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 January 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

Contents

Looking Forward

North East Cyber Crime January Summary

Total Cyber Reports (compared to January 2024)	↑	**175 (+70%)**
Hacking -Social Media and Email	↑	**131 (+63.8%)**
Hacking - Personal	↑	**18 (+157%)**
Hacking Extortion	↑	**15 (+150%)**
Computer Virus/ Malware	↑	**11 (+10%)**

INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR ↑

Hacking – Social Media and Email

Hacking – Social Media and Email reports are up 64% and account for 75% of all the Cyber reports to Action Fraud in January 2025. Reports for this category are rising month on month in line with national reporting.

Meta platforms accounts tend to be targeted the most but some victims report their retail apps for Amazon and Very hacked.

SIM swap takeover reports have continued this month with 8 victims with no specific network provider or demographic targeted.

AI-Driven Phishing Attacks

There has been a significant increase in highly personalised phishing scams targeting corporate executives. Fraudsters are leveraging artificial intelligence to analyse online profiles, crafting convincing emails that mimic legitimate communications. This advancement has lowered the barrier for sophisticated cybercrimes, making it challenging for traditional email filters to detect malicious content.

North East Fraud January Summary

DECREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Fraud Reports (compared to January 2024)	**669 (-14.6%)**
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Online Shopping and Auctions	**151 (-18.8%)**
Advance Fee Frauds	**79 (-4.8%)**
Other Consumer Fraud	**55 (-21.4%)**
Cheque, Plastic Card and Online Bank Accounts	**50 (-18%)**
Investment Fraud	**31 (-32.6%)**

Surveys

Fake phishing emails and text messages from well known retailers such as Boots, Lidl and Marks & Spencer's are currently being circulated in the North East. Consumers are offered free gifts to complete a survey about recent purchases. Bank details are required to pay a small fee for postage. Victims also report being flooded with other scams following this.

HMRC Scams

Following on from the deadline for HMRC Self Assessments at the end of January, fraudsters continue to impersonate HMRC to target victims.

There has also been an increase this month in the number of cold calls (some automated) stating the victim has a debt to HMRC or owes tax which must be paid immediately otherwise bailiffs will visit their homes. £25,312 has been stolen this month through HMRC scams. Customers can report suspicious communications to HMRC by:

- forwarding suspicious texts claiming to be from HMRC to 60599
- forwarding emails to phishing@hmrc.gov.uk.
- reporting tax scam phone calls to HMRC on GOV.UK.

Job Scams- Training Courses

The number of job scams continues to increase with job seekers approached in several ways; phishing text messages, Facebook posts and fake advertisements for popular recruitment firms.

Victims report paying in advance for online training courses for positions that do not exist. Following completion, further paid mandatory training courses are required with prices increasing with no end in sight.

ENGAGEMENT EVENTS

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

Teams from a wide variety of roles at Citizens Advice Northumberland took part in a Fraud Awareness workshop.

Operation Lazio – working with cadets to improve their knowledge of Fraud through workshops is still ongoing across the three police force areas.

600 staff from the NHS, North Tees and Hartlepool took part in an online session to build resilience against Fraud.

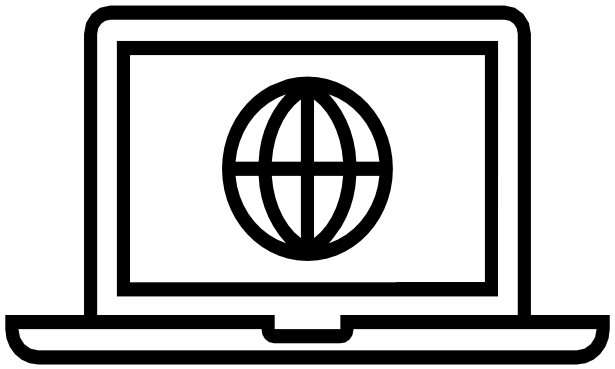
The team attended Nissan wellbeing month to speak with staff in the plant to raise awareness of Fraud and how to report Fraud.

Sunderland University hosted a refreshers event where we spoke with students and staff who received copies of our ‘Student guide to Fraud’.

.

Horizon Scanning

Monitoring Threats



Customers that have booked accommodation on Booking.com are being targeted!

There has been an increase of reports from victims that have booked accommodation on booking.com. It is likely that there has been a large scale phishing attack on hotel/accommodation providers where criminals have been able to take over their accounts and message the customers who have bookings using in-app messaging, email and WhatsApp requesting payment or card details.

It is likely as the school holidays and the summer season approaches that more people will have bookings through booking.com.

Advice:

- If you receive an unexpected email or message about your booking, ignore it and report to report@phishing.gov.uk or 7726.
- Do not give your card details via email or message, if in doubt, contact the hotel or accommodation provider direct via a trusted phone number where possible.

WARNING! FAKE SURVEYS!

There has been an increase in reports of fake surveys. The surveys are under the guise of being from Boots and M&S, but they could be sent using other company names. The email or message states you can claim a freebie or an item if you fill out the survey. However, the link takes you to a website that asks you to enter personal information.

What can you do to protect yourself?

- If you do receive a ‘survey’ ask yourself if the ‘freebie’ or ‘gift’ is worth giving out your personal information for.
- Try to avoid entering personal details online.
- Check the source, if the source can not be trusted .. Do not go ahead and fill anything out.

SCAM WARNING

Fraudsters target Booking.com users with scam emails

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

CITY OF LONDON POLICE

NCA
National Crime Agency

FAKE DEBT COLLECTION SCAM

Victims have been receiving phone calls from criminals purporting to be debt collectors. They threaten the victim with someone coming to their address to remove property to the value of the debt they ‘owe’, often claiming the victim has missed a court date.

Victims have reported that the calls seem legitimate as the criminals on the other end give a reason that resonates with the victim as a service they have used in the past.

The criminal then states if a bank transfer is made the debt collector will not attend the address and then email ‘court documents’ to the victim that look real.

How to protect yourself:

- Remember, criminals use pressure tactics on you to try and get you to send payment.
- If in doubt, HANG UP!
- Do not be scared to check it out.
- Do not make any payments via bank transfer to someone making an unsolicited phone call.
- If you are feeling pressured and worried, speak to someone you trust before making any decisions.

AI-Driven Phishing Attacks – Ways to Prevent or Mitigate their impact

Personal Data Hygiene

•Limit the amount of **publicly available personal information** that attackers can use to personalise phishing attacks.

• Review privacy setting on social media.

Employee Training & Awareness

• Businesses should conduct regular **phishing simulations** to test employees' ability to spot AI-generated phishing emails.

•Train employees on **social engineering tactics**, emphasizing the risks of **personalised scams** using AI.

•Encourage a **zero-trust approach**, where employees verify unexpected requests through alternative channels.

Two-Factor Authentication

•Enforce **2FA on all accounts** to prevent unauthorised access, even if credentials are stolen.

•Consider **passwordless authentication**, such as biometric verification, to further reduce phishing risks.

Considerations:

- You can also use AI functions to mitigate risk, such as AI threat detection, to monitor typos, AI powered email filters.
- Have a plan in place:

Businesses – what plan do you have in place for phishing emails?

Who do employees report to?

How is it dealt with?

What's Happening Next?

Are you planning a holiday this year?

Spot the signs of Holiday Fraud

•You're contacted out of the blue by a travel agent or company you've never spoken to before, offering a holiday at a very low price.

•The details, pictures or address of the property or hotel on offer look suspicious, or independent website reviews are negative or don't exist.

•You're asked to pay using bank transfer or cash; pay by credit or debit card if you can for extra protection.

•Don't reply to unsolicited emails, texts, social media or calls with holiday offers. Links and attachments in emails may lead to malicious websites or download viruses.

• Book a holiday directly with an airline or hotel, or through a reputable agent. Check whether they're a member of the Association of British Travel Agents (ABTA).

• Be extra cautious if you're asked to pay using bank transfer or cash; pay by credit card if you can as section 75 provides protection.

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.

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** **Sarah McCluskey –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.