

North East



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 September 2023 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 Dependant category selected. In September 2022 there were 87 total Cyber reports, in comparison, there has been 82 reports in September 2023 a decrease of 5.74%. In September 2023 the highest reported category was NFIB52C Hacking of social media and email with 63 reports. This is consistent with August 2023 figures.

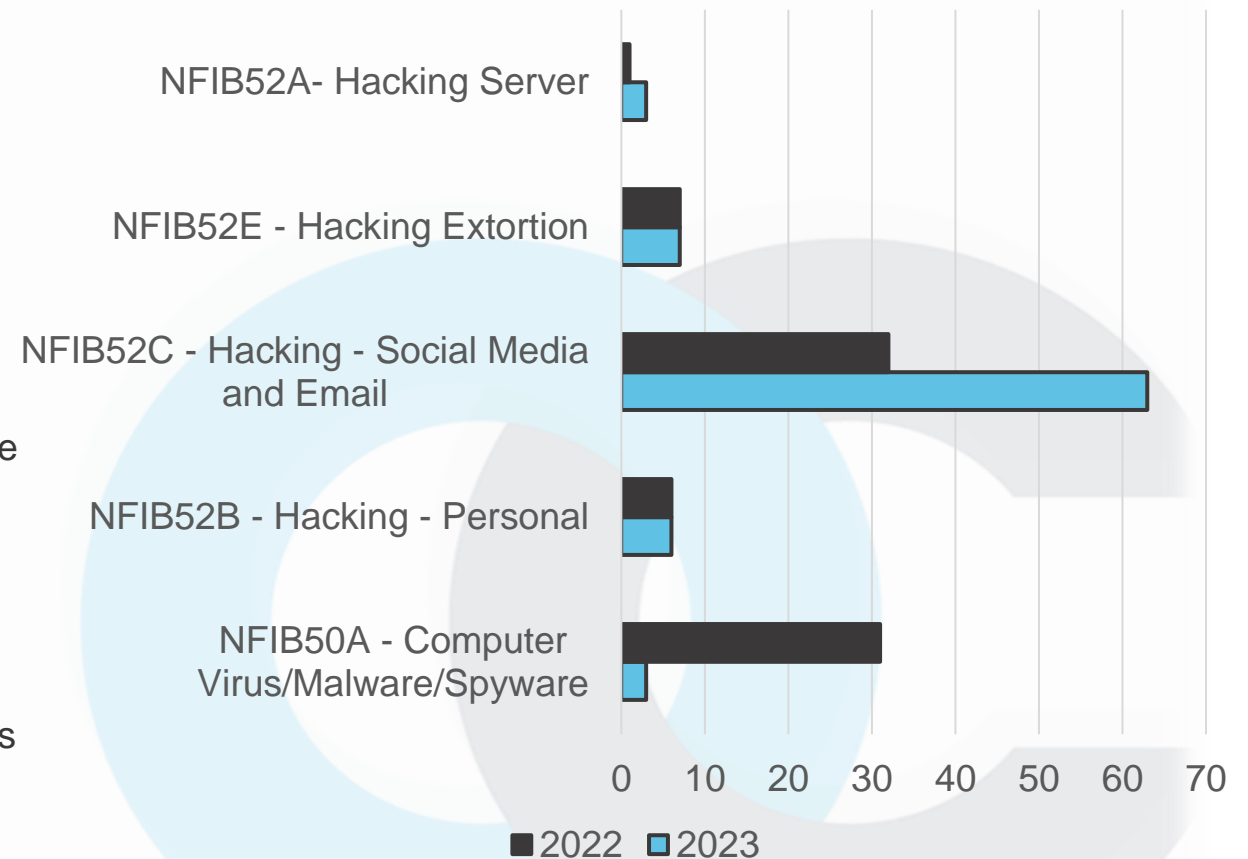
## Hacking:

A hacker is a person who can access other people's computers and modify programmes or information. Hacking happens when a hacker exploits a security breach in a network or computer and is able to access the information through the internet. Safety tips to protect you and your computer from hacking


- Configure and use email filters to block spam
- Install and use a firewall, pop-up blocker and spyware detector
- Ensure that your virus definitions are up to date and run anti-virus and spyware detectors/cleaners regularly
- Learn how to configure your computer to keep all of these solutions working efficiently

Total Reports: Sept 22: 87 Sept 23: 82 ↓ 5.74%

## Cyber Categories - September 2022 & 2023



# Fraud Category North East Victim Reports

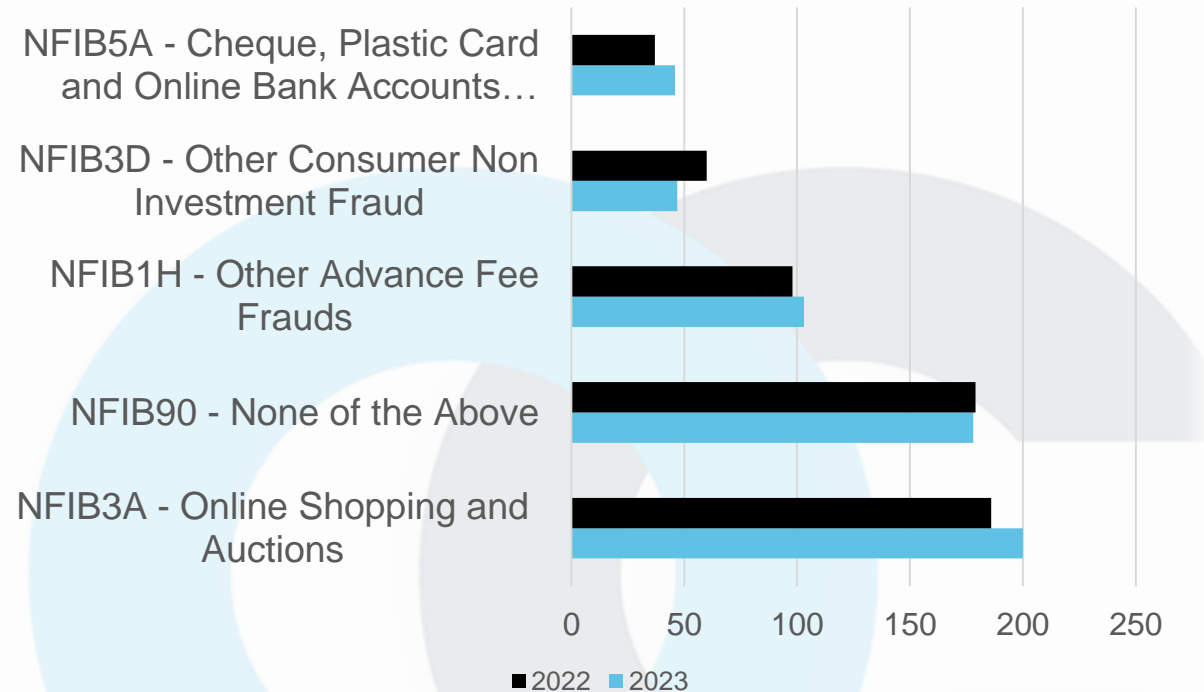
Total Reports: Sept 22: 721    Sept 23: 795     10.3%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 795 reports in September 2023, a 10% increase in reports when compared to September 2022. Throughout September 2023 the most reported category remains NFIB3A - 'Online shopping and Auctions' with 200 reports,

Chinese students studying at universities and colleges across the UK are falling victim to fraudsters over the telephone claiming to be officials from organisations such as the Chinese Embassy, Immigration or Customs Services, the Chinese Police, or Royal Mail. The scammers claim they are investigating international crimes and require the victim to transfer large sums of money to an account in China to be checked. One student in Northern Ireland was scammed out of £200,000 after the caller claimed the student was suspected of money laundering and threatened with arrest if they didn't pay.

Since the beginning of August there have been 9 similar offences reported in the North-East. The total loss reported has been £260,000 with the greatest individual loss of £104,000.

Fraud Categories - September 2022 & 2023



# Employment Opportunity Scam

Victims have reported a scam where they have seen a job advertisement on social media for what appears to be real companies offering victims freelance job opportunities. The roles are to "boost" products, apps or videos using software created by the Fraudsters. Other roles advertised are for data submissions and marketing .

## What is an 'employment opportunity' scam

- The victim pays a small fee and installs the software before receiving "orders" or "tasks" to complete.
- They report receiving a small payment or commission in order to convince them that the job is legitimate.
- The victim is instructed to deposit their funds into cryptocurrency accounts or wallets but later find that they are unable to withdraw the funds they have deposited and earned.

## How to protect yourself

- Research the company offering the job opportunity.
- Be wary of any job offers that offer good pay for very little experience.



Job Vacancy



# Engagement Events

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

The team have attended fresher events across the region this month. Along with delivering inputs at Universities for International Students on how to keep themselves safe from Fraud.

Students at Hartlepool FE College and Middlesbrough FE College have received Fraud Awareness inputs this month. Along with a 'Football Against Fraud' workshop delivered to FC apprentices.

The team have been involved in various different Victim Care and Advice Service (VCAS) and Age UK Fraud Awareness events throughout the month.

A number of cease and desist notices have been served throughout the region this month to those suspected to be involved in money laundering activity.





# Deep Fakes

## Deep Fakes, what are they and how are they used by criminals?

Deep Fakes are created by using a digital version of someone through technology called machine learning. The technology maps a person's face and mouth movements so that they can be copied. The technology can mimic a person's visual appearance and voice. Deep fakes are used by criminals by tricking a victim into thinking they are engaging with a real person. Deepfakes are increasingly being used in Romance Fraud Scams as the victim is manipulated into believing they are in a genuine relationship when in fact, the victim is conversing with deepfake technology during video calls for instance.

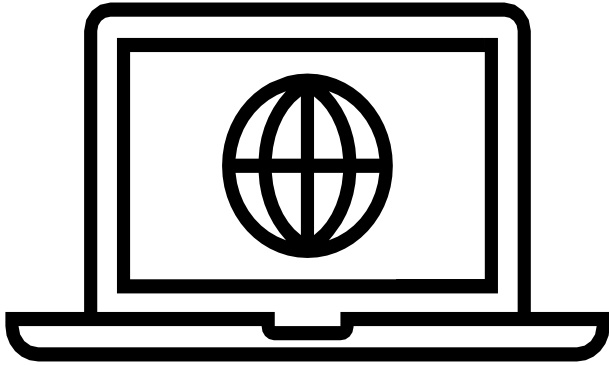
## How to spot Deep Fakes?

With developing technologies deep fakes are becoming more advanced and realistic however there is some signs to look out for. Fuzzy or blurred backgrounds, inconsistent body movement or inconsistent background or noise. Another sign of a deep fake in use is its lack of ability to converse with a side profile. Deepfake model technology is mostly developed by utilising front view profiles therefore a side profile check is an effective authentication.

Always remember if the content of the call seems strange or out of context verify what you are being told by other means.

# Horizon Scanning

## Monitoring Threats



The Cricket World Cup is running between Thursday 5th October – 19th November with all games held in India. As a result, fans may be tempted to access the games utilising streaming services to avoid payment and subscription charges. Fans accessing illegal streaming sites may become victims of Fraud and data theft. These sites are often used to distribute malware such as banking trojans, info stealers, cryptocurrency miners and other unwanted software onto a victim's device.



Direct Line Groups (including Direct Line, Churchill and Privilege) have announced that they will pay back policyholders, who have been overcharged for their car or home insurance, back dating to 1st January 2022. The estimated total of payback equates to roughly £30 million. Fraudsters may exploit this news through phishing campaigns (unsolicited emails). It is highly likely that Fraudsters will contact the public advising that a small fee is required to process their refund. This type of scam will look to collect both personal and financial information from the victim.



# International Students Targeted In The North East

International Students in the North-East and their families have suffered recent scams whereby thousands of pounds have been paid to criminals through Fraud. On one occasion, a student's parents have been contacted in China and convinced that their son had been kidnapped, they paid £56,000. On another, the student was contacted by someone purporting to be the police; he has sent 8 payments totalling around £200,000 (170 0000 RMB).

Beware of any communication from somebody who you don't know.  
Beware of any communication that is out of the ordinary.  
**Never Assume. Don't Believe. Always Confirm.**

If in doubt, hang up and report to Action Fraud and speak to University Staff.

Please make family members aware that they could be targeted and asked to pay large sums of money.

**If you believe you have been a victim of Fraud, Report it to Action Fraud on 0300 123 2040 or via [www.actionfraud.police.uk](http://www.actionfraud.police.uk)**

# DON'T GET YOUR FINGERS BURNT

Shop savvy this Black Friday and stay alert to online scams.  
If a deal looks too good to be true, then it probably is.



**#ShopSavvy** this Black Friday



**TO STOP FRAUD™**

# What's Happening Next?



## BLACK FRIDAY - 24<sup>TH</sup> NOVEMBER 2023

As Christmas approaches there will be many deals and offers up for grabs. In November shoppers will be able to take advantage of Black Friday and Cyber Monday sales. Online shopping Fraud is the highest reported Fraud in the North East and has remained so for quite some time, it is even more important to be cautious when shopping the sales when consumers will most likely increase spending during this period. Ensure that website domains are legitimate and use a credit card where possible as this offers more protection.

### Advice

- Use a credit card where possible (especially for large purchases) as they provide more protection under Section 75 of the Consumer Credit Act.
- Read reviews of the website you are purchasing from, be wary of new websites that have only been online for a short time.
- Always type the web address into your browser and be wary of accessing links through unsolicited emails.
- If you're asked to make a bank transfer instead of using a secure payment system.





# 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 – Engagement Officer Claire Hardy– Intelligence Analyst Nicola Lord– Intelligence Analyst</b>
<b>Reviewed By</b>	<b>D/Inspector Paddy O’Keefe</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.