job scams continue to target people in the North East so be vigilant when receiving ‘out of the blue’ job offers that are too good to be true.

There has been an increase in reports from people reporting that they have received a text claiming to be from the Department for Work and Pensions (DWP). The text states the person is eligible for an energy support grant or something similar and provides a Fraudulent link to click on to ‘claim’ the grant.

- Do not click on links sent through unsolicited texts or emails.
- If in doubt, contact DWP on a phone number you trust to check it out.

Travellers are being warned over fake ESTA websites

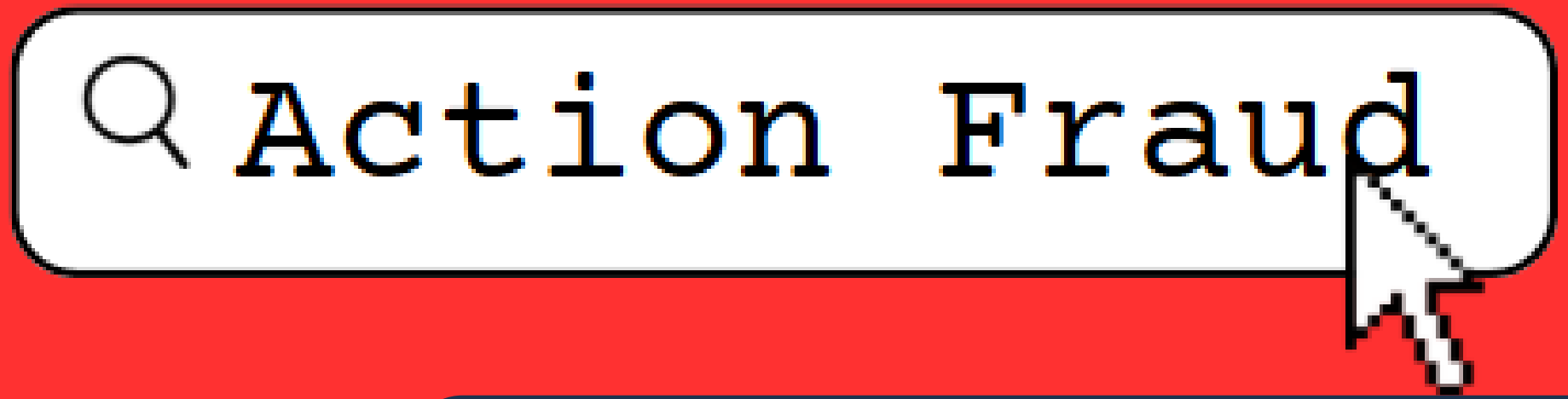
Reports have been received from victims applying for Electronic System for Travel Applications (ESTA), the websites look legitimate however charge the victim an inflated price with no ESTA submitted.

Do your research, make sure you know how much you should be charged before making a payment.

Check the URL to ensure it is secure and you are using the correct/official website.

Check any reviews for the website you are using and if in doubt do not enter any personal information or payment details.

Reports received that the use of the Action Fraud website and the Action Fraud logo has been used to target victims. The logo has been used on WhatsApp to try and add a layer of legitimacy to the contact.



- If using the Action Fraud website, check the URL is correct.
- Double check any communication received from ‘Action Fraud’.
- Be aware there are websites and communication that are being set up to appear like they are Action Fraud.

THINKING OF INVESTING IN CRYPTO?

Don’t assume it’s real

Professional-looking websites, adverts or social media posts don’t always mean that an investment opportunity is genuine. Criminals can use the names of well-known brands or individuals to make their scams appear legitimate.

Don’t be rushed or pressured into making a decision

A genuine bank or financial organisation won’t force you to part with your money on the spot. Always be wary if you’re pressured to invest quickly or promised returns that sound too good to be true.

Stay in control

Avoid uninvited investment offers, especially those over cold calls. If you’re thinking about making an investment, get independent advice and thoroughly research the company first.

Three in prison after Courier Fraud Investigation

Detectives from the North East Regional Organised Crime Unit (NEROCU) have secured jail sentences for organised criminals following their latest investigation into Courier Fraud.
On Friday (June 13), the three appeared at the same court and were sentenced as follows:

Imran Miah, years and six months imprisonment, Andy Munoz-Cadena, two years and six months imprisonment and Shamant Sheraji, two years and three months imprisonment.

Between October and November 2020, the three men contacted victims claiming to be police officers. These victims were informed that their bank accounts were under threat and encouraged to remove cash from their accounts to secure the money, which would ultimately be collected by a courier who attend their home address.

As soon as officers identified the criminal operation a police investigation was quickly launched and NEROCU officers, supported by Cleveland Police were able to identify the three men and swiftly arrested them before the victims lost any money.

All three were charged with Conspiracy to Commit Fraud by False Representation and, thanks to the strong evidence put before the court, all three men pleaded guilty at Teesside Crown Court.

No bank or police officer will contact them to withdraw money from their account. Hang up and call their bank's Fraud Team by dialling 159.

Find out more:
actionfraud.police.uk/ticketfraud

In 2024, £9.7M was lost to ticket fraud.

Follow our top tips to protect yourself against ticket fraud.

- **Buy safely**
- **Payment**
- **Account security**

STOP! THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

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

STAR
STAR.ORG.UK
SECURE TICKETS *from* AUTHORISED RETAILERS™

What's Happening Next?

It has been announced that winter Fuel Payments are making a return. This means that there may be scams targeting those who are struggling or hoping to be entitled to the payment. To find out if you are eligible, you can use the official government website.

The payment will automatically be made to everyone born before 22nd September 1959. If your income exceeds £35,000, HMRC will recover the payment after it is made. More details will be confirmed by the end of June 2025.

Advice

- Ensure you are using an official government website by checking the URL.
- Do not use companies claiming that they can apply for the payment on your behalf.
- Be mindful that fraudulent texts may be sent with fake links.
- Remember, the payment is automatically made to EVERYONE born before 22nd September 1959. Do not try to claim it or allow anybody to claim it on your behalf.

North East RECCC
Regional Economic Crime Coordination Centre

North East ROCU
Regional Organised Crime Unit Network

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.

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	**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.