

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 March 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.

Contents

Looking Back



- [Action Fraud: Regional Cyber Summary](#)
- [Action Fraud: Regional Fraud Summary](#)
- [Engagement Events](#)










Contents

Looking Forward




- [Horizon Scanning](#)
- [What's Happening Next](#)

North East Cyber Crime March Summary

Total Cyber Reports (compared to February 2024)	 192 (+47%)
 Hacking -Social Media and Email	 135 (+34%)
 Hacking - Personal	 35 (+337%)
 Computer Virus/ Malware	 11 (+37%)
 Hacking Extortion	 10 (+25%)


Hacking- Personal category has seen a dramatic spike across the region this month compared to March 2024. The rise in this category is primarily down to one individual reporting multiple device compromises as part of the initial breach.




SIM swapping 

SIM takeover reports have continued this month with 10 victims with no specific network provider or demographic targeted.

Hacking -Social Media and Email
Hacking – Social Media and Email continues to rise this month with multiple account compromise from an email breach featuring throughout the reporting. Of note Facebook continues to be the most accessed social media platform with a rise this month in Facebook hacking and account takeover to sell fake Oasis tickets.


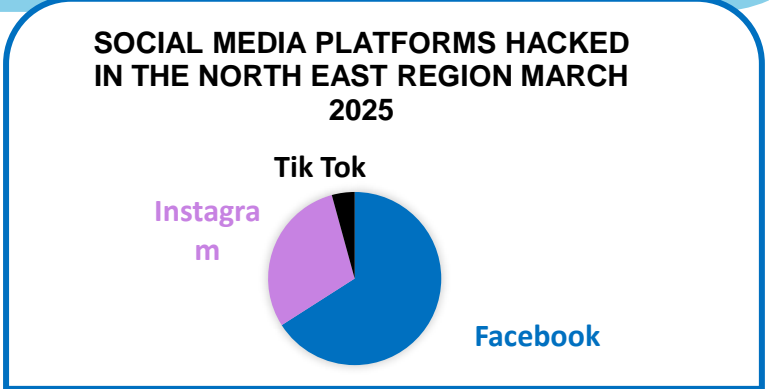


**INCREASED THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR** 

Boots Medicare Kit Phishing Emails 

National reporting indicates a rise in this method of phishing emails. Whilst in the region we have not seen a trend emerge yet, this month a charitable organisation was targeted and became victim to this scam. It is imperative to stay vigilant when receiving emails from unknown sources. This scam claims the recipient has been selected to participate in a customer satisfaction email to receive a free “Medicare Kit”. It will prompt the user the click on hyperlinks by using urgent language such “*Hurry up! You are among the few to be selected, and the invitation to participate in our survey will only be available for the next 48 hours. Click the button below to get started*”. It will use familiar branding language to legitimise the email such as “*Are you a Boots Advantage Card Holder*”. Clicking the hyperlinks will possibly result in a request to enter personal details or will download malware on to the user’s device.

Amazon Hacking
March 2025 has seen over a 100% increase of Amazon account hacks compared to March 2024. The reporting suggest that hackers are using the victims account to order parcels with the victim first becoming aware when they receive a parcel or receive notification that a parcel has been delivered to an unknown address.

North East Fraud March Summary

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



Total Fraud Reports (compared to March 2024)	719 (4.4%)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Online Shopping and Auctions	132 (-19%)
Advance Fee Frauds	91 (+13.8%)
Other Consumer Fraud	65 (+18.2%)
Investment Fraud	47 (+34.3%)
Cheque, Plastic Card and Online Bank Accounts	44 (-4.4%)

Whiskey Investment Scam



After a BBC news investigation uncovering a whiskey cask investment scam, North East victims have started to submit reports. One victim reports having £26,300 stolen by investing in casks that do not exist, despite certification in place for 'London Cask Traders'. It is expected more victims will come forward in the next few months.

Mobile Phone Contracts



Phone contract scams are increasing in frequency with at least 26 reported in March alone across all phone providers. Criminals contact victims impersonating phone companies and offer discounted phone contract deals, they use the victims personal data to take a phone contract in their name and it is often the wrong phone. When the victim receives the phone they are given a postal address to 'return' it.

'Hi Mum/Hi Dad' Text Messages

Phishing text messages purporting to be from children are still being sent in large volumes. This has been an ongoing scam for a number of years and request that victims send them money under the guise of losing their phone needing to pay bills or some other emergency.

ENGAGEMENT EVENTS

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



This month as part of the ongoing Operation Lazio County Durham and Darlington Police Cadets have been spreading the message about how to stay safe and fraud awareness in Durham City Centre.

Students at Sunderland College (Bede, Hartlepool and City Campus) took part in Fraud Awareness workshops as part of their 'preparation for life roadshow'. As well as Darlington and Middlesbrough Colleges taking part in sessions.

Darlington Council staff and Councillors have taken part in an online fraud Awareness input.

Durham, Teesside and Northumbria Universities have all taken part in various events across the month from stalls to staff inputs, making staff and students more resilient against Fraud.

Hutton Henry and Bowburn Community Groups received Fraud Awareness sessions.



COURIER FRAUD



Criminals targeting vulnerable people pretending to be a police officer, bank official or figure of authority.

If you have suspicions, hang up & call them back on a trusted number from a website or bank statement.



If you're a victim report it to Action Fraud & your bank immediately.

Business Banking Customers Are Being Targeted.

Business banking customers have been called on business lines by a threat actor purporting to be from their bank.

HOW IT WORKS:



The customer receives a phone call from a criminal claiming to be from the bank. They have knowledge of recent transactions on the account and state that there has been suspicious activity on the account.



The customer is then directed to a website which mirrors the official bank website. Some of the links on the website download an app called Any Desk to the customers computer and the threat actor then states they are reversing the suspicious transactions and the customer needs to authorise them.



However, the criminal then asks the victim to approve payments and input a code which sets up call forwarding, this then allows the criminal to speak to the bank impersonating the victim.

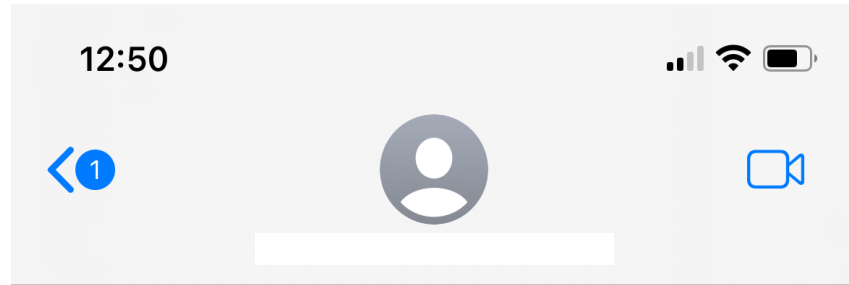
HOW TO PROTECT YOURSELF AND YOUR BUSINESS:

- If in doubt, hang up.
- Use a trusted number to call back and check it out.
- Do not give any personal details or sensitive information.

Remember, not everyone is who they say they are!

11
reports
in the
North East
in 2025

EVRI



iMessage
Today 12:50

EVRI mail package in the process of transportation, due to damage to the outer package, address information is lost, can not be delivered. Please be sure to update the delivery address information in the link within 12 hours.

<https://evri-uk.motorcycles/uk>

(Please reply Y, then exit the SMS, re-open the SMS activation link, or copy the link to open in Safari)

The EVRI team wishes you a great day!

The sender is not in your contact list.

[Report Junk](#)

There has been an increase in Fraudulent Evri delivery texts similar to the one pictured (left).

When victims reply 'Y' and receive a link they are taken to a page that looks similar to the Evri website, the website requests personal information and requests the victim to card details.

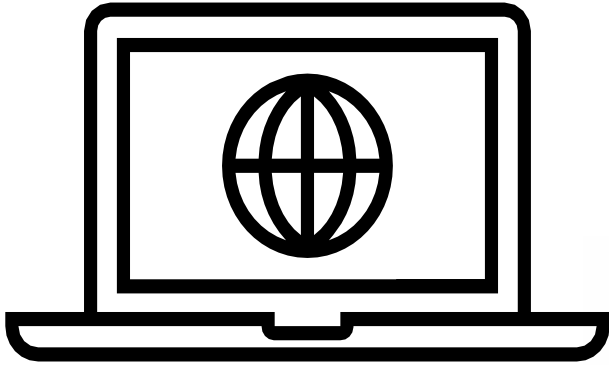


- Do not reply to the text and do not click any links.
- If you have entered any personal details, contact your banks Fraud team immediately by dialling 159.
- Forward any suspicious texts to 7726 to be investigated.

If you think you have been a victim of Fraud, contact Action Fraud at www.actionfraud.police.uk or call **0300 123 2040**.

Horizon Scanning

Monitoring Threats



Parents are being warned about a phishing email being sent to those with children in the Russell Foster Youth League. The email states they have not paid fees and provides a malicious link which looks to collect sensitive and personal information, as well as asking parents to input their card details.



Victims are reporting that they are being contacted by criminals purporting to be from sky or mobile phone companies. They are being offered deals for phone contracts. However, these deals are fake and once the victim agrees to take the contract out, the criminal takes a contract out using the victims details and sends the wrong mobile phone and then asks the victim to return it using a fake address.

STOP!
THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

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

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

#TicketFraud

Secure your accounts.

Protect your important online accounts, such as your email or the accounts you use to buy tickets, with passwords that you don't use anywhere else. Use three random words to create strong and memorable passwords.

● Buy safely ● Payment ● **Account security**



WATCH OUT FOR ROGUE TRADESMEN

Trading Standards have reported that businesses in the North East have been targeted by rogue tradesmen.

So far there have been reports that the tradesmen approach those with land/car parking areas stating they have materials left over from work they are doing locally and offer them a 'discounted' price for chippings or tarmac to be laid on the area.

The work is then carried out in some degree but of a really poor standard and then employees are intimidated into agreeing rates over text at an inflated price for the poor work carried out. The tradesmen then contact the owner of the land and show the 'agreement' in order to obtain large sums of money for the 'service' they have carried out.

It is important to be wary when being approached by builders or tradesmen and use websites such as check a trade or check online reviews before agreeing for them to carry out work.

JOB

offer



Have you received a text message with an 'out of this world' job offer?

Victims are reporting receiving a message offering a full time remote job.

If victims reply they are asked to invest a small amount of money and see a high return at first, however they are encouraged to invest more and then the criminal disappears, along with the money.

This could also be to approach people to become 'money mules' to launder criminal funds. This involves transferring money through bank accounts and carries a 14 year prison sentence.

Forward any suspicious text messages to 7726 to report them.



SIM SWAP FRAUD

In recent months, we have seen an increase in the number of Sim Swap Fraud.

Sim Swap Fraud is where a criminal will pretend to be you and try to convince your phone network that you need a replacement sim for your phone. If successful this will allow them to take control of your mobile phone number, which means they can potentially hijack your calls and texts, as well as your online banking details.

Things to look out for

- You've lost the ability to make call or texts. This could mean they have deactivated your sim and are using your phone number
- You receive a notification that your sim card or phone number has been activated on a different device
- Your login details stop working for your accounts

Protect yourself

- Watch out for Phishing attempts and report any to report@phishing.gov.uk or forward to 7726
- Look after your digital footprint and be careful what you share on social media
- If your phone stops working call your bank and your mobile network provider
- Use the three random word method to create a strong password and make sure its different for each account.

What's Happening Next?



Free gift/Easter egg

Easter is around the corner and that usually means scam texts about claiming 'free easter eggs' are on their way too. Every year victims receive text messages (usually via WhatsApp) with a link to take them to claim their 'free Cadbury easter egg'. Similar reports have also been received reporting that victims received a message from 'LIDL' and other reputable companies have been named. The message states the recipient has 'won' a free item or can claim a discount/cheap item if they enter some personal details.

- Avoid clicking links that are sent over messages, especially unsolicited messages.
- Do not enter any personal information or bank details in order to receive a 'free gift' or discount.

Financial Markets

With the uncertainty over the current financial markets criminals may use this to their advantage to push opportunities for cryptocurrency investments to investors who would usually avoid virtual currencies.

There may also be an increase in the number of investment Frauds as people seek to take advantage of low stocks.

- If you are looking to invest, ensure you have carried out due diligence. You can check investment companies are FCA registered using the FCA website.
- Be wary of companies overseas, they may not be regulated.





 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.



Emails

Forward Fraudulent emails to
report@phishing.gov.uk



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.



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	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.