

# 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 September 2025 data with a forward outlook.

Please contact the Regional Economic Crime Coordination Centre (RECCC) if you have any questions: [RECCC@durham.police.uk](mailto: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 September Summary

INCREASED THIS MONTH  
COMPARED TO THE SAME  
MONTH LAST YEAR



Total Cyber Reports (compared to September 2024)		 205 (+23.5%)
	Hacking -Social Media and Email	 174 (+30.8%)
	Hacking - Personal	 20 (+42.9%)
	Hacking - Extortion	 6 (-33.3%)
	Computer Virus/ Malware	 5 (-44.4%)
	Hacking - Server	 0 (-100%)

## Android Banking Malware Targeting UK on The Rise

The Credit Industry Fraud Avoidance System (CIFAS) along with UK intelligence services and cybersecurity researchers have highlighted a steep increase in Android malware campaigns targeting banking fraud in the UK. In the first half of 2025, over 200,000 people are likely to have been exposed to malicious applications (apps) designed to capture banking credentials but masquerading as legitimate tools.

These apps often mimic useful tools and request permissions that allow them to intercept one-time passcodes, monitor transactions, and take over banking applications. Cyber and fraud criminals are evolving their delivery methods, shifting away from simple phishing emails toward more convincing mobile-first approaches.

As mobile fraud tools become more sophisticated, customers need to be extra vigilant when downloading apps especially those offered via unofficial app stores or those requesting excessive permissions.

## Extra vigilance around scam messages

As we start to enter the festive season, we always see an increase in scam messages being reported. This is largely due to a lot of people relying on parcels to be delivered, which a lot of companies will communicate delivery updates via text. Please be extra vigilant of scam text messages, emails, websites and adverts over the coming months.












More information on how to spot and report scam messages can be found here - [Phishing: Spot and report scam emails, texts, websites and... - NCSC.GOV.UK](#)

# North East Fraud September Summary

INCREASED THIS MONTH  
COMPARED TO THE SAME  
MONTH LAST YEAR



£3.7 Million loss  
this month (-65%)

Total Fraud Reports (compared to September 2024)		 789 (+22.1%)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
	Advance Fee Frauds	 148 (+76.2%)
	Online Shopping and Auctions	 138 (+10.4%)
	Other Consumer Fraud	 76 (+40.7%)
	Investment Fraud	 66 (+78.4%)
	Cheque, Plastic Card and Online Bank Accounts	 51 (+30.8%)

## BBC iPlayer



Fraudsters have been targeting victims through their Smart TVs. This month, 4 victims report pop up warning messages on their screens highlighting issues with their BBC iPlayer. A call was then received from someone claiming to be from the BBC who would resolve the issue. Victims were asked for personal and banking information then asked to authorize payments. In some instances, they were asked for authorization codes which were discovered to be banking payment codes to enable theft from the victims bank accounts.

One victim struggling to download the app was contacted on Facetime after providing basic information and offered support. They were asked to download an app for the 'support' to access his laptop. This was then used to access the victims bank accounts.

## Number Spoofing

Legitimate technology utilised by businesses to make it easier for customers to return calls is being misused by nuisance callers and fraudsters. Number spoofing allows fraudsters to get around call-blocking devices to trick the public into accepting calls they would rather ignore. 56% of fraud victims who were defrauded after receiving fake phone calls or texts reported it involved number spoofing.

Fraudsters don't just impersonate company numbers – they can spoof personal mobile numbers too. This tends to be uncovered once a stranger starts calling or messaging angrily about contact they believe came from you. This can be intimidating and stressful.

# North East Fraud September Summary

## Social Media Customer Service Scam

The image shows the logo for the 'Lemfi' app, which consists of the word 'LEMFI' in white capital letters on a green rectangular background.

There is trend emerging where victims report being targeted by fraudsters after posting complaints and issues with companies on Social media sites. Either the initial account registering the complaint is fake or the victim is approached using a fake customer service account. Victims are asked to download an app called Lemfi to receive compensation.

After posting on X about a problem with British Airways, one victim received a response from the BA Helpdesk support team with further contact via WhatsApp. They were offered £500 compensation and were asked to download Lemfi in order to receive the payment. They were asked to verify the account by authorising a £500 payment which the victim refused to do.

Another victim raised a complaint on the Boots Facebook page and thought it had been picked up by customer service. The fraudster asked for their telephone number via Facebook messenger then made contact and talked them through setting up an account with Lemfi. The victim was asked to add £130 into the Lemfi account as verification and was informed the fraudster would refund the money. They asked the caller to pay a further £209 into the account at which point suspicions were raised and the victim requested a refund and the fraudster became aggressive.

## Rental Fraud



There is usually a seasonal increase each August and September with students renting properties for the new academic year but this month the increase is greater.

One victim tried to rent a property using Open Rent. They believed they were speaking to an Estate Agent who said the property had gone but there was new one available. They were shown around the house and were happy with it. Rent was paid upfront in full. When the victim went to the property to get the keys the estate agent did not turn up. There was another couple there that advised that the same agent was meant to give them keys for the same property. There have been several victims reporting having money stolen from fraudsters after finding properties through online letting listing sites Open Rent or Open Door.

## Cyber Crime Officer Call

Impersonation calls tend to come from fake bank staff and police officers. This month, a victim has reported receiving an unusual call from a fraudster purporting to be a UK based Cyber Crime officer. The fake officer stated that withdrawals had been made from their cryptocurrency wallet. The victim was asked to provide evidence of transactions and personal information to prevent fraudulent activity.

# ENGAGEMENT EVENTS

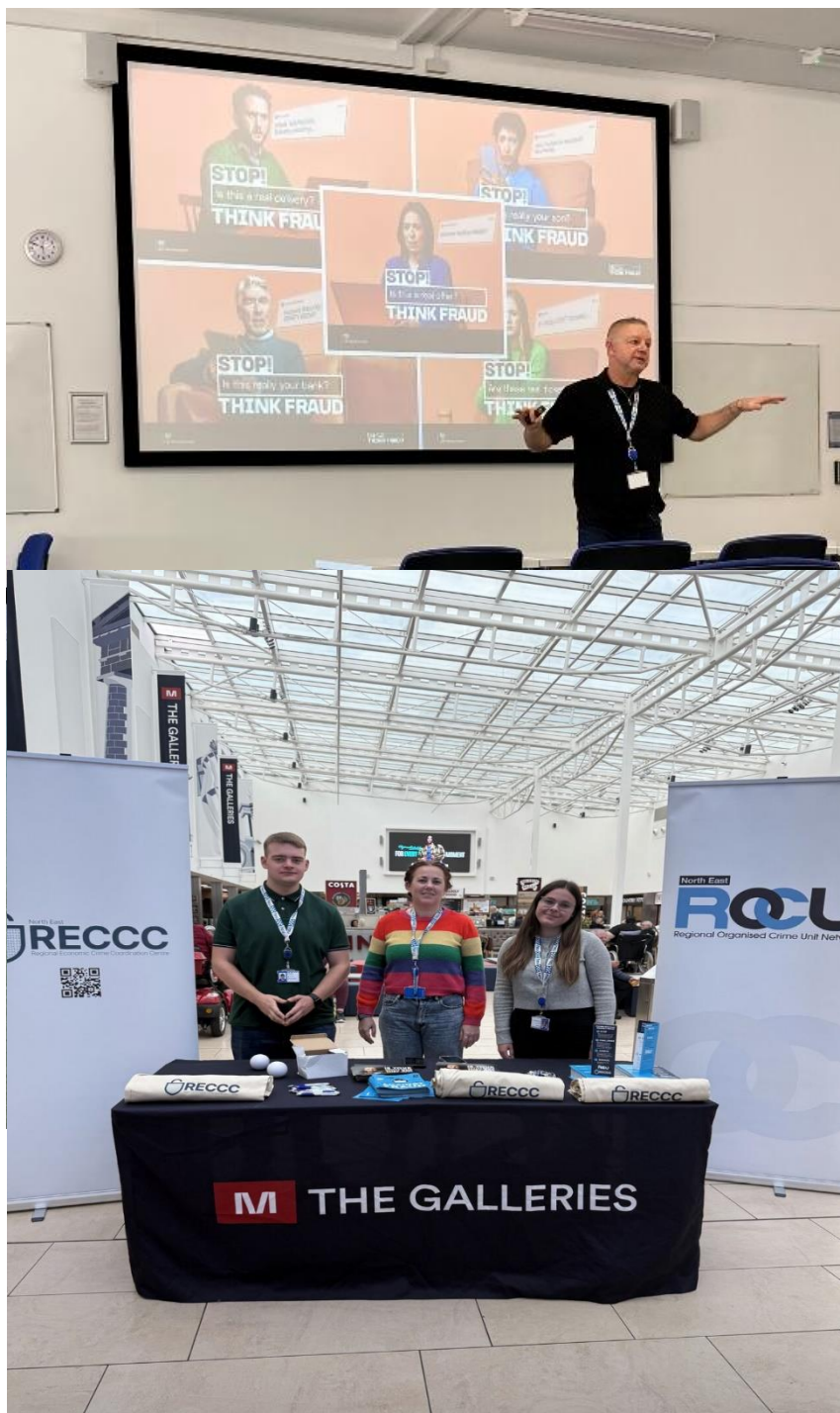
Below is just some of what the team have been up to this month...

This month the team have attended freshers events across the region for Colleges and Universities including Teesside University, Durham University, Northern School of Art, Darlington College and Sunderland University.

Online Fraud Awareness workshops have been delivered to ITEC apprentices, Citizens Advice Gateshead, Baltic Apprenticeships, Tees Valley Learning Partnership and Darlington Extra.

Air Cadets across Durham, Grange Ladies, KLEEK apprenticeships and New Marske Ladies Fellowship have received Fraud Awareness inputs.

The Bread and Butter Thing at Billingham, Darlington and Hartlepool and The Galleries have all had visits to advise staff, volunteers and customers how to keep themselves safe.





# What can you do to protect your business from Cyber Crime and Fraud?

Sign up for Police CyberAlarm provided for free from your local police force, it detects and provides regular reports of suspicious cyber activity and vulnerabilities enabling your business or organisation to identify and mitigate its cyber risks. Find out more and sign up here:

**[Police CyberAlarm](#)**

Obtain 'Cyber Essentials' certification and receive other Cyber Security Services from police-led [NEBRC | Business & Cyber Resilience Centre for North East SMEs](#)

Get in touch at [RECCC@durham.police.uk](mailto:RECCC@durham.police.uk) to book in for a FREE Cyber or Fraud Awareness session for you and your staff. We have teams covering Northumbria, Durham and Cleveland Police Force areas.

For advice and guidance visit :

[National Cyber Security Centre - NCSC.GOV.UK](#)

[Cyber security guidance for organisations | Action Fraud](#)



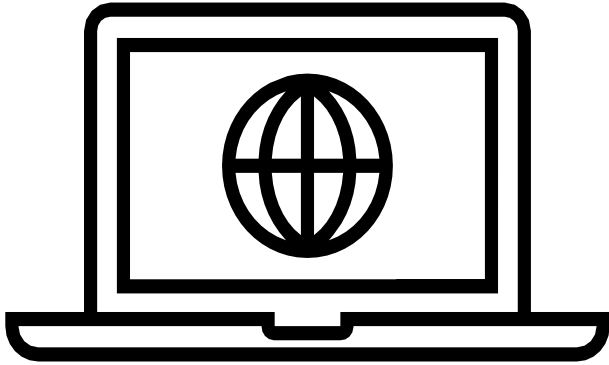
**SAFER BUSINESS ACTION WEEK**  
**10<sup>th</sup> November 2025**

National Business Crime Centre (NBCC)



# Horizon Scanning

## Monitoring Threats



### WhatsApp Gold Scam

There is a 'WhatsApp Gold and Martinelli video' fake warning message circulating on WhatsApp. The message warns the person receiving it that there are messages circulating to upgrade to 'WhatsApp Gold' and promises benefits like free flights, upgraded video calling and other enhanced features (this is true, there are scam messages of this nature).

It asks that you click the link, If you do it will take you to a website with malware on it that can steal your personal data. The message also warns of a 'Martinelli video', there is no evidence this video exists but there is a potential it could be sent in another message, if you receive it, delete it.

- Updates for WhatsApp updates will happen automatically in the App.
- If you do receive the message do not reply or forward it and you can report to Action Fraud.
- Make sure you do any software updates on your phone.







# 5 Ways To Protect Yourself From Number Spoofing Scams



Although you can't stop scammers from attempting to spoof numbers, you can take steps to reduce the risk and protect yourself if you're targeted:

**1. 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.


**2. Don't give out sensitive information on incoming calls:** Hang up, wait for five minutes and either call the firm on a trusted number (such as on the back of your debit card or on its official website) or dial 159 to connect to your bank's fraud team.

**3. Landline call blocking:** Ask your provider whether it offers a call screening service such as BT Call Protect and Sky Talk Shield, which allow you to screen unrecognised numbers and block unwanted callers.


**4. Mobile call blocking:** Check iPhone and Android settings for call blocking, spam protection and caller ID verification. These services aren't perfect, but they can help.

**5. Call-blocking phones** Switch to a call blocking phone or a True-Call Device that plugs into your existing handset. Both will let calls from your contacts come through, but will ask other callers to leave a message so you can decide whether to pick up.




 Cyber threats are one of the biggest risks facing small organisations today — but protecting your business doesn't have to be complicated or costly. Join us for a free, practical webinar designed to help small businesses, charities and public sector teams strengthen their cyber resilience.


Using official guidance from the **National Cyber Security Centre (NCSC)**, we'll explore the five essential steps from the NCSC Small Business Guide — simple, effective actions to reduce the likelihood and impact of cyber incidents.

 In this session, you'll learn how to:

- ✓ Safeguard your critical business data
- ✓ Protect against common online threats
- ✓ Keep your devices and systems secure
- ✓ Manage access and authentication safely
- ✓ Build a culture of cyber awareness and resilience

Delivered by Regional Cyber Protect Officers from the **North East Regional Organised Crime Unit (NEROCU)**, this session includes practical tips, real examples, and information on free referrals to the **North East Business Resilience Centre (NEBRC)** and **Police CyberAlarm**.

 Whether you're a business owner, team leader, or staff member, this webinar will give you the confidence and knowledge to take control of your organisation's cyber security.

 Multiple dates in December 2025 and January 2026

 Online – Free to attend  <https://lnkd.in/e-jwRhpe>



# What's Happening Next?



The Financial Conduct Authority (FCA) have started to consult on a redress scheme for those who have had Discretionary Commission Agreements (DCA) on their vehicles since 2007 to 2024. They are expected to make their final decision in November on how lenders will compensate consumers. The expectation is that the payment will be on average £700.

It is likely that criminals will try to target consumers, we are asking people to remain vigilant and avoid using third party companies to make claims where possible.

## **Advice:**

- You do not need to use a third party or law firm to make a claim, and they are likely to take a large cut from any compensation if you do.
- There is a free tool on the Martin Lewis website which you can use to aid your claim.
- Be wary that you could receive communication via email, phone or letters claiming to be from lenders or claims firms. Always double check and use numbers you know to be legitimate.



# What can we do for you?



If you think any groups that you attend or run could benefit from the services we offer, please get in touch at [reccc@durham.police.uk](mailto:reccc@durham.police.uk)



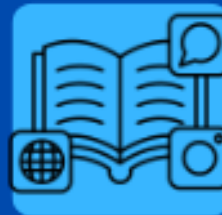
Advice  
Stalls and  
Events



A link between  
yourselves and  
NEROCU



Monthly  
Newsletter



Staff  
CPD/Inputs/  
Workshops



 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](http://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](mailto: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

<b>Distribution List</b>
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 it's 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.**



<b>Protective Marking</b>	<b>Official – Law Enforcement</b>
<b>Version</b>	<b>Final</b>
<b>Purpose</b>	<b>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.</b>
<b>Owner</b>	<b>NEROCU</b>
<b>Authors</b>	<b>Megan Turner – 3P Officer Claire Hardy– Economic Threat Desk Analyst Nicola Lord –Cyber Threat Desk Analyst</b>
<b>Reviewed By</b>	<b>SGT Emma O'Connor</b>

## 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.