

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 November 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



- Regional Cyber Summary
- Regional Fraud Summary
- Engagement Events

Contents

Looking Forward



- Horizon Scanning
- What's Happening Next

North East Cyber Crime November Summary

AI Voice Impersonations



Sophisticated AI Voice generated scams are becoming more prevalent as AI technology advances. AI technology can quickly clone someones voice to sound like they are in distress. The scammers target individuals closest and trusted to the individual they are impersonating. Often these scams entail asking family and friends to send money urgently to assist in an upsetting situation.

If you receive a call asking for urgent money, pause and verify before acting. It is recommended that families agree a 'safe word' to be used in scenarios like these to help identify if the call is part of a scam.

Fake Shopping Sites



The busy online presence over the Christmas period, Black Friday sales and Christmas deals are all opportunities for Cybercriminals to take advantage of. Cybercriminals set up fake websites that mimic those of reputable retailers by using professional and familiar graphics, logos and slogans alongside attractive offers to scam victims. These sites may lack proper security features such as HTTPS in the URL and are designed to steal payment details or personal information.

Last year, the National Cyber Security Centre reported over £11 million lost to fake retail sites during the holiday season.

Stick to trusted retailers and look for the HTTPS in the URL. Make sure to also implement web filtering and firewalls. Report Fraud can provide further advice to stay protected online.

[Online shopping fraud - Report Fraud](#)

Ticket Sale Law Changes



In November, the government announced plans to make it illegal for tickets to concerts, theatre, comedy, sport and other live events to be resold for more than their original cost.

Ticket touting has become increasingly sophisticated in recent years with touts buying large volumes of tickets online, often using automated bots, before relisting them on resale platforms at hugely inflated prices. The proposals will stamp out this practice, improving access for genuine fans when tickets originally go on sale and ending rip-off pricing on the resale market.

Some official resell platforms are concerned the changes will push customers towards more illicit ways of obtaining tickets and increase fraud risks.

Smart Devices



Over the Christmas period it is likely there will be an increase of smart home devices gifted. Hackers often target these devices by exploiting default passwords or outdated firmware, potentially gaining access to personal networks and sensitive data. It is essential that default passwords are changed immediately, and device software is updated.

North East Fraud November Summary

Police Impersonations with Spoofed Numbers

Two residents in the North East were scammed out of £1000 each by fraudsters impersonating police officers. Both victims received calls from numbers that had been spoofed from local police stations to appear legitimate.

Victims were asked to attend their local supermarket to purchase gift cards and send photos of the codes via WhatsApp.

Both victims were in their early 20's, were from ethnic minorities and were made to feel afraid. One victim was told they were part of a police investigation and needed to pay to clear their name. Another was called from someone claiming to be from the government and was told their National Insurance number was being misused. They were told to expect a call from Cleveland Police and were directed to check the telephone number on the police website. The next call they received was a spoof of this number. After sending codes for 2 x £500 gift cards the victim became suspicious and approached a member of staff in Asda who reported the crime to police.

Gift Card Fraud

Be aware and be vigilant when buying gift cards for Christmas as there has been an increase in Fraud linked to gift cards purchased from supermarkets.

The code in gift cards should remain hidden until the intended recipient uses them. Sometimes it is hidden by foil, sometimes the card needs to be ripped opened to access it. Scammers are going into supermarkets to access the code on the gift card, record the number and will then put the compromised card back. They wait for the card to be activated or to have money put on and drain it as soon as they can, often well before the recipient would think to use it.

Buyers are advised to look for signs of tampering, keep the receipt, and the recipient should access it as soon as possible, log in, check it's online and spend the balance as soon as able to.

The Gift Card and Voucher Association are working hard to stay ahead of fraudsters with better packaging, training, technology and monitoring. They are also working with retailers to share intelligence, strengthen security, and ensure that gift cards remain a safe, convenient and popular way to gift.

North East Fraud November Summary

Fake Business Project Identity Theft

Young people are being targeted through Social Media under the guise of being offered business opportunities.

Fraudsters are offering a cash payment of £500 as part of an 'Amazon Business Project' who then use the victims' details to set up a business in their name.

One victim was told that as residents in China can't have an Amazon account, their details would be used to create an account to sell items. The Fraudster took a photo of the victim with the money, pay slips and their provisional driving license. Bank accounts and Companies House records have been set up in their name using the information supplied.

Parking Notification Text

Phishing text messages claiming the recipient owes money in an unpaid parking fine are still being circulated in the North East.

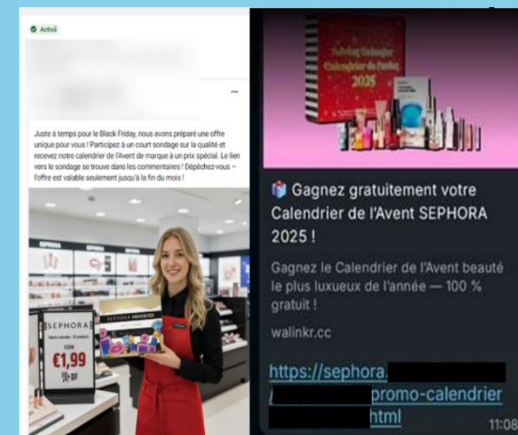
One victim (who had recently disputed a parking fine), reported clicking on the link which took them to a sophisticated copy of a government website. After entering their postcode, it brought back their registration number and other details but the PCN number and amount did not tally with the original fine the victim had received and disputed.

Sephora Advent Calendars

A phishing scam promising a free Sephora Advent Calendar for 2025 is spreading across Europe via WhatsApp messages, fake Facebook advertisements, and fraudulent websites. The fake ads use stolen product images, localised currencies, and phrases like "secret offer" or "limited-time Black Friday deal" to add a sense of urgency and appear credible.

Recipients receive a link asking them to complete a short survey which connects to a fake site mimicking Sephora branding. Following completion, victims are told they have "won" and must share the link with all WhatsApp contacts. Victims are then redirected to fake checkout pages where personal and payment details are requested.

Sephora has confirmed there is no giveaway or promotion and warned users not to share personal or payment information. Remain cautious and verify websites and social media channels are legitimate before entering any sensitive information.



NCSC Proactive Notifications Service

A service that responsibly reports vulnerabilities to system owners to help them protect their services.



About the NCSC Proactive Notifications Service

Working with Netcraft, the NCSC: identifies organisations operating without essential security services/ sends these organisations emails to help them install software updates that can reduce vulnerabilities

This notification is based on scanning open source information, such as publicly available software versions. The service was launched to responsibly report vulnerabilities to system owners to help them protect their services.

This coordinated approach reinforces the broader national effort to make the UK the safest place to live and work online. The service is part of the NCSC's new approach to Active Cyber Defence, and will be delivered as a Minimum Viable Product (MVP) as a pilot, enabling a thorough assessment of its value and the advantages it can offer.

How the NCSC Proactive Notifications Service works

The service discovers vulnerabilities using Netcraft's reach across the internet. Netcraft and the NCSC work together to mutually agree in-scope vulnerabilities for scanning.

Scanning and notifications are based on external observations, such as the version number publicly advertised by the software, and are in compliance with the Computer Misuse Act.

Our default contact method is to contact relevant parties via email.

Organisations are ultimately responsible for the security of their own networks and data, and for determining the steps to protect themselves. This includes identifying and addressing vulnerabilities in their systems. The Proactive Notifications Service does not cover all systems or vulnerabilities, so must not be relied upon as the sole source of security alerts. It is for organisations to determine whether and how to implement the recommendations from this Service

NCSC Early Warning Every day, UK organisations are targeted by cyber criminals – whether for their data, their funds, or simply to cause disruption. Early Warning is a free service from the NCSC that notifies organisations of potential cyber threats before they cause harm. By signing up, you'll receive timely alerts about malicious activity targeting your network – giving you the chance to take action early and reduce risk. The more information you share with the NCSC Early Warning service about your IT estate, the more effectively monitoring can be tailored, ensuring you receive relevant, actionable notifications.

For more information on these services please visit:

<https://www.ncsc.gov.uk/information/proactive-notifications-service>

Have you received an email from the NCSC Proactive Notification Service?

Here's how you can be sure this email is legitimate:

- the email has come from a netcraft.com address
- the email is in plaintext format - it may contain clickable links, but if you are concerned by them you can copy and paste the text into a browser
- the email does not include any attachments
- the email does not ask you for personal or other information, or for payment

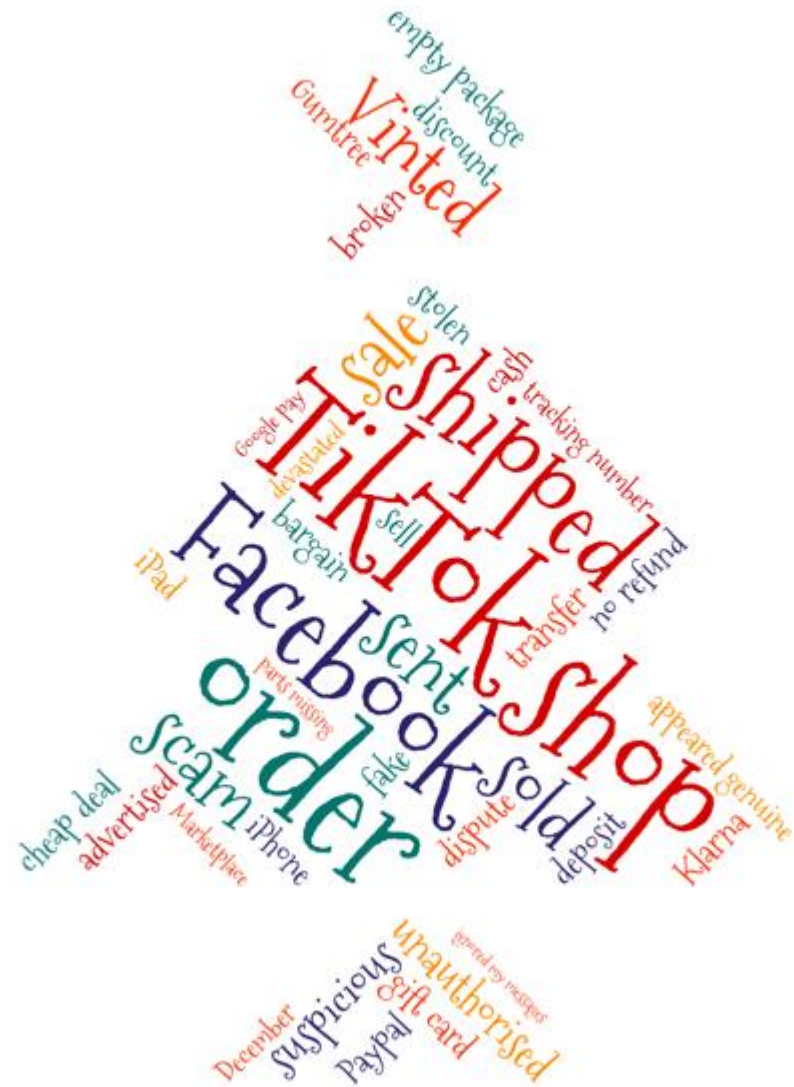
If you have received such an email and are still concerned by it, you can contact acdenquiries@ncsc.gov.uk for further advice

HAVE A FRAUD FREE CHRISTMAS

Online Shopping and Auction Fraud continues to be the most reported Fraud in the North East.

During the festive season this is expected to rise further as consumer's spending increases over the festive period. Some tips on how to have a Fraud free Christmas are on the next page.

Merry Christmas from everyone here at the North East ROCU.



Keywords have been taken from Online Shopping and Auction Fraud victim reports to Action Fraud – October 2025

Festive Shopping Tips

Check you are using genuine website domain addresses when shopping online.

If you are using Facebook Marketplace, try to see the item in person.

Check reviews of websites before purchasing.

Always use a credit card for large purchases over £100, they offer more protection through section 75 of the consumer credit act.

REMEMBER!!!

If it seems too good to be true, it probably is.

Be wary when looking for deals, especially on social media.

COURT RESULT



A Fraudster who swindled almost six million pounds of public money has been stripped of his assets and ordered to pay back his illicit profits – despite his previous attempts to fight and appeal court rulings.

Stanley Miller was jailed in 2018 for eight years and three months after he was caught out in a complex series of Frauds which saw him pocket over five million of taxpayers' money. A complex investigation pieced together by HMRC found the 64-year-old had been deliberately evading paying VAT, Income Tax and National Insurance between 2008 and 2016, as well as laundering money and benefitting from criminal cash.

In October 2018, Miller went to trial at Newcastle Crown Court, and he was found guilty of four counts of being concerned in fraudulent evasion to the tune of £1,055,294 and one count of cheating the public revenue to the tune of £4,897,045

After conviction, a thorough financial investigation was launched by the North East Regional Organised Crime Unit (NEROCU) to strip Miller of his illicit funds and illegally purchased properties.

They collated a strong evidence case file, presented it at court this month a Judge ruled in their favour and ordered Miller to pay back £5,470,258. If he fails to do so within three months, he will be ordered to carry out a sentence of 10 years imprisonment.

Criminals often think they can conceal accounts, finances and luxury items, so when they are released, they can return to the lifestyle their illegal activity afforded them. However, this isn't the case.

For some offenders prison might not seem like much of a deterrent if they have a nice home and a healthy bank balance to return to, which is why we carry out comprehensive investigations to ensure these people are stripped of criminal assets and shown that crime doesn't pay.





Tell the Police about cyber crime and fraud

reportfraud.police.uk or call 0300 123 2040

Report Fraud has replaced Action Fraud, for use in England, Wales and Northern Ireland.

Anyone searching for how to report cyber crime or fraud, or trying to use Action Fraud, will, from 4 December 2025, be redirected to the new service, which can be reached directly online at reportfraud.police.uk or by calling 0300 123 2040.

Report Fraud will provide:

- A clear and simple reporting process to tell the police about cyber crime and fraud
- Guidance on what to report and how that information is used
- Further support information for victims

ENGAGEMENT EVENTS

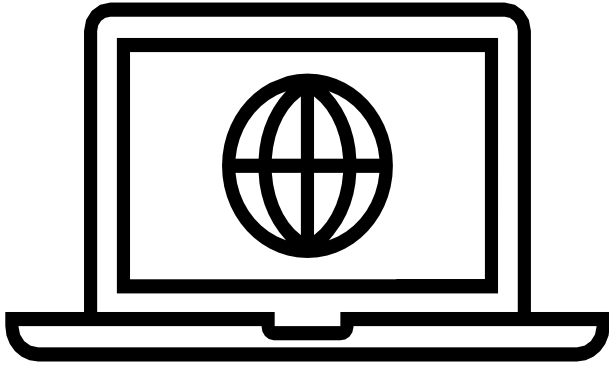
Below are just some of the events the team have attended this month...

- Sensory Support Drop-In for adults in Middlesbrough who are partially sighted, blind, deaf or hard of hearing.
- Fraud Roadshow Stalls at all North-East Universities
- Neighbourhood Policing team briefing sessions at Cleveland and Durham Police
- Fraud Watch - Hamsterley Mill Residents Association
- Fraud Forum Skipton Building Society - Hexham Branch - Staff Input followed by Info Stall event in-branch for customers.
- Fraud Foundation Presentation at Regional Digital Inclusion Meeting in Morpeth



Horizon Scanning

Monitoring Threats



In October last year, there was a ruling around **PPI compensation for car owners**. Consumers who believe they weren't told key details about their motor finance arrangement, such as commission payments, will need to complain to their lender if they haven't already done so. The compensation scheme will open in early 2026. Once it does, lenders will contact those who've complained, asking if they want to opt in to have their case reviewed. Those who haven't complained will be contacted by their lender within six months of the scheme starting and will have six months to opt in.

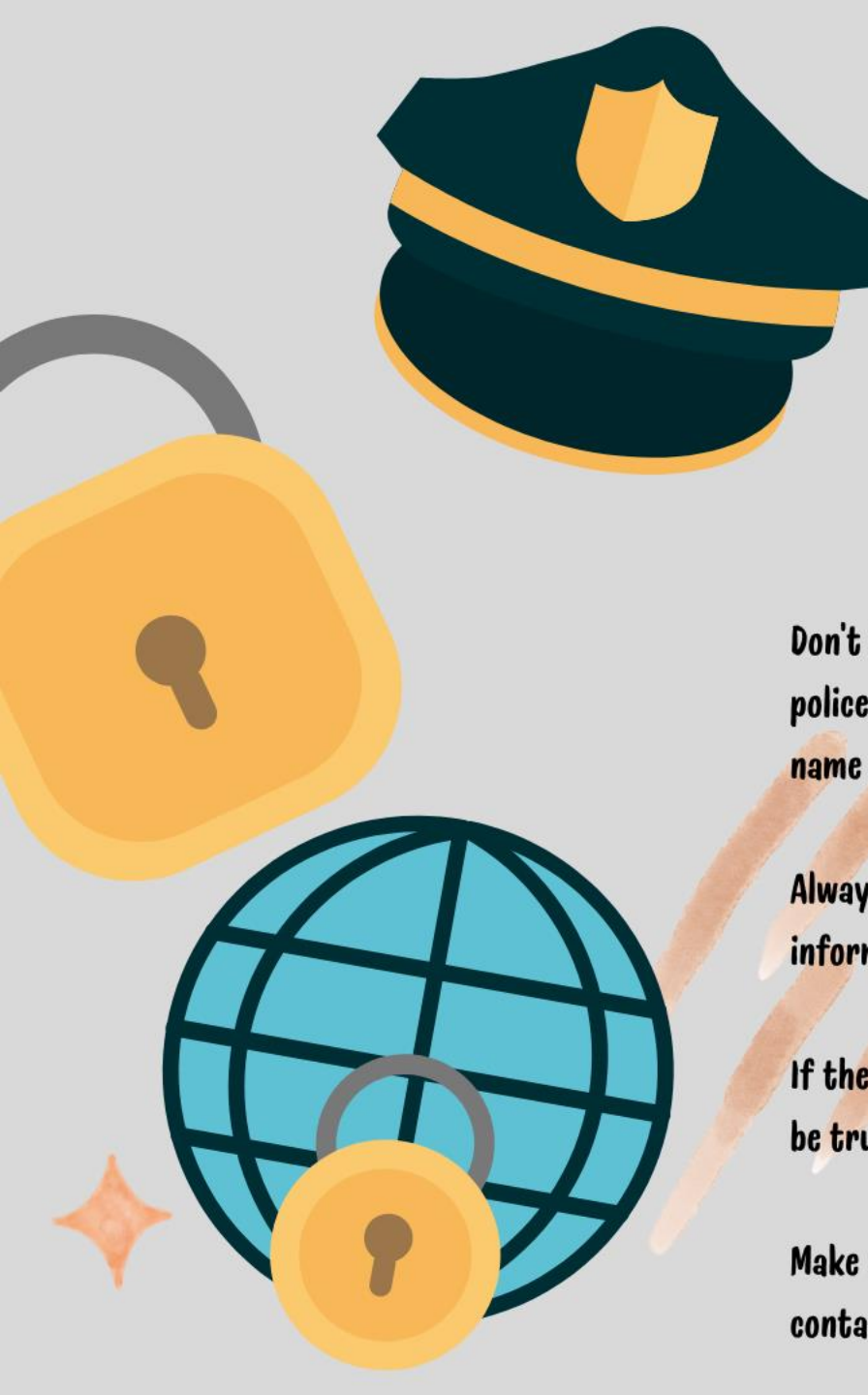
Be mindful if you use a claims management company (CMC), you'll need to give part of your payout to that firm if your claim is successful. There are many adverts on social media encouraging drivers to sign up with these companies. The FCA and the Solicitors Regulation Authority (SRA) have urged consumers not to rush to sign up with CMCs or law firms, as they may charge fees of up to 30% from any award.

Fraudsters are using this as a ruse to steal from victims. Some are stealing personal and financial information. Others are claiming they have a cheque to post but need a payment in advance to cover administration or courier costs.



Selling on Facebook Marketplace?

- Check buyer profiles and reviews.
 - Always ask to be paid in cash rather than by bank transfer, cheque or PayPal to reduce the risk of fraud against you.
 - If you're meeting someone in person, arrange your meeting in a public, well-lit area. Create and share your meeting plan with a trusted friend or family member.
 - If you're posting an item, consider using a tracked and insured postage service so that you have proof of delivery and protection against false claims that the item wasn't received.
- 



The bank or police will never ask you for money or gift cards

Don't trust the name or number on your phone: If you receive a call or message claiming to be from your bank, the police, a government department or any other trusted source, never assume it's genuine, regardless of the number or name displayed on your phone.

Always be suspicious of any unexpected calls that pressure you into providing your personal or financial information.

If they claim to be someone you know or from an organisation, hang up and call them back on a number you know to be true.

Make sure the line is clear before making a call to your bank or the police. Call 159 (the universal safe number) to contact your bank

What's Happening Next?



Looking to escape the cold weather?

After Christmas people will start to look for an escape from the cold weather. Watch out for adverts on social media selling fake holidays and flights.

- Ensure that you are using a legitimate website.
- Make sure your holiday is ABTA or ATOL protected.
- If you are waiting for a refund, ensure you are speaking to the airline or company before sharing any information.

January Sales

As Christmas is approaching people may hope to bag themselves a bargain. Be vigilant when using websites and always check they are secure and the website address is correct before entering any personal or sensitive information. Please follow the advice given in this document to keep yourself safe when making the most of the January sales.





SEASONS

Greetings

FROM EVERYONE AT

North East

ROCU

Regional Organised Crime Unit Network





 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



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	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.