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 October 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

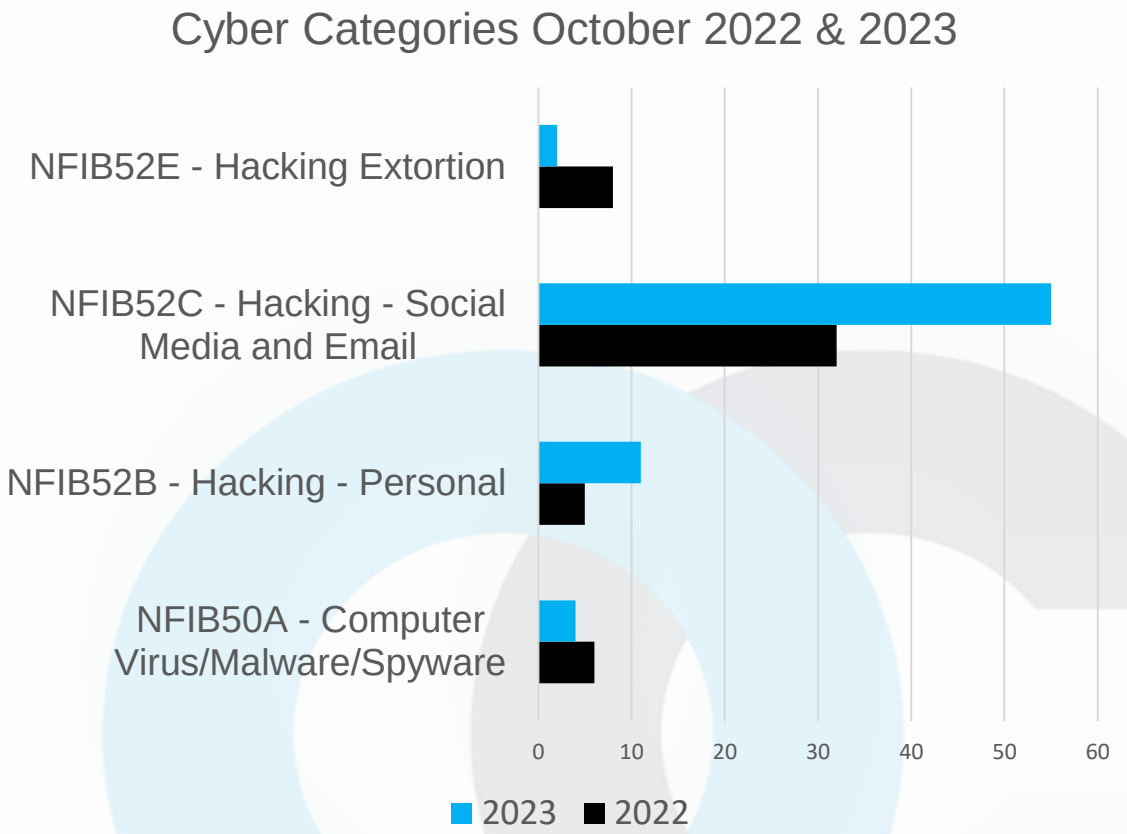
Total Reports: Oct 22: 51 Oct 23: 72 ↑ 41%

This data represents the number of reports received from Action Fraud with a Cyber category selected. In October 2022 there were 51 total Cyber reports, in comparison, there has been 72 reports in October 2023, an increase of 41%. In October 2023, the highest reported category was NFIB52C Hacking- Social Media and Email with 55 reports. This is consistent with September 2023 figures. NFIB52E- Hacking Extortion has seen a decrease of a 120% this reporting period.

The National Cyber Security Centre provide a toolkit for organisations to check their organisations email cyber security. This tool is a free government service and allows organisations to check any email domain. This toolkit can check for:

1.Email anti-spoofing. Preventing cyber criminals sending emails pretending to be you (known as spoofing).
2.Email privacy. Making it harder for cyber criminals to intercept and read your email in transit.
If any issues are found, the NCSC provides step-by-step guidance on what you should do.

https://emailsecuritycheck.service.ncsc.gov.uk/



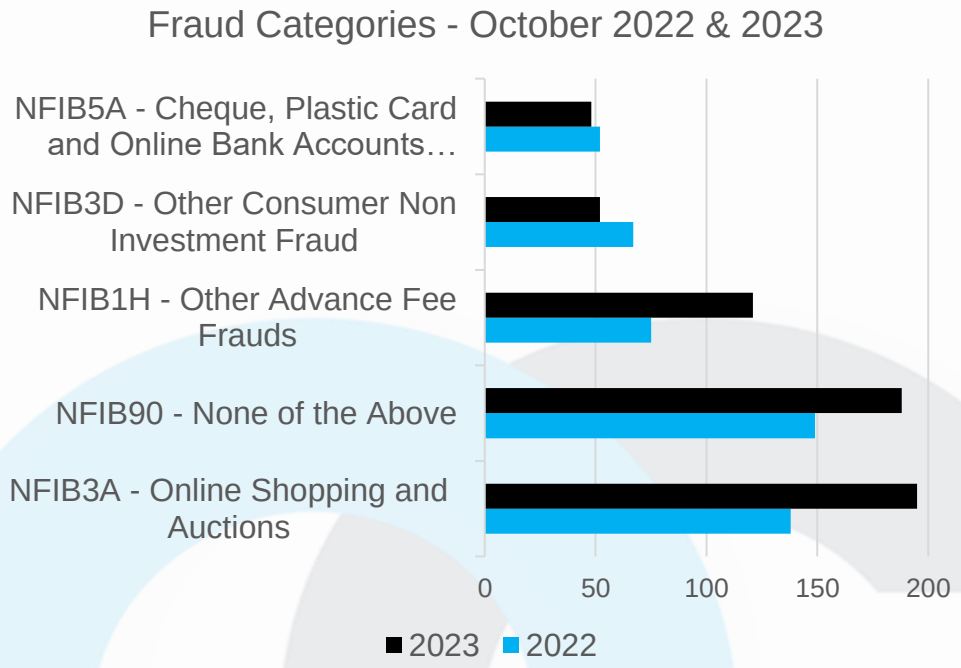
Fraud Category
North East Victim Reports

Total Reports: Oct 22: 629 Oct 23: 775 ↑ 23%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 775 reports in October 2023, a 23% increase compared to October 2022. Throughout October 2023, the most reported category remains NFIB3A - 'Online shopping and Auctions' with 195 reports, an increase of 41%.

This month, victims report when selling items on Facebook Marketplace they have been subject to spoof emails from prospective buyers. Some of the emails look like they're from PayPal or the seller's bank confirming that they have paid for the item or are holding funds for the sale. Victims have posted the items only for the payment never to appear.

Victims buying items have been subject to Advance Fee Frauds by paying insurance or a deposit for goods that have not arrived and do not exist. Most goods in this instance are higher value electrical items or vehicles.



National analysis by NFIB has highlighted an emerging threat where Fraudsters are adopting a new MO claiming to be 'High Court Enforcement Bailiffs'. Under this alias, they chase potential victims for payment of generic unnamed 'debts', fake driving fines, timeshare debts or media services debts. The victim is contacted via calls, texts or letters and told that their fake 'debts' total from £700 to £2800. Time pressures are given to the victim; advising them that they are required to pay the fine within 48 hours in order to avoid their assets being seized.
Regional work by the RECCC's Threat Desk has identified that this has been seen in the North East where both individuals and small businesses have been contacted. A total of 9 victims have reported this scam during October.

"WANT TO MAKE SOME EASY MONEY"

MONEY MULING

A money mule is someone that's recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Criminals will often use fake job adverts or create social media posts about opportunities to make money quickly, in order to lure potential money mule recruits. Money muling is a form of money laundering, and can carry a prison sentence of up to 14 years.

If you have been a victim of fraud or cyber crime, please report it to Action Fraud at Actionfraud.police.uk

"EASY MONEY"

Be extremely cautious about offers or opportunities to make "easy money", and never give your financial details to anyone you don't know and trust.

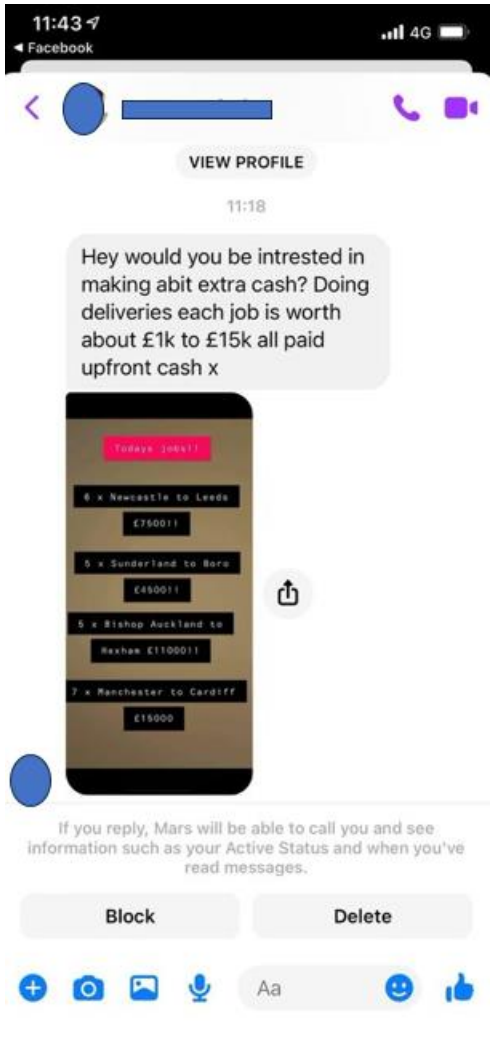
JOBS

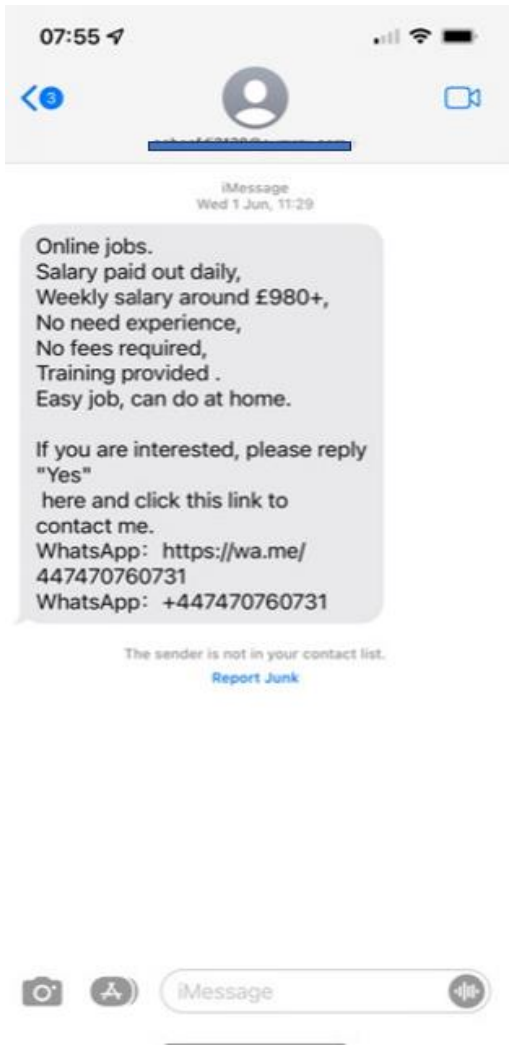
No legitimate employer will ever ask you to use your own bank account to transfer their money. Don't accept any job offers that ask you to do this.

TELL YOUR BANK

If you've already shared your bank details and have received money into your account, but suspect it could be part of a money muling fraud, you should notify your bank immediately.

EMMA9 (European Money Mule Action)





During November European Money Mule Action Campaign the RECCC will be attending Universities across the North East to raise awareness amongst students and staff around ‘money muling’.

We have already carried out a number of surveys to find out what students know about this subject and if they are being targeted with texts that are shown on the left.

Every Monday night we are running a Fraud Roadshow at Durham University where students and staff have asked any questions they may have. We have focussed this on ‘money muling’ due to the ongoing campaign.

Money mules will also be targeted in this month of action by our Proactive Economic Crime Team (PECT).

Engagement Events

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

The end of October marked the start of our ‘Fraud Roadshow’ that we will be hosting at various Durham University campuses throughout the month of November. We have already had some great feedback from students and staff.

Barclay’s bank at Cramlington invited us along to do an input with customers with great interaction from all involved.

We also travelled to Barnard Castle to deliver an input to U3A (a group of charities who offer the chance to those who no longer work to come together to learn for fun).

Also, getting the chance to visit Great North Air Ambulance headquarters to deliver a workshop to staff (as you can see by the picture, members of the team were pleased the helicopter returned while we were there).

The RECCC hosted a workshop at the Cyberfirst Education Conference which saw those from this sector developing their knowledge around Fraud.

Festive Shopping Tips

Check you are using genuine website domain addresses when shopping online.
If you are using Facebook Marketplace try to see the item in person.
Check reviews of websites before purchasing.

Always use a credit card for large purchases over £100, they offer more protection through section 75 of the consumer credit act.

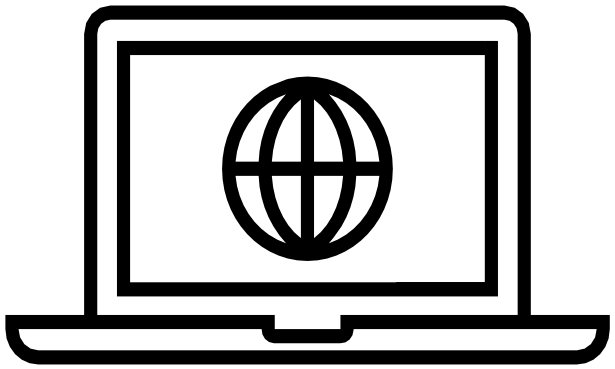
REMEMBER!!!

If it seems too good to be true, it probably is.

Be wary when looking for deals, especially on social media.

Horizon Scanning

Monitoring Threats



Courier Collection Scam

There have been several reports of victims selling items on Social Media sites when the scammer will arrange for a courier to collect their item. In some instances, the scammer has told the seller that as they can't come in person to collect the item for sale and will send a courier with a known company such as DPD instead. They may even send the seller a link to a fake website or an inauthentic email. The scammer will then ask the seller to pay for insurance for the safe delivery of the item. After the seller has entered their card details or made a payment, the buyer will no longer be in contact and will disappear.

Booking.com Scam

Booking.com users are being targeted by threat actors who are compromising hotel systems with the use of malware, before exploiting this access to send legitimate looking messages to customers who have bookings. Victims receive the fraudulent messages via the hotel's official Booking.com account, a malicious link within the message leads victims to a phishing page, mirroring Booking.com's interface which is prepopulated with the victim's personal details and requests the victim to enter and confirm payment details or risk the booking being cancelled. There have been three recent victims in the North East with an average loss of £630.

Courier Fraud Criminals Sentenced

A great result for the high harm team after they secured a sentence of over 15 years imprisonment for 29 victims who had seen a financial loss of over £100,000, after being targeted by four courier fraud criminals.

Zaki Chowdhury, 28, Muhammad Patel, 28, Raees Modan, 28, and Hamid Dahir, 27, are adjusting to prison today after a judge sentenced them to a total of over 15 years behind bars for their involvement in a fraud which targeted 29 victims back in 2018.

The victims, from across the UK, were then told the relative had been in possession of fraudulent bank cards and that the money from their own bank account had been compromised.

This was a complex investigation which culminated in the identification, arrest and conviction of those responsible.

ChatGPT

freepik.com

What is ChatGPT?

- ChatGPT was released in 2022 by a company OpenAI which was founded by Elon Musk.
- ChatGPT is an Artificial Intelligence powered language model.
- The technology chats in a conversational way, answering questions from the user. The online chatbot has been trained on lots of information and data from the internet - it can have a human-like conversation answering questions, admitting mistakes and rejecting any inappropriate questions.(BBC)

How ChatGPT is exploited by criminals?

- The use of ChatGPT has been seen in romance scams and has been dubbed ‘LoveGPT’. ChatGPT increases the believability of online dating conversations, and the generative AI technology allows it to engage in conversation with potential victims on behalf of the criminal. ‘LoveGPT’ has been seen on platforms such as Bumble, Facebook dating, Plenty of Fish, Tinder and OkCupid.
- Researchers have found that the technology has a variety of capabilities including the original task of creating profiles on various platforms, replying to messages on each platform, requesting a phone number and even constructing a first contact message.
- Generative AI helps reduce the workload of fraudsters and allows them to generate even more illicit funds as AI provides a readymade scripts to scam victims.

Actions for people using dating platforms.

- Trust, but verify: If a conversation feels too perfect or a profile too polished, do some digging. A quick reverse image search can reveal if that profile picture is borrowed from elsewhere.
- Stay vigilant: Bots like LoveGPT thrive on our desire for connection. Be wary of profiles that seem too eager to share personal stories or ask for personal information.
- Prioritise safety: Never share personal details like your home address, workplace, or financial information with someone you've just met online, no matter how genuine they seem.

What’s Happening Next?

Christmas is approaching and with this in mind it is likely that we all will be expecting more parcels than usual. We may see an increased in ‘parcel delivery scams’ that may look similar to the ones listed below:

- A card will be posted through the victim's door stating they have missed a parcel delivery and on the card there is a contact number. When victims are contact the number, they are finding it is a premium rate number and they are being charged hundreds of pounds to call it.
- An email or a text message stating the victim has missed a parcel delivery and they need to click a link and enter details or make a payment to retrieve the parcel.

- If you receive a card/letter posted through your door, try and use or search for a trusted number rather than using the one that is given.
- Try and keep track of the parcels you have ordered and when you should be expecting them.
- If you have any doubts, contact the delivery company and query it, using a genuine phone number from the company's website.
- Don’t click on any unsolicited email or text message links.

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.