

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 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





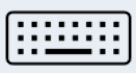







- [Horizon Scanning](#)
- [What's Happening Next](#)

North East Cyber Crime December Summary



INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

 Total Cyber Reports (compared to December 2023)		160 (+61%)
 Hacking -Social Media and Email		120 (+66.7%)
 Hacking - Personal		21 (+162.5%)
 Computer Virus/ Malware		12 (No change)
 Hacking Extortion		7 (+40%)

Account Hacking

There have been an increase in reports of online shopping and social media accounts being hacked. Some of those that have been named in victims reports include Klarna, Next, Instagram, Trainline, Amazon and Air BnB.

How to prevent hacking:

Reports of account hacking continues to rise. Some simple steps to try and protect your accounts.

- Long, strong and unique passwords on your accounts. Try to use three different words and a variety of numbers and symbols.
- Two Factor Authentication on all of your accounts, especially social media accounts.
- Try to use different passwords across your accounts, not just the same one.
- Don't click on any links sent in unsolicited messages or emails.
- Avoid doing 'questionnaires' on social media as these are tactics to try and get memorable information you may have used for your accounts.
- Make sure your anti virus software is updated.


There have been reports of victims receiving calls from Fraudsters claiming to be from BT and stating they need personal information from the victim. They have reported that the victim has issues with their account or internet and have even asked for driving licence details. Remember, do not give out personal information and if in doubt, hang up! Wait for half an hour or use a different phone to call BT on a legitimate number to check if they made the call. You can report scam calls to 7726.

North East Fraud December Summary






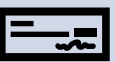



**DECREASED THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR**



**Total Fraud Reports
(compared to December 2023)**

 **631
(-18.2%)**

TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:

	Online Shopping and Auctions	 134 (-24.3%)
	Advance Fee Frauds	 93 (+19.2%)
	Other Consumer Fraud	 50 (-7.4%)
	Cheque, Plastic Card and Online Bank Accounts	 47 (-14.5%)
	Investment Fraud	 37 (-67.5%)

Impersonation Scam

Fraudsters impersonating banks, phone companies or Amazon continue to target victims in the North East and across the UK. As more safeguarding measures are put in place, Fraudsters cold call victims for one-time passwords. There have been an increasing number of reports where the criminal mentions 'Action Fraud' reporting to the victim to add an element of legitimacy to their script.

Booking.com

Locally there has been an increase in the number of reports from victims who have lost money when paying for accommodation they have reserved on Booking.com. This follows a National trend. Individuals were defrauded after receiving unexpected messages and emails from a Booking.com account belonging to a hotel they had a reservation with, which had been taken over by the fraudster. Using this account, the criminals send in-app messages, emails, and WhatsApp messages to customers, deceiving them into making payment and/or requesting credit card details. The specific account takeovers are likely to be the result of a targeted phishing attack against the hotel or accommodation provider, and not Booking.com's system or infrastructure.

Advance Fee Fraud

There has been a rise in reports of Advance Fee Fraud, this is where the victim pays a sum of money upfront and does not receive goods or service. Ensure you are using reputable trades people before leaving a deposit for any work. If you are purchasing goods off a selling site such as Facebook Marketplace, always try to see the item in person prior to purchasing.

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.



Image (right) keywords have been taken from Romance Fraud victim reports to Action Fraud – July to December 2024

ENGAGEMENT EVENTS

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

2025 is off to a busy start and already throughout the end of December and the start of January the team have been delivering Fraud awareness inputs across the region and already established some growing connections for some projects throughout the year. Watch this space ...

A variety of different departments working for Northumberland Citizens Advice, including the debt and money advice teams have received Fraud Awareness inputs which should help them in their day to day working.

Operation Lazio which is an operation to increase awareness amongst police cadets has started again in Durham, Cleveland and Northumbria Police Forces.

If you are in the North East and feel your organisation, group or company could benefit from the work we do, please get in touch using the email address on the front page.

How to spot the signs of Romance Fraud!

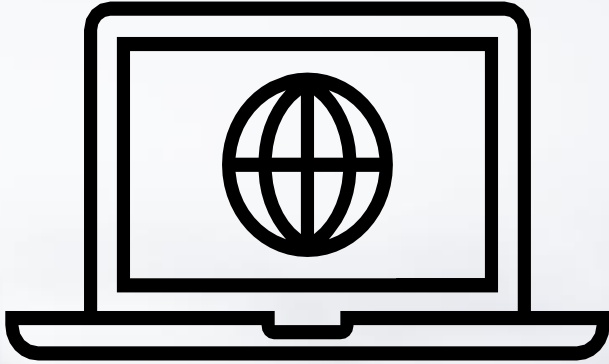
- You've struck up a relationship with someone online and they declare their love for you quickly. Many fraudsters claim to be overseas because they work in the military or medical profession.
- They make up excuses as to why they can't video chat or meet in person and will try to move your conversations 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**.
-

Horizon Scanning

Monitoring Threats



Fake Websites

Watch out for fake websites, victims have been targeted by purchasing goods through fake websites. One of the examples was an advert showing 'Homebase is closing down' and the victim has made a purchase on the fraudulent website.

This has been seen using different websites such as Wilko when they ceased trading. Be wary when making purchases online and always check the website you are using is the correct one, criminals can push their websites to be the first one that appears in search engines.

Advice:

- Always check the URL you are using.
- Read online reviews.
- Do not use bank transfer as a method of payment.
- Look out for a padlock, although this can be forged by criminals so still carry out other checks.
- Check the fine print.

There has been in a rise in reports of a scam whereby victims receive a phone call from someone purporting to be from Klarna. It is claimed that it is the Fraud department or that there is suspicious activity on the victim's account. The victim is provided with personal information to make it look legitimate and then asked to provide a one-time pass code.

What can you do?

- Hang up and check your account using your Klarna app or log in using the website.
- Do not give out any personal or sensitive information.
- Ensure your account is protected with a strong password.
- Do not answer calls from unknown numbers.
- Remember, even if someone provides personal or sensitive information it does not mean they are legitimate.

Klarna®

Buy now. Pay later. No fees.

NEVER GIVE ANYONE YOUR ONE

TIME PASS CODE!!!!!!!

Total amount lost to Romance Fraud in the North East 2024

The figure on the right is the total amount victims in the North East have paid out to Romance Fraud scams in 2024.

£2,457,552

North East

ROCU

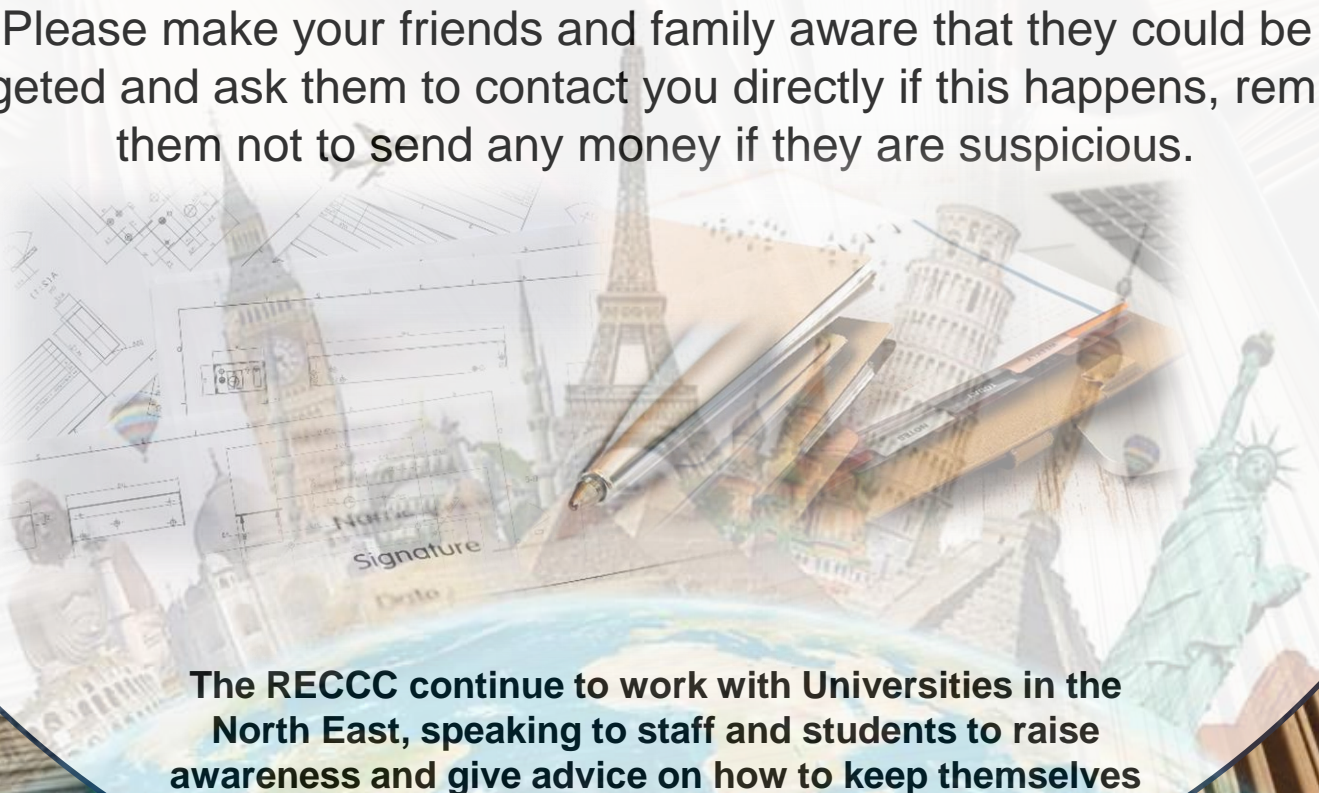
Regional Organised Crime Unit Network

International Students

are often targeted with Fraud claiming they face deportation/are part of an investigation, there are problems with their visa or stating they need to pay fees.

There have also been various tactics used to obtain money from the student or the students family in the form of fake kidnaps and ransom, sometimes even contacting the families of the student.

Please make your friends and family aware that they could be targeted and ask them to contact you directly if this happens, remind them not to send any money if they are suspicious.



The RECCC continue to work with Universities in the North East, speaking to staff and students to raise awareness and give advice on how to keep themselves safe.

Beware of
“too good
to be true”
holiday deals

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

 **ABTA**
Travel with confidence



What's Happening Next?



HMRC

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 2025 deadline for submitting tax returns.

Between the months of November 2023 and October 2024 HM Revenue and Customs (HMRC) received more than 144,000 reports about tax scams, a 16.7% increase from the previous year.

Advice:

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](https://www.gov.uk).

LA Fires

There have been donation pages set up for LA with the ongoing fires in the area. Celebrities have posted on social media that they have had pages using their names asking for donations.

Advice:

- If you want to donate, try to research proper channels to do so.
- If something has celebrity endorsement, look into it, it could be fake.
- Always keep in mind that criminals look to exploit these type of emotional events.





 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 2024 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– Economic Threat Desk Analyst Sarah McCluskey –Cyber Threat Desk Analyst
Reviewed By	SGT Emma O'Connor

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.