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 December 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

Contents

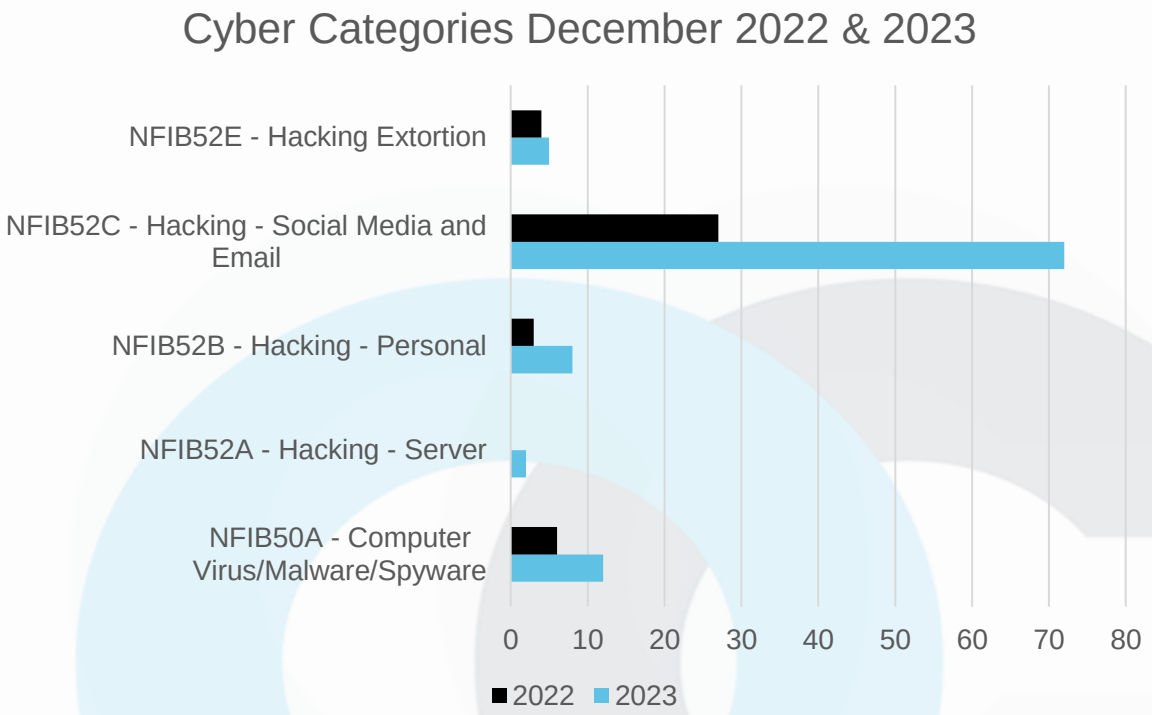
Looking Forward

Cyber Dependent North East Victim Reports

Total Reports: Dec 22: 40 Dec 23: 99 ↑ 147.5%

This data represents the number of reports received from Action Fraud with a Cyber category selected. In December 2022 there were 40 total Cyber reports, in comparison, there has been 99 reports in December 2023, an increase of 147%. In December 2023, the highest reported category was NFIB52C Hacking- Social Media and Email with 72 reports. This is consistent with November 2023 figures. December 2023 figures show an overall increase across all categories consistent with National reporting.

11% of victims reported multiple accounts targeted in one incident in December 2023. Most of the multiple accounts fall within the category NFIB52C- Hacking Social Media and Email.



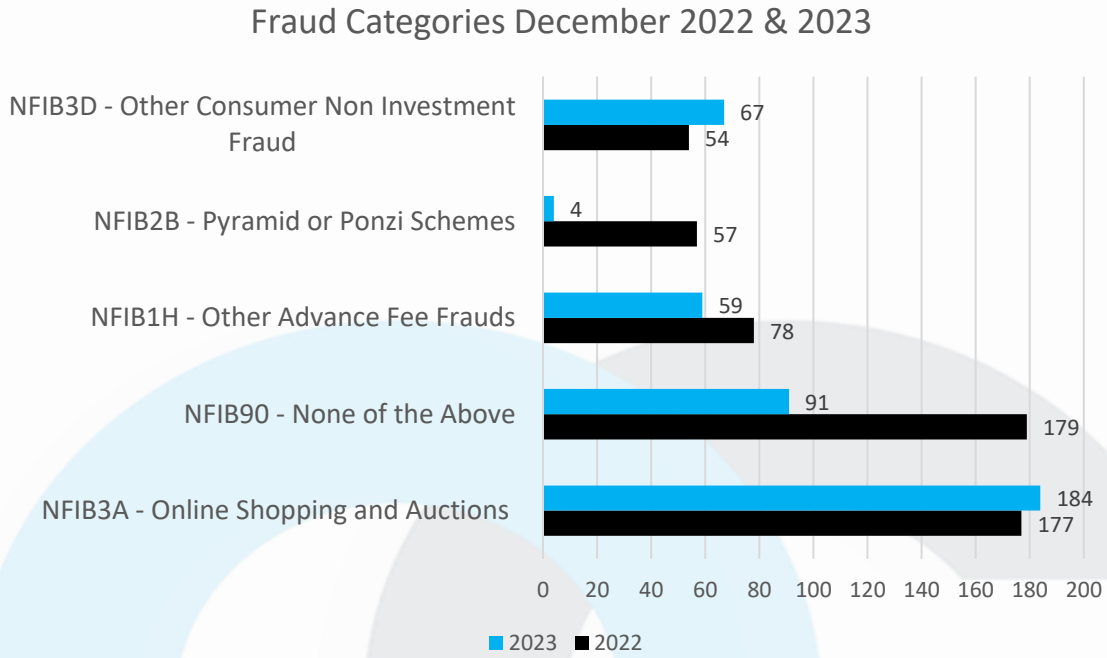
Fraud Category
North East Victim Reports

Total Reports: Dec 22: 575 Dec 23: 771 ↑ 34%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 771 reports in December 2023, a 34% increase compared to December 2022. Throughout December 2023, the most reported category is NFIB90 - 'None of the Above' with 179 reports, an increase of 96%.

The increase in reporting of Ponzi or Pyramid schemes has continued into December. 78 victims across the North-East have now reported losing money in the Coscoin or Cosetek scheme which closed late November. Victims have lost a total of £215K. NFIB2B – Pyramid or Ponzi Schemes have appeared in the top 5 reported Fraud categories as a result. The average age of victims is 42.

Ticket Fraud remains at a high level for both concert and sporting events. 15% tickets were for Newcastle United games. Tickets were purchased from a site called PremierTicket Hub which has since closed down.



NFIB19 - Fraud by Abuse of Position of Trust has increased by 200% with 12 reports in December 2023. Most of these reports relate to vulnerable victims having money removed from their bank accounts by offenders known to them. On some occasions, by family members. The average loss is £3,200. Reports have been submitted by third parties such as other family members, local authority staff or police officers.

Engagement Events

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

This month is the start of Operation Lazio which is an engagement operation across the 3 forces involving Police Cadets; the theme is Building Resilience Against Fraud; the cadets/cadet leaders will be taking part in a combination of presentations and workshops designed to increase awareness of fraud and provide a solid foundation for the cadets and cadet leaders to deliver their newfound knowledge into communities.

In addition to this Fraud Awareness sessions have taken place at Marton Community Centre and Durham Cyber at Home Group, Spennymoor.

Fraud Foundation Workshops have been completed at MPCT Darlington and Tees Components, Skelton.

Lost Pet Scam

Criminals are targeting victims who have placed lost pet posts on Facebook. They are contacting victims claiming to be veterinary practices that their missing pets have been taken to and demanding payment for injuries.

If you having a missing pet and have posted on missing or lost pet sites on Facebook or other social media sites, be wary of this scam.

- **If in doubt, hang up and contact the veterinary practice yourself.**

If you believe you have been a victim of Fraud, contact your bank immediately and report the incident to Action Fraud https://www.actionfraud.police.uk/ or call 0300 123 2040

Financial Advisor - Jailed For Defrauding Clients

A financial advisor who stole almost £2 million from victims by selling bogus investment plans has been jailed for 7 years. Stephen Rae was convicted at Newcastle Crown Court in June 2023, after admitting he defrauded 16 separate clients between June 2014 and January 2016.

The victims all believed they had been investing their hard-earned cash and pensions into a range of legitimate financial schemes – but never saw their profits materialise.

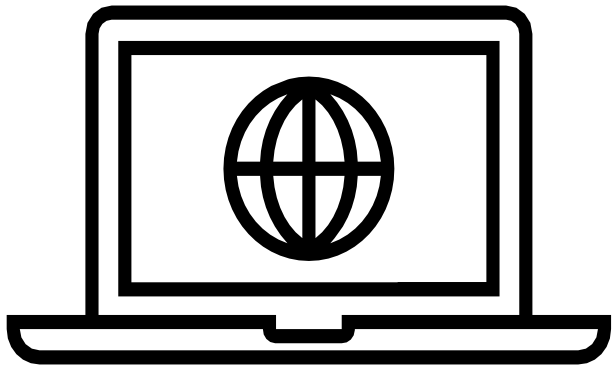
In 2015 two victims reported Rae to Durham Constabulary and Action Fraud respectively after they sent him six-figure sums to invest.
After their returns failed to materialise, both women reported Rae after he repeatedly ignored their calls and correspondence.

When Action Fraud referred the case to Northumbria Police, specialist officers launched a thorough investigation and executed a warrant at Rae's home in South Shields, in which they noted a range of luxury cars, including an Aston Martin Vanquish parked up at the property.

Officers seized Rae's laptop and devices and uncovered the financial records of 113 clients – as well as banking records confirming clients had invested almost £2.8 million with him.

Horizon Scanning

Monitoring Threats



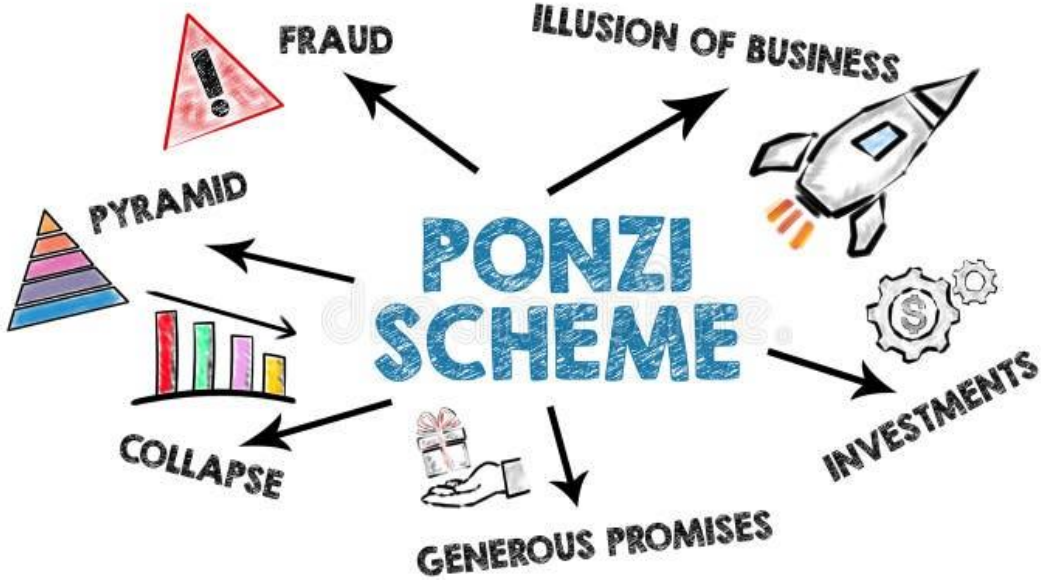
In the North East, 78 victims have reported a total loss of £214, 869 to an investment scam. Victims have invested money in a cryptocurrency investment platform called Coscoin, also known as Cos or Cosetek.

The platform claims people can double their investment, however reports from across the UK have shown that people have been unable to access or withdraw their money since the end of November.

The structure of Coscoin, believed to be based in Washington USA, appears to also incentivise users to recruit further people to the platform in what appears to be a Ponzi/Pyramid Scheme.

Every investment carries a degree of risk, when investing keep in mind the following:

- If it sounds too good to be true, it probably is.
- Don't invest more than you can afford to lose.



If you believe you have been a victim of Fraud, contact your bank immediately and report the incident to Action Fraud https://www.actionfraud.police.uk/ or call 0300 123 2040

What is Romance Fraud?

Fake profiles are used by criminals to build a relationship with you on social media platforms, dating websites or gaming sites. They use information found on social media to create fake identities to target you. Once a relationship has evolved, they convince you to send them money.

They often go to great lengths to gain your trust and convince you that you're in a genuine relationship before appealing to your compassionate side to ask for money. Criminals will use language to manipulate, persuade and exploit so that requests for money do not raise alarm bells. These requests might be highly emotive, such as claiming they need money for emergency medical care, or to pay for transport costs to visit you if they are overseas.

The total loss to victims of Romance Fraud in the North East totals

£2,451,378

for 2023

The total number of victim reports for Romance Fraud in the North East for 2023 is

263

Image (right) keywords have been taken from Romance Fraud victim reports to Action Fraud – November and December 2023.


IS YOUR
PERFECT MATCH
REALLY WHO
THEY SAY
THEY ARE?
#RomanceFraud
ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

How to spot the signs

•You've struck up a relationship with someone online and they declare their love for you quickly. Many fraudsters claim to be overseas because they work in the military or medical profession.

•They make up excuses as to why they can't video chat or meet in person and will try to move your conversations off the platform you met on.

•When they ask for financial help, it will be for a time-critical emergency, and the reason will be something that pulls at the heartstrings. They may get defensive if you decline to help.

•Their pictures are too perfect – they may have been stolen from an actor or model. Reverse Image Search can find photos that have been taken from somewhere else.

•They tell you to keep your relationship private and not to discuss anything with your friends and family.

How to protect yourself

•**STOP**: Take a moment to stop and think before parting with your money or information.

•**CHALLENGE**: Is this person really who they say they are? Could it be fake? It's OK to reject, refuse or ignore any requests for your financial or personal details. Criminals will try to rush or panic you.

•**PROTECT**: Contact your bank immediately if you think you've been victim of a scam and Report it to **Action Fraud.**

What's Happening Next?

Doing your tax returns?

Self-Assessment customers are urged to be vigilant and on the lookout for scam texts, emails and phone calls from Fraudsters ahead of the 31 January 2024 deadline for submitting tax returns.

HM Revenue and Customs (HMRC) received more than 130,000 reports about tax scams in the 12 months to September 2023, of which 58,000 were offering fake tax rebates.

What should you do?

Customers can report any suspicious communications to HMRC:

- Forward suspicious texts claiming to be from HMRC to 60599
- Forward emails to phishing@hmrc.gov.uk.
- Report tax scam phone calls to HMRC on GOV.UK.

Further guidance on how to identify tax scam phone calls, emails and text messages can be found here.

PHISHING

What is phishing?

'Phishing' is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

Why you should report phishing scams:

The National Cyber Security Centre (NCSC) is a UK government organisation that has the power to investigate and take down scam email addresses and websites.

Reporting a scam is free and only takes a minute. By reporting phishing attempts, you can:

- reduce the amount of scam communications you receive
- make yourself a harder target for scammers
- protect others from cyber crime online

As of December 2023, the number of reports received stands at more than 27m reported scams, which has resulted in 161k scams being removed across 295,300 URLs.

If you believe you have received a phishing email, text or call you can report at **report@phishing.gov.uk**. Please see www.NCSC.gov.uk for further advice around phishing emails, texts and calls.

If you have been a victim of phishing please report **to www.actionfraud.police.uk.**

Beware of "too good to be true" holiday deals

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

ABTA
Travel with confidence

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	**T/Sergeant Brian Collins**

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.