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 February 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 February Summary

INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Cyber Reports (compared to February 2024)		**147 (+77%)**
	Hacking -Social Media and Email	**114 (+107%)**
	Hacking - Personal	**12 (+33%)**
	Computer Virus/ Malware	**11 (+22%)**
	Hacking Extortion	**9 (+13%)**

Hacking – Social Media and Email

Social Media and Email Hacking reports are up 107% and account for 77% of all the Cyber reports to Action Fraud in February 2025. Reports for this category are rising month on month in line with national reporting.
Of note, although 114 incidents have been reported the actual number of victims is 62. The data shows that victims suffered multiple account compromises from the initial breach, often reporting an email hack alongside other social media accounts.
This is in line with national figures as reporting indicates an increase in blackmail phishing emails alongside social media and email hacking. As a result, the compromised password is then used to access multiple accounts belonging to the victim. This is particularly damaging if it is the victims email password as this will most likely be linked to a wide range of accounts such as streaming services, network providers, leisure accounts, insurance and retail accounts.

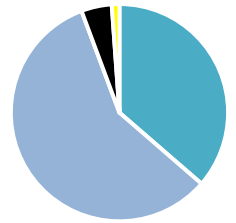
SIM swapping

SIM takeover reports have continued this month with 7 victims with no specific network provider or demographic targeted.

Facebook Hacking

Cyber criminals are hacking Facebook accounts to sell fake Oasis and Black Sabbath concert tickets. 11 reports have been received this month. Criminals are posting tickets for sale on the victims page and messaging the victims contacts. It is highly likely cyber criminals are using both these bands as they are performing reunion concerts in 2025 and therefore tickets will be limited and in high demand.

Social Media Platforms Hacked in the NE region Feb 2025



North East Fraud February Summary

DECREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Fraud Reports (compared to February 2024)	**643 (-17.7%)**
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Online Shopping and Auctions	**135 (-5.6%)**
Advance Fee Frauds	**73 (-19.8%)**
Other Consumer Fraud	**58 (-1.7%)**
Cheque, Plastic Card and Online Bank Accounts	**47 (-28.8%)**
Investment Fraud	**41 (-21.2%)**

Cash for Cures & Dating Scam

Callous and heinous fraudsters have targeted vulnerable victims in the North East facing serious health conditions with limited treatment options through hybrid Romance Fraud Scams. Using AI deepfake technology to pretend to be rich public figures, they convince the victim that they are in a relationship before offering to discover a cure for their illness. Regular payments to assist finding a cure are required using gift cards.

Celebrity AI Enabled Impersonation Frauds

Since the beginning of the year there has been an increase in the number of Action fraud reports involving Celebrity Impersonations enabled by AI Deep Fake technology.

Prominent business leaders and politicians such as Elon Musk, Kier Starmer and Martin Lewis have been faked and used in a variety of fraud types. Previously, this type of technology was mainly used in high return frauds such as Investment scams but it has developed in use as technology as become more accessible.

It is expected that this will become more widespread and we will see more reports targeting vulnerable victims

Lottery/ Competition Scams

There have been a number of reports this month for fake lottery and competition scams. They often come in the form of a letter, email, text or social media message claiming that you have won a prize for a competition you did not enter.

Victims contacted on social media were told to pay hundreds of pounds in fees using gift cards to claim their winnings. Suspicion was raised in one case when the criminal demanded more money following payment. AI Deepfakes with celebrities have been used to advertise such fake competitions.

Fake phishing letters from the National Lottery have also been received in the North East stating that as a loyal customer the recipient had 10 free lines and to call the 0800 number quoted.

North East Fraud February Summary

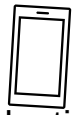
Website Design Scams

Website design scams have been going for a few years and usually contact potential victims through phishing emails or direct messaging but Cleveland residents are starting to see offers to produce a website on local community social media pages.

The ‘free of charge’ offer to assist the fake designers portfolio will ultimately cost the victim to retain ownership or make any change to the no-cost website. It is often a front for a scam.

One UK-based company employs agents to scour Facebook groups for eager prospects using this exact bait. These "agents" promise free websites but deliver far less than they claim. They will register your domain taking control and making it challenging for you to regain ownership later. They will charge a hosting fee annually. The website is poor quality and a cloned copy of countless others with a swapped logo, some text changes and maybe a photo. Due to relentless upselling, any slight amendment will cost more than you expect.

Online Shopping and Auctions



Whilst there has been an overall reduction in reports under the ‘Online Shopping and Auctions’ category, there has been a significant increase in the Durham force area.

Some reports were from victims buying cars in either poor condition and losing deposits or full payment. Cars were purchased through Ebay sites or privately through social media.

Many victims also reported having money stolen when selling mobile phones on Facebook Marketplace. With iphones posted out to buyers, fake proof of funds transferred at the point of postage has meant victims have lost both their handset and payment despite the victim being careful.

There are a handful of potential linked reports in the South Durham area with a male attending the victims’ home in person to purchase an iphone and showing funds being transferred from his Metro bank account to the victim. There has also been report in the Cleveland area using the same MO to steal a quad bike.

ENGAGEMENT EVENTS

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

The team have taken part in ‘Sunderland Financial Wellbeing Week’ which saw partners such as Stop Loan Sharks, Barclay’s, Citizen’s Advice, Money Wise, Gen Too and others come together for a week of action to raise awareness of illegal money lending, help with finances and Fraud awareness.

Deaflink, Golden Age People, Northumberland Council ‘Communities Together and Retired Men’s Forum all received Fraud Awareness inputs.

A massive 2877 Durham University students received an online input around Fraud Awareness, Teesside University hosted ‘money week’ where students attended our stall at the event and Northumbria University took part in a session to raise awareness of Romance Fraud.

Virgin Bank staff at Hartlepool took part in a staff CPD session to raise awareness of the Fraud trends in their area and customers also received advice in branch.

Self Help Tool Centre

Your free Self Help Tool Centre - Get Safe Online

Get Safe Online have a handy self help centre where they have tools that can help to make people more resilient against Fraud.

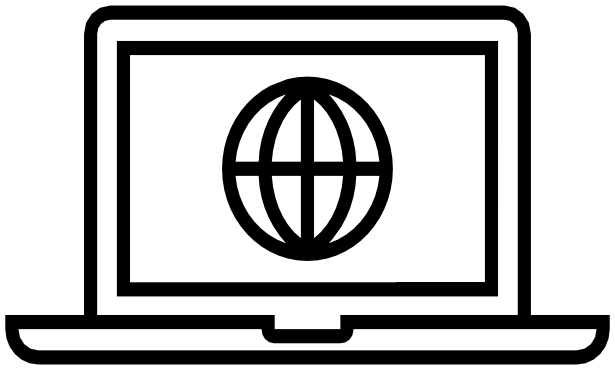
Please use these tools (right) to help you check out potential fake websites, check photos and test your knowledge on how to spot a scam. You can use the link above or the website listed to access the Self Help Tool Centre.

- **Check a website**
- **Check a photo**
- **Check a physical location**
- **Check for a data breach**
- **Check if you can spot a phishing email**
- **Check your social media footprint**
- **Store all your passwords securely**
- **Check the strength of passwords**
- **Manage your passwords in one place**
- **Ask Silver**
- **Spot the AI**

https://www.getsafeonline.org/selfhelpcentre

Horizon Scanning

Monitoring Threats



Elon Musk's name used in various Fraudulent activity

There has been a rise in reports of Fraud involving Elon Musk's name. Due to the media focussing heavily on America due to the recent elections and Elon Musk's participation in this, there have been a number of different methods criminals have used to try and extort money from victim's. This has included Romance Fraud where the victim has been involved in what they believe to be a relationship with Elon Musk and have been asked to transfer money. Emails offering to pay for victim's electricity bills have also been sent.

- If you see emails using Elon Musk's name, be aware his name is being used for various different Fraud types.
- Be wary when dating online, always think 'is this person who they say they are?'
- Do due diligence when investing money, always check it out before parting with cash.

Fake Employment Opportunities

Speaking with members of the public, people are stating that they have received text/WhatsApp messages offering them job opportunities. These are fake job advertisements marketed as 'easy money' 'quick cash' or something similar. However, this is a recruitment campaign for criminals to find people to launder the money they have made through the proceeds of crime. They will ask you to transfer money to another bank account to 'clean' it and take a cut for yourself. This is illegal and carries a 14 year prison sentence.

- Report any suspicious texts by forwarding to 7726.
- Do not reply to unsolicited texts.
- If you are approached with job offers from unknown people/numbers, be cautious.

CITY OF LONDON POLICE

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

Cyber Aware

Protect your devices with the latest software updates

Software updates help keep hackers out

Out-of-date software, apps, and operating systems contain weaknesses. This makes them easier to hack. Companies fix the weaknesses by releasing updates. When you update your devices and software, this helps to keep hackers out.

Automatic updates

Turn on automatic updates for your devices and software that offer it. This will mean you do not have to remember each time.

Gift Card Fraud

How to protect yourself :

- **The police, banks and other reputable organisations will never ask you to purchase a gift card.**
- **Avoid giving out any details or PINs from gift cards.**
- **Be aware of people online striking up relationships and requesting you to purchase gift cards.**
- **If you receive an email from a work colleague, check it out with them in person where possible.**

Members of the public and sometimes businesses/employees are targeted with 'Gift Card Fraud'.

The criminal (often presenting as the victim's colleague/manager or organisations such as the police, bank, DVLA and HMRC) asks the victim to purchase gift cards, usually from supermarkets.

Methods that have been used are phone calls, emails (even emails purporting to be from the victim's place of work, requesting the gift voucher for a colleague) and messages on social media or emails.

Once purchased, victim's are asked to pass over details from the gift card.

Gift cards are popular with criminals to launder money as they are difficult to trace compared to bank transfers.

£58K

Stolen in the North East throughout February

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

X CYBER ATTACK

On the 10th March X suffered a Denial- of- Service Cyber Attack resulting in users unable to access their accounts for several hours. Monitoring platform ‘Downdetector’ confirms it had more than 1.6 million reports of problems with the site. To keep your X account and all other social media accounts secure please follow the below steps:

Use a strong password that you don’t reuse on other websites.

Use two-factor authentication.

Require email and phone number to request a reset password link or code.

Be cautious of suspicious links and always make sure you’re on twitter.com before you enter your login information.

Never give your username and password out to third parties, especially those promising to get you followers, make you money, or verify you.

Make sure your computer software, including your browser, is up-to-date with the most recent upgrades and anti-virus software.

LOOKING FOR A PERSONAL LOAN?

Customer's who are looking for a loan are being targeted by criminals. There has been an increase in reports from people who have applied for loans and not received them, had loans taken out using their details or applied for loans and have been asked to pay a fee to release the funds.

ADVICE

- **If you have been sent an email to apply for a loan as an existing customer from a company you hold a loan with, visit the website or app and do not do this through an email/message link where possible.**
- **Check out reviews for the company and always check the website domain.**
- **If possible, use a trusted credit reference agency such as credit karma or clearscore to keep check on any new credit applications made in your name.**
- **Before parting with your details ensure you have checked out everything you can.**
- **If suspicious, do not go ahead with the application.**
- **If you think you have given away your details or have not received your loan/asked to pay a fee, report straight away to Action Fraud and the credit agency.**

What's Happening Next?

Carabao Cup final is the 16th March, this creates the perfect opportunity for criminals to target Newcastle fans through the resale of tickets.

The number of reports for Ticket Fraud has doubled this month in the Northumbria area. Several victims report having money stolen whilst buying tickets for the football Carabao Cup Final. Each victim paid an average of £336 for non existent tickets after asking on social media if anyone knew anyone selling tickets to the match at Wembley.

Tickets are often put up for resale on Social Media sites offering tickets but then victims are disappointed when the tickets are fake or they do not receive the tickets at all.

What should you do?

- Buy tickets from reputable sellers, try to avoid buying from random people on social media.
- Use a credit card where possible for better protection under Section 75.
- Try to use the box office site, official website or reputable ticket seller when purchasing tickets.
- Avoid paying directly into someone's bank account.

You should report to Action Fraud online or by calling 0300 123 2040 or online at actionfraud.police.uk

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**
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.