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 2025 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

Contents

Looking Forward

North East Cyber Crime October Summary

INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Cyber Reports (compared to October 2024)	**227 (+40.1%)**
Hacking -Social Media and Email	**179 (+55.7%)**
Hacking - Personal	**27 (+58.8%)**
Computer Virus/ Malware	**11 (-56%)**
Hacking - Extortion	**9 (+80%)**
Hacking - Server	**1 (+100%)**

Argos Account Hacking

The 28th - 30th October saw a spike in Argos hackings with 8 reports across the region. Victims reported that orders had been made from their account with the majority receiving an email stating their order would be ready to collect. Two of the reported incidents confirmed that orders had been collected. The collection points and orders were out of the North- East region with the Argos stores located in Thames Valley, The Midlands, London and Herefordshire.

Sextortion Emails

There has been several reports of victims receiving sextortion emails this quarter often initiated by an email account hack and a bribe demanding a Bitcoin payment. These sextortion emails were generated from the victim's own email account and included the victim's username and password indicating the scammer has successfully hacked the victim's account. Further advice on what to do if you receive a threatening email can be found on page 13.

WhatsApp verification code scam

This month has seen WhatsApp verification code scams in the region. Victims reported that they had received a meeting invite that appeared genuine due to the name and WhatsApp profile image. To access the meeting, the victim was instructed to provide a code that was sent to their phone. Once the victim shared this, they lost access to their WhatsApp account.
The scam entails a fraudster who has already obtained the victims number. They then enter it into the WhatsApp login page to trigger a genuine message from WhatsApp obtaining a verification code. The victim will receive this genuine message and a WhatsApp message from the scammer impersonating one of their contacts or an organisation and will try to persuade the victim to share the code they have just received. Once obtained the scammer can takeover the account and access the victims contacts. Often the scammer will message the contacts asking for money.

North East Fraud October Summary

£4.8 Million loss this month (+10%)

INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

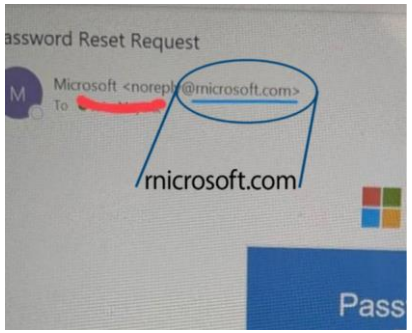
Total Fraud Reports (compared to October 2024)	**806 (+7.3%)**
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Advance Fee Frauds	**172 (+97.7%)**
Online Shopping and Auctions	**141 (-8.4%)**
Other Consumer Fraud	**86 (+17.8%)**
Investment Fraud	**54 (+5.9%)**
Cheque, Plastic Card and Online Bank Accounts	**41 (+2.5%)**

Black Friday Deals

The official date for Black Friday this year is Friday 28th November. Over recent years, sales had moved to cover the whole weekend including 'Cyber Monday' but this year some retailers have advertised deals starting as early as the beginning of November. The number of reports for "Online Shopping" Frauds tends to increase around this time in line with the increase in online spending. Fraudsters will use fake social media adverts, phishing emails and spoofed retailer websites to lure potential victims.

The average shopper expects to spend £299 on Black Friday itself, up £83 from 2024. Cyber Monday spending is also set to rise, reaching £229 on average, an increase of £70 on last year.

In October, victims in the North East reported ordering goods from the Sports Direct website, later to find the site was a spoof and money taken from their account. The copycat website impersonated Sports Direct's site and advertised heavily discounted items. With accurate branding, the site appeared genuine and harvested personal and payment information at the point of purchase.



Phishing Microsoft Messages

We wish to highlight a fake email seemingly from Microsoft asking the recipient to click on a link to reset their password. This image shows how scammers are going to greater lengths to hide their identity. In this example the letters **r** and **n** placed next to each other appear as the '**m**' in Microsoft. As more users access their emails from their mobile phones with a smaller screen, details like this are not as visible.

North East October Trends (cont'd)

Energy Hacking

A victim has reported that their Octopus energy account was hacked and their credit was transferred out. The victim was logged out of their account and a refund request was submitted with new bank details added to the account. This type of hacking is not commonly reported however; it could become a more common MO over the winter months due to individuals accruing credit over the year to cover higher winter fuel costs.

Sim Swap

Sim swapping has increased across the region, specifically in relation to E-sims. Once the suspect gains control of the victim's telephone number they can bypass two factor authentication requiring a phone verification code sign in to access other apps and accounts. Victims have reported numerous fraudulent payments made after the sim transfer including purchases and finance taken out in their name.

Life Insurance Scams

Over the last few months, North East victims have reported receiving phone calls from Fraudsters claiming to be from their Life Insurance company. The victims report the callers knew their basic personal information.

Pressure was applied by the caller stating their life insurance policies were about to run out and the victims would lose money. This was likely a ruse to obtain banking information or to encourage the victim to click on a link they would send as part of the new policy process.

Legal & General have just published the following article on how to identify and keep safe from scammers - Life insurance scams | Legal & General

ENGAGEMENT EVENTS

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

KLEEK hairdressing apprenticeships had 6 sessions of Fraud and Cyber Awareness workshops with Northumbria and Durham Police Cyber Crime Teams getting involved. Lots of fun was had during the cyber escape room.

Darlington Rotary Club, SEARCH Newcastle, GenToo Washington invited us to deliver a Fraud Awareness session.

HSBC and Skipton Building Society have hosted staff Fraud awareness sessions in branch with a stall for customers to come and speak all things Fraud afterwards.

Teesside University, Durham University, Sunderland University and Northumbria University all hosted us to provide information and advice stalls for student and staff who all received our ‘student guide to Fraud’ booklet.

Systems running Windows 10 without security updates will continue to function but will be increasingly vulnerable to cyber threats such as malware and viruses. Meanwhile, companies and organisations may find that unsupported software does not meet regulatory compliances.

Concerningly, a report by Which? has found that an estimated 21 million people in the UK are still using Windows 10 and around a quarter of those surveyed said they will continue to use this operating system (OS) even without security updates. Where computers are compatible, they can be upgraded to Windows 11 for free. However, older systems may not be able to do this.

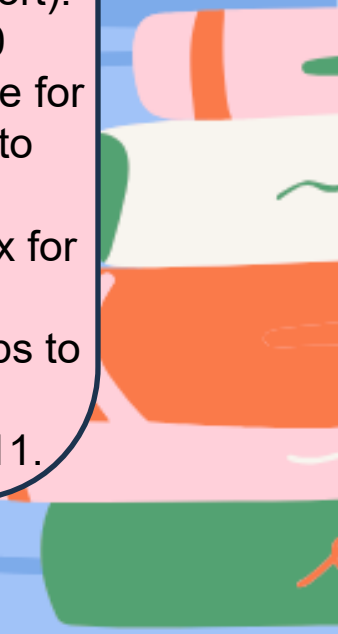
AFTER 14TH OCTOBER 2025, MICROSOFT WILL NO LONGER AUTOMATICALLY PROVIDE UPDATES, SECURITY FIXES OR TECHNICAL ASSISTANCE FOR WINDOWS 10.

Millions of PCs at risk

Which? recommend the following alternatives:

•Opting in for the one-year Extended Security Updates (ESU) programme. This will provide an extra year of security updates for Windows 10 (but no other updates and no technical support). Users can either pay a fee, redeem 1000 Microsoft reward points or join the programme for free if they agree to back up their settings to OneDrive.

- Switching to a free OS like ChromeOS Flex for laptops or Linux.
- Upgrading outdated components on laptops to make them Windows 11 compliant.
- Buying a new computer with Windows 11.



Find out more:
www.gov.uk/stopthinkfraud

SHOP ONLINE SECURELY THIS FESTIVE SEASON

ADD TO CART

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

STOP! THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

Festive Shopping Tips

Always use a credit card for large purchases over £100, they offer more protection through section 75 of the consumer credit act.

Check you are using genuine website domain addresses when shopping online.
If you are using Facebook Marketplace, try to see the item in person.
Check reviews of websites before purchasing.

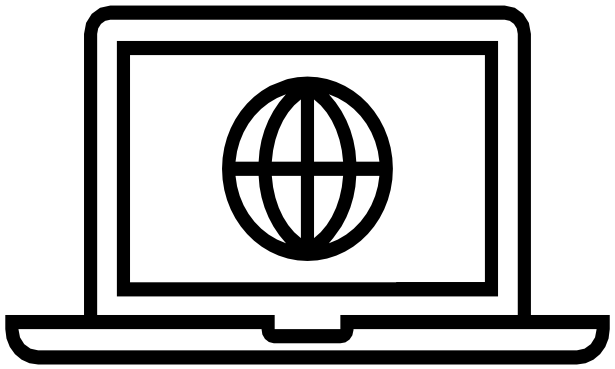
REMEMBER!!!

If it seems too good to be true, it probably is.

Be wary when looking for deals, especially on social media.

Horizon Scanning

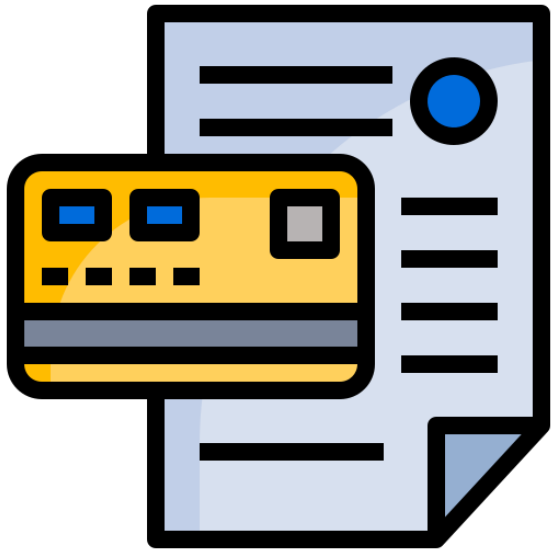
Monitoring Threats



Check your bank statements!
Beware, people have noticed a payment on their bank statements to ‘Argos’ that they have not made. When victims have contacted their bank they have found a recurring payment has been set up on their account to pay this amount regularly.

What can you do:

- Regularly check bank statements.
- Try to identify any unknown payments, even small amounts.
- Payments could show as legitimate companies.



What is a Money Mule?

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.

As usual we are running our Fraud Roadshow along with other events throughout November to raise awareness amongst students who are often targeted by this.

14 YEAR PRISON SENTENCE

KNOW THE SIGNS :

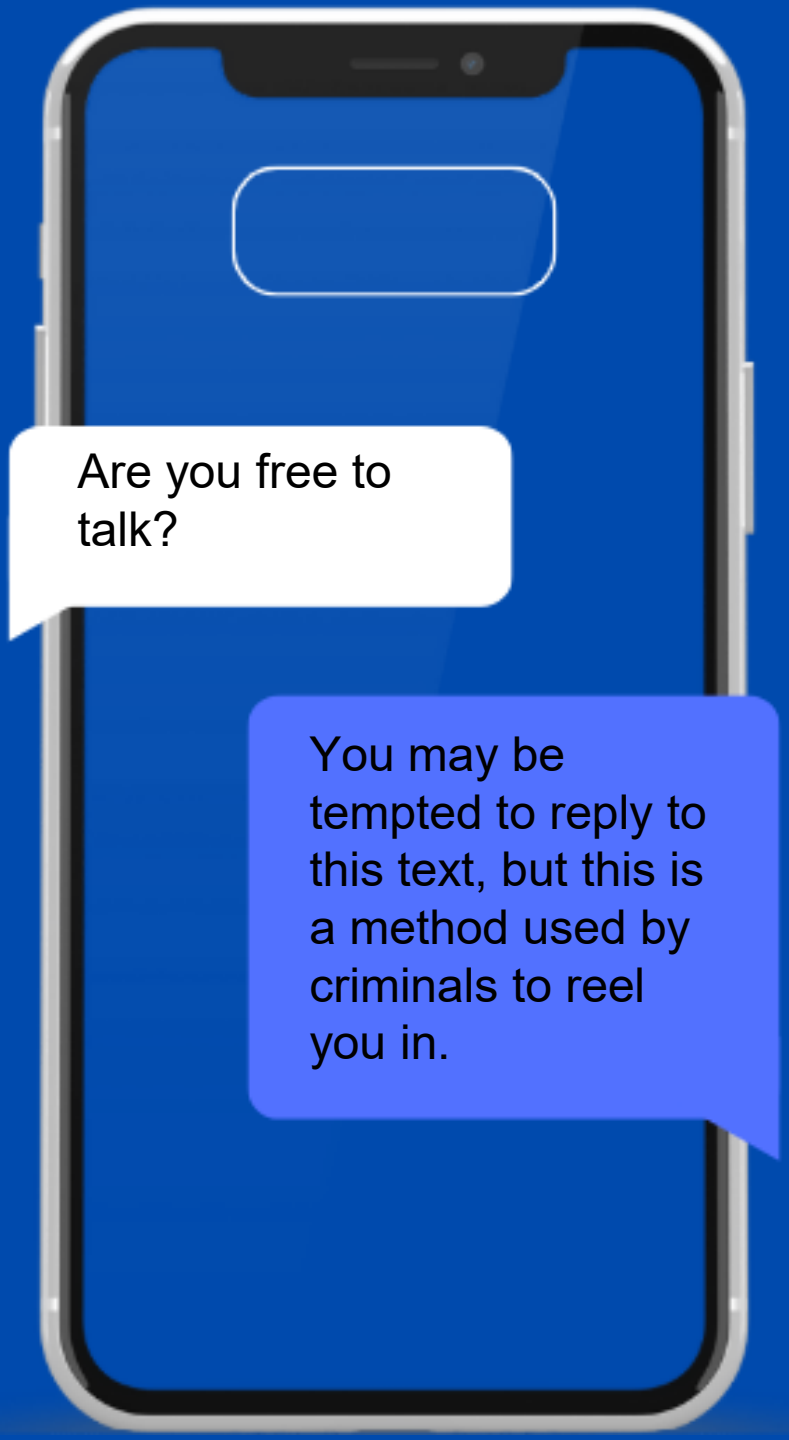
- Job offers using social media or even job websites offering ‘quick cash’ or ‘easy money’.
- Someone requesting to use your bank account/transfer money.
- Someone you do not know asking for your bank details.

Have you received a text like this?

This is a method criminals use to try and get victims to engage with them. It is natural to be curious as to who it is texting and find out what they want. Criminals are using this to their advantage.

Do not reply and report the text by forwarding it to 7726. If you do respond they will see your number as an active phone number with someone who is willing to respond to unknown numbers.

Watch out for texts asking if you are busy, open-ended questions or anything trying to get a response from unknown numbers that you don't have saved.



National Cyber Security Centre

Sextortion phishing scams
How to protect yourself

This guidance explains what to do if you've received an email that's trying to blackmail you. The email may state that your login details have been compromised, or may threaten to reveal some compromising information (such as a video of you visiting an adult site). You can protect yourself by following the steps below.

What is a sextortion scam?

A **sextortion scam** is when a criminal attempts to **blackmail** someone, usually by email. The criminal will claim they have login details or a video of the victim visiting an **adult website**, and will threaten to disclose this unless the victim pays a **ransom** (often in Bitcoin).

The criminals behind these attacks do **not** know if you have a webcam, or know if you've visited adult websites. They are attempting to **scare their victims** into paying a ransom, and will send millions of emails in the hope that someone will pay. They'll often include technical sounding details to make the email sound convincing. It may also include a password the victim uses or has used.

Sextortion is an example of a **phishing attack**, where victims receive emails that try and **trick them** into doing the wrong thing.

What to do if you've received a threatening email

Don't communicate with the criminal

As with other phishing attacks, our advice is to **not** engage with the criminal. If you have received an email which you're not sure about, forward it to the NCSC's Suspicious Email Reporting Service (SERS): report@phishing.gov.uk, and then delete it.

Should I pay the ransom?

If you are tempted to pay the ransom, you might be targeted with future scams, as the criminal will know they have a 'willing' customer.

Check if your accounts have been compromised

Do not worry if your password is mentioned. It has probably been discovered from a previous data breach. You can check by visiting https://haveibeenpwned.com/

www.ncsc.gov.uk
@NCSC
National Cyber Security Centre
@cyberhq

Change any passwords that are mentioned

If a password you still use is included, then change it immediately. For advice on how to create good passwords, please visit www.cyberaware.gov.uk .

If you've already paid the ransom....

If you have already paid the ransom, then visit Action Fraud for further advice (www.actionfraud.police.uk).

CYBER CRIMINALS ARE TARGETING CALENDARS

If you receive an email with an invite or a Microsoft 365 document, even if it looks like it is legitimate and comes from a trusted source, please be wary. The email may contain a link that takes you to a website to enter your personal or financial information. It may even ask you to log in to your email account to steal your credentials.

Watch out for unsolicited emails with calendar invite or shared Microsoft 365 documents, criminals are using this method to target people.

How to protect yourself from 'Calendar Phishing'

- If you receive an invite or something is added to your calendar, be wary of clicking on it or any links. It may take you to a website that asks for personal details.
- Change your calendar settings to not allow meetings to be automatically added.
- Make sure 2 Step Verification is enabled.
- Keep your software updates as it may contain patches that fix any issues.

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.

Black Friday, Cyber Monday and Christmas are approaching with people spending more than any other time of year online.

Always check the URL addresses of the websites you are using, 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.

What can we do for you?

If you think any groups that you attend or run could benefit from the services we offer, please get in touch at reccc@durham.police.uk

- Advice Stalls and Events
- A link between yourselves and NEROCU
- Monthly Newsletter
- Staff CPD/Inputs/ Workshops

North East RECCC
Regional Economic Crime Coordination Centre

North East ROCU
Regional Organised Crime Unit Network

For more information search 'nerccu police'

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.

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.

Emails

Forward Fraudulent emails to
report@phishing.gov.uk

Phone Numbers

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

Handling Instructions

Distribution List
NEROCU
North East Police Forces

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** **Nicola Lord –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.