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 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

Contents

Looking Forward

North East Cyber Crime July Summary

52% THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Cyber Reports (compared to July 2025)	84 (-52%)
Hacking -Social Media and Email	58 (-57%)
Hacking - Personal	10 (-62%)
Computer Virus/ Malware	4 (-60%)
Hacking - Extortion	3 (-25%)
Hacking – PBX/ Dial Through	7 (+700%)
Denial of Service Attack	1 (+100%)

WhatsApp Usernames

WhatsApp is rolling out a new feature "usernames". This is intended to improve privacy to allow communication without sharing your phone number. You will instead share your username and a key with people before they could message you, if you chose to use the username function. There won't be a public directory of usernames therefore individuals can't be contacted unless someone knows their username. While high profile organisations and individuals will be verified, there are concerns that criminals will use this opportunity to adapt usernames that closely match reputable companies, fake customer support or that of friends.

It is advised that individuals:

- Don't choose usernames that reveal personal information, such as your full name or dob.
- Be wary if someone contacts you unexpectedly.
- Check for signs that the account is genuine or verified before responding to any requests.
- Keep WhatsApp updated.
- Use 2FA to add an extra layer of protection.

NCSC new guidance for organisations:

The guidance, split into three sections, provides a structured approach to response and recovery. The first section focuses on the initial hours and days. The second stage involves building and implementing a recovery programme to restore core business functions. The final stage is the long-term rebuild, focusing on addressing the issues that contributed to the incident and rebuilding in a more secure and resilient way.

The full guidance is available at:
https://www.ncsc.gov.uk/collection/what-to-do-when-cyber-attacks-disrupt-your-organisation

North East Fraud July Summary

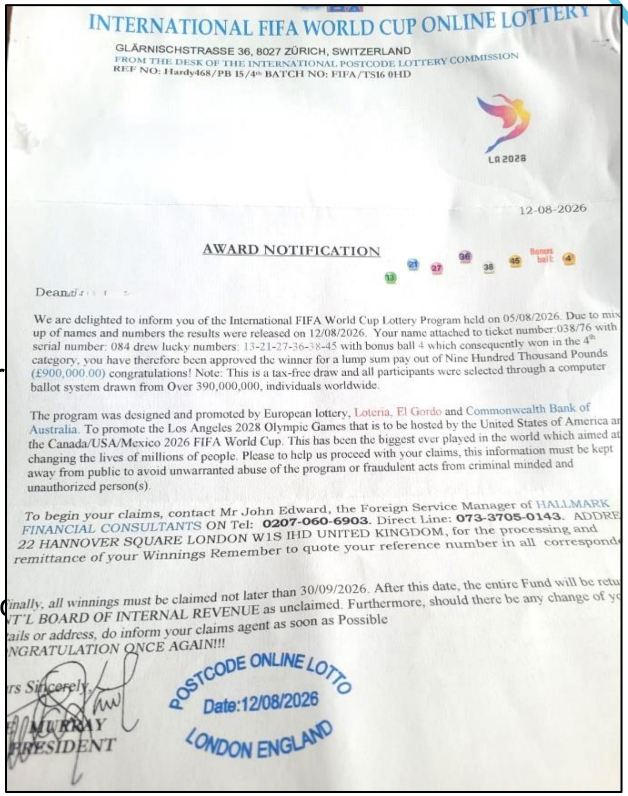
LOWER THIS MONTH THAN THE SAME MONTH LAST YEAR

Total Fraud Reports (compared to July 2025)	690 (-27%)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Advance Fee Frauds Cheque, Plastic Card and Online Bank Accounts	128 (-38%)
Cheque, Plastic Card and Online Bank Accounts	124 (+181%)
Online Shopping and Auctions	93 (-38%)
Investment Fraud	79 (-4.8%)
Other Consumer Fraud	39 (-60%)

Note: the large increase in **Cheque, Plastic Card and Online Bank Accounts is due to changes in national data recording with new data sources included**

Scam Letter through the post?

Although most fraud is now cyber enabled with victims targeted through their digital activity, be mindful that some Fraudsters still use letters through the post as a way of contacting victims.



INTERNATIONAL FIFA WORLD CUP ONLINE LOTTERY

GLÄRNISCHSTRASSE 36, 8027 ZÜRICH, SWITZERLAND
FROM THE DESK OF THE INTERNATIONAL POSTCODE LOTTERY COMMISSION
REF NO: Hardy468/PB 15/4th BATCH NO: FIFA/TS16 0HD

LA 2028

12-08-2026

AWARD NOTIFICATION

13 21 27 36 38 45 Bonus ball: 4

Dear

We are delighted to inform you of the International FIFA World Cup Lottery Program held on 05/08/2026. Due to mix up of names and numbers the results were released on 12/08/2026. Your name attached to ticket number:038/76 with serial number: 084 drew lucky numbers: 13-21-27-36-38-45 with bonus ball 4 which consequently won in the 4th category, you have therefore been approved the winner for a lump sum pay out of Nine Hundred Thousand Pounds (£900,000.00) congratulations! Note: This is a tax-free draw and all participants were selected through a computer ballot system drawn from Over 390,000,000, individuals worldwide.

The program was designed and promoted by European lottery, Loteria, El Gordo and Commonwealth Bank of Australia. To promote the Los Angeles 2028 Olympic Games that is to be hosted by the United States of America ar the Canada/USA/Mexico 2026 FIFA World Cup. This has been the biggest ever played in the world which aimed at changing the lives of millions of people. Please to help us proceed with your claims, this information must be kept away from public to avoid unwarranted abuse of the program or fraudulent acts from criminal minded and unauthorized person(s).

*To begin your claims, contact Mr John Edward, the Foreign Service Manager of HALLMARK FINANCIAL CONSULTANTS ON Tel: **0207-060-6903**. Direct Line: **073-3705-0143**. ADDRE 22 HANNOVER SQUARE LONDON W1S IHD UNITED KINGDOM, for the processing and remittance of your Winnings Remember to quote your reference number in all correspond*

inally, all winnings must be claimed not later than 30/09/2026. After this date, the entire Fund will be retu NT'L BOARD OF INTERNAL REVENUE as unclaimed. Furthermore, should there be any change of yo ails or address, do inform your claims agent as soon as Possible NGRATULATION ONCE AGAIN!!!

rs Sincerely,

MURRAY
PRESIDENT

POSTCODE ONLINE LOTTO
Date:12/08/2026
LONDON ENGLAND

A current letter is in circulation from the fake World Cup Lottery Fund telling the victim they have won a large amount of money on a lotter that they haven't entered.

People throughout the Northeast have received these letters and others like them. The letter asks the victim to contact them, either by phone call or by e-mail. This will be t obtain your personal or bank details. They might even ask the victim to send money to release your winnings!

- Never trust an unsolicited letter or email.
- Never use unknown phone numbers or email addresses.
- No matter how legitimate the letter may seem, always check details.

Mandate Fraud/Payment Diversion Fraud

This is where the criminal pretends to be someone who you owe money to

They target both individuals and businesses and use deceit to impersonate the person or organisation you are conducting business with

Resulting in the transferring of money or information to the criminal

A simple example would be that you owe money to a tradesperson for work carried out. The criminal has hacked somebody in that organisation or in the supply chain and sends you an email pretending to be the tradesperson you want to pay.
The criminal provide details for a bank account which is under their control

As soon as you send the money it is stolen

A recent example in the North East involved an unknown person pretending to be a solicitor

The unknown person contacted a property buyer and requested payment to a bank account that belonged to them and not the solicitor

Protect Yourself:

Check Email Addresses
Verify Payments

Signs To Look Out For Include Email Spoofing, Creating a Sense Of Urgency, Altered Payment Instructions & Impersonation Of Executives Or Suppliers

PAY POINT SCAMS

PAYPOINT SCAMS - offenders using barcodes displayed on mobile phones or tablets to fraudulently obtain cash from retailers

How the scam works

Offenders enter a retail premises and present a barcode on a mobile phone or tablet, claiming it authorises a cash payout…

To make the transaction appear legitimate, they may:

- ✓ Claim they are due a payment
- ✓ Display a company name or reference number on screen
- ✓ Pressure staff to process the transaction quickly
- ✓ In some cases, offer incentives for processing the transaction

These Scams have started to hit North East Retailers

The method is simple. The offenders rely on confusion, urgency and misplaced trust to walk away with cash

HOW TO STOP IT:

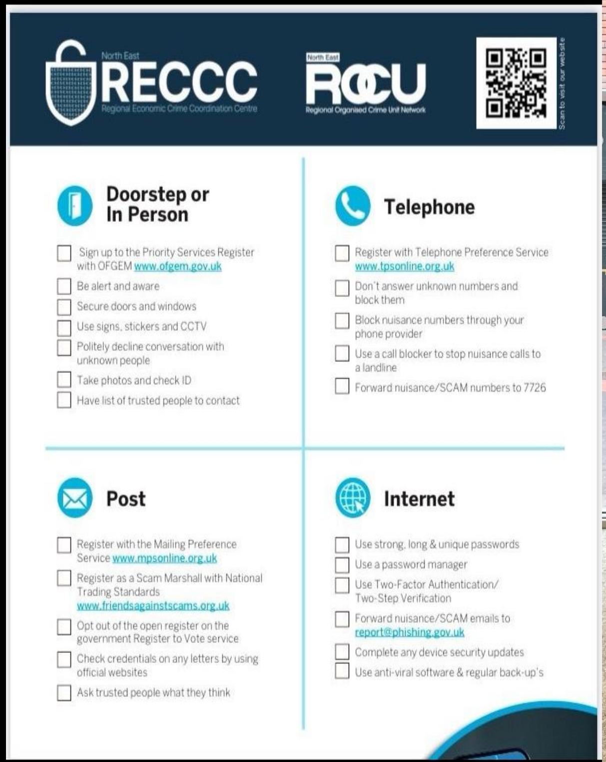
The fraud occurs when the offender persuades or confuses the cashier into acting against the instructions on the display, so…

- ✓ Trust what your PayPoint display is telling you
- ✓ Do not trust the person in front of you who is telling you otherwise
- ✓ Refuse Payment
- ✓ Report as a Crime

Engagement Events

This month we have visited and worked with:

- ✓ Gentoo Housing
- ✓ Barclays Bank
- ✓ Anchor Housing
- ✓ Durham University
- ✓ Age UK Durham
- ✓ Hazel Grove Residents Group Saltburn
- ✓ Northern Learning Trust
- ✓ Teesdale Valley Day Clubs
- ✓ Lloyds Halifax Banking Group


North East RECCC Regional Economic Crime Coordination Centre

North East ROCU Regional Organised Crime Unit Network

Doorstep or In Person

- ☐ Sign up to the Priority Services Register with OFGEM www.ofgem.gov.uk
- ☐ Be alert and aware
- ☐ Secure doors and windows
- ☐ Use signs, stickers and CCTV
- ☐ Politely decline conversation with unknown people
- ☐ Take photos and check ID
- ☐ Have list of trusted people to contact

Telephone

- ☐ Register with Telephone Preference Service www.tpsonline.org.uk
- ☐ Don't answer unknown numbers and block them
- ☐ Block nuisance numbers through your phone provider
- ☐ Use a call blocker to stop nuisance calls to a landline
- ☐ Forward nuisance/SCAM numbers to 7726

Post

- ☐ Register with the Mailing Preference Service www.mpsonline.org.uk
- ☐ Register as a Scam Marshall with National Trading Standards www.friendsagainstscams.org.uk
- ☐ Opt out of the open register on the government Register to Vote service
- ☐ Check credentials on any letters by using official websites
- ☐ Ask trusted people what they think

Internet

- ☐ Use strong, long & unique passwords
- ☐ Use a password manager
- ☐ Use Two-Factor Authentication/ Two-Step Verification
- ☐ Forward nuisance/SCAM emails to report@phishing.gov.uk
- ☐ Complete any device security updates
- ☐ Use anti-viral software & regular back-up's

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

Contact us at:

RECCC@durham.police.uk

Community Empowerment: Teesdale Valley Day Clubs

Day Clubs across Teesdale Valley have welcomed us through their doors during July & August 2026.

The Teesdale Valley Day Club organisation hosts events in their part of rural County Durham with the aim of reducing social exclusion and isolation.

Along with Age UK Durham and Durham Community Action, NEROCU Fraud Engagement Team have supported with a Fraud Watch Roadshow for the linked communities.

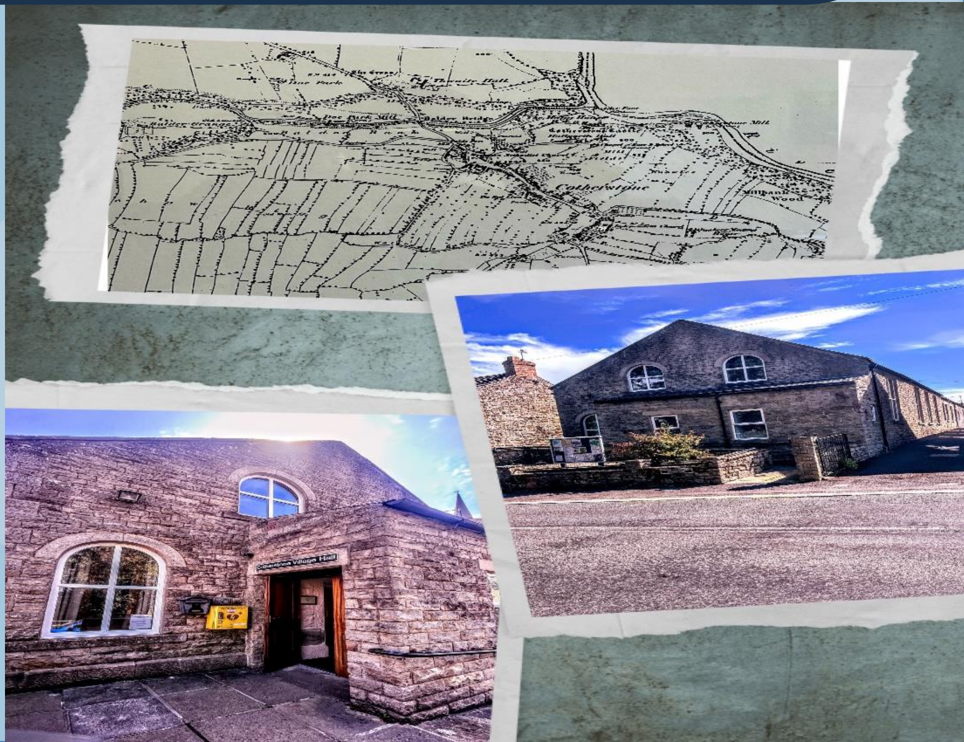
Fraud Watch Roadshows have been held in:

Cotherstone
Mickleton
Startforth
Winston
Middleton-in-Teesdale
Staindrop
Barnard Castle
Evenwood
Woodland

Do you want to know more about Fraud Watch Roadshows for your Community?

Contact us at:

RECCC@durham.police.uk



🏧 DON’T GET DISTRACTED - STAY SAFE AT THE CASH MACHINE

Criminals are targeting people at cash machines using various distraction techniques to obtain your card details, or to obtain your card.

These criminals will either –

- ask for help, or
- Talk to you while an accomplice swaps your card or takes your cash

🚨 **IF SOMETHING GOES WRONG**
Contact your bank immediately if your card or banking details may have been compromised

🚨 **IF YOU SEE SOMEONE ACTING SUSPICIOUSLY OR ARE CONCERNED PHONE 999.**

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

🛡️ **CASH MACHINE SAFETY**

DON’T LET DISTRACTION COST YOU
Someone may try to distract you while you use a cash machine to steal your **cash, card or personal details**.

🔴
STOP
If someone approaches or distracts you, stop your transaction.

🟠
PROTECT
Cover your PIN and keep your card and cash secure.

🟡
CHECK
Never accept help from a stranger or hand over your card.

🟢
LEAVE
If you feel uncomfortable, cancel the transaction, take your card and cash, and walk away.

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 student's 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 continues to work with Universities in the Northeast, speaking to staff and students to raise awareness and give advice on how to keep themselves safe.

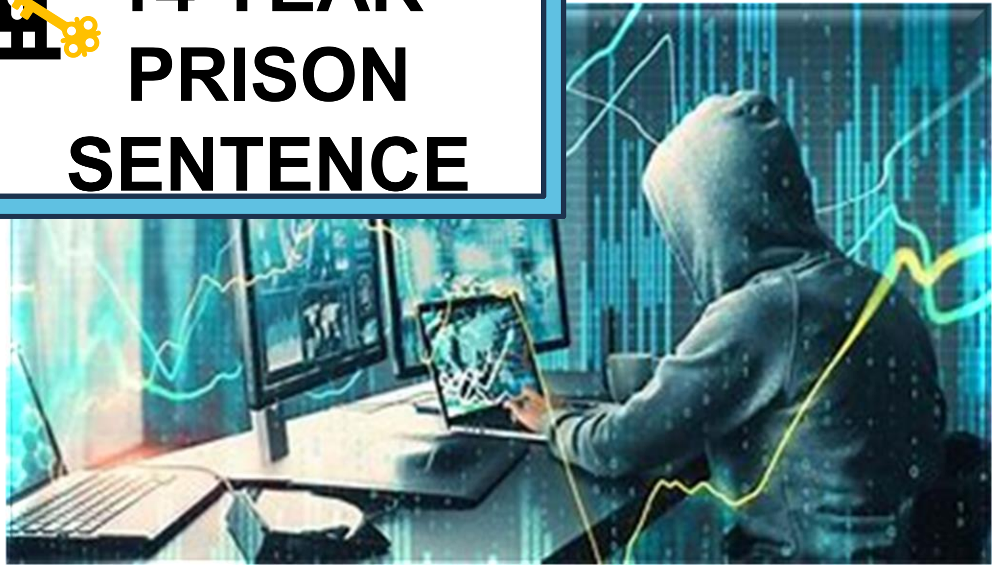
What is a ‘Money Mule’?

What is a ‘Money Mule’?

Criminals target people to launder their illegally obtained money. Students are still the most common demographic. It can be via social media, texts, in person, online or via email. They often make an offer of 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, could result in imprisonment and financial difficulties.

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



Be aware :

- Never let anyone use your bank account, either to receive or transfer money – even if they offer you money in return.
- Be wary of easy money or online job offers that ask you to move money on someone else’s behalf.
- If something ‘feels suspicious’ stop and ask for help from your bank or university.

What's Happening Next?

<u>National Campaigns:</u>

- ✓ Fraud by Abuse of Position campaign starts Monday 7th September
- ✓ The Take Five to Stop Fraud's next campaign, 'The Art of Impoliteness' launches on Tuesday 8th September 2026

<u>Regional Events:</u>

- ✓ Fraud & Scams Talks with Castles & Coast
- ✓ Fraud Watch Roadshows at Lloyds & Halifax Banks – check your local branch for info
- ✓ Fraud Watch Roadshows & Talks at Teesdale Valley Day Clubs – check your club for info
- ✓ Fraud Watch Roadshow & Talk at Seaham U3A
- ✓ Fraud Champions Course for Cleveland Police
- ✓ Fraud Protect sessions with Anchor Housing

If you'd like further information or would like to invite the RECCC to your event, please email us at:

RECCC@durham.police.uk

We are happy to help where possible to facilitate a strong and engaged North East Network.

Horizon Scanning

Monitoring Threats

Authorised Push Payment fraud

Authorised card payments are common within romance, investment and bank impersonation scams. Criminals will pretend to be your bank or the police and ask you to move funds to another account you hold. The criminal will likely already have stolen your card details and other data (usually via phishing emails) meaning they can trigger payments and ask you to approve them in your app, pretending this will reverse or block fraudulent attempts. These “me to me” transfers are not covered by APP fraud reimbursement rules. Never trust an unsolicited call or message and always check via a proven and trusted number for your bank.

TikTok Shop

Criminals have been setting up TikTok accounts and advertising items for sale on the TikTok shop marketplace. The items are actually on other online marketplaces (like Amazon) and the criminal seller uses compromised accounts to purchase the products, at no cost to themselves. Help prevent this from happening by changing your relevant password, which will likely have been compromised in a data breach. If you believe you are victim of this fraud, contact your bank immediately.

As always – if you receive an unexpected text / call / email, treat it with suspicion and do not trust it. Never click on a link. Verify any information via trusted means.

Think SCAM –

Stop – take 5 minutes

Check – look at the details

Ask – aske trusted people

Manage – report the issue to report fraud or police.

Report Fraud

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** **PC Andy Hampson – Engagement Officer**
Reviewed By	**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.