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 January 2024 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

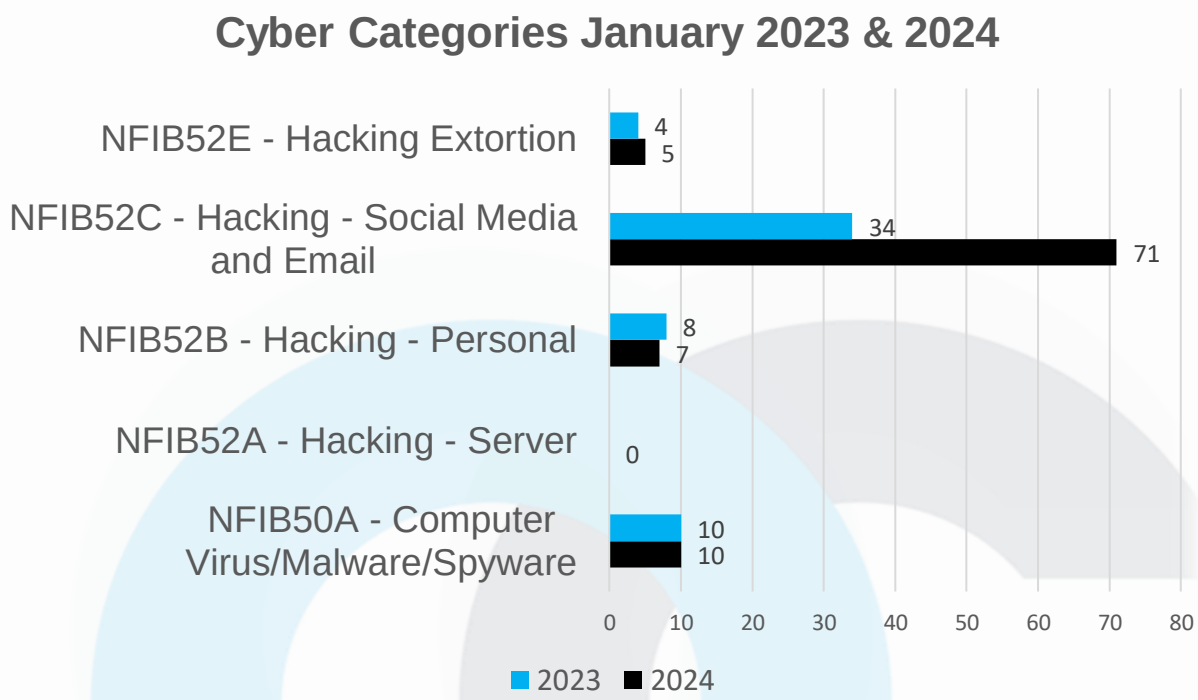
Looking Forward

Cyber Dependent North East Victim Reports

Total Reports: Jan 23: 56 Jan 24: 93 ↑ 66%

This data represents the number of reports received from Action Fraud with a Cyber category selected. In January 2024 there were 93 total Cyber reports, in comparison, there were 56 reports in January 2023, an increase of 66%. In January 2024, the highest reported category was 'Hacking- Social Media and Email' with 71 reports. This is consistent with December 2023 figures.

Phishing emails have been circulating informing the recipients that they need to renew their TV Licence. Some of the emails claim that the bank has declined a direct debit request and urging individuals to update their details to stay licenced. Other emails state that an issue has arisen with the most recent pre-authorised direct debit payment and recipients are advised to set up a pre-authorised debit. It is believed once the recipient has clicked the link in the email it will lead them to enter financial/personal details or download malicious malware. Between 1st January and 15th January, the Suspicious Email Reporting Service received 6,307 reports relating to TV Licence scams. Phishing emails with this MO may increase within the beginning of the year and potentially give the impression that recipients have missed their renewal.



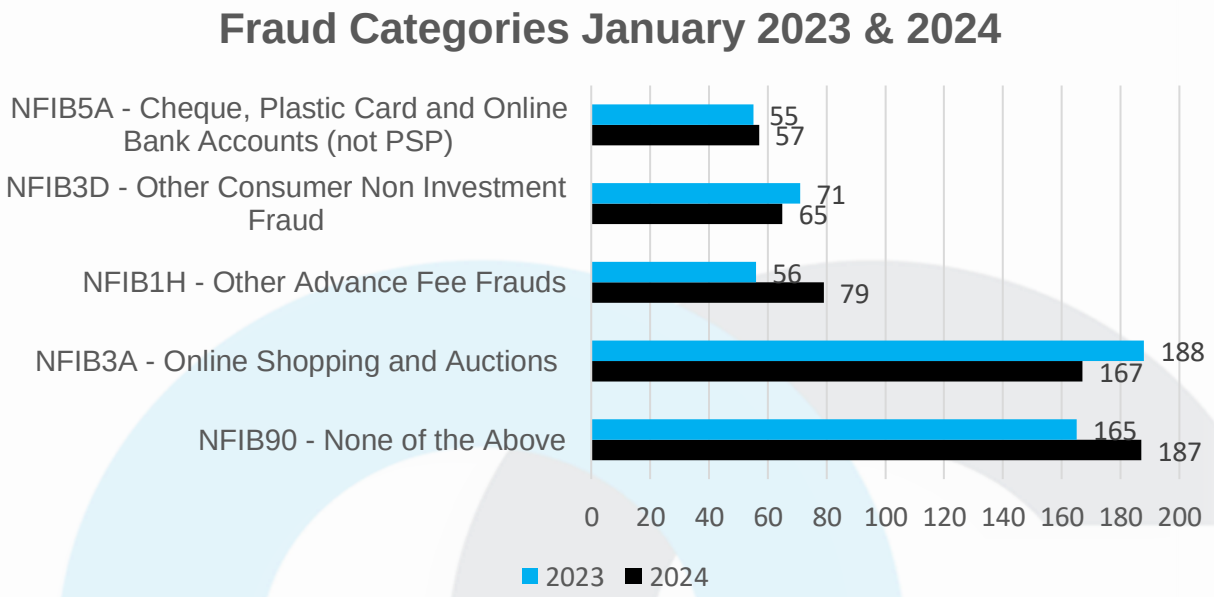
Fraud Category
North East Victim Reports

Total Reports: Jan 23: 714 Jan 24: 731 ↑ 2.4%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 731 reports in January 2024, a small increase of 2.4% increase compared to January 2023. Throughout January 2024, the most reported category remains 'Online Shopping and Auctions' with 167 reports but it is worth noting that this has reduced by 11.2%.

Victims across the North-East report receiving calls from their bank's Fraud departments or police officers (similar to Courier Frauds) but have been asked to transfer money directly from their online banking accounts to the scammer's accounts. Depending on the amount, victims have been asked to transfer money in smaller denominations to several accounts. This MO removes the opportunity for banking staff to interject if they suspect coercion by seeing the victim face to face.

Reports are also coming in whereby the victim is called from their bank claiming fraudulent activity and asked to provide security information including verification codes.



Engagement Events

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

The RECCC have continued Operation Lazio with police cadets across the region, delivering workshops and inputs on fraud awareness. Some of the groups have already been in the community delivering their own presentations.

The Northumberland Library Fraud Roadshow has been running throughout the month, so far we have covered Alnwick, Bedlington, Hexham and Cramlington.

The team have been to Newcastle University, Sunderland University and Durham University delivering inputs to staff, students and attending events.

Workshops and awareness sessions have been delivered to The Skills Academy in Billingham, a number of U3A groups and Stockton Riverside College.

No matter how long you've been speaking to someone online or how much you trust them, if you have not met them in person, it is important that you do not:

- Send them any money
- Allow them access to your bank account
- Transfer money on their behalf
- Take a loan out for them
- Provide copies of your personal documents such as passports or driving licenses
- Invest your own money on their behalf or on their advice
- Purchase and send the codes on gift cards from Amazon or iTunes
- Agree to receive and/or send parcels on their behalf (laptops, mobile phones etc.)

Total amount lost to Romance Fraud in the North East 2023

North East ROCU
Regional Organised Crime Unit Network

There has been an increase in the number of calls made by criminals looking to exploit members of the public by claiming to be the police.

Calls have been a variety of different stories where the scammer asks the victim to attend a police station in London or stating the victim has been involved in a crime as a victim/suspect or is part of an investigation.

- Be wary of phone calls claiming to be from the police.
- If in doubt, check it out! Hang up and dial 101.
- The police would never ask you for your card details or PIN.

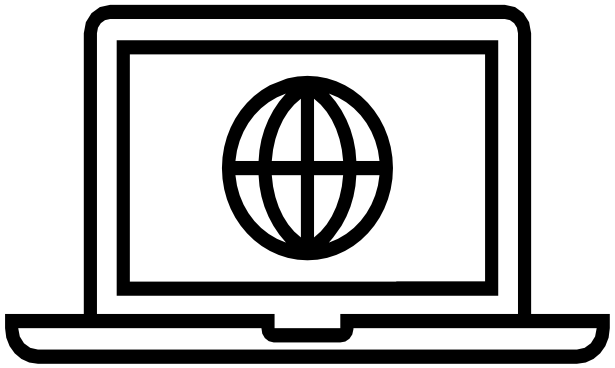
If you think you have been a victim of fraud, contact action fraud at www.actionfraud.police.uk or call **0300 123 2040**.

Horizon Scanning

Monitoring Threats

17% of reported Romance Frauds reported in the North East have been extorted after sharing intimate photos online with criminals who had struck up an online romance with the victims. The criminals ask for money not to publish the images online.

- Don't trust that someone is always who they say they are.
- Be mindful that once you share photos online they then can be shared for others to see.



'Anydesk' is a legitimate German based company whose product is being misused by UK nationals to commit significant amounts of fraud. Victims are duped into giving out their credentials which are used to empty accounts.

Victims in the North East have reported losses of over £22,000 this month. Victims receive calls from a variety of sources including Amazon, the High Court and Virgin Media. Victims were encouraged to download an app called 'Anydesk' to receive monies owed or to receive assistance following alleged fraudulent activities on accounts. The scammers then take over the victims phone and accounts.

It is important to be extra vigilant when receiving unexpected phone calls. If in doubt, hang up.

STOP! THINK FRAUD

Giving you the knowledge and tools you need to stay ahead of scams.

The government have launched the STOP! THINK FRAUD campaign.

You can access the campaign here : [Stop! Think Fraud - How to stay safe from scams (stopthinkfraud.campaign.gov.uk)]

In just one year,
1 in 17
adults were victims of Fraud.
Access advice on how to protect yourself from Fraud, information on how to report Fraud and steps to recover if you have been a victim.

What's Happening Next?

'Easter Egg Scam'

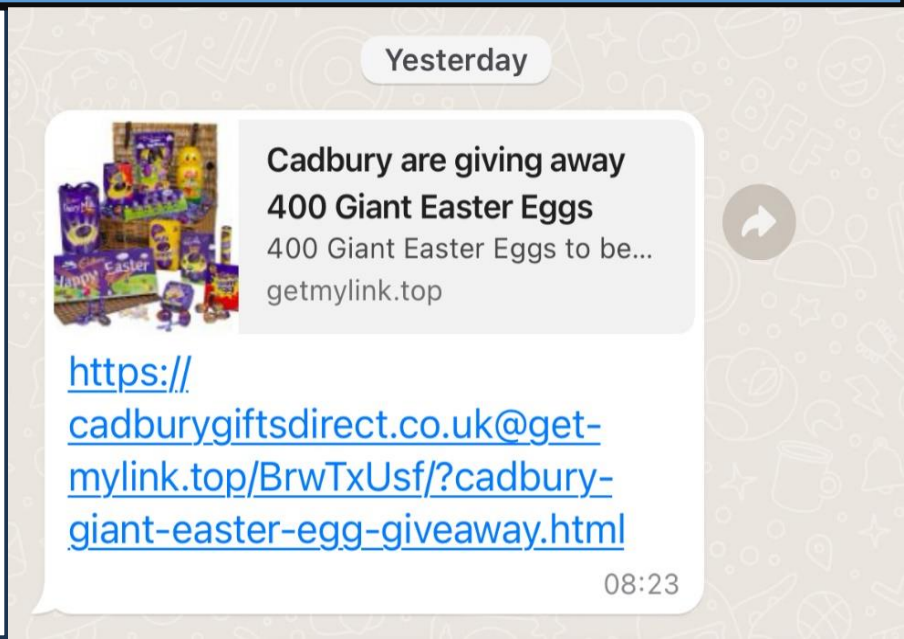
It's that time again, every year around Easter we see an increase in 'easter egg scam' WhatsApp messages.

If you receive a WhatsApp message similar to the one below, this is a scam. Free easter egg messages have already started circulating in 2024.

What should you do?

- Do not click the link and do not forward the link to other contacts.
- Do not give out any personal information.
- Report the message to Whatsapp.

If you think you have been a victim of fraud, contact action fraud at www.actionfraud.police.uk or call **0300 123 2040**.



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**
Reviewed By	**T/Sgt 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.