

# 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 2024 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](#)
- [Action Fraud: Cleveland](#)
- [Action Fraud: Durham](#)
- [Action Fraud: Northumbria](#)
- [Engagement Events](#)

# Contents

Looking Forward












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

# North East Cyber Crime October Summary

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



<b>Total Cyber Reports (compared to October 2023)</b>	 <b>162 (+125%)</b>
 <b>Hacking -Social Media and Email</b>	 <b>115 (+109%)</b>
 <b>Computer Virus/ Malware</b>	 <b>25 (+525%)</b>
 <b>Hacking - Personal</b>	 <b>17 (+54%)</b>
 <b>Hacking Extortion</b>	 <b>5 (+150%)</b>

## Hacking – Social Media and Email



Hacking – Social Media and Email reports account for 70% of all the Cyber reports to Action Fraud in October 2024. Reports for this category are rising month on month in line with national reporting. Financial motivations continue to drive Social Media hacking reports. This has been highlighted in Sim-Swapping reports and takeovers of WhatsApp accounts through the ‘One-Time-Passcode Vishing’ method. It is also visible with the increasing number of compromised Facebook accounts used to advertise fraudulent concert tickets.

## Parking Fine



The Parking Fine Phishing scam has continued across the region for October, accounting for the rise in the Computer Virus/Malware category. The EVRI phishing scam text has also continued in reporting across the region in October.

## WhatsApp



WhatsApp account hacking has continued this month. The most common reported method continues to be through an invitation link to join a video call for either a church group or work group. The victim receives a 6 digit code which is shared with the suspect who then gains access to their WhatsApp account and contacts family and friends requesting money for an urgent/distressing situation.

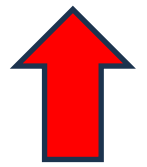
## Klarna



There has been a number of reports from the region from victims who were led to believe that they had been contacted by Klarna, regarding suspicious transactions on their accounts. As part of their ‘verification’ process, the victim has been asked to confirm they are the account holder by reading the code that sent to them. The victims then start to receive notifications on the Klarna App with regards to transactions being made. The victim also received an email from Klarna requesting a payment of £1,500.

# North East Fraud October Summary











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



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

**907  
(+ 17.3%)**

## TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:

	<b>Online Shopping and Auctions</b>	<b>194 (-0.5%)</b>	
	<b>Advance Fee Frauds</b>	<b>102 (-15%)</b>	
	<b>Other Consumer Fraud</b>	<b>87 (+67.3%)</b>	
	<b>Investment Fraud</b>	<b>57 (+23.9%)</b>	
	<b>Cheque, Plastic Card and Online Bank Accounts</b>	<b>49 (+2.1%)</b>	

### Mobile phone Upgrades/ Free watch

An unexpected call from your phone provider offering an upgrade or great new deal may appear wonderful but when a phone contract is taken out in your name without your knowledge it could be a very costly affair. To further entice victims to sign up for mobile phone contract upgrades offered by their provider out of the blue, scammers are offering free watches or gifts for a limited time only. Victims signing up for cold call upgrades have new phone contracts taken out in their names without their knowledge.

### Rogue Traders

Reports have increased significantly against last month. Most of the reports are concerning builders and companies offering home improvement services. In most of these reports, the victims have looked online for companies rather than the cold calling methods seen previously. Large deposits or upfront payments for materials were made and the scammers either did not show up, left work unfinished or completed work to a poor quality.

### Advent calendars

Shoppers looking for a good deal on a luxury advent calendar are being warned to watch out for online scams. People should watch out for fraudsters offering deals that appear too good to be true ahead of Black Friday sales.

Fraudulent adverts on social media platforms for beauty brands including Rituals or Space NK are currently targeting customers in the North East. Most start with the line 'My sister works for....' but not all. Consumers buying non beauty calendars such as Marvel and WERA from Ebay also report losses.

### Universal Credit/ Child Maintenance Scam Text Messages

This month, further new scam phishing text messages have been circulated claiming to be from the DWP regarding Universal Credit and Child Maintenance payments. Within the messages, there are links to spoofed DWP webpages requesting personal and bank details as part of a fake 'assessment' process.

# ENGAGEMENT EVENTS

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

The European Money Mule Action campaign has still been running throughout October and the beginning of November. We have spoken to hundreds of students at Durham University during our Fraud Roadshow to highlight the dangers of being approached to become a money mule.

A number of different groups of international students across the region have had inputs about the type of Fraud that might target them while studying in the UK.

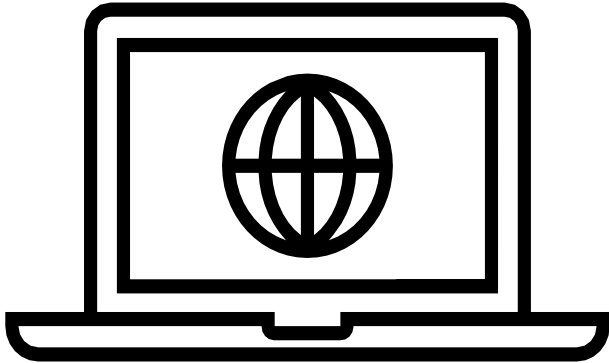
The team hosted a stall at North Tees and Hartlepool NHS Trust 'festival of finance' and spoke to staff and members of the public to raise awareness of Fraud.

Business owners in Cleveland were invited to a workshop hosted by the RECCC and Cleveland Cyber Crime team that focussed on financial wellbeing, Fraud advice and Fraud types.



# Horizon Scanning

## Monitoring Threats



We have previously identified caution when purchasing tickets, especially for popular events like Oasis concerts. In the last few weeks there have been a further increase in scams relating to Oasis tickets. Social media accounts have been reportedly hacked and then posts have been uploaded on to the hacked account offering Oasis tickets for sale.

With news that Oasis will be cancelling tickets sold by third parties, there is the possibility this will drive further demand to purchase from unknowingly from hacked 'friends' on Facebook after fans lose out.

- Ensure all social media is protected using two factor authentication.
- Be wary of buying any tickets from social media or websites that are not legitimate.



Sponsored ads on Facebook offering a free Sephora mystery box after completing a survey are being circulated. Once complete, bank details are requested to cover postage costs. Fake Facebook users claim to have received the box and leave positive feedback on the post.

Remember, if it seems too good to be true .. It probably is!



# NHS DENTIST SCAM

Dentists are in high demand across the country, people are being placed on huge waiting lists to be seen by an NHS dentist. This has created a desperate need for some people to receive dental care, especially those who cannot afford the prices of a private surgery.

Facebook community groups are being used to target victims who are being told appointments are available and to book an appointment they need to fill out a form with payment details on a Fraudulent website.

The website is made to look legitimate with dentistry certificates, the name of a real dental surgery is used to make it look legitimate and once payment is made it becomes apparent there is no appointment.

## **Need to find an NHS dentist?**

The below links are to the legitimate NHS website, this is the **ONLY** authentic way to find an NHS dentist:



[www.nhs.uk](http://www.nhs.uk)

[www.nhs.uk/service-search/find-a-dentist](http://www.nhs.uk/service-search/find-a-dentist)



.....  
.....  
.....  
**Payment upfront? Think twice  
before you pay!**

Scammers often demand payment in advance for goods or services that never arrive. If you're asked to pay upfront, take a moment to stop, think and challenge the request

#TakeFive



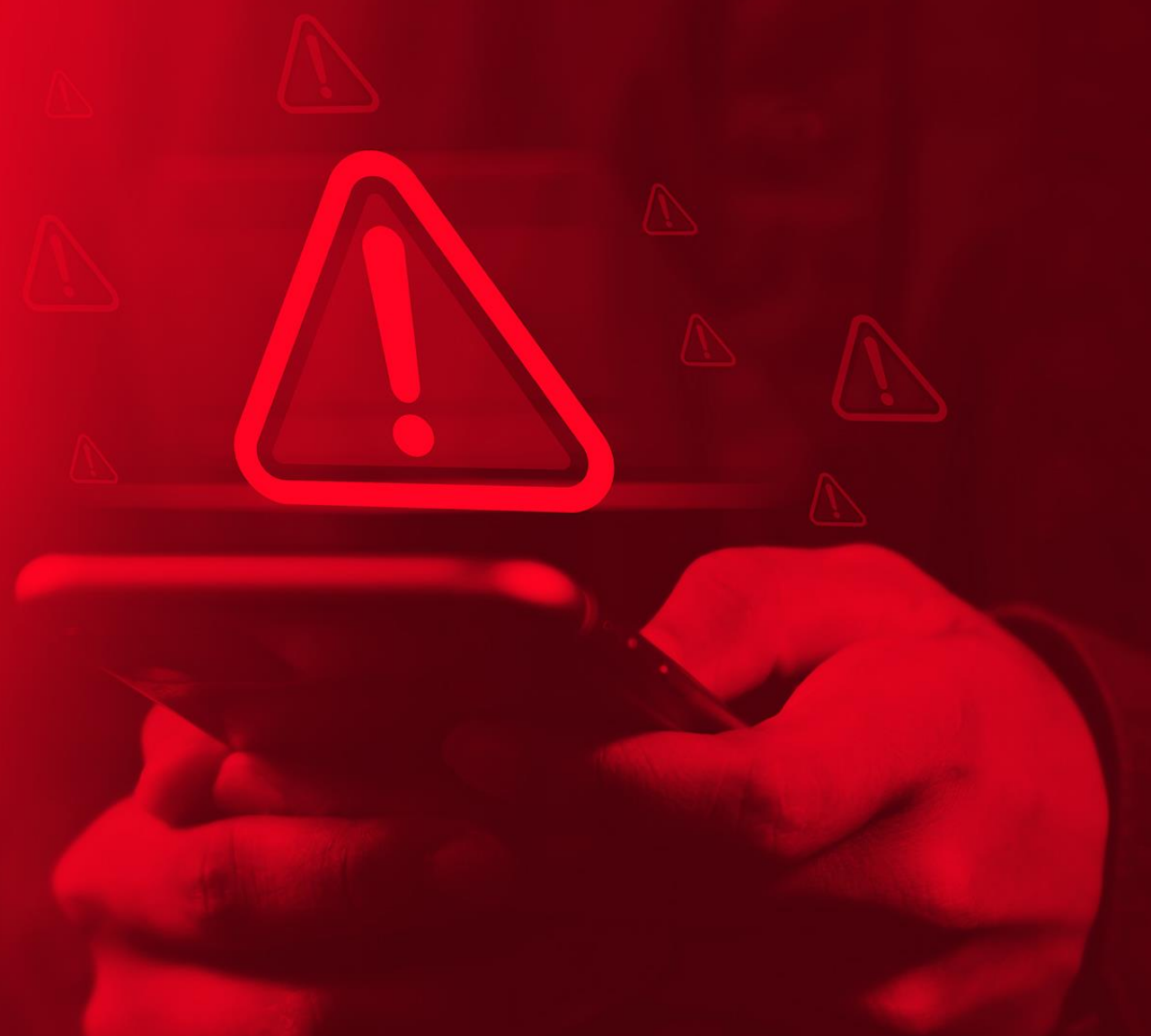
**ALWAYS STOP AND  
THINK!**



 [actionfraud.police.uk/phishing](https://actionfraud.police.uk/phishing)

# Report phishing

**ActionFraud**  
National Fraud & Cyber Crime Reporting Centre  
 [actionfraud.police.uk](https://actionfraud.police.uk) 



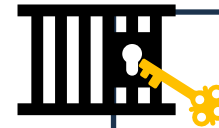
# European Money Mule Action

10

## What is a 'Money Mule'?

Criminals who have illicit funds often target people to launder. This was mainly students but recently there has been an increase in other age categories being approached. It can be via social media, texts, in person, online or via email, they may make an offer of a job to 'earn quick/easy cash'. However, they will request that money is passed through the persons bank account to 'clean it', this is illegal and classed as money laundering and could result in imprisonment.

European Money Mule Action (EMMA10) runs every November. As usual we are running our Fraud Roadshow along with other events to raise awareness amongst students who are often targeted by this.



**14 YEAR  
PRISON  
SENTENCE**

## KNOW THE SIGNS :

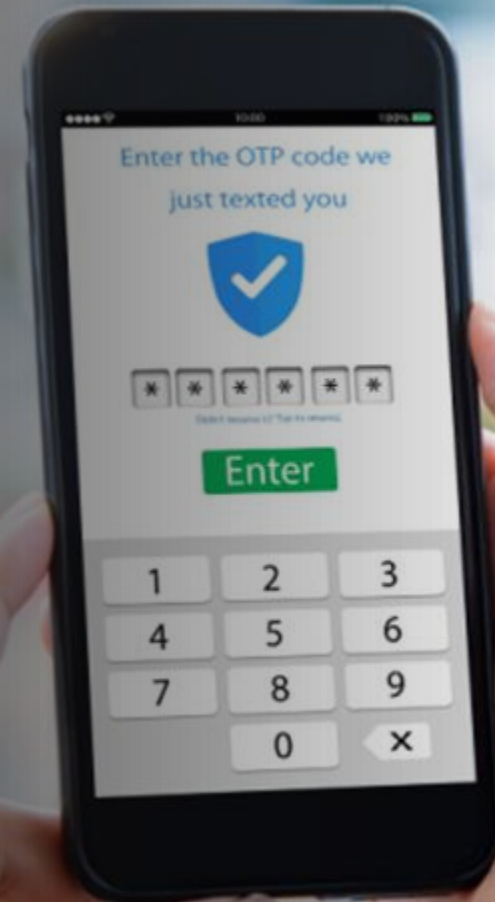
- Job offers using social media or even job websites offering 'quick cash' or 'easy money'.
- Someone requesting to use your bank account/transfer money.
- Someone you do not know asking for your bank details.



## One-Time Passwords

- You wouldn't share your PIN .....
- ~~Never share verification codes, 2FA codes or one-time passwords, in SMS or over the phone.~~
- If you think you may have given sensitive details, such as payment information to fraudsters, let your bank know what's happened immediately.

If you have been a victim of fraud or cyber crime, reports it to Action Fraud online, or by calling 0300 123 2040.



# What's Happening Next?



## **Criminals don't stop for Christmas!**

They target shoppers online, taking advantage of those looking for deals. Be wary of online sellers using platforms such as Facebook Market Place, never make an upfront payment for an item that you have not seen in person.

Always check the URL addresses of the websites you are using as criminals use fake websites to scam people.

### Advice:

- Always stop and think before parting with personal/financial info.
- Read online reviews from reputable sources to check websites are genuine.
- Use a credit card for large purchases to provide extra financial protection through section 75 of the Consumer Credit Act.



# NHS

**No NHS service would under any circumstances call members of the public and attempt to sell products.**

If you receive such a call, you need to be aware that it is a scam call. If you get a call from any NHS organisation, staff will be happy to provide their full name, the team they work for, their base and contact details, and the reason for their call. If the person calling you will not provide this information, end the call. Do not share any personal information. Please report this to the appropriate NHS Counter Fraud team either at the organisation or at NHS Counter Fraud Authority - [www.cfa.nhs.uk](http://www.cfa.nhs.uk)

**NHS England administer the NHS App upon which people can sign up and receive/send messages. This is the safest way of contacting or staying in touch with their GP practice.**

**You can ring the NHS organisation concerned to check the authenticity. You would do this by calling the reception of the hospital, practice, or clinic to verify. Only use contact details that you know to be true.**



 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](http://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](mailto: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

<b>Distribution List</b>
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.**



<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 – 3P Officer Claire Hardy– Economic Threat Desk Analyst Sarah McCluskey –Cyber Threat Desk Analyst</b>
<b>Reviewed By</b>	<b>T/Sgt Brian Collins</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.