

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 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 Cyber Crime June Summary



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

Total Cyber Reports (compared to June 2025)		 116 (-26.6%)
	Hacking -Social Media and Email	 98 (+8.9%)
	Hacking - Personal	 9 (-60.9%)
	Computer Virus/ Malware	 4 (-80)
	Hacking - Extortion	 4 (-50%)
	Hacking – PBX/ Dial Through	 1 (+300%)
	Denial of Service Attack	 1 (no change)

Cyber threats from hostile states are increasing

The National Cyber Security Centre (NCSC) has warned that cyber threats from hostile states are increasing. Between May 2025 and May 2026, the NCSC managed more than 200 incidents affecting UK critical national infrastructure, with around 75% linked to state actors such as Russia, China and Iran. Organisations are encouraged to strengthen cyber resilience by understanding their risks, implementing basic cyber security controls, and ensuring they can respond to and recover from incidents quickly. The NCSC also warns that Artificial Intelligence (AI) is likely to increase the scale and speed of future cyber attacks, making it even more important to address vulnerabilities now.

Further information is available at: <https://www.ncsc.gov.uk/news/ncsc-ceo-hostile-states-linked-to-three-quarters-of-cyber-attacks>

Artificial Intelligence (AI) is rapidly changing the cyber threat landscape

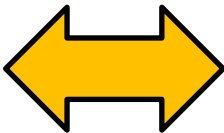
The Five Eyes cyber security agencies have warned that Artificial Intelligence (AI) is rapidly changing the cyber threat landscape. While AI can improve cyber defence, it is also enabling attackers to operate faster, at greater scale and with increased sophistication. The agencies stress that cyber security is a business risk, not just an IT issue. Leaders should prioritise cyber resilience by implementing strong security foundations, reducing vulnerabilities, strengthening access controls, maintaining up-to-date systems, and testing incident response plans regularly. The statement highlights the need for organisations to act now, as cyber threats are evolving quickly and AI is accelerating the pace of change. Organisations that invest in cyber resilience today will be better protected against future threats.

Further information is available at: <https://www.ncsc.gov.uk/news/the-ai-shift-in-cyber-risk-why-leaders-must-act-now>

North East Fraud June Summary

Total Fraud Reports (compared to June 2025)		 723 (-1%)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
	Advance Fee Frauds Cheque, Plastic Card and Online Bank Accounts	 154 (+21.3%)
	Cheque, Plastic Card and Online Bank Accounts	 130 (+217%)
	Online Shopping and Auctions	 103 (-30%)
	Investment Fraud	 62 (+8.8%)
	Other Consumer Fraud	 38 (-45.7%)

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



SIMILAR LEVEL THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Fake Customer Service Phone Numbers

Virgin Media & O2 are urging customers to stay alert after new research reveals AI tools are directing customers to fake customer service phone lines – putting millions of consumers at risk of Fraud. Around 1 in 8 people have been presented with a fake customer service number via search engines or AI tools. A further 1 in 5 say they’re unsure whether a number they encountered online was genuine. Criminals are exploiting AI-powered tools so that consumers looking to contact trusted brands are shown fake phone numbers, websites and search results, which they use to capture data and perpetrate fraud. One in ten consumers always assume the top search result is official, a figure that jumps to one in five among 25–34-year-olds. Trust in AI is also high, with 10% of people – and almost one in five older Gen Z and Millennials relying on phone numbers generated by AI tools.

Fake Vehicles on Ebay

Fraudsters have stolen thousands selling campervans and other vehicles that do not exist on Ebay. Victims across the UK have turned up at an address in Northumbria to view or collect the vehicle they have paid thousands for in deposits. The homeowner was entirely innocent and knew nothing of the sales.

The fraudsters created fake, believable persona’s including wife’s name and their personal history and reason for selling. They have even engaged in phone calls with the victims where their fake grandchildren could be heard playing in the background.

Research into the Ebay handles, seller names and telephone numbers has identified that this is part of a linked series where at least an additional 8 victims have purchased campervans and other vehicles and were directed to addresses In Cumbria, Norwich and Devon in addition to the Berwick incidents.

Campervan Nightmares

Campervan Fraud is where criminals pretend to be the owners of Campervans and advertise them for holiday bookings or for sale

Of course, the criminals don't own these Campervans, and as well as victims having the money they have paid stolen, they have the additional heartache of ruined holidays and future plans

The Fraudsters will advertise on well known accommodation and buying/selling websites



Please take care when buying items and holidays and accommodation on the Internet

Do not respond to unsolicited communications with holiday offers

Keep your digital hygiene updated
Only use https padlock websites

Use reverse image search tools where items are pictured
Research the seller

Pay Safely and with protection
Be cautious when asked for payment by transfer or cash



Engagement Events

This month we have visited and worked with:

- ✓ Isc2 North East England Quarterly Chapter Meeting
- ✓ St Teresa's Hospice Wellbeing Group
- ✓ Hartlepool Business Forum
- ✓ ZOPA Fraud Investigation Unit
- ✓ Durham University
- ✓ Halifax Bank
- ✓ Lloyds Bank
- ✓ Teesdale Valley Day Clubs
- ✓ Acklam Hub
- ✓ The Hub At Seahouses

Want to be a part of our growing Fraud Protect Community?

Contact us at:

RECCC@durham.police.uk



FRAUD ALERT

The Best Time To Stop The Crime  IS WHEN THE PHONE RINGS

Recent incidents of Impersonation Fraud and Courier Fraud have been reported in the North-East.

IMPERSONATION FRAUD

Criminals pretend to be someone you trust.

 Police Officer  Bank Employee  Other
Trusted Organisations

COURIER FRAUD

Fraudsters may tell you:

 Your money is at risk  Your bank card is needed
for investigation  You must move money to a "safe
account"

VERIFY INDEPENDENTLY

 Bank: Call the number on the back of your card or
159

 Police: Call **101**

 If someone is at your door and you feel at risk, call
999

 Never use contact details provided by the caller

PROTECT YOURSELF

 Don't answer unknown numbers

 If you answer, let them speak first

 If you don't know them – HANG UP

 Never trust unexpected calls claiming to be from
the Police or your Bank

 Speak to someone you trust

REPORT IT

reportfraud.police.uk | 0300 123 2040





REGISTER NOW

<https://www.cyberalarm.police.uk/>

Police CyberAlarm provides three layers of protection:

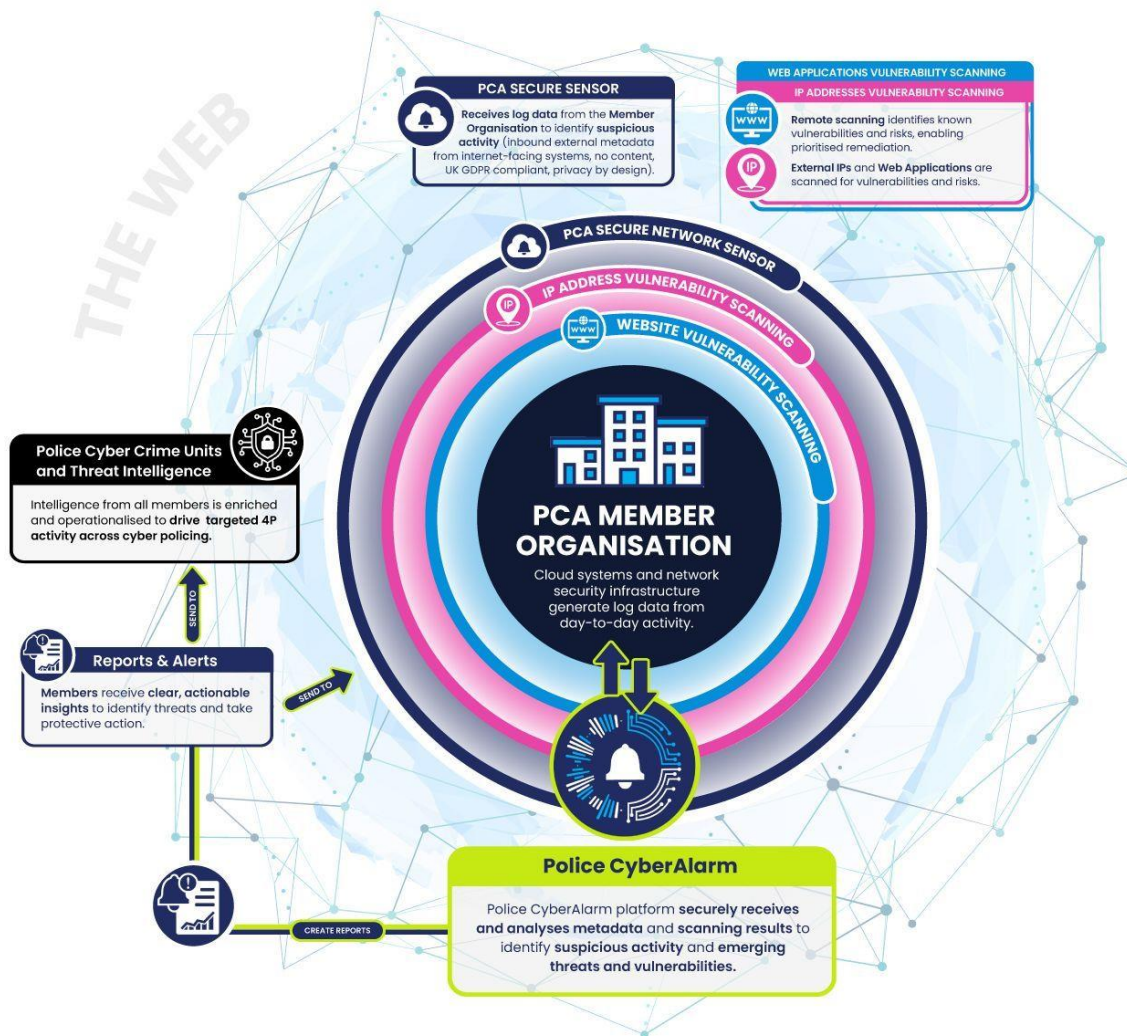


For Your Business

- ✓ Early visibility of cyber threats targeting your organisation.
- ✓ Improved resilience with minimal effort.
- ✓ Clear, actionable reports to support decision-making.
- ✓ Home Office funded, trusted service delivered by UK policing.
- ✓ Prioritised vulnerabilities so you know what to fix first.

Supporting UK Policing (4P Impact)

- | PROTECT | Targeted police interventions to support UK organisations and strengthen cyber resilience. |
|---------|--|
| PREVENT | Early visibility to enable Cyber Choices and other preventative interventions. |
| PURSUE | Enhanced intelligence to identify and target UK-based threat actors. |
| PREPARE | Improved national, regional and sector insight into the cyber threat landscape. |



Police CyberAlarm continues to grow with the launch of the CyberAlarm Secure Sensor, the latest capability available through the new Police CyberAlarm platform.

The Secure Sensor is simple to install and provides organisations with an additional layer of protection by increasing visibility of suspicious network activity and helping identify potential cyber threats earlier.

Police CyberAlarm now offers three fully funded protection levels:

- IP Address Scanning - helping identify vulnerabilities on internet-facing systems and networks
- Website URL Scanning - checking public-facing websites for weaknesses and security issues
- CyberAlarm Secure Sensor - providing additional visibility of suspicious network activity and contributing to a stronger national cyber threat picture

Together, these capabilities help organisations identify cyber risks earlier, improve cyber resilience and take practical steps to strengthen their security.



Police CyberAlarm is part of the National CyberCrime team hosted by City of London Police.

Project Lazio

Project Lazio is an initiative developed by officers at NEROCU, which is aimed at Uniformed Cadets in the North-East

The cadets and cadet leaders learn the basics of Fraud Protection and become an extension of the National Fraud Protect Network



Police Cadets in Northumbria, Durham & Cleveland Police Force areas and Air Cadets from Squadrons across the North-East have taken the skills into the community

Please contact us at reccc@durham.police.uk if your Uniformed Cadet group are interested in joining us Building Resilience Against Fraud



What's Happening Next?

National Campaigns:

- ✓ Ticket fraud awareness campaign via social media
- ✓ Advanced fee fraud awareness from National Trading Standards
- ✓ Student focused rental fraud awareness from the Home Office

Regional Events:

- ✓ Barclays Bank are running Community Van events throughout July and August – check details via the Barclays website
- ✓ 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 Protect Talk for International Students at Durham University

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.



30 minutes of free cyber security advice with a Cyber Advisor

- Practical guidance to improve your cyber security posture
- Insights into the Cyber Essentials certification process
- Clear, jargon-free advice you can act on immediately

🏠 / NCSC Cyber Advisor / Free Advice



What's the programme about and who can apply?

We know that navigating cyber security can be challenging, especially for smaller organisations. That's why we're offering 30 minutes of free, actionable advice tailored to your business needs.

During the session, you'll receive:

- Practical guidance to improve your cyber security posture.
- Insights into the Cyber Essentials certification process.
- Clear, jargon-free advice you can act on immediately.

This is a no-strings-attached opportunity to get expert advice and take the first step toward protecting your organisation from cyber threats.

This programme is open to SMEs that:

- Have fewer than 250 employees
- Are actively considering Cyber Essentials certification
- Are ready to engage with a Cyber Advisor to discuss their current cyber security setup



What is a Cyber Advisor?



Sign up

Check your eligibility by confirming that you are an SME organisation that has not held Cyber Essentials previously.



Answer a few questions

Provide some basic information about your business to help us tailor the advice to your needs.



Book your session

An NCSC-assured Cyber Advisor will contact you to schedule your free 30-minute consultation.



Get expert advice

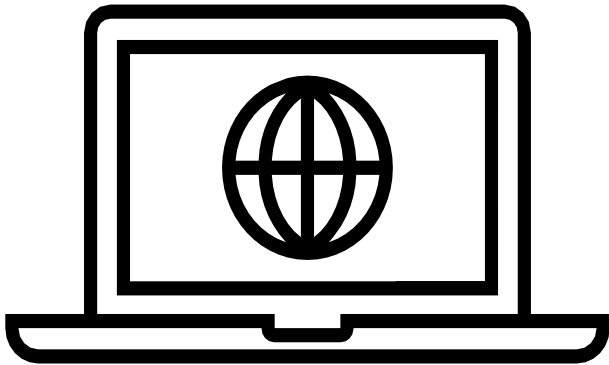
Receive actionable recommendations to improve your cyber security and prepare for Cyber Essentials certification.

SIGN UP NOW

<https://iasme.co.uk/cyber-advisor/free-advice/>

Horizon Scanning

Monitoring Threats



Beware of holiday scams fuelled by social media

- Criminals are pretending to be legitimate customer service agents on social media. Always book through trusted and official travel agents. If the offer looks too good to be true, it likely is. If the offer looks tempting, do your research.
- If it looks suspicious, report it to the social media platform by clicking the three dots in the top right corner and clicking 'report'

Illegal weight loss drugs

- Criminals are exploiting the current trend and use of weight loss drugs. These drugs should only be prescribed by authorised doctors and issued by registered pharmacists. No pharmacy is permitted to sell/dispense these drugs via social media. If you have already bought and used these drugs from social media, seek medical help as soon as possible. Report any social media to reportfraud.police.uk or call 0300 123 2040

Hot weather scams

- Criminals are taking advantage of the hot weather by offering free air conditioning units from a fake Curry's email and a cheap air conditioning unit sold via a fake Aldi website. Always double check emails and website offers by first going on to trusted, legitimate websites and checking to see if the offer is on there first. Fake websites can be reported to the National Cyber Security Centre and scam emails forwarded to

report@phishing.gov.uk

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 – ask trusted people

Manage – report the issue to report fraud or police.





[15 Jul 2026] Helping small businesses with free, hands-on cyber consultancy

URL: <https://www.ncsc.gov.uk/blogs/helping-small-businesses-with-free-hands-on-cyber-consultancy>

[13 Jul 2026] UK and Allies urge critical sectors to improve defences against Russian intelligence targeting

URL: <https://www.ncsc.gov.uk/news/uk-and-allies-urge-critical-sectors-to-improve-defences-against-russian-intelligence-targeting>

[09 Jul 2026] Cyber Essentials Pathways: from proof of concept to cyber confidence

URL: <https://www.ncsc.gov.uk/blogs/cyber-essentials-pathways-from-proof-of-concept-to-cyber-confidence>

[07 Jul 2026] Cyber Shield: The path to an agentic AI future for cyber defence

URL: <https://www.ncsc.gov.uk/blogs/cyber-shield-the-path-to-an-agentic-ai-future-for-cyber-defence>

[01 Jul 2026] Building more resilient CNI: what industry pen testers told us

URL: <https://www.ncsc.gov.uk/blogs/building-more-resilient-cni-what-industry-pen-testers-told-us>

[22 Jun 2026] The AI shift in cyber risk: why leaders must act now

URL: <https://www.ncsc.gov.uk/news/the-ai-shift-in-cyber-risk-why-leaders-must-act-now>

[18 Jun 2026] Alert: NCSC issues advice following global targeting of Fortinet firewalls and VPN gateways

URL: <https://www.ncsc.gov.uk/news/advice-following-global-targeting-of-fortinet-firewalls-and-vpn-gateways>

[18 Jun 2026] The 'vibe coding spectrum' approach to AI-assisted software development

URL: <https://www.ncsc.gov.uk/blogs/the-vibe-coding-spectrum-approach-to-ai-assisted-software-development>

[17 Jun 2026] NCSC CEO: Hostile states linked to three-quarters of cyber attacks affecting UK's critical systems

URL: <https://www.ncsc.gov.uk/news/ncsc-ceo-hostile-states-linked-to-three-quarters-of-cyber-attacks>



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**

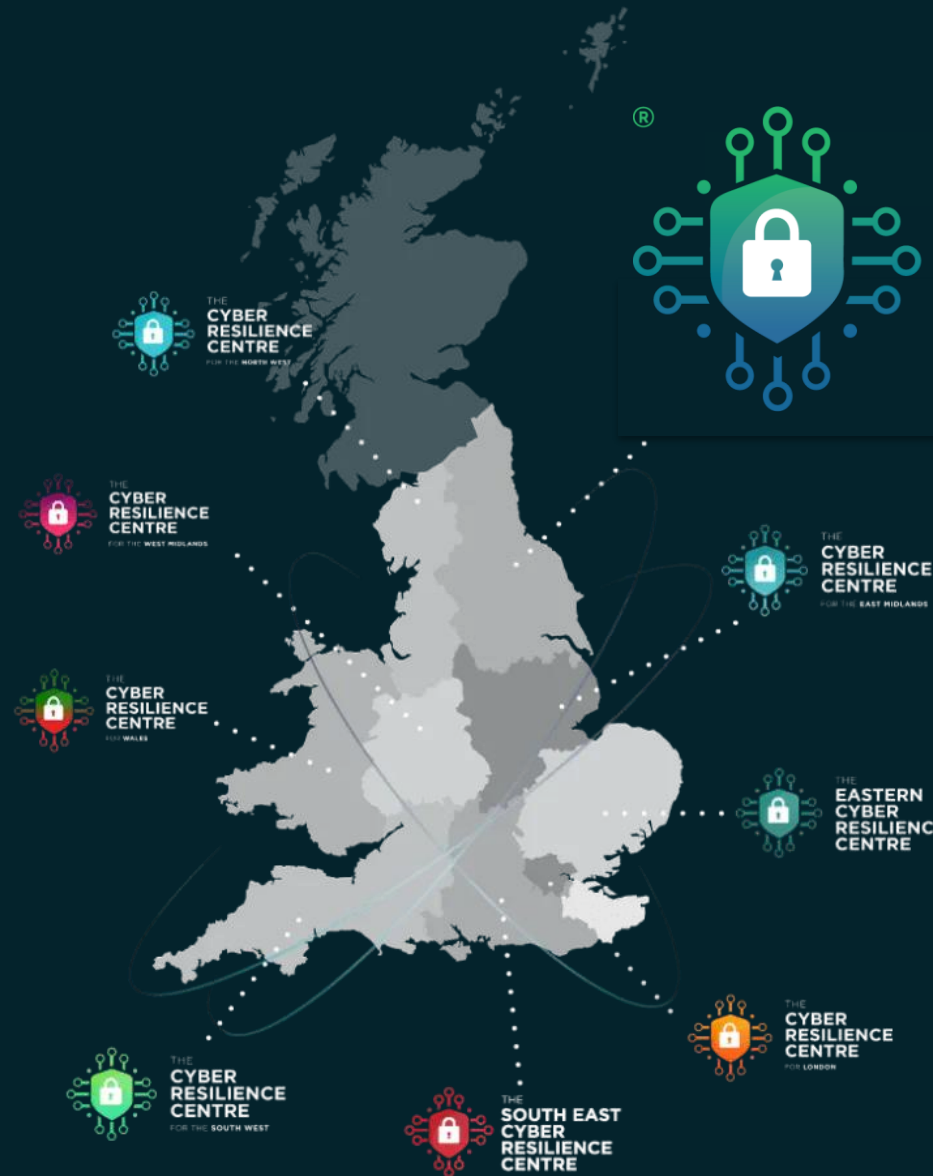


National Network of 9 Centres



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:**





 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

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	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.