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 April 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 April Summary

DECREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Cyber Reports (compared to April 2025)	**110** (-11%)
Hacking -Social Media and Email	**74** (-26%)
Hacking - Personal	**18** (+38%)
Computer Virus/ Malware	**10** (+233)
Hacking - Extortion	**5** (-16%)
Denial of Service Attack	**1** (No change)

Online shopping accounts hacked

In the region we have received reports of Ocado account hackings where customers have reported they have received a notification of a large payment leaving their account and items purchased that they did not make or authorise. The purchased items were then delivered to an address unknown to the victim.

Action you should take if your account is hacked or you notice unusual activity:

- Contact your account provider for help and support for account recovery process.
- Check your email filters and forwarding. Cyber criminals are known to set up a forwarding rule to automatically receive a copy of all emails sent to your account, which could allow them to reset your passwords.
- Change passwords. You should immediately change the password for the hacked account. It's also important to change the password for any accounts where you use the same password. This is important because cyber criminals know people often use the same password for different accounts, and so will try the same 'hacked' password across multiple accounts
- Log out of all devices and apps in your account when you have changed your passwords. This means a cyber criminal won't be able to use your old password to access your account.
- Set up 2 step verification and ensure all your devices and apps are updated. Tell your contacts in case they receive any unusual requests or links and check your bank account for any unusual transactions or purchases.
- Report to Report Fraud.

North East Fraud April Summary

DOWN THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

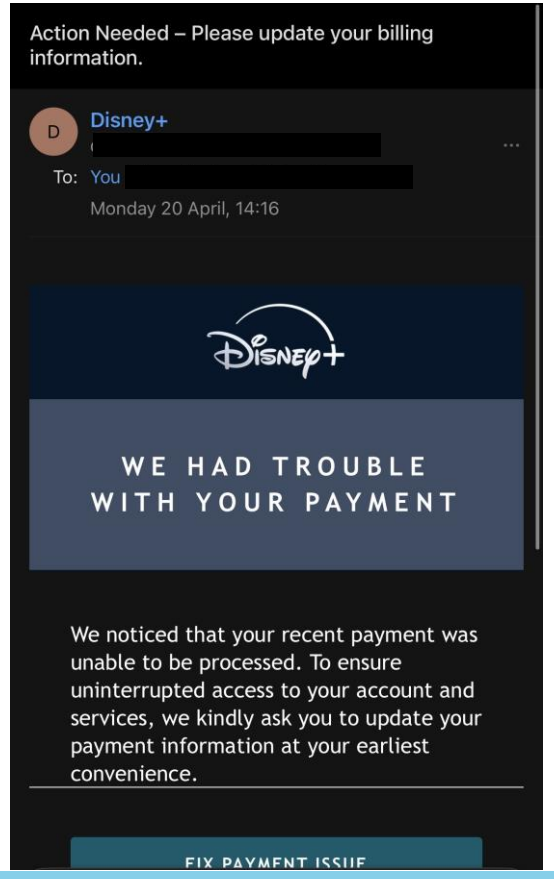
Total Fraud Reports (compared to April 2025)		**681 (-4.6%)**
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
Advance Fee Frauds	⟷	**124 (+0.81%)**
Online Shopping and Auctions	↓	**115 (-13.5%)**
Cheque, Plastic Card and Online Bank Accounts	↑	**112 (+211%)**
Investment Fraud	↑	**71 (+26.8%)**
Other Consumer Fraud	↑	**69 (+11.3%)**

TV Streaming Services

Victims have reported receiving scam emails from streaming services such as Netflix and Disney plus.

The emails are often disguised as billing issue reports and are designed to steal banking and credit card details. These emails frequently claim your payment failed, your membership is suspended or you need to update your details to continue watching

The messages are fake and have not been sent from your provider. Report these emails to report@phishing.gov.uk



Political AI investment deepfakes

The volume of political deepfakes has risen sharply in recent years. Since the beginning of 2025, over 1,000 English-language social media posts featuring AI-generated images or videos linked to prominent political figures, issues, or events have been found.

The videos and reels are based on genuine news reports or reputable TV programmes and adapted to advertise Investment Frauds which are then shared across social media platforms. A recent one circulating across the North East shows Nigel Farage accusing the Bank of England of retaining investment opportunities only for the wealthy. He then shares the details of the £250 minimum investment plan to ‘help’ hard working people. This is a scam using deepfake technology to adapt the original footage to use in the fraud.

TSB found that 90% of customers had seen an investment ‘opportunity’ on social media, with more than 43% considering investing as a result. Of the 31% who acted on financial advice from social media, more than half had money stolen through these frauds.

Fake Days Out

There is a trend emerging where attractive or reasonably priced days outs and events advertised on social media turn out to be fake. Most of the photos and videos used to advertise the events have been altered using AI.

As the school summer holidays approach, it's likely that more of these events will appear in social media feeds as scammers look for new ways to steal from victims. Some examples this year have included tickets for non-existent Christmas markets at Buckingham Palace and Hot Air Balloon festivals.

Scammers also duplicate social media pages for legitimate events and organisations to hijack their ticket sales. Events popular with scammers include lantern or hot air balloon festivals featuring breathtaking AI imagery. Tickets are sold but there is no event. Also be mindful of 'Ghost' craft fairs and 'secret venue' film screenings and concerts that promise to reveal the top-secret location on the day of the event, only after tickets have been purchased.

What to look out for:

- Pay attention to the web address and branding to ensure it's the legitimate site. Stick to the official website to buy tickets.
- There may be a low number of likes for the page. Comments are often turned off or there are lots of positive bot reviews with similar wording.
- Location. If there's no specific address listed but just a vague description, such as 'central Newcastle', that's a red flag, as is having incorrect contact details on the 'About' page.
- Price and urgency. A very low price or claims of 'only a few remaining' are also warning signs to watch out for.

If you spot a misleading advert for a fake event or attraction on Meta platforms (Facebook, Instagram or Threads), you can click the three dots in the feed and 'Report ad' or search for the company and its advert through the Meta Ad Library. TikTok and X have their own in-app reporting tools. You can also complain about an advert to the Advertising Standards Authority and flag a ticketing scam to Report Fraud.

Banking Scams

Your bank will never contact you and ask you to state your details or ask you to transfer funds / make a payment.

- Never trust a call or message claiming to be from your bank
- Do not divulge any personal or banking information
- Do not click on any links

What to do?

- If you are contacted via telephone, hang up and phone your bank on a trusted number – this can be found on the back of your debit card
- If you do not have the number to hand, phone 159. This is a free service call centre, which will put you through directly to your bank.
- It is advised you make this call on a different phone or wait 15 minutes before making the call – the criminal may have kept the line open

REPORT IT!
You can report any scam to reportfraud.police.uk
or call 0300 123 2040

Report Fraud

BEWARE OF PAYPAL SCAMS

The Fraud

- People are receiving messages, seemingly from the official PayPal address
- These messages state that the recipient is due a small refund (usually 1p)
- They then state the small amount is to confirm the account, before then sending a larger amount
- It asks you to call a number if you didn't authorise this to 'immediately secure your account and request a refund'
- On calling the number, the criminal requests personal information
- Some victims reported their account hacked while others reported financial loss

How to spot it

- Double-check the contact details – are you asked to call, email or follow a link that isn't associated with the brand it claims to be from?
- Have you been asked for personal or financial information?
- Check for poor spelling, grammar and general presentation?
- Are you being rushed or pressured?

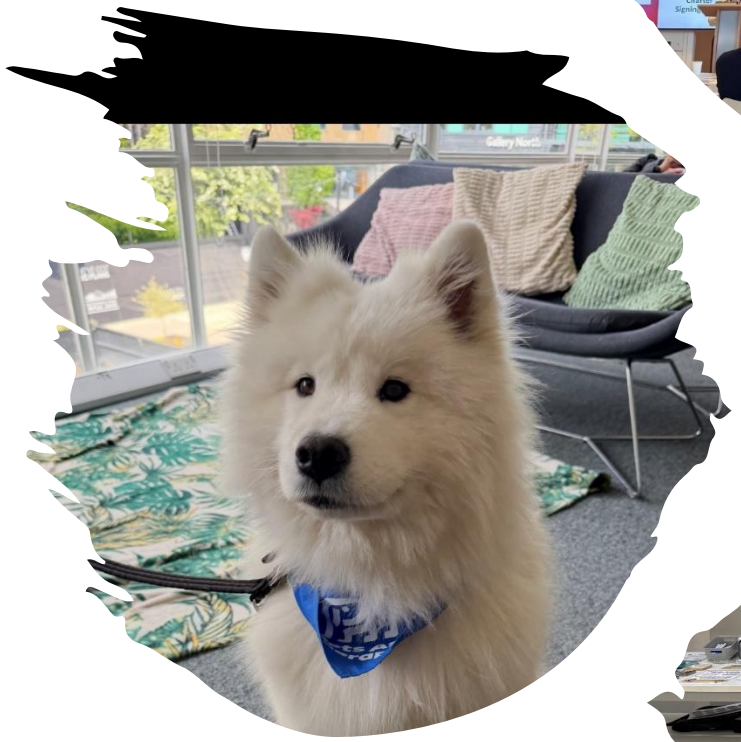
What to do

- Do not call the number or reply to the email
- Log in to your PayPal account or App, change your password and make sure it is strong and unique
- Make sure two factor authentication is enabled
- Report suspicious emails to phishing@paypal.com, then delete them
- If you have passed bank details or lost money, immediately contact your bank and contact report fraud.police.uk or call 0300 123 2040

ENGAGEMENT EVENTS.

This month we have visited and worked with:

- Northumbria University (assisted by the lovely service dog – Meidik, pictured)
- Middlesbrough College
- Sunderland council
- St Bede's Church, South Shields
- Thriving Together – At Felton Village Hall
- Stop Loan Sharks
- Sunderland University
- Northumberland Council
- The Cyber Resilience Centre
- Gateshead Citizen's Advice



Want to be a part of our growing community? Contact us at –

RECCC@durham.police.uk

What's Happening Next?

National:

- Throughout May, *Romance Fraud* campaign.
- There will be an increase in media regarding the risk of 'Holiday insurance fraud'.

North East region upcoming events:

- 27th May – Sacred Heart Church, Boldon
- 28th May – Northumbria university budget breakfast
- 4th June – Mobile phone security session, St. James Church, Mill Lane, Hebburn
- 5th June – Merchandise drop - All saints Church, Newton Hall, Durham

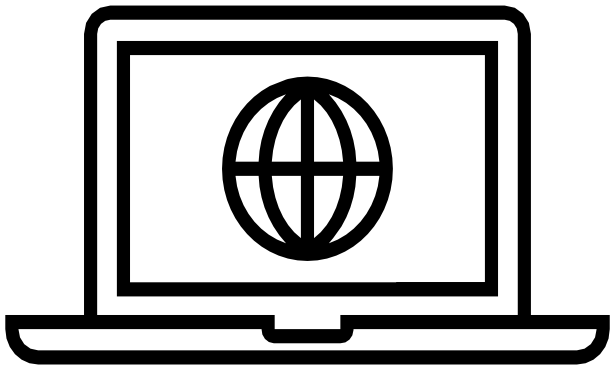
If you'd like further information about any of these events, or would like to invite the RECCC to your event, please email us at –

RECCC@durham.police.uk

We are happy to help where possible and facilitate a strong and engaged North East Network.

Horizon Scanning

Monitoring Threats



Barclays bank scam

- SCAM texts pretending to be Barclays claim that a direct debit has been set up and gives a number to call. Calling it connects you to scammers posing as the bank, to obtain your personal and financial information. Forward any such text message to **7726**

FCA scam text

- A similar message is doing the rounds in relation to the FCA (Finance Conduct Authority), in which they provide a phone number and then try and obtain personal and bank information, claiming that victims have been identified via a 'Report Fraud Data Breach'. Do not use the phone number and forward the text to **7726**

TV license email scam

- An email has been reported circulating, stating that recipients TV licenses could not be renewed. It then goes on to provide link in order to rectify the problem. Do not click on the link and forward the email 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 – aske trusted people
Manage – report the issue to report fraud or police.

ATM SKIMMING

Across the country there have been reports of an increase an increase in the use of skimming devices attached to ATMs

Things to look out for:

- Obstructions in the card reader slot
- Use a phone torch light flashed into the card reader slot which could show something between the credit card slot at the back (see arrow in photo 2)
- Is the gate at the back of credit card reader open?
- Slight resistance when sliding the card in
- A clear ‘join’ where the camera mount meets the machine

PASSWORD MATTERS

- Use a strong password: Make your password at least 12 characters long (3 random words), and include a mix of uppercase and lowercase letters, numbers, and special characters.

- Use a unique password for each account: Don't reuse the same password for multiple accounts.

- Use a password manager: A password manager can generate and store your passwords, and some can even automatically enter them for you.

- Use 2 Step Verification : 2SV adds an extra layer of security by requiring a second factor of information.

- Be aware of phishing attempts: Be cautious of any attempts to trick you into sharing your password.

THE CYBER RESILIENCE CENTRE NETWORK

Police-led, **Business**-focused
Enquiries@nebrcentre.co.uk

Police-Led, Business Focused
Here to protect businesses from online fraud and cybercrime

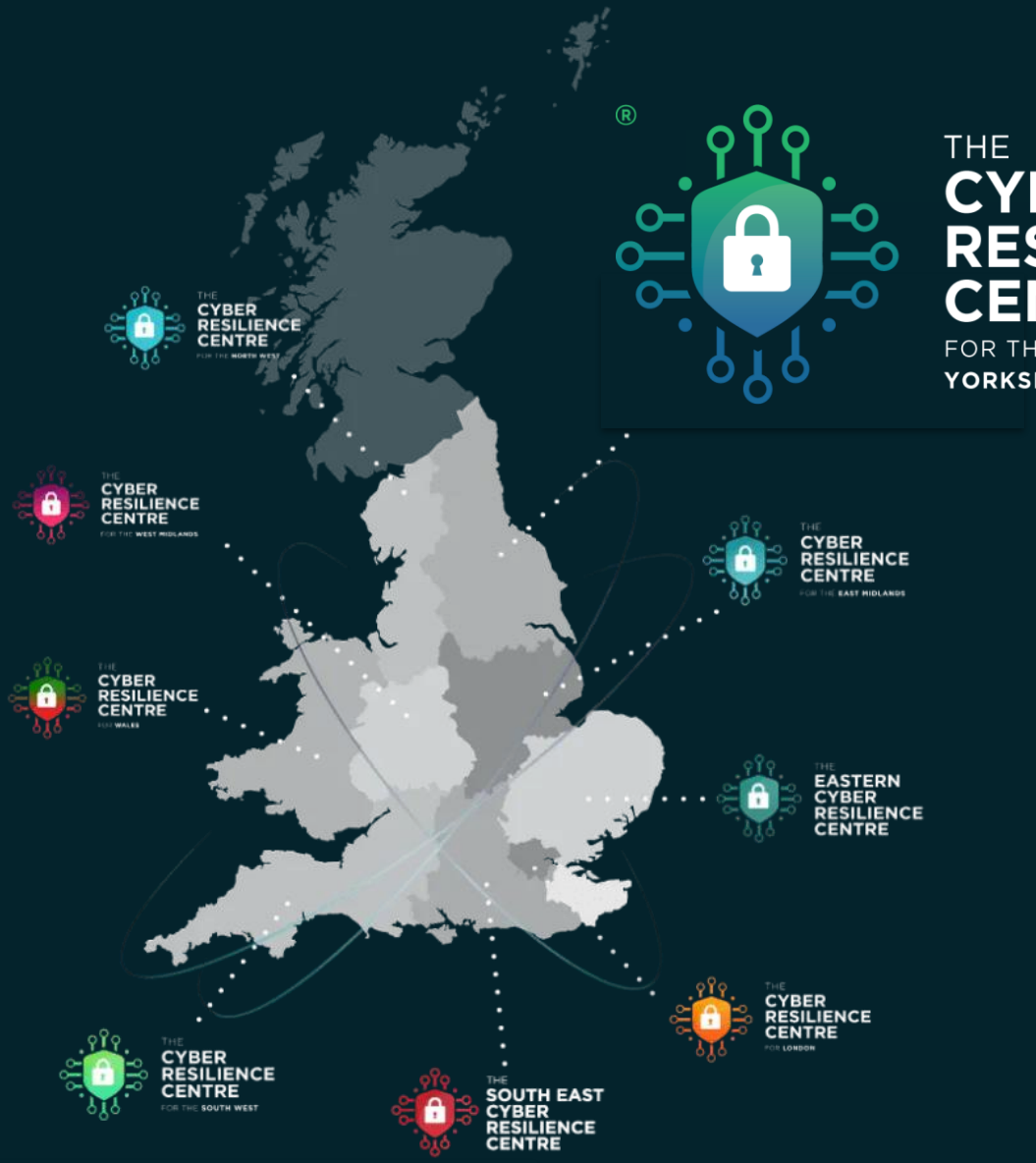
Supporting Sole traders, Micro, Small and Medium businesses, charities and standalone schools

National Network of 9 Centres

Home Office

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:

This docum

North East RECCC Regional Economic Crime Coordination Centre

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

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	**Claire Hardy– Economic Threat Desk Analyst** **Nicola Lord –Cyber Threat Desk Analyst** **PC Brian Collins – Engagement Officer**
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.