

North East

ROCU

Regional Organised Crime Unit Network

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 August 2023 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](#)
- [Courier Fraud Advice](#)
- [What's Happening Next](#)
- [Remote Access Fraud Advice](#)

Fraud Category North East Victim Reports

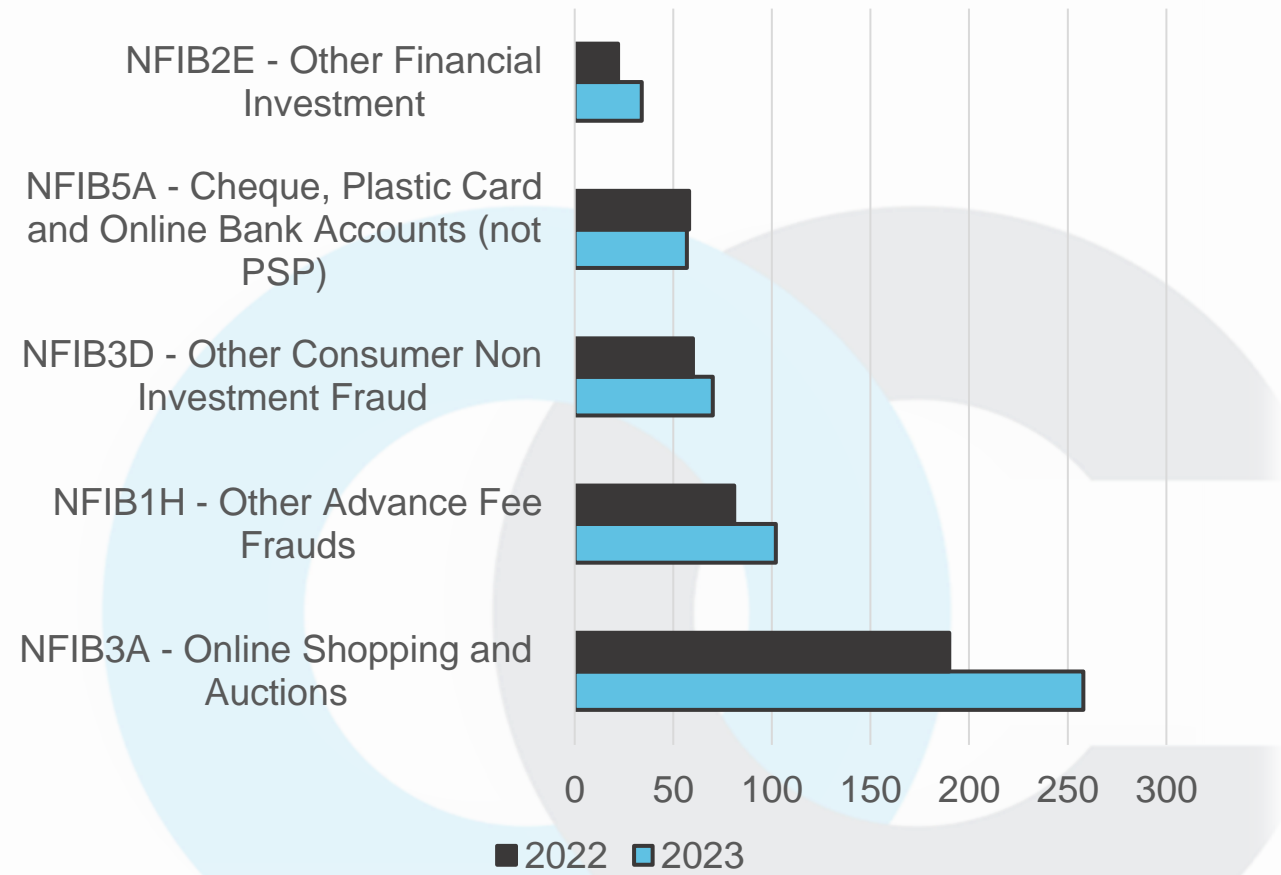
Total Reports: Aug 22: 758 Aug 23: 903  19.1%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 903 reports in August 2023, an increase in reports of 19% when compared to August 2022. Throughout August 2023 the most reported category remains NFIB3A - 'Online shopping and Auctions' with 258 reports, this is over double the next highest reported category.

With University terms beginning it is important to be aware of money mules. Research has shown that those aged under 35 and unemployed or studying are most likely to be targeted as money mules thus putting students in our area at risk of being exploited.

A money mule is a person who receives money from a third party in their bank account and transfers it to another one or takes it out in cash and gives it to someone else, obtaining a commission on the way. The terms of money muling are designed to be attractive with little work involved for instant profit. However, even if money mules are not directly involved in the crimes that generate money, they are accomplices as they launder the proceeds of such crimes. If you suspect you are being recruited for money muling it is important you do not engage and inform the police.

Fraud Categories - August 2022 & 2023




Cyber Dependent North East Victim Reports

This data represents the number of reports received from Action Fraud with a Cyber category selected. In August 2022 there were 63 total Cyber reports, in comparison, there has been 82 reports in August 2023 - an increase of 30.2%. Through August 2023 the highest reported category was NFIB52C Hacking of social media and email with 56 reports.

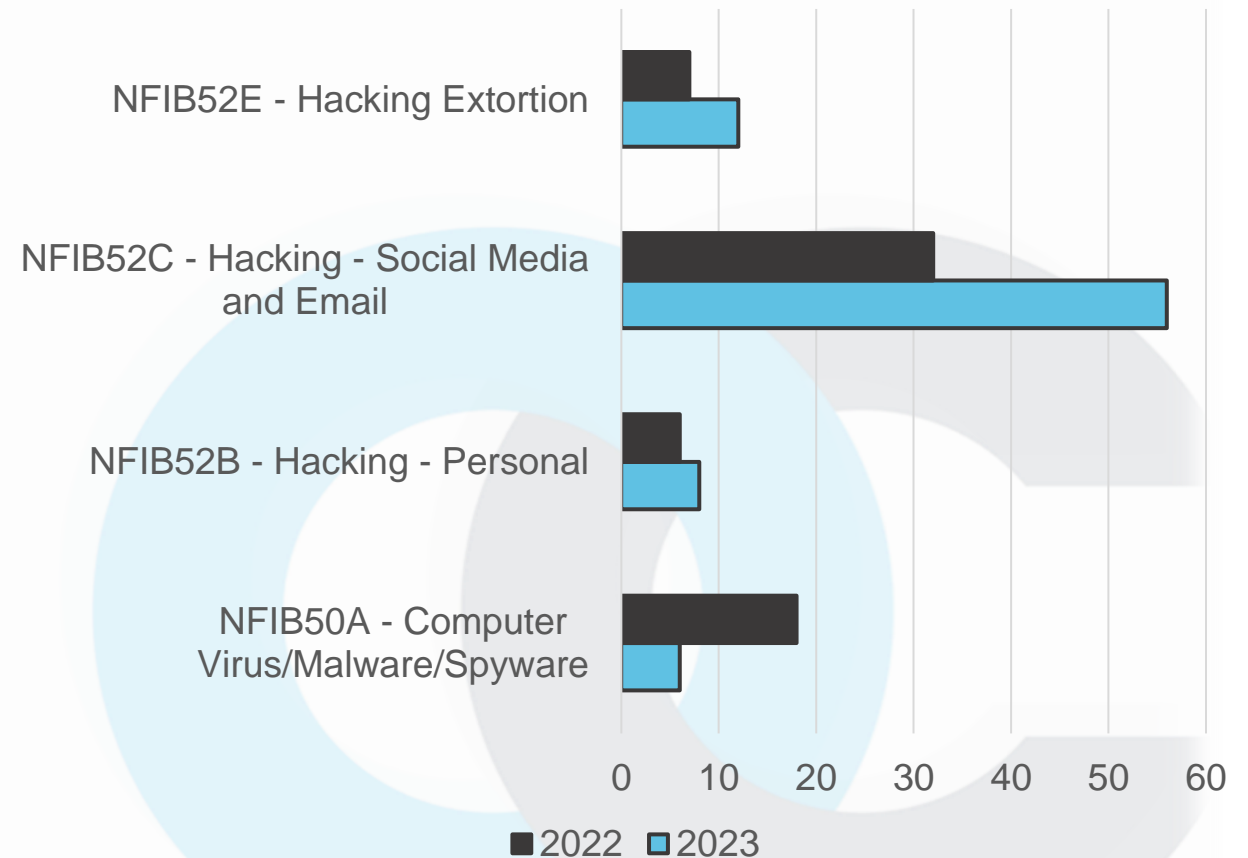
Ransomware is a form of malware that provides criminals with the ability to lock a computer from a remote location. The programmes/virus' can be installed through corrupted CD's and USB sticks or by opening a malicious email attachment or a link. Once the virus is installed on a device or system the devices are locked, with the files and folders stored on them unable to be accessed until the device is unlocked via pin or password - usually at a cost to user!

To avoid accidentally installing malware on a device:

- Only open links and attachments on recognizable emails
- Use trusted and recognized websites
- Ensure you have an up-to-date firewall and internet security installed

Total Reports: Aug 22: 63 Aug 23: 82  30.2%

Cyber Categories - August 2022 & 2023



COMMON EXAMPLE OF COURIER FRAUD



**Phone call
out of the blue**



**Claims to be your
bank or police**



**Advices of an issue
with your card**



Asks for your PIN



**Sends courier to
collect your card**



DO NOT PANIC
TO STOP FRAUD

ActionFraud

National Fraud & Cyber Crime Reporting Centre

actionfraud.police.uk

Courier Fraud

Increase in reports in the North East

There has been an increase in reports of Courier Fraud in the North East. Courier Fraud often takes the form of a phone call received from someone who may know personal information such as your full name and address, they may purport to be from a bank or the police. They request that the victim withdraws a sum of money from the bank (they often stay on the phone to direct the victim as they withdraw the money) or ask the victim to purchase high value goods and send a courier to collect it/them. It is likely they will make out there has been a fraudulent transaction on your card and state they need to send a courier to pick the card up and ask you to write down your PIN. The criminal may tell you to phone your bank but will not hang up the line, leading you to believe you are speaking to the bank but you are actually still in contact with a criminal.

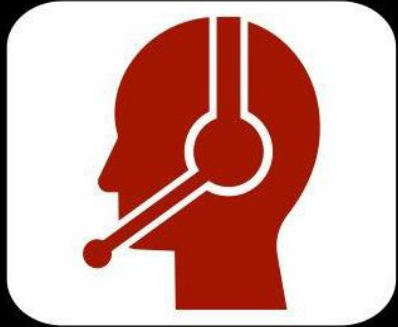


ALWAYS REMEMBER:

- Your bank or the police will never contact you to verify personal details, your PIN, offer to pick up your card by courier or ask you to transfer money.
- The police will not contact you out of the blue to participate in an investigation in which you need to withdraw money from your bank or to purchase high value goods.

If you believe you have been a victim of Courier Fraud, contact your bank immediately (try to use a different phone if possible) on a number you know to be correct, such as the one listed on your statement, their website or on the back of your debit or credit card. Also, report it to Action Fraud on 0300 123 2040 or via [actionfraud.police.uk](https://www.actionfraud.police.uk).

Spot the signs of courier fraud



Someone claiming to be from your bank or the police call you to tell you about fraudulent activity but is asking you for personal info or your PIN to verify who you are.



They're offering you to call back so you can be sure they're genuine, but when you try to return the call there's no dial tone.



They try to offer you peace of mind by having somebody pick up the card for you to save you the trouble of having to go to your bank or local police station.

Engagement Events

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

The team have attended various events throughout the month, including a lot of fresher's events across Cleveland, Northumbria and Durham force areas as Colleges and University's return after summer break. There have also been inputs around money muling to students and financial wellbeing sessions with international students.

A Fraud foundation workshop has been implemented with the citizens in policing team at Cleveland Police to enable them to deliver Fraud prevention advice.

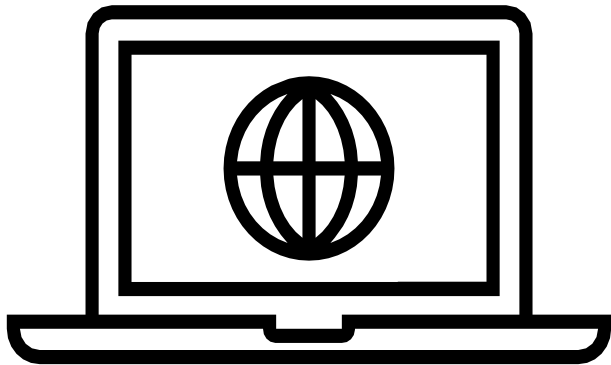
We have been at Wynyard Business Park with Safer Communities providing Fraud advice to residents.

Durham Cyber Crime Team and the RECCC held the first digital drop-in session in Darlington which enabled members of the public to speak to us on a 1-2-1 basis which gave us the opportunity to secure their devices and answer questions.



Horizon Scanning

Monitoring Threats



Due to retail store Wilko going into administration there have been adverts on Facebook that look identical to the Wilko branding and include links to a professional looking website offering 90% off items. While it displays Wilko branding and products, it is a Fraudulent website designed to steal victims personal and financial information. Wilko have ceased trading online and only have sales in stores.



Natwest have identified a phishing scam that is targeting Natwest and RBS customers. The email usually states that the customers mobile number has been changed and directs the victim to click a link if they have not made this change. The link then takes the victim to a website that looks like a Natwest website but is Fraudulent and requests sensitive information like customer number and card details. If you are unsure contact your bank directly, the number should be on the back of your card and do not give out any personal or sensitive information.

What's Happening Next?



Students return to College and University

As students return to College and University there may be an increase in certain scams targeting this group. This could be via competitions on social media such as 'win back to school supplies' with the aim of collecting persona data. Facebook Marketplace is used to sell items students may need at a discounted price with no intention of ever sending the items. There may also be an increase in financial aid scams as students start to apply for their student loans and grants, often around this time there are companies or websites that offer to help students with their applications. It is important to ensure you are using the official application processes and if you are unsure do not provide any personal information.

Cost of living payment

It has been announced that there is a further cost of living payment that will be made of £300 in October or November. Last time payments were made there was a spike in reports of scams relating to the payment. Remain vigilant and remember that you do not need to apply or make a claim for the payment, it will be made directly into your bank account if you are eligible for the payment.





Remote Access Scams

Only install software or grant remote access to your computer if you are asked by someone you know and trust.

ActionFraud

National Fraud & Cyber Crime Reporting Centre

actionfraud.police.uk

Remote access scams

Increase in reports targeting businesses



Since June 2023 Action Fraud report that remote access scams targeting businesses resulted in losses totalling over £3.8M.

Based on analysis of crime reports by the National Fraud Intelligence Bureau, scammers will generally use the following tactics to target businesses:

- **Contact the victim claiming to be a representative from their bank** or from a financial services vendor used by the victim's business.
- **Convince the victim to install a piece of software** that enables remote access to their computer, claiming that it's required to install an important software update.
- At some point during the call, the victim is **instructed to login to their online banking account**. Once the victim has done this, the remote access software is used to blur the victim's screen whilst the scammer makes fraudulent transactions from the victim's account without their knowledge.
- The victim is also **asked to read out a series of numbers the criminal claims they have sent to the victim's mobile**. In reality, the numbers are a one-time verification code from the victim's bank which, if shared will allow them to transfer money out of the victim's bank account.

Some victims reported a slightly different account of how the fraud was perpetrated. However, the goal usually remains the same – to convince victims to login to their online banking account whilst the criminal has remote access to their computer.

Remote access scams

Increase in reports targeting businesses

How to protect your business from remote access scams

- Your bank will never ask you to grant them remote access to your computer or smartphone. Never install any remote access software on your device as a result of an unsolicited call, browser pop up, or text message.
- The one-time verification codes sent to you by your bank to authorise transactions on your account should **never be shared with anyone, not even bank employees.**
- If you believe your laptop, PC, tablet or phone has been infected with a virus or some other type of malware, follow the National Cyber Security Centre's guidance on recovering an infected device – <https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take>

Received a suspicious call from someone claiming to be from your bank? Hang up, wait a few minutes, then call your bank using the contact number on the back of your debit card, or use the contact information on their official website or app.

If your business has fallen victim to fraud or cyber crime, report it to Action Fraud at **www.actionfraud.police.uk**, or by calling **0300 123 2040**.

Handling Instructions

Distribution List
NEROCU
North East Police Forces

Copyright © NEROCU 2023 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	Megan Turner – Engagement Officer Olivia White – Intelligence Analyst
Reviewed By	D/Inspector Paddy O’Keefe

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.