

# 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 July 2024 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](#)

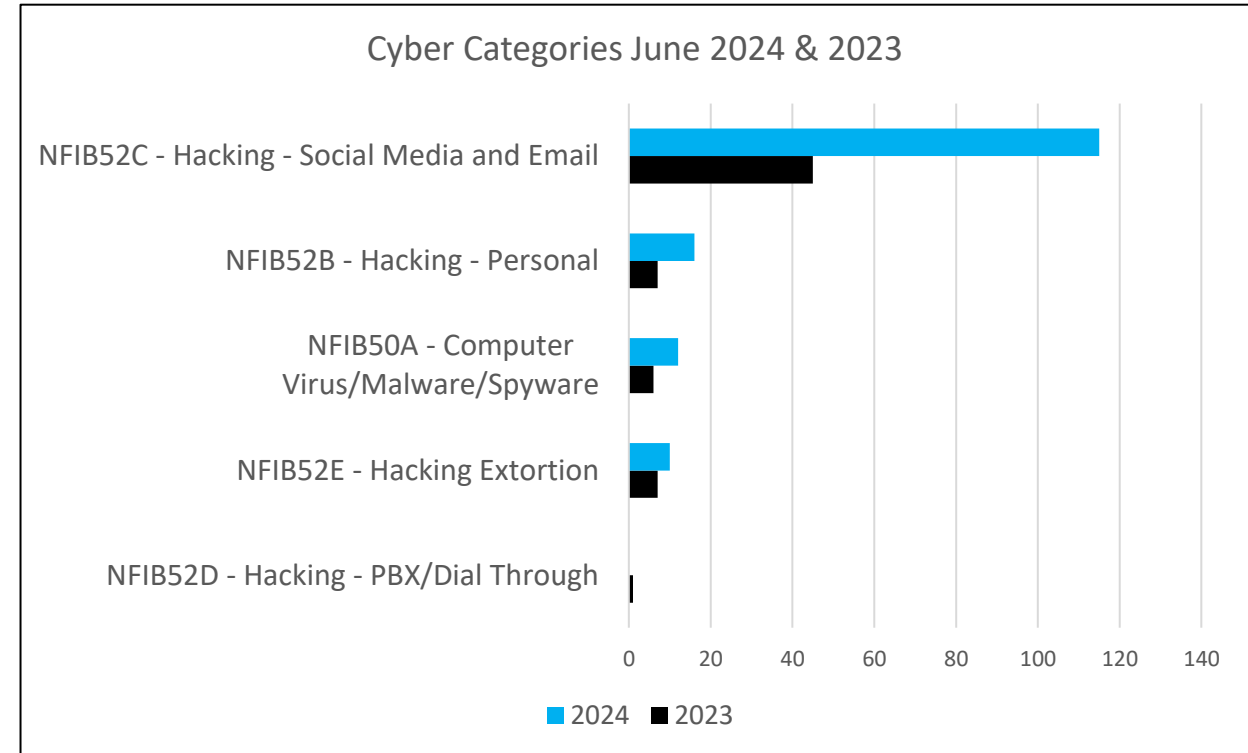
# Cyber Dependent North East Victim Reports

This data represents the number of reports received from Action Fraud with a Cyber category selected. In June 2024 there was a total of 153 Cyber reports, in comparison, there were 66 reports in June 2023, an increase of 131%. The highest reported category was 'Hacking – Social Media and Email' with 115 reports. The age category 18-30 reported the most 'Hacking – Social Media and Email'.

'WhatsApp Vishing' has increased substantially, accounting for 10% of Hacking-Social Media and Email in June 2024, in comparison to 0 reports in June 2023. This rise coincides with the publication of an Action Fraud alert aiming to raise awareness on WhatsApp vishing.

The criminal will contact the victim posing to be a member of that group, often via a WhatsApp audio call, with the intention of building up trust in order to perpetrate the scam. The scammer will often change their profile picture and display name, so at first glance it would appear to be a member of the group. The scammer will say they are sending a six-digit code which will allow the victim to join an upcoming video call for the groups members. In reality, the code is a six digit 2-step Verification (2SV) code for their own WhatsApp account, and if the code is shared, the criminal can log into the account and lock the victim out. The criminals will repeat this tactic with other WhatsApp contacts in an effort to steal other accounts. Once they have access, they have been known to message friends and family in the victims contact list asking them to urgently transfer them money.

Total Reports: June 23: 66 June 24: 153 ↑ 131%



Within the Hacking – Social Media and Email Fraud/Cyber Fraud category, there has also been a rise in reports regarding 'Sim-Swapping' in our region, in line with national reporting. One victim reported the suspect proceeded to access their online banking, change the password and transfer funds.

# Fraud Category North East Victim Reports

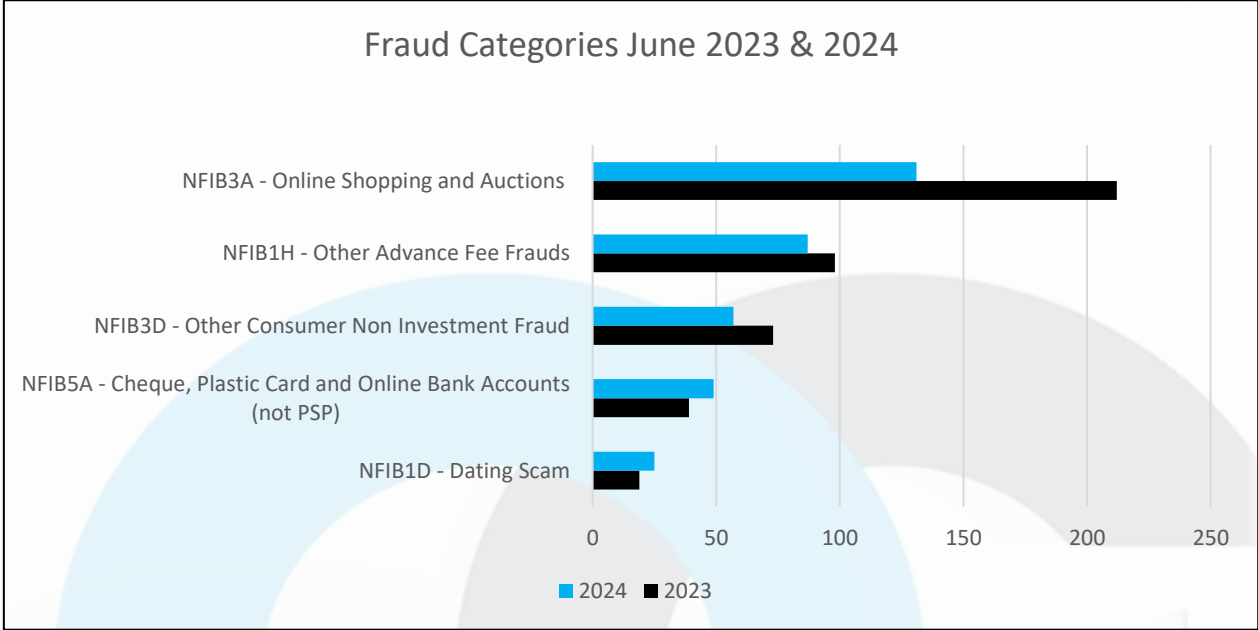
Total Reports: June 23: 805 June 24: 667 ↓ 17.1%

This data represents the number of reports received from Action Fraud with a Fraud category selected. Although the number of Frauds reported in June 24 (656 reports) is higher than June 23s' level, the number of reports is in line with last month.

Throughout this month, the most reported category remains 'Online Shopping and Auctions' with 131 reports but it is worth noting that this has reduced by 31%.

We have had reports over the last few months about scams linked to booking driving lessons online. We have had 8 victims report to us how they have lost and average of £370 when looking for a driving instructor online. Scammers on social media are impersonating driving instructors and, in some cases, established driving schools to take payments for fraudulent lessons. Instructors have been found or recommended on Facebook and Instagram with fees paid up front.

They are offering lesson prices that are often too good to be true. Some have gone further by asking for a deposit to be paid immediately with the balance to be paid in instalments. Once the money is received, the scammer disappears with the customers' cash, they then close down their social media presence.



Reports of frauds linking to property rental are on the rise. Victims report paying deposits for properties that do not exist and report identity theft after providing personal details online. Due to high levels of demand, time pressures are usually put on the victim to act quickly due to the fear of losing the property to another renter.

# Engagement Events

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

The team hosted a Fraud Awareness event at Barclay's Bishop Auckland and also visited the Barclay's Washington Galleries new flex pod to speak with members of the public.

A Fraud Awareness session was held for the Saltburn Neighbourhood Action Plan, where over 50+ members of the community, partners and stakeholders were in attendance.

Durham University finance teams took part in a Fraud Foundation Workshop to increase awareness of money muling and Fraud types.

County Durham and Darlington NHS Trust wellbeing team, share knowledge and awareness of Fraud to share this with service users.

Fraud Foundation Workshop Durham Carers.

Fraud Awareness sessions were held at Hemlington Hub Middlesbrough Council for the digital inclusion leads and Starfish health and wellbeing services.

Citizen's Advice Senior Management Team in Northumberland also had an input from the RECCC.





# QR Code and Parking Fraud

**There has been an increase in reported 'Car Parking Frauds'**

**Victims report downloading apps purporting to be 'Ringo' or 'paybyphone'.**

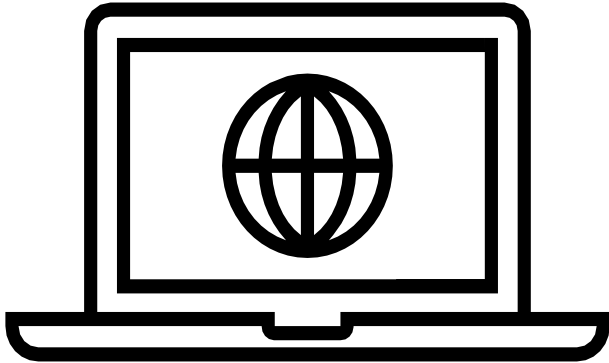
**There have also been instances when victims have paid for parking using a scanned QR code, the QR code was found to be a sticker placed over the legitimate sign by criminals to take the payment themselves or download malware onto the handset or device.**

## **ADVICE**

- **Check the physical code on car park machines/notices. Has it been tampered with or has a 'sticker' been placed over the original sign?**
  - **If the criminals get your details, check for irregular transactions – no matter how small. Contact your bank on a trusted number and explain the situation ASAP!**
- **The criminals may have your phone number – so be wary of people contacting you claiming to be from the bank or police!**

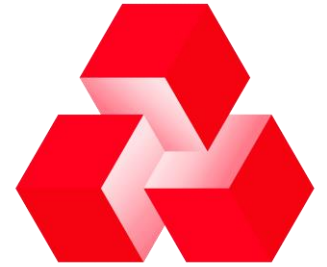
# Horizon Scanning

## Monitoring Threats



Action Fraud have received over 150 reports have of an impersonation scam this month, the email is replicating Natwest, claiming that the contact number on customer accounts has changed and the email includes a malicious link to try and obtain personal data.

- Do not click on any links
- Always contact the bank by using a legitimate contact number rather than using the one on the email.



**NatWest**

**The Suspicious Email Reporting Service (SERS) received 5,102 phishing emails between 17<sup>th</sup> June and 1<sup>st</sup> July.**

The emails impersonate Royal Mail, informing the recipient of a missing letter and providing links to track the missing item. The links are believed to be fraudulent and will risk the recipient disclosing sensitive data or being exposed to malware. The emails use various techniques to appear genuine, consistent in design and use Royal Mail branding. The supposed missing letter is purported to come from HMRC, which would create a sense of urgency for recipients and increase the chances that they fall for the scam.





**As University students new and returning are approaching their new start of term, it is important to revisit some of the Fraud types that are used across the region to target this demographic.**

---

Students are often the main target of criminals trying to launder money through bank accounts, they offer 'quick cash' in return for making various transactions. This is called money laundering (money muling) it is a criminal offence and carries a sentence of up to 14 years in prison.

If anyone approaches you to use your bank account report it to staff at the University and Action Fraud.

WhatsApp groups have been used to target members by building trust and talking outside of the group before asking for money.

Make sure you don't give any personal information out in group chats and be wary of anyone trying to contact you outside of the chat if you do not know them in person.





## **International Students**

are often targeted with Fraud claiming they face deportation/are part of an investigation, there are problems with their visa or stating they need to pay fees.

There have also been various tactics used to obtain money from the student or the students family in the form of fake kidnaps and ransom, sometimes even contacting the families of the student.

Please make your friends and family aware that they could be targeted and ask them to contact you directly if this happens, remind them not to send any money if they are suspicious.

The RECCC continue to work with Universities in the North East, speaking to staff and students to raise awareness and give advice on how to keep themselves safe.





#DontBeUsed



# Becoming a money mule

can lead to issues around getting a mortgage, phone contract, loans etc.





#TurnOn2SV

**If your email or social media account has been hacked, report it.**

- **1. Use a strong and different password for your Email and Social Media accounts**

Your email and social media passwords should be strong and different from all your other passwords. Combining three random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.

- **2. Turn on 2-step Verification (2SV) for your Email and Social Media accounts**

2SV gives you twice the protection so even if cyber criminals have your password, they can't access your email or social media account. 2SV works by asking for more information to prove your identity.

For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password. You won't be asked for this every time you check your email or social media.

**ActionFraud**  
Report Fraud & Internet Crime  
**actionfraud.police.uk**

If one of your online accounts has been hacked, report it to Action Fraud by visiting [www.actionfraud.police.uk](http://www.actionfraud.police.uk), or calling 0300 123 2040.



# What's Happening Next?



## Returning to University and need accommodation?

Criminals use a variety of websites and social media platforms to advertise properties, often at attractive costs and in desirable locations. The offers will appear professional and genuine, accompanied by the expected photos, reviews and contact information.


Due to high demand for accommodation, the criminal will apply pressure and students will often be asked pre-viewing, to pay upfront fees in order to secure the property, however once the person pays the fees they find that they have been scammed and the person advertising the property does not own it and they are left with no accommodation and have had their money stolen.

## What can you do to protect yourself?

- Try to view the property in person if this is possible.
- Check any websites contact details and geographical addresses.
- Reverse image search accommodation photos.
- Discuss with family and friends before going ahead with a payment .





 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 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.**



|                           |   |
|---------------------------|---|
| <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<br/>Claire Hardy– Economic Threat Desk Analyst<br/>Sarah McCluskey –Cyber Threat Desk Analyst</b>  |
| <b>Reviewed By</b>        | <b>T/Sgt Brian Collins</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.