

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 September 2026 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



- Regional Cyber Summary
- Regional Fraud Summary
- Engagement Events

Contents

Looking Forward



- Horizon Scanning
- What's Happening Next

North East Fraud September Summary

 **MORE REPORTS THIS MONTH THAN LAST**

Total Fraud Reports (compared to August 2026)		 693 (+3.4)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
	Online Shopping and Auctions	 135 (+6.3%)
	Advance Fee Frauds	 127 (-5.2%)
	Cheque, Plastic Card and Online Bank Accounts	 99 (+10%)
	Investment Fraud	 63 (-7.4%)
	Other Consumer Fraud	 46 (+39.4%)

Spoofing of Police telephone numbers

This month, victims across the UK have reported receiving calls from Police around fraudulent activity on their bank accounts. The callers are actually criminals impersonating police officers to gain access to their bank accounts or their money. The criminals have utilized ‘number spoofing’

This tactic manipulates the caller ID shown on the recipients' phone to make the call appear to come from a legitimate police number.

The criminals have used old telephone numbers for Cleveland, Durham and Northumbria police force’s which are no longer in use. This has happened to Forces across the UK.

If you receive a call claiming to be from the Police, be mindful that Police officers will never call you about your bank accounts and ask you to move money or withdraw cash or need access to your bank cards. Hang up immediately.

Whatsapp Screenshare

There is a growing trend with scammers using WhatsApp to take over mobile devices, gain access to banking apps and empty accounts.



Fraudsters impersonating police officers, banking staff and the FCA are cold calling victims about fraudulent activity on their accounts. They ask victims to move the conversation onto WhatsApp and are asked to share their screen. In some instances, the victim is asked to click on a link. Some victims have had their bank accounts emptied in this manner.

What it is...when criminals offer you tickets that are fake or do not exist

When you buy tickets from a fake website or agent, but the event and/or the tickets turn out to be bogus

Ticket Fraud



TICKET SCAMS

**Buy tickets
online securely**

HOW TO STOP IT:

Only buy from genuine box office, promoter, agent or ticket website

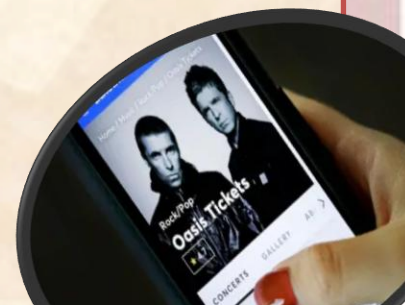
Avoid paying for tickets by bank transfer

Secure your email account with passwords and 2-Step Verification

Beware Ticket Spam

Look for STAR logo
Society of Ticket Agents and Retailers

www.star.org.uk



North East

ROCU

Regional Organised Crime Unit Network



Do you want to be a part of our growing Fraud Protect Community?

Contact us at:

RECCC@durham.police.uk

Engagement Events

This month we have visited and worked with:

- ✓ Anchor Housing
- ✓ Darlington College
- ✓ Prior Pursglove 6th Form
- ✓ Durham University
- ✓ Newcastle University
- ✓ Sunderland University
- ✓ Northumbria University
- ✓ Northern School of Art
- ✓ Lloyds Halifax Banking Group
- ✓ Middlesbrough College
- ✓ Saltburn Library
- ✓ Northumbria Veterans Network
- ✓ Sunderland College
- ✓ Northumberland College



North East



Regional Organised Crime Unit Network

Do you want to be a part of our growing

Fraud Protect Community?

Contact us at:

RECCC@durham.police.uk



What's Happening Next?

Next month...

- ✓ Fraud & Scams Talks and Fraud Protect Roadshow at Gateshead Business Expo
- ✓ Fraud Watch Roadshows at Lloyds & Halifax Banks – check your local branch for info
- ✓ Fraud Watch Roadshows at Durham University Colleges – ask your college for dates and times
- ✓ Fraud Watch Talks at Warm Welcome Groups in Stockton and Gateshead Veterans
- ✓ Fraud Protect Online Sessions with NHS
- ✓ Digital Inclusion with Age UK in Guisborough
- ✓ Fraud Protect Workshops with Northumbria Police Cadets and students at Darlington College and Redcar & Cleveland College



Email and social media hacking

How to protect yourself



Email and social media hacking are the most reported forms of cyber crime in the UK. Here are some useful tips on how to stay safe on social media and how to secure your accounts against hacking.



How to protect yourself:

- Use **passkeys** wherever they are available. They are more secure and easier to use.
- Where passkeys are unavailable, use **strong passwords**, for example generated by a password manager and **enable 2SV**.
- Think about who has access to the content you're posting. Make sure your **privacy settings** are configured so that it's only visible to the people you want to see it, for example only your friends.
- Try not to share too many **personal details** that a fraudster could use to build a picture of you. They can use facts such as your birthday, where you live, family relationships or pet names to steal your identity or make their fraud more convincing.



Tell the police about cyber crime and fraud at **reportfraud.police.uk** or by calling **0300 123 2040**

reportfraud.police.uk

@reportfrauduk

BLACK FRIDAY – NOVEMBER 27TH - CYBER MONDAY – NOVEMBER 30TH

DON'T LET A DEAL BECOME A SCAM

⚠ Fake offers, phishing messages and copycat websites spike during big sales.

▶ RED FLAGS

- “Too good to be true” prices or countdown pressure
- Unexpected delivery, refund or payment messages
- Web addresses with misspellings or odd domains
- Requests for gift cards, bank details or one-time codes

🛡 SHOP SAFELY

- Type the retailer’s address yourself or use its official app
- Check the seller, reviews, returns policy and final price
- Pay by card or a trusted payment service
- Use unique passwords and turn on 2-step verification

Never share a one-time passcode with someone who contacts you.

STOP • CHECK • THEN PAY

Already clicked or paid? Contact your bank immediately and report the message.



If you are a victim of fraud, contact report Fraud on
0300 123 2040



SCAM

Don't let them take over your account!

Scammers trick people into sharing their WhatsApp verification code or linking a new device. Once they have access, they can impersonate you, contact your friends and family, and even steal money.



WHAT CAN HAPPEN?



They impersonate you
Scammers can message your contacts, pretending to be you.



They can ask for money
Your friends and family might receive urgent requests for cash.



They can access your data
They may read your messages, see your personal information and use it for further scams.



You could lose your account
You may be locked out and lose control of your WhatsApp.

HOW TO STAY SAFE



Never share your verification code
WhatsApp will never ask you for this code.



Turn on two-step verification
Add a PIN and recovery email in Settings > Account.



Verify unusual requests
If a friend asks for a code or money, call them on their usual number.



Check linked devices
Go to Settings > Linked devices. Log out anything you don't recognise.



Don't click suspicious links or scan unexpected QR codes
They can give scammers access to your account.



STOP! THINK FRAUD!

A few seconds of checking could save your account, your contacts and your money.





 **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**



Police-Led, Business Focused
Here to protect businesses from online fraud
and cybercrime



**Supporting Sole traders, Micro, Small and
Medium businesses, charities and standalone
schools**

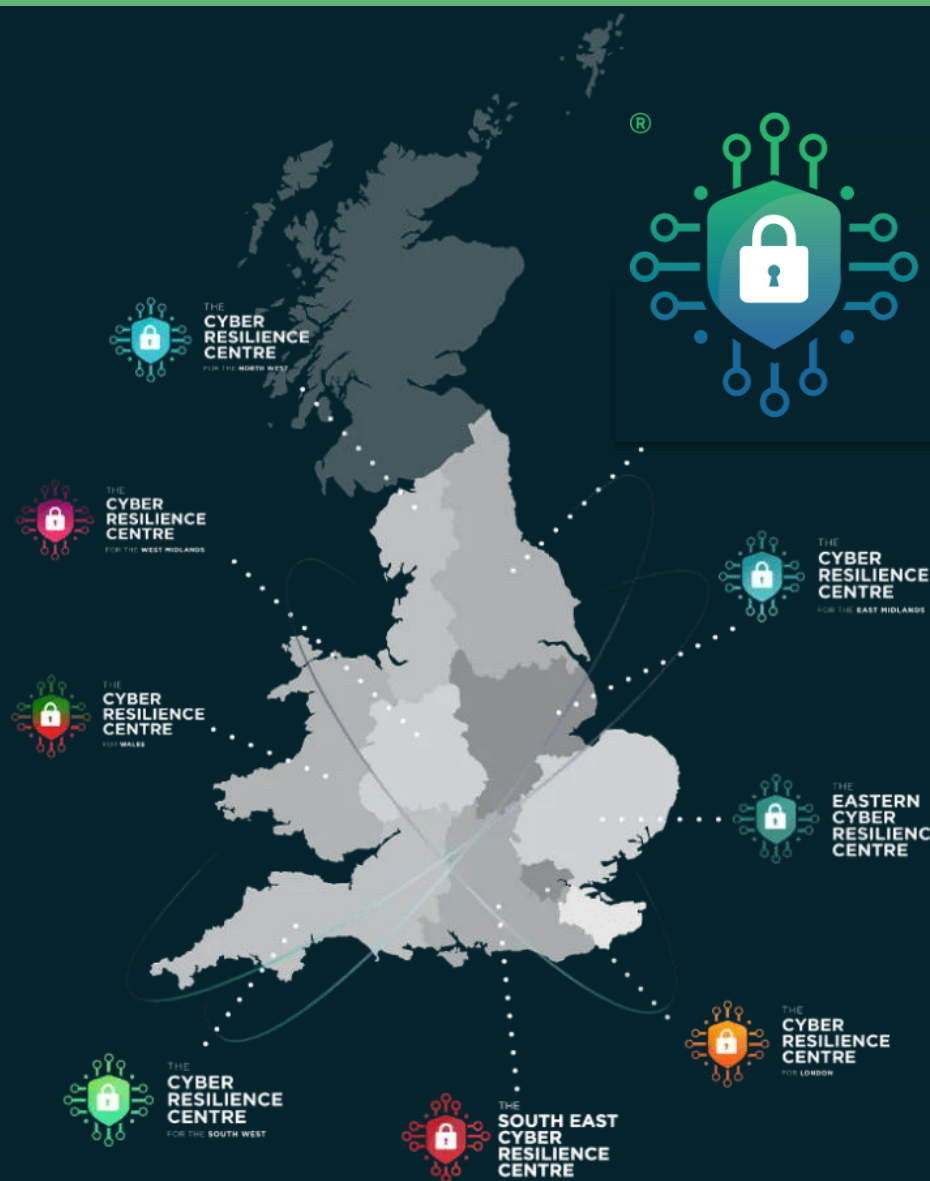


National Network of 9 Centres



Fully funded services:

- Free membership
- Monthly newsletter with tips and guidance
- Cyber security services
- 1-2-1 Support
- Links to Policing
- National Cyber Security Centre (NCSC) Resources



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE NORTH EAST
YORKSHIRE | THE HUMBER

**Join your local
CRC, the North
East Centre:**



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 its 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	Claire Hardy – Economic Threat Desk Analyst Nicola Lord – Cyber Threat Desk Analyst PC Brian Collins – Engagement Officer PC Andy Hampson – Engagement Officer
Reviewed By	D/Sgt Paul Mann

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.