

# 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 2025 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.

# North East Cyber Crime April Summary

INCREASED THIS MONTH  
COMPARED TO THE SAME  
MONTH LAST YEAR



Total Cyber Reports (compared to April 2024)		 142 (+42%)
 Hacking -Social Media and Email		 101 (+36.5%)
 Computer Virus/ Malware		 21 (+110%)
 Hacking - Personal		 13 (+117%)
 Hacking Extortion		 6 (-40%)
 Denial of Service Attack		 1 (+100%)

## Cyber Attacks

It has been well publicised that Marks & Spencer, Harrods and The Co-op have been targeted in well orchestrated cyber attacks significantly affecting their businesses. Please see page 7 for advice on how to protect yourself if you feel like you have been affected as a customer.

## Cloned Businesses

Local businesses have had goods or payments stolen through fraudulent, cloned companies. Businesses believe they are selling to reputable companies without knowing that these businesses have had their identities stolen and cloned. The cloned companies have usually been hacked. Some of the victims are current business customers so checks will not necessarily have taken place at point of order. Goods purchased are usually items that the fraudster will sell easily.

## Spyware






Spyware variants MOONSHINE and BADBAZAAR are being used to target mobile devices of individuals around the world. Threat is to members of the Uyghur, Tibetan and Taiwanese communities alongside other civil society groups. Once installed, the apps have been observed variously accessing functions including microphones, cameras, messages, photos, and location data, including real-time tracking, without the user being aware.

# North East Fraud April Summary

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



Total Fraud Reports (compared to April 2024)	<div>↑</div> 696 (+16.2%)
---	------------------------------

TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
	Online Shopping and Auctions	<div>↑</div> 133 (+12.7%)
	Advance Fee Frauds	<div>↑</div> 104 (+112%)
	Other Consumer Fraud	<div>↑</div> 62 (+1.6%)
	Investment Fraud	<div>↑</div> 56 (+19.2%)
	Cheque, Plastic Card and Online Bank Accounts	<div>↓</div> 36 (-16.3%)

## Planning a Wedding?



Over the last few months there has been an increase in the number of reports from victims who have had money stolen when booking their wedding. Although the number of reports linked to venues is low, scammers found online offering services such as cars, videography, photography for large deposits are on the increase.

## Fake Website Ads



We are seeing more fake adverts on social media for well known retailers offering bargains or reduced items. Seasalt Cornwall has issued a warning about fake adverts claiming they are closing stores and offering massive discounts. They are not legitimate and are unrelated to the company.

Phishing emails from fraudsters claiming to be Tesco offering cheap Wagyu beef to loyal customers after completion of a survey have been circulated this month too. One victim reported being signed up for an AI writing tool subscription after entering details and payments for postage.

Victims report similar scams for Costco.

## DWP Winter Fuel Payments



Fake text messages from the DWP reminding residents across the North East to apply for their Winter Fuel Allowance before the deadline have increased their circulation this month as the weather improves. Victims were asked to click on a link to complete the form with personal and bank details. One victim reported having £300 taken from their bank account instead of receiving it.

# North East Fraud April Summary (Continued)

## Identity Theft

A victim in the region has been contacted by her bank about fraudulent activity and asked to provide a picture of herself and driving licence. This was an impersonation fraud likely to steal the victim's identity to open bank accounts or apply for loans.

## HMRC Automated Calls

This month there has been a high number of victims who have received automated calls from the HMRC to alarm the recipient. The message says that they have evaded tax or that there is a warrant out for their arrest or they were to be charged with a crime. The message states to press 1 to speak to an advisor though in one a victim was asked to press 1 to speak to a lawyer or press 2 to pay charges for the case to be dropped.

Half the victims reporting were from ethnic minorities. One victim had over £10,000 stolen.

In two reports, references were made to having the right papers and threats to have the victims VISA or passport cancelled were made.

## Fake Government Grant Offer

Frauds involving applications for fake Government grants are on the rise.

A friend messaged the elderly victim to encourage an application for a Government Grant and to make contact with an agent on Facebook. To release the grant the victim would have to pay 10% of the promised £72,000 using Apple gift cards.

The friend in the initial message had been hacked and luckily the victim did not lose any funds.

A further victim has reported a £200 loss after paying a fee with gift cards after receiving a text from 'Old Help and Grant' to receive £65,000.

## Driving lessons

This month, victims have had over £2.5K stolen after booking driving lessons with instructors found on social media. The social media pages are fake versions of National companies with local franchises. This MO has been used for a while but the number of reports is increasing.

# ENGAGEMENT EVENTS

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



This month the team have been continuing to work with Stage Fright to produce a short film about Romance Fraud that is accessible for people who are neurodivergent.

Northern School of Art hosted a wellbeing event for students where we handed out our 'Student Guide to Fraud' booklets.

Yarm Wellness Centre hosted the Veterans Breakfast and also a pensioners afternoon, members received Fraud awareness advice and referrals for call blockers were made.

Skipton Building Society took part in some Fraud awareness staff CPD and also hosted the team in branch to talk to customers.

Headway Wearside, a support group for those with brain injuries took part in an informal Fraud awareness session and discussed a wide range of scams they had experienced.

Recovery Connections took part in a staff CPD workshop to increase their knowledge of Fraud that targets the North East.



# DRIVING SCAMS

## BEWARE DRIVERS ARE BEING TARGETED!!

People renewing their driving licences or changing details are being targeted. Victims report thinking they are using a legitimate government website that they have googled, only to discover they have paid an inflated price and do not receive their new licence. One victim has reported paying £102.

This is in addition to fake driving lessons that are being advertised on social media for a while.

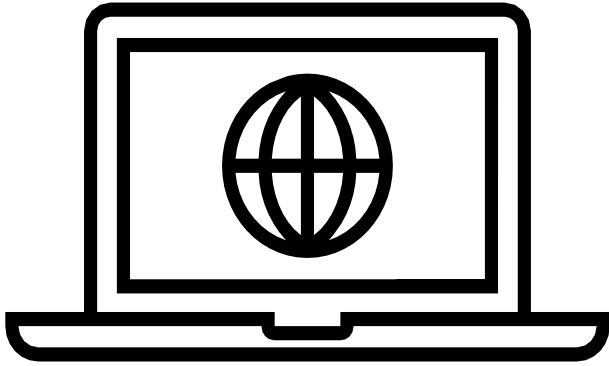
### How to keep yourself safe:

- Always check the web domain is correct when using a website.
- When using google, try not to click on ads to access websites.
- Be wary of lessons that are advertised on social media.
- If in doubt, do not enter personal details or make a payment.



# Horizon Scanning

## Monitoring Threats



The National Cyber Security Centre is investigating a cyber attack that targeted M&S in April. The chain suffered massive disruption to its operations.

This could be an opportunity to exploit consumers due to the confusion and suspension of online orders. There is the potential that other well known high street brands may be targeted.

Some other high street brands have already started to put out messaging in relation to cyber attacks. There is little known about how the cyber attacks have happened or how it affects customers. However, there is the potential they have accessed personal data or information on purchases. It is especially important that if you receive any unsolicited communication to keep in mind it may not be the business contacting you.

Things you can do:

- Update passwords to ensure any used on the platform have not been breached.
- Do not click on any links received from unsolicited emails or texts.
- Do not answer phone calls from unknown numbers.



# WELCOME TO OUR HAPPILY NEVER AFTER

---

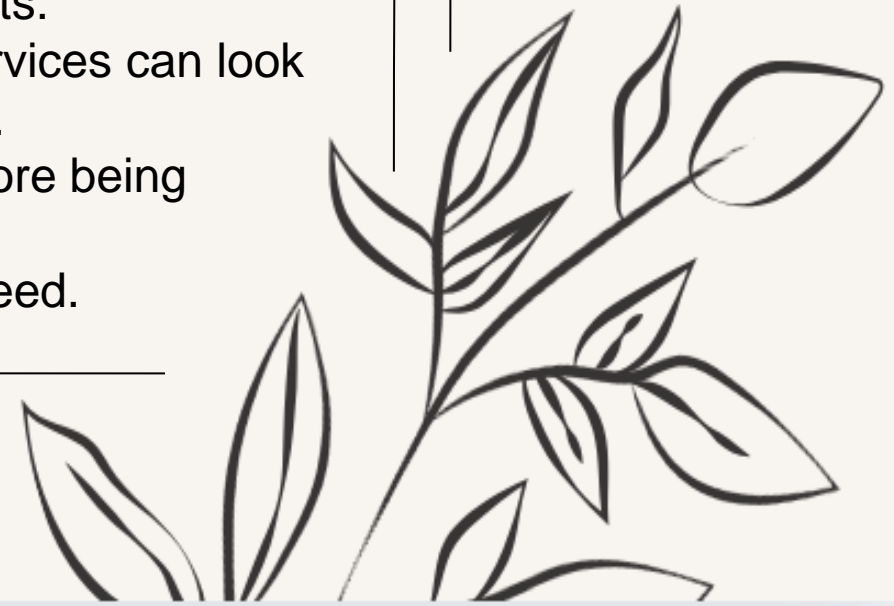
DON'T LET CRIMINALS RUIN  
YOUR BIG DAY!

---

FR  
+  
AUD

**When booking venues and other services,  
ensure that you have checked them out.**

- Consider using locations that have been recommended or check reviews.
  - Consider making payments in person and double check emails to ensure they are from the correct person/company before making any payments.
  - Websites and social media accounts offering to provide wedding services can look professional, try to have a look through previous work.
  - Take the time to make sure you are happy with everything before being pressured in to making a payment.
  - Make a record of all the details and everything that is agreed.
- 





There continues to be an increase in calls and messages (including on social media platforms) offering **fake job opportunities**.

There has been a rise in phone calls with an automated service requesting the victim to add them on WhatsApp to receive a job offer.

There have also been reports of advertisements for jobs making TikTok content or to leave reviews.

Advice:

- Report any unsolicited calls/messages to 7726.
- If you receive a job offer 'out of the blue' it is most likely fake.
- -If it is too good to be true, it probably is!

# WE'RE HIRING

CRIMINAL&CO

## Fraud Victim

- Must answer phone calls to unknown numbers.
- Must accept 'out of the blue' job offers.



There have been reports of fake website adverts on social media.

Be wary of clicking on adverts on social media, a large portion of these are fake adverts that lead to malicious websites.

Always check the website domain before entering any personal or sensitive details.



## OUR SERVICES

BE CAREFUL

WHAT YOU CLICK ON

ON SOCIAL MEDIA

[www.thisisafakewebsite.com](http://www.thisisafakewebsite.com)



## A Man-in-the-Middle

**(MITM) attack** is a type of cyberattack where a malicious actor secretly intercepts and potentially alters the communication between two parties who believe they are directly communicating with each other. This can occur on unsecured or compromised networks, such as public Wi-Fi, where the attacker positions themselves between the victim and the intended destination (like a website or server). The attacker can eavesdrop on sensitive data such as login credentials, financial information, or private messages—and in some cases, modify the data in transit without either party being aware. MITM attacks exploit weak encryption, lack of authentication, or user negligence, making them a serious threat to both personal and organisational cybersecurity.



## MITM Protection Checklist



### Network & Encryption

- Use **HTTPS** for all web communications
- Implement **SSL/TLS certificates** correctly and keep them updated
- Use **DNSSEC** to protect DNS queries from spoofing
- Require **VPN use** on public or untrusted networks
- Enable **end-to-end encryption** for emails, messaging, and file sharing
- Implement **certificate pinning** for critical web and mobile applications



### User Awareness

- Train users to avoid public Wi-Fi for sensitive work
- Educate staff to **never ignore SSL/TLS browser warnings**
- Provide **phishing awareness training**
- Encourage use of secure, trusted apps and extensions only



### Authentication & Access Control

- Enforce **multi-factor authentication (MFA)** wherever possible
- Avoid password-only authentication for critical systems
- Regularly update and enforce **strong password policies**



### System & Device Security

- Keep **software, operating systems, and browsers** updated
- Update router firmware and change **default admin credentials**
- Use **WPA2/WPA3 encryption** on wireless networks
- Disable **WPS (Wi-Fi Protected Setup)** on routers



### Monitoring & Protection Tools

- Deploy **Intrusion Detection/Prevention Systems (IDS/IPS)**
- Monitor network traffic for unusual patterns or unauthorized access
- Enforce email security standards (**SPF, DKIM, DMARC**)

# What's Happening Next?



With Summer around the corner social events will naturally start to increase. As a result those who wish to attend concerts, music festivals and other events and have missed out on ticket sales will look to purchase them from ticket resale sites or often use social media.

The total stolen in the North East due to Ticket Fraud in 2024 was:

**£154,981**

## What should you do?

- Buy tickets from reputable sellers, try to avoid buying from random people on social media.
- Use a credit card where possible for better protection under Section 75.
- Try to use the box office site, official website or reputable ticket seller when purchasing tickets.
- Avoid paying directly into someone's bank account.

You should report to Action Fraud online or by calling 0300 123 2040 or online at [actionfraud.police.uk](https://actionfraud.police.uk)





# Cyber HIT Session

- **Cyber HIT Session- Support and guidance for sole traders**
- Welcome to our online event where we will provide **support and guidance** specifically tailored for **sole traders**. Join us for a **Cyber Security HIT Session** where you will learn valuable tips and tricks to protect your business from cyber threats. Our experts will cover topics such as cybersecurity best practices, data protection, and how to stay safe online while running a small business. Don't miss out on this opportunity to enhance your knowledge and safeguard your business in the digital world!

A link to the event will be sent closer to the time.

For more information on the work we do, please visit our website at [www.nerccu.police.uk](http://www.nerccu.police.uk)

[Cyber HIT Session- Support and guidance for sole traders Tickets, Multiple Dates | Eventbrite](#)

- **Dates & Times:**
- 02/06- 14:30-15:00
- 04/06- 10:00-10:30
- 05/06- 18:00-18:30
- 11/06- 13:00-13:30
- 16/06- 12:00-12:30
- 17/06- 18:30-19:00







 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 2025 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 it's 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 Nicola Lord –Cyber Threat Desk Analyst</b>
<b>Reviewed By</b>	<b>SGT Emma O'Connor</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.