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 November 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.

North East RECCC Regional Economic Crime Coordination Centre

NERCCU North East Regional Cyber Crime Unit

Contents

Looking Back

Contents

Looking Forward

Cyber Dependent North East Victim Reports

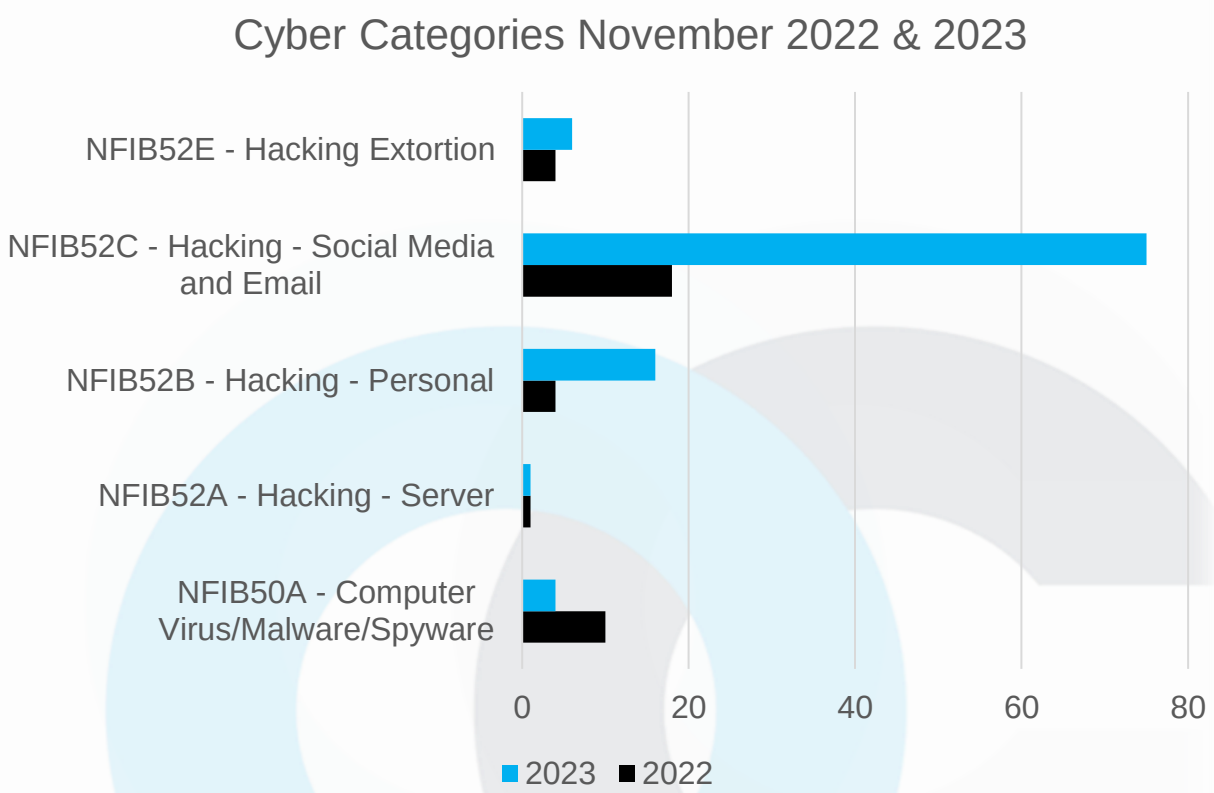
Total Reports: Nov 22: 37 Nov 23: 102 ↑ 175%

This data represents the number of reports received from Action Fraud with a Cyber category selected. In November 2022 there were 37 total Cyber reports, in comparison, there has been 102 reports in November 2023, an increase of 175%. In November 2023, the highest reported category was NFIB52C Hacking- Social Media and Email with 75 reports. This remains at the levels seen last month. Hacking – Personal has also seen a significant rise this month with 16 reports compared to 4 in November 2022. NFIB52E- Computer Virus/Malware/Spyware has seen over a 50% decrease this reporting period.

Action Fraud data shows multiple reports for the same victim reporting Hacking- Social Media and Email. Hackers have gained access to one of the victim's accounts and from this they have been able to access the victim's other social media platforms. This month Email and Facebook are the most reported primary platforms compromised.

Hacking- Personal data mainly shows that victims have received an email link which they have clicked allowing the hacker to access their device and their social media accounts.

Please see the Cyber Protect slide for advice on protecting accounts and devices.



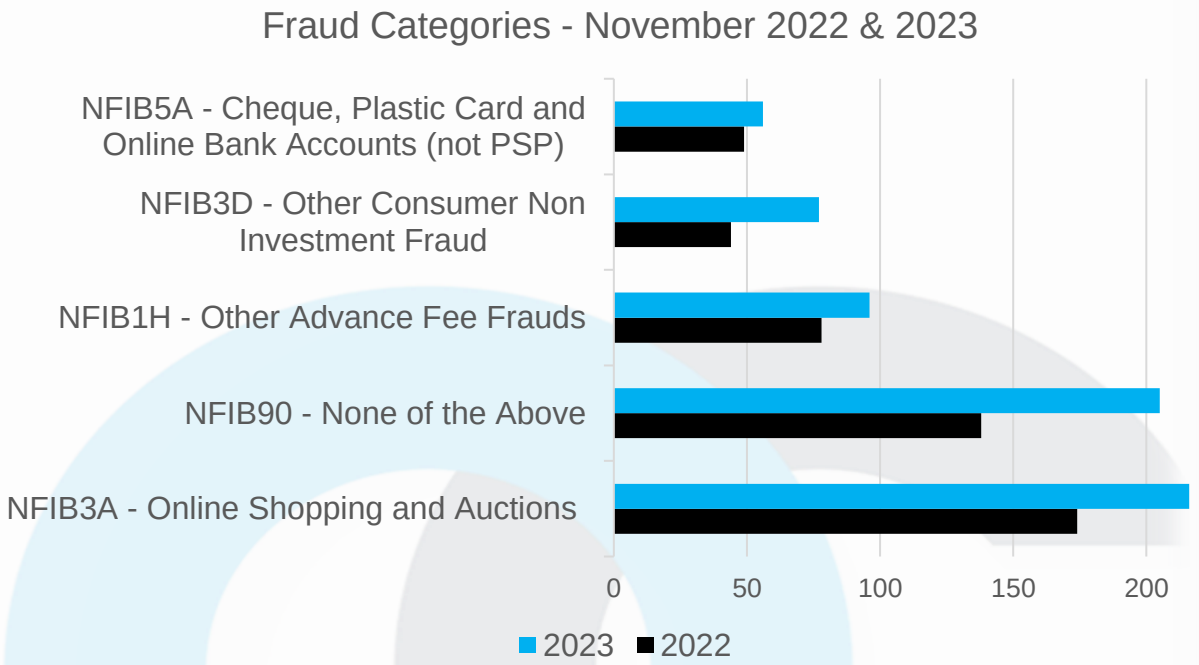
Fraud Category
North East Victim Reports

Total Reports: Nov 22: 608 Nov 23: 850 ↑ 40%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 850 reports in November 2023, a 40% increase compared to November 2022. Throughout November 2023, the most reported category remains NFIB3A - 'Online Shopping and Auctions' with 216 reports, an increase of 24%.

There has been a substantial increase in the reporting of Ponzi or Pyramid scheme Frauds. It is estimated that at least 75% of the reports for November are linked to the same scheme which closed down on 23rd November after a final push for investment. It is estimated that victims in the North East have lost over £110K in total.

There has been an increase in Ticket Fraud with 33 reports made in November alone. Most of the reports are for concert tickets with a third for Taylor Swifts concerts in 2024. Victims report seeing tickets advertised for sale on Facebook and X (Twitter) through acquaintances or mutual friends whose social media accounts have been hacked by scammers.



There is an increase in NFIB3D Other Consumer Non-Investment Fraud. A third of all of November's reports relate to variations of historic mobile phone contract scams. Victims have been scammed into taking out mobile phone contracts for Fraudsters.

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 increase further as we are in the month's when consumer's spend a lot more than usual. Some common scams are listed below:

Facebook Marketplace

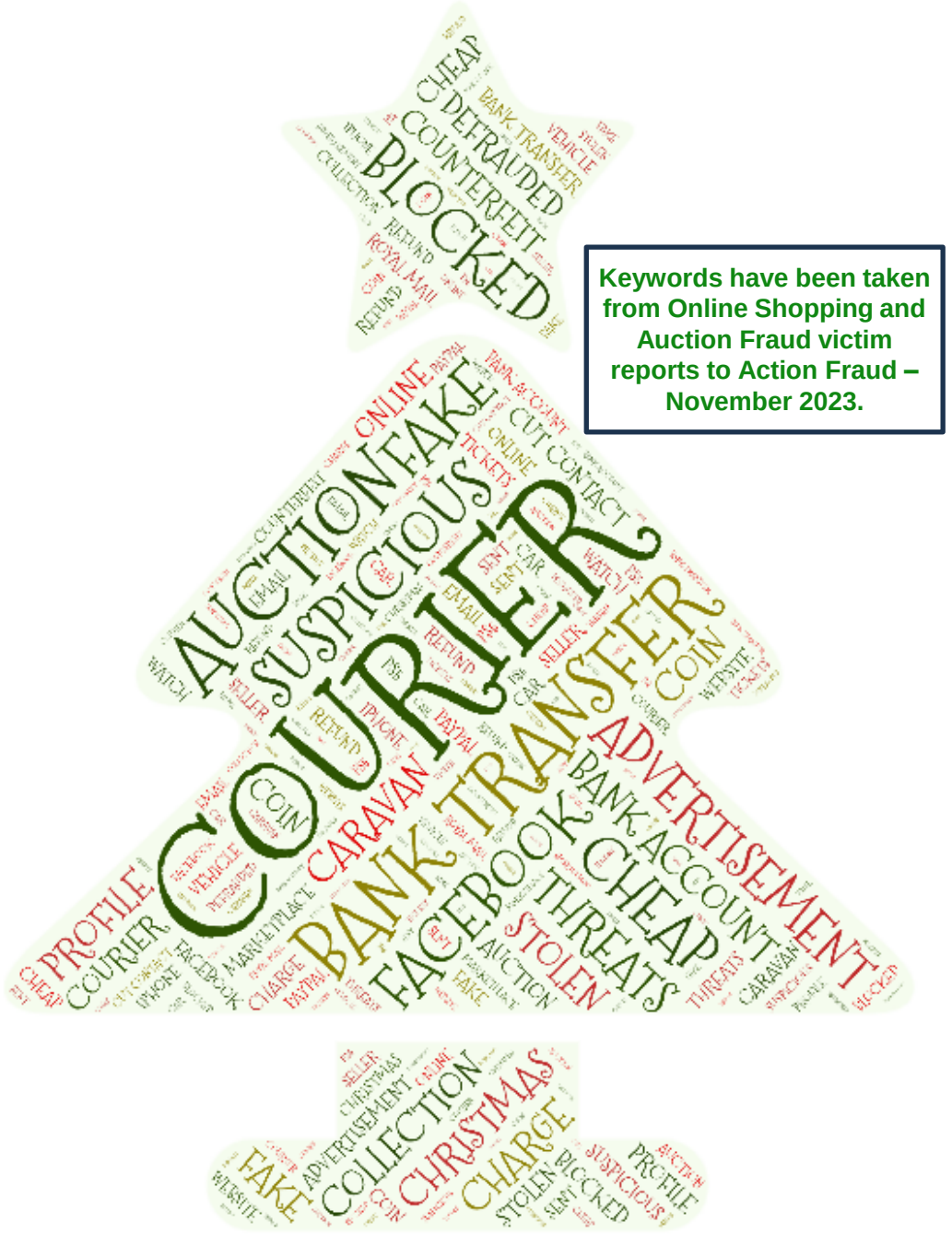
Sending the seller a fake PayPal Invoice to show payment.

Facebook Marketplace

A deposit is paid by the victim for a car or caravan and then the seller disappears.

Facebook Marketplace

Offering to send a courier to collect item and asking victim for a payment.



Keywords have been taken from Online Shopping and Auction Fraud victim reports to Action Fraud – November 2023.

HM Government

Shop securely online this festive season

- Research sellers, check they're legitimate.
- Use a credit card or secure payment platform.
- Only provide enough details to complete your purchase.

Search Cyber Aware

Cyber Aware

Take your email security **to another level**

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Engagement Events

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

Another busy month for the engagement team. We have attended the 'Festival of Finance' for NHS staff at Hartlepool and North Tees hospital.

We have taken part in the European Money Mule Action campaign which ran throughout November, we worked with Universities in the area to carry out a research survey to find out what students know about money mules. We have worked with Northumbria, Sunderland, Teesside, Durham and Northern School of Art to put on information stalls, inputs and events for students and staff.

In Darlington we attended Darlington Carers Event working with Barclay's. As well as inputs and awareness sessions for staff and service users at Darlington Job Centre.

Fraud workshops have been delivered for Military Preparation College for Training (MPCT) students at the Beacon of Light and Teesside.

Durham University Fraud Roadshow

10
University Colleges visited around campus.

Fraud awareness training delivered to staff at the university.

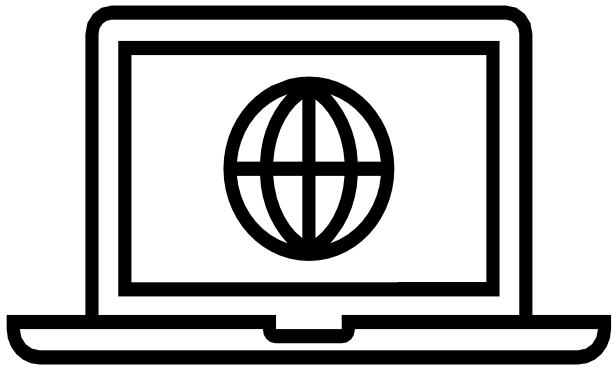
Money mule surveys carried out with students as part of the European Money Mule Action campaign.

11
Fraud Roadshows held by the RECCC throughout November.

6000
Contact with over 6000 students, advice given around money muling and Fraud awareness.

Horizon Scanning

Monitoring Threats



There have been a number reports of a phishing campaign to do with NHS prescriptions. Recipients have received an email purporting to be Lloyds Direct encouraging them to sign up to the service to easily manage prescriptions and have them delivered for free. The email contains a link which is believed to download harmful malware on to the victim's device and/or harvest personal and financial information.

LloydsDirect

A drug initially produced to treat diabetes has been remarketed and endorsed by celebrities and influencers as a weight loss drug ‘Ozempic’, nicknamed ‘the skinny jab. Due to this, there has been a shortage of the drug. This has resulted in high prices and counterfeit versions being produced. Fraudulent online Pharmacies and social media scams have profited. It’s likely the high demand for this drug will continue and criminals will continue to exploit this, leading to financial loss and possibly health problems for the victim.

Cyber Protect Advice

Hacking Social Media and Email:

Cyber Protect messaging is an important intervention in social media and email hacking. Implementing basic cyber security measures can prevent suspects gaining access to primary accounts. The two main pieces of advice which assist with this are for social media and email users to:

1.Use a separate password for email accounts (ensuring passwords are strong and not easily guessed)

2.Activate 2 factor authentication (also known as 2 step verification) on all online accounts where possible. Most, if not all, social media platforms have this setting which can be activated by the user

Personal Hacking:

When it comes to clicking links and allowing suspects to take over devices, users are advised to be cautious. However, phishing emails are becoming more sophisticated. It is advised that users ensure devices and apps are up to date, whilst also using anti-virus software applicable to devices.

What's Happening Next?

Thinking of getting a new phone for Christmas?

This scam begins with a phone call, claiming to be on behalf of a mobile service provider, offering an upgrade or free gift. Having gathered the necessary personal details, the scammer then contacts the phone company, which posts out a new handset to the victim's address.

When it arrives, the victim is contacted again and told that the wrong phone has been sent and is asked to post it back – this time, to the scammer's address. On some occasions, a courier has been sent to collect it.

Once the scammer receives the new phone, they disappear – leaving the victim with no phone and a new, more expensive contract. The Fraud is uncovered once the victim realizes they are paying for multiple mobile phone contracts.

What should you do?

- If you receive a call out of the blue offering a good deal or refund, do not provide personal or banking information. Contact your network provider on a trusted number.
- If you receive a mobile phone you didn't order, contact the network provider on a trusted number and request any contract is cancelled. Ensure the address you return to is legitimate.
- Ensure documents with personal information on is shredded before throwing away.
- Monitor your credit score so you can see any credit searches made under your name.

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	**Megan Turner – Engagement Officer** **Claire Hardy– Intelligence Analyst** **Nicola Lord– 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.