

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 April 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



- [Action Fraud: Regional Cyber Summary](#)
- [Action Fraud: Regional Fraud Summary](#)
- [Engagement Events](#)


Contents

Looking Forward



- [Horizon Scanning](#)
- [What's Happening Next](#)

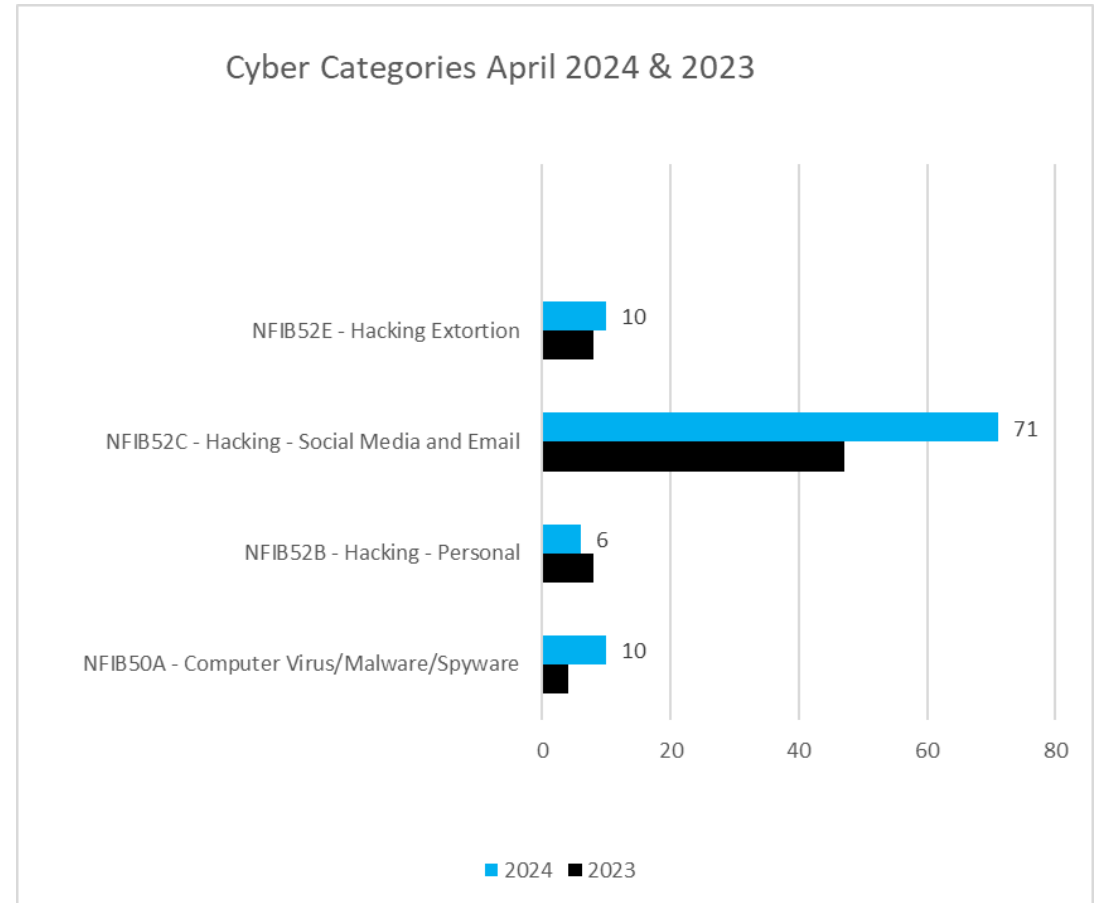
Cyber Dependent North East Victim Reports

Total Reports: April 23: 67 April 24: 97  44%

This data represents the number of reports received from Action Fraud with a Cyber category selected. April 2024 there was a total of 97 Cyber reports, in comparison, there were 67 reports in April 2023, an increase of 44%. In April 2024, the highest reported category was 'Hacking- Social Media and Email' with 71 reports. The age category 18-30 reported the most 'Hacking-Social Media and Email' reports, followed closely by the 51-60 age category.

In the month of April, within the Hacking-Social Media and Email reports, Email and Facebook are the most reported primary platforms compromised. Action Fraud data shows hackers have gained access to one of the victim's accounts and from this they have been able to access the victims further social media platforms.

Phishing scam from EVRI, we have seen reports on this in April in the region. Victims are receiving a text message that appear to be from the Evri delivery service that say they need to pay for redelivery. The text includes a link to a fake Evri website, where victims of the scam can enter their bank details. Although the amount of money they are claiming is small, the scammers are reportedly looking to steal people's payment details



Fraud Category North East Victim Reports

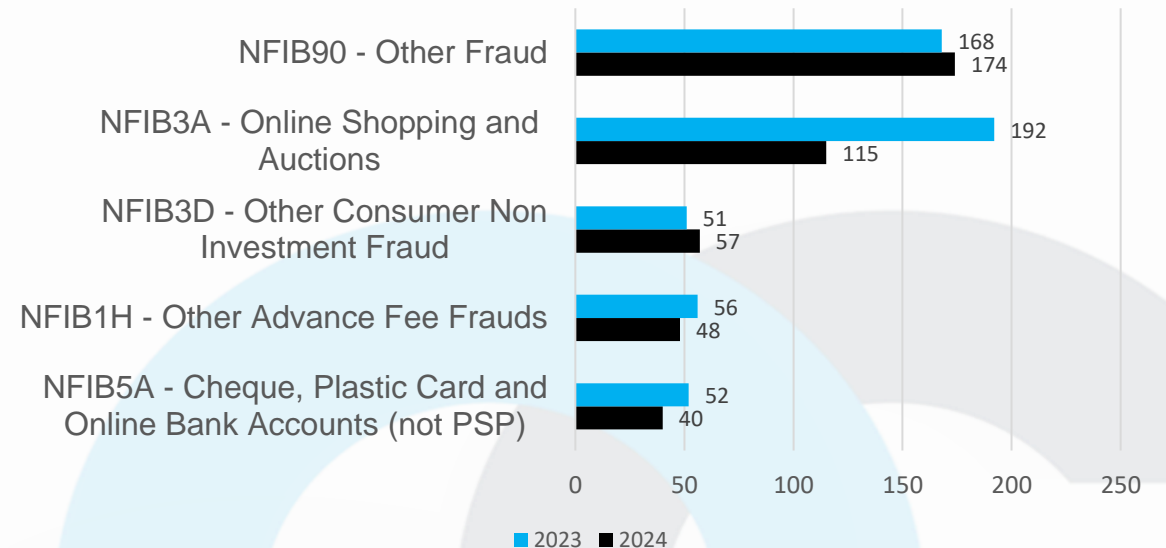
This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 575 reports in April 2024, a reduction of 13.9% compared to April 2023. Throughout this month, the most reported category after the general category 'Other Fraud' remains 'Online Shopping and Auctions' with 115 reports but it is worth noting that this has reduced by 24.5%.

Reports for 'Fraud Recovery' scams have doubled this month compared to April 2023. Fraud Recovery Scams are when someone who has been a victim of Fraud in the past is contacted again by fraudsters. They pretend to be a government, police or law agency official or company who can help recover the money that was lost but ask for a fee to get it back.

- Be ready for fraud recovery scams if you've been a victim in the past.
- Challenge any calls, letters or emails from people you don't know or companies you've never contacted.
- If you're asked to pay, or give your bank account details, end all contact.
- Ask how they found out that you had been a victim. Any report of fraud is protected by law and can't be shared with anyone else outside of law enforcement agencies.

Total Reports: Apr 23: 667 Apr 24: 575 ↓ 13.9%

Fraud Categories April 2024 & 2023



We would like to thank members of the public who have made changes to stay safe from Fraudsters, which may have contributed to the lower numbers of Fraud reports this month. We urge readers to continue to be vigilant and help spread the message to their friends and families to help keep themselves safe.

Engagement Events

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

This month the team have visited Barclay's Headquarters with Barclay's Local Champions to work with staff to increase awareness of the threat of Fraud in the local area with more CPD sessions lined up.

We took part in 'The Preparation for Life Roadshow' at Bede College and Hartlepool Sixth Form speaking to students about money muling and checking their password security.

A Fraud foundation information session with Durham Carers to increase their knowledge around Fraud and Economic Crime.

We worked with Cleveland Police Cyber Team to deliver to University of the 3rd Age (U3A) in Hartlepool. We have also visited Allendale Warm Hub Network to speak to the group about Courier Fraud and Fraud awareness.

HAVE YOU BEEN CONTACTED BY THE POLICE AND ASKED TO HELP AN INVESTIGATION?

THE POLICE WILL NEVER
CALL YOU TO ASK YOU TO
VERIFY YOUR PERSONAL
DETAILS OR PIN BY PHONE
OR OFFER TO PICK UP YOUR
CARD BY COURIER.

STOP! THINK FRAUD.



REPORTS OF FRAUD CAN BE MADE TO ACTION FRAUD ONLINE OR BY CALLING 0300 123 2040

Business Banking Customers Are Being Targeted.

Multiple business bank customers have been called on business lines by a threat actor purporting to be from their bank.

HOW IT WORKS:



The customer receives a phone call from a criminal claiming to be from the bank. They have knowledge of recent transactions on the account and state that there has been suspicious activity on the account.



The customer is then directed to a website which mirrors the official bank website. Some of the links on the website download an app called Any Desk to the customers computer and the threat actor then states they are reversing the suspicious transactions and the customer needs to authorise them.



However, the criminal then adds new beneficiaries to the account and the customer is authorising payments to the newly added beneficiaries.

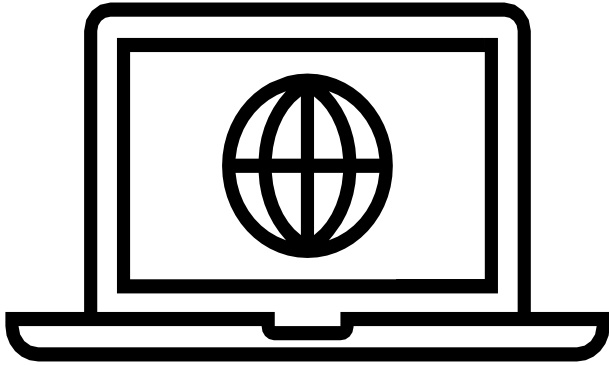
HOW TO PROTECT YOURSELF AND YOUR BUSINESS:

- If in doubt, hang up.
- Use a trusted number to call back and check it out.
- Do not give any personal details or sensitive information.

Remember, not everyone is who they say they are!

Horizon Scanning

Monitoring Threats



Well known brands are being used to advertise fake giveaways by criminals looking to exploit members of the public. The fake giveaways are advertised on social media and via phishing emails.

Some of the brands that have been impersonated are SHEIN, impersonated on Instagram offering gift cards to users and also sending malicious links via email.

Asda is another company that has been impersonated on social media, mainly Facebook on buying and selling pages and other community groups, offering a giveaway of a '£250 voucher'. The link takes the user to a fake website and steals the users personal details once entered.

If in doubt remember to avoid clicking on unknown links and if it sounds too good to be true, it probably is!

FAKE GIVEAWAYS

A number of fake giveaways are circulating on social media and via phishing emails.



PHISHING

'Phishing' is a cybercrime in which a target is contacted by email, telephone or text message posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details and passwords. The information is then used to access important accounts and can result in identify theft and financial loss.



Criminals like to phish for your information

How you can stay safe;

- Avoid clicking on links in emails, texts and on social media
- Avoid giving out any personal or financial information unless it is to an organisation you know and trust.
- Review your privacy settings within your social media accounts.

If you believe you have received a phishing email, text or phone call you can report it at report@phishing.gov.uk. Please see www.NCSC.gov.uk for further advice on phishing.

If you think your information might have been stolen, call your bank immediately and report it to www.actionfraud.police.uk

McAfee scam emails

Action Fraud has received 4,531 reports since 1st April 2024 relating to fake emails purporting to be from McAfee. The emails state that the recipient's computer "could be at risk" from "viruses and other malware" if they don't renew their anti-virus subscription. The links in the emails lead to phishing websites that are designed to steal your personal and financial information.

HOW TO DEAL WITH SUSPICIOUS MESSAGES

If you have doubts about a message, contact the organisation directly. **Don't** use the numbers or address in the message - use the details from their official website. Your bank (or any other official source) will never ask you to supply personal information via email.

Spotted a suspicious email? Forward it to the Suspicious Email Reporting Service (SERS) - report@phishing.gov.uk

Subscription Details

Subscription: **Expired**

Your Antivirus Protection Has Expired!!

Account ID :	██████████
User :	██████████
Safe status :	Suspended
Discount :	85% Renewal discount

Your Antivirus Protection has Expired Today: **Fri,19 Apr-2024**

It is **HIGHLY** recommended that you renew your subscription now to continue protecting your device. A special discount is available for activations on Fri,19 Apr-2024.

After the expiration date, your computer becomes vulnerable to a wide array of virus threats.

Without protection, your device is at risk of being infected by viruses and other malware!

You are entitled to the discount: **85% discount on renewal for 1 year**

The offer expires: **Fri,19 Apr-2024**

Renew Subscription

Thinking of investing?

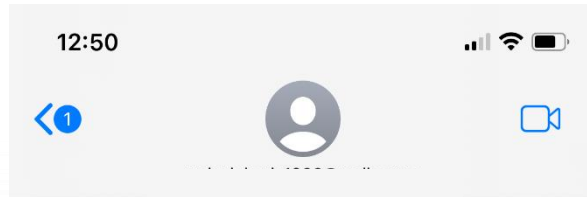
Did you know that the Financial Conduct Authority has a tool that allows you to check if the company you are thinking of investing with are on the Financial Services Register?

Almost all financial services in the UK must be authorised and registered.

To search the warning list for unauthorised companies or for more advice, visit:
www.fca.org.uk/scamsmart



EVRI



iMessage
Today 12:50

EVRI mail package in the process of transportation, due to damage to the outer package, address information is lost, can not be delivered. Please be sure to update the delivery address information in the link within 12 hours.

<https://evri-uk.motorcycles/uk>

(Please reply Y, then exit the SMS, re-open the SMS activation link, or copy the link to open in Safari)

The EVRI team wishes you a great day!

The sender is not in your contact list.

[Report Junk](#)

There continues to be an increase in Fraudulent Evri delivery texts similar to the one pictured (left) throughout the North East. The latest victim in the North East has had £4000 stolen from their account.

When victims reply 'Y' and receive a link they are taken to a page that looks similar to the Evri website, the website requests personal information and requests the victim to card details.



- Do not reply to the text and do not click any links.
- Forward any suspicious texts to 7726 to be investigated.
- If you have entered any personal details, contact your banks Fraud team immediately by dialling 159.

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

HAVE THE BANK CALLED AND ASKED YOU
TO WITHDRAW MONEY TO HELP SECURE
YOUR ACCOUNT?

YOUR BANK WILL NEVER
CALL YOU AND ASK YOU TO
WITHDRAW CASH TO HELP
SECURE YOUR ACCOUNT

NOR WILL THEY ASK YOU TO
TRANSFER YOUR MONEY TO
AN UNKNOWN ACCOUNT

STOP! THINK FRAUD.



REPORTS OF FRAUD CAN BE MADE TO ACTION FRAUD ONLINE OR BY CALLING 0300 123 2040

Data from Action Fraud shows that 22,530 people reported that their online accounts had been hacked in 2023, with victims losing a total of £1.3 million.

Secure your email and social media accounts



What can you do to avoid being a victim?

- Use strong and different password for your email and social media accounts
- Turn on 2-step Verification (2SV) for your email and social media accounts

If you have been a victim of fraud or cybercrime report it at www.actionfraud.police.uk or by calling 0300 123 2040

What's Happening Next?



Olympics – Paris, July 2024

With 1.42 billion expected in revenue from the sale of tickets for the 2024 Olympics in Paris, it is no surprise that this is a major target for criminals to exploit. During the champions league final at Stade Le France in May there were fake tickets detected, it is likely that this will also happen at the Olympics. It is important to be vigilant when purchasing tickets and protect any accounts you use to purchase tickets with strong passwords and security.

Euros – June 2024

In addition to the Olympics, The UEFA European Championships start in June. As with what is stated above, be on the look out for fake ticket sales and fake merchandise as criminals will look to exploit the high demand for these events. Be wary of any adverts on social media and try to use official websites where possible.



STOP!
THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

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

STAR SECURE
TICKETS from
AUTHORISED
RETAILERS™
STAR.ORG.UK

#TicketFraud

Secure your accounts.

Protect your important online accounts, such as your email or the accounts you use to buy tickets, with passwords that you don't use anywhere else. Use three random words to create strong and memorable passwords.

● Buy safely ● Payment ● **Account security**





For more information search 'nerccu police'



Scan to visit our website



BUILDING RESILIENCE AGAINST FRAUD

How to report



Police

All Fraud in the UK is reported to the police at Action Fraud by phone or online:
0300 123 2040
www.actionfraud.police.uk

Action Fraud is the central reporting point for all reports of fraud, your local police force will be informed by Action Fraud.



Emails

Forward Fraudulent emails to
report@phishing.gov.uk



Banks

Dial 159 (Stop Scams UK Anti-Fraud Hotline)
An automated line which Takes you through to your Bank's Fraud team .

For alternative ways of contacting your bank only use the contact details on your bank card or the official website.



Phone Numbers

Forward phone numbers Sending you Fraudulent Messages or calls to **7726**

Handling Instructions

Distribution List
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.



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 – 3P Officer Claire Hardy– Intelligence Analyst Sarah McCluskey –Cyber Threat Desk 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.