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 June 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 June Summary

SLIGHT INCREASE THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Cyber Reports (compared to June 2024)		**158 (+3.2%)**
	Hacking -Social Media and Email	**90 (-21.7%)**
	Computer Virus/ Malware	**36 (+200%)**
	Hacking - Personal	**23 (+43.7%)**
	Hacking Extortion	**8 (-20%)**
	Denial of Service Attack	**1 (+100%)**

Device Antivirus/Malware

This is software that's been made by someone so your computer, laptop, tablet or mobile phone doesn't work as it's supposed to.

In some cases, it also collects information or data saved on your device and passes it on.

Protect yourself

- Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.
- Take care downloading files. If you don't know someone who's sent you an email with an attachment, or you're not sure about a website offering a file to download, don't do it out of curiosity.

Spot the signs

- You're being offered or told to download something from a website that you haven't visited before and doesn't look legitimate, or from a stranger who's sent you an email.
- Your internet connection or the computer's general performance suddenly becomes very slow, you can't access files or programs, or you're unable to log in at all.
- There are signs other people have accessed password protected accounts, or your bank statements shows things you've bought or withdrawals you can't remember making.

Denial of Service Attack

A denial of service (DoS) attack is an attempt to overload a website or network, with the aim of degrading its performance or even making it completely inaccessible. Typically, a successful DoS attack will result in loss of availability of part, or all, of a system, and consume time and money to analyse, defend and recover from.

Reporting a DoS attack to UK authorities using the cyber incident signposting service helps inform the wider threat picture, to understand the prevalence, scale and impact of such attacks in the UK.

North East Fraud June Summary

£4 Million loss this month (+81%)

INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Fraud Reports (compared to June 2024)	**744 (+11.2%)**
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Online Shopping and Auctions	**128 (-3.0%)**
Advance Fee Frauds	**117 (+36.1%)**
Other Consumer Fraud	**88 (+57.4%)**
Investment Fraud	**62 (+87.9%)**
Cheque, Plastic Card and Online Bank Accounts	**33 (-32.7%)**

Investment Fraud

The number of Investment Frauds has almost doubled this month with North East victims reporting over £1 Million stolen. Most victims report seeing adverts for investments endorsed by professional figures such as Martin Lewis.

Fake News sites are fueling Investment Fraud globally. One cybersecurity firm has uncovered more than 17,000 fake news websites used to fuel global Investment Fraud campaigns spanning at least 50 countries. Threat actors often create fake news websites that closely mimic legitimate media outlets like the BBC, using familiar branding and layouts to appear authentic. These sites are promoted through paid advertisements on platforms such as Google and Facebook, typically featuring sensational headlines that promise "life-changing" investment opportunities or celebrity-endorsed cryptocurrency schemes.

Advance Fee Fraud Increases

Job Scams are driving the current increase in Advance Fee Frauds. Over the last few months, users report being inundated with messages and adverts on social media and mobile phones offering lucrative jobs which are fake. Victims now report receiving pre-recorded telephone calls from unknown mobile numbers asking them to add their number on WhatsApp. To report the calls, send CALL followed by the mobile number to 7726 and block the number off your handset

Courier Frauds

From mid June, there has been a rise in reported incidents of Courier Fraud across the North East. Over a two day period, Cleveland Police received two reports in which victims were targeted and handed over significant amounts of cash to people who had called them purporting to be police officers.

A joint operation was immediately initiated by the NEROCU, Cleveland Police and the Metropolitan Police.

This resulted the identification of a London-based suspected organised crime group. A robust response resulted in the arrest, charge, and remand of two suspects.

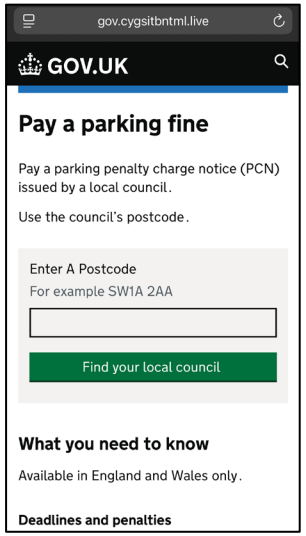
North East Fraud June Summary

Contract Termination Experts
This month, victims report receiving phishing emails from a company called 'Termination Experts' requesting money for carrying out a service they never requested. Victims were told they owed money for cancelling subscriptions to Netflix, Amazon Prime and gym subscriptions after never using their service. There are online reports of victims across the UK and this is likely to become a trend across the rest of the North East.

Apple Gift Cards
Victims report receiving emails from friends and family asking them to purchase Apple gift cards on their behalf from Amazon as they were having difficulties accessing their accounts. The digital gift cards were then to be emailed back to the fraudsters. Family and friends were likely hacked.

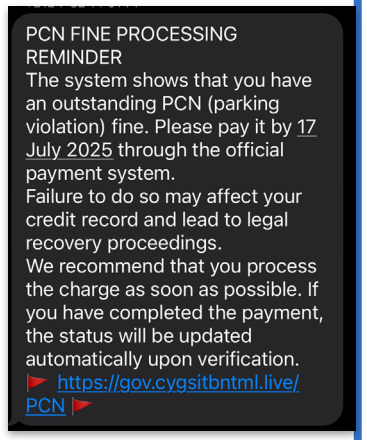
Helen Skelton Cryptocurrency Scam
There is a new celebrity deepfake being used to advertise cryptocurrency investments. TV Presenter Helen Skelton has now been added to the list which includes Martin Lewis, Kier Starmer, Elon Musk and Alan Sugar with their images being used to sell cryptocurrency investments.

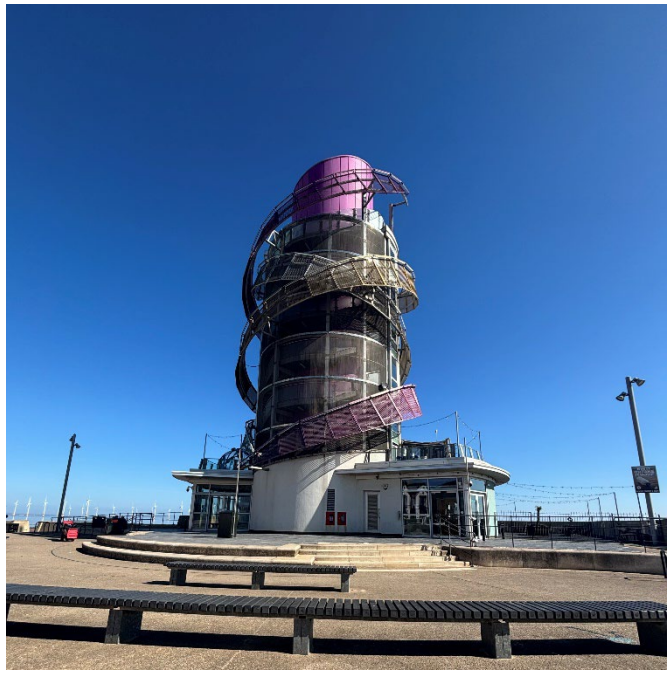
Car finance refund scam
Adverts on Instagram for car finance refunds are increasing. One victim enquired and was redirected to Tik Tok where direct debit and banking information was requested to check for eligibility. Money was subsequently stolen from the victim's bank accounts.



Fake Parking Ticket

Phishing text messages (some claiming to be from the government) about an outstanding parking ticket are being circulated. Messages include threats of prosecution and credit rating being affected. Victims are asked to click on a link, and complete information and pay the outstanding amount.





ENGAGEMENT EVENTS

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

This month has seen the team far and wide across the region.

We joined the Parkinson Group at the Gateshead Marriott Hotel and the NHS for a conference at Durham Cricket Club.

Sgt Emma O'Connor also appeared on Dave Robson Zetland FM show on July 11th to talk about all things romance fraud.

We have started visiting the newly opened Digital hubs across the County Durham area.

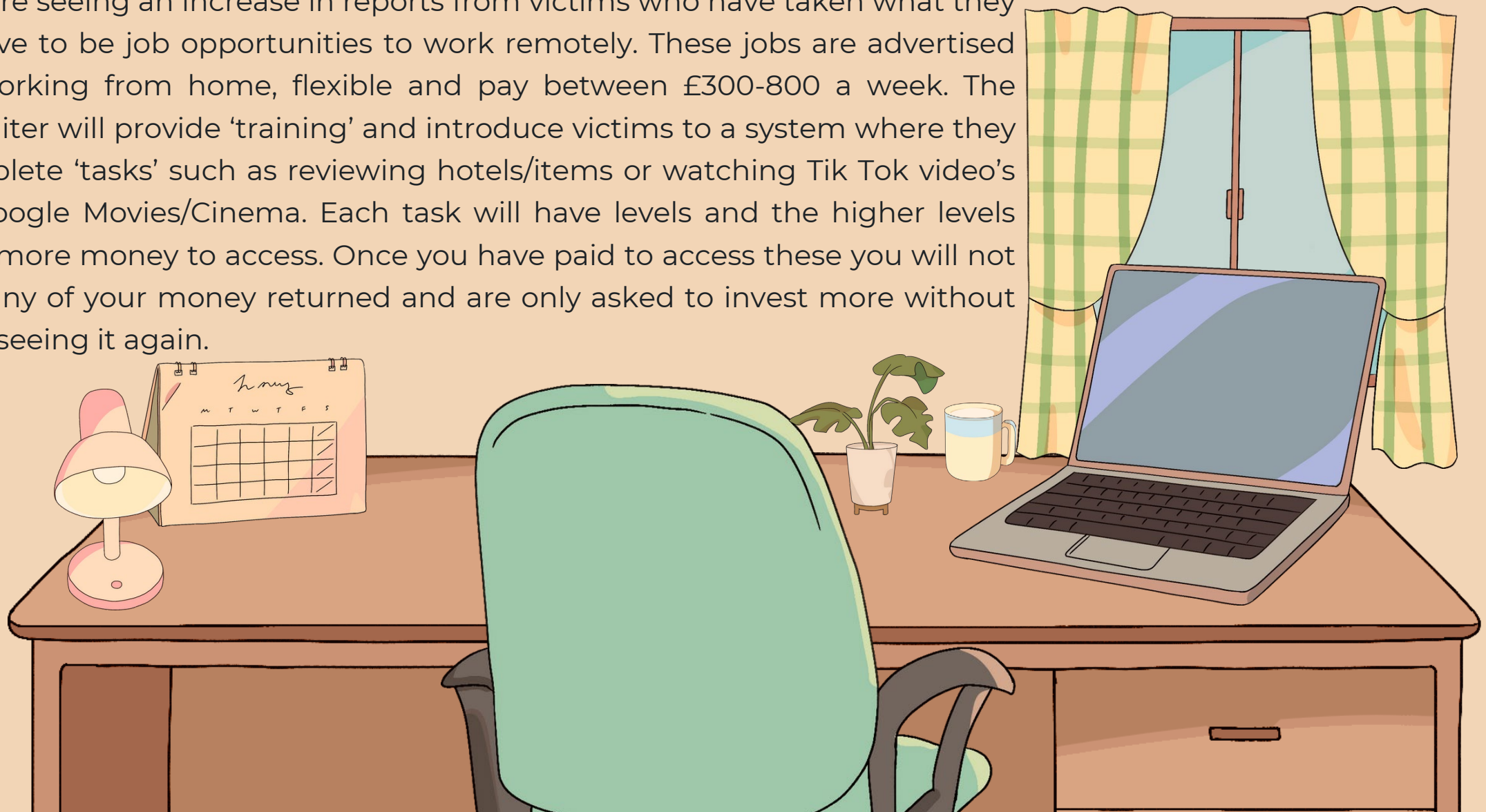
PC Andy Hampson presented his work at Durham University alongside one of the Student money advisors at the National Association of Student Money Advisor Conference in Manchester.

PROTECT YOURSELF FROM HOLIDAY FRAUD:

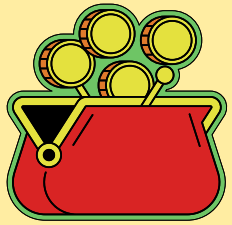
- Research the company you're booking through, read reviews and be cautious of any "too good to be true" offers.
- Make sure you're on a genuine seller's website by double checking website links.
- Avoid clicking on links from social media, message or email – always visit the seller's website directly.
- Search accommodation on other websites to check prices and make sure the location exists.
- Always use a secure payment platform from trusted retailers – avoid paying with bank transfer.
- If you're booking a package holiday, make sure the tour operator or travel company is a member of a recognised trade association such as **ABTA** or **ATOL**.
- When waiting for a refund, always make sure you're talking to the genuine company or airline.

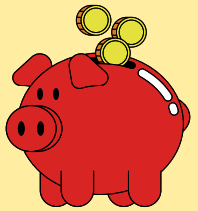
WANT TO WORK FROM HOME?

We are seeing an increase in reports from victims who have taken what they believe to be job opportunities to work remotely. These jobs are advertised as working from home, flexible and pay between £300-800 a week. The recruiter will provide 'training' and introduce victims to a system where they complete 'tasks' such as reviewing hotels/items or watching Tik Tok video's or Google Movies/Cinema. Each task will have levels and the higher levels cost more money to access. Once you have paid to access these you will not see any of your money returned and are only asked to invest more without ever seeing it again.



THE BANK OR POLICE WILL NEVER ASK YOU FOR MONEY



·Police and bank staff will never ask you to play a proactive part in an investigation.

·The police or your bank will never:

- **Contact you to withdraw cash or transfer money to help secure your account**
- **Never phone and ask you for your PIN or banking information**
- **Never ask you to purchase or send cash, foreign currency, jewellery, gold bullion or other items**
- **Never ask a courier to collect or for you to post cash or other expensive goods for safe keeping**

·Your bank or the police will never call you to ask you to verify your personal details or PIN by phone or offer to pick up your card or pin by courier. Hang up if you get a call like this. If you are told to call another number immediately to verify the person on the phone, hang up the phone and wait five minutes before using the same phone line; fraudsters may stay on the line after you hang up and listen in. Alternatively, use a different line altogether to call your bank or the police.

·If you need to, call your bank from the number on the back of your card or 159 to speak directly to your bank.

·Your debit or credit card is yours - don’t let a stranger take it off you.

·Speak to friends or family before taking action. Alternatively call 101, or Action Fraud. Always call 999 in an emergency.

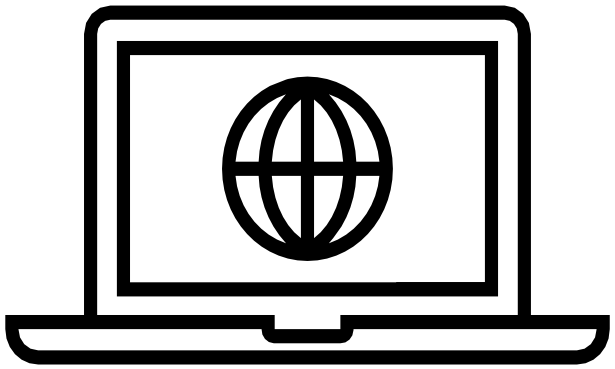
Don't be fooled by ticket fraudsters

With a host of sporting and music events set to take place this summer, be wary of fraudsters selling fake or non-existent tickets to events.

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

Horizon Scanning

Monitoring Threats



We are still seeing high numbers of job scams being reported. Victims can be approached by text message, Phone calls, the use of job apps (Such as Reed or Indeed) or by word of mouth through friends.
We urge people to talk to friends and family before accepting these 'remote high paying jobs' to check in with them to ensure that any job offers are legitimate.

DWP **Official Notice**:
According to DWP (Department **for Work and** Pensions) records, **you have not yet** submitted an **application** for Winter **Heating Allowance** for **2024-2025**. It **is important that** you complete **your application** by 17 June 2025 **to ensure** you receive your £300 allowance.
If **you do** not **submit** your application **by the** deadline, you will **not** be able **to** receive the **subsidy**. Please **complete your application as** soon as **possible** using the **link below**:

https://govuk.com-subsidyreh.cfd/uk?EpB=Mn7Ug8

(**Please** reply **Y**, **then exit the SMS and open** it again **to activate** the **link**, **or** copy the link **to** your Safari **browser and open** it)

With the Government and national media coverage around the winter heating allowance we are seeing a number of scam texts circulating encouraging people to follow links to apply for theirs.
Please do not click these links and report the messages to 7726 to help us take these numbers out of circulation.

Hello, I'm from the HR team at FlexJobs.
We've noticed that your CV has generated a lot of interest in the market, so we'd like to tell you about an exciting online job opportunity.
We offer flexible, remote part-time or full-time positions, as well as comprehensive pre-employment training, and it's completely free.
You can work according to your schedule and only need to devote 60 minutes a day.
Daily salaries range from £300 to £800, and we guarantee a minimum salary of £8,000 per month, paid daily.

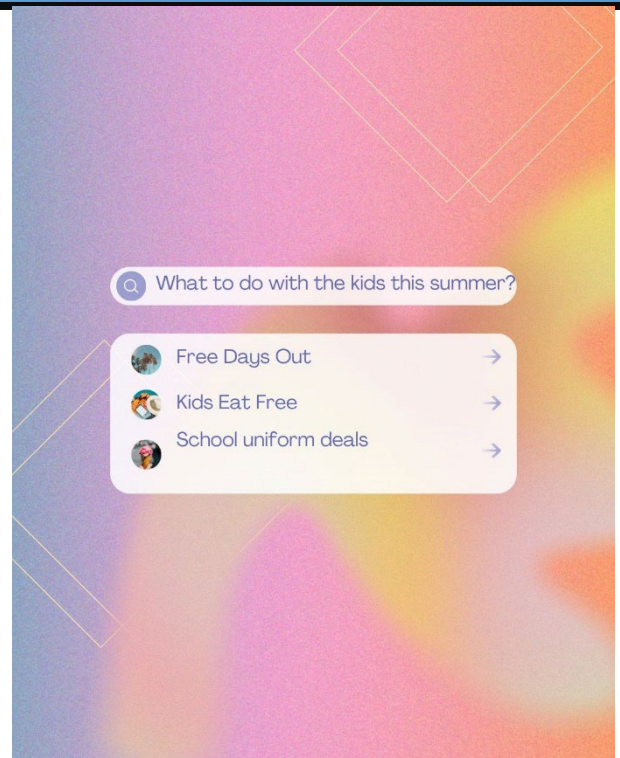
If you are interested in this opportunity, please feel free to contact me via WhatsApp: https://wa.me/447436617251?rog=krGTGw
(Please reply "1", then reopen this message and click the link to contact)

Hello, we would like to invite you to become our online employee, the job is very simple, just use your mobile phone, work in your spare time, and earn 300 to 800 pounds a day. Send a message via WhatsApp to get an instant reward of 8 pounds, please reply to this message and click on the link to learn more or add WS mobile number: https://wa.me/

What's Happening Next?

As we look towards the kids summer holidays please be cautious around offers such as;
-Free or discounted meals out
-Free or discounted days out
-Back to School offers from retailers
Whilst there will be legitimate offers from retailers out there for these, criminals will also use this as an opportunity to create scams with similar offers to steal your money and personal information.

Advice
-Fraudulent texts or social media post/pages may circulate with fake links
-These links may appear to be the retailers website, double check the website address to ensure it's the real deal
-Check TrustPilot reviews for the website/retailer, these will usually give you a good idea if there is a scam running
-Report text messages to 7726
-Report ad's to social media platform or the Advertising Standards Agency (asa.org.uk)



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

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.

North East ROCU Regional Organised Crime Unit Network

North East RECCC Regional Economic Crime Coordination Centre

NERCCU North East Regional Cyber Crime Unit

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.