

North East

ROCU

Regional Organised Crime Unit Network

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 September 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 September Summary

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



Total Cyber Reports (compared to September 2023)		173 (+110%)
Hacking -Social Media and Email		131 (+107%)
Hacking - Personal		14 (+133%)
Computer Virus/ Malware		18 (+500%)
Hacking Extortion		9 (+29%)

The increase in the number of reports for Cyber categories for September has largely been due to the Parking Fine Phishing scam.

Further information can be found on Page 15

Hacking – Social Media and Email



Hacking – Social Media and Email reports account for 75% of all the Cyber reports to Action Fraud in September 2024. One business has reported having their email account hacked through a phishing scam. The suspect sent invoices with their bank details on to customers from the compromised account.

Advice page 17

Hacking Extortion




Hacking Extortion reports have increased by 29% in comparison to September 2023. Age category 18-30 account for 77% of the reports, and within that category 66% reported the Extortion was by Email. One victim reported receiving an email, stating they have videos of the victim, and they have 48hours to send payment before the videos are sent to the victims' contact list. Another victim reported they had received an iMessage with two photos of themselves naked along with personal information from their SnapChat account, if they did not pay the money requested the images would be uploaded online.

Advice page 10











North East Fraud September Summary

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



**Total Fraud Reports
(compared to August 2023)**  **637 (-19.8%)**

TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:

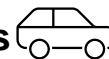
 Online Shopping and Auctions	125 (-37.5%) 
 Advance Fee Frauds	75 (-27%) 
 Other Consumer Fraud	54 (-15%) 
 Cheque, Plastic Card and Online Bank Accounts	39 (-15%) 
 Investment Fraud	39 (-43%) 

Ticket Scams



Ticket fraud reporting numbers have tripled this month with consumers trying to buy tickets for Oasis and Coldplay concerts.

Parking Fine Scam Messages



There are reports of a scam text message being circulated around the country claiming the recipient has an outstanding parking fine or PCN which needs paying urgently. There is a link in the message to enter personal details onto a highly authentic spoofed government website. 17 reports have been made to Action Fraud so far this month.



ADVICE PAGE 12

Winter Living Expenses Scam texts



A phishing text message about a UK government living expenses subsidy is being circulated. The scam message asks the recipients if they are eligible to click on a link to update personal information to apply as soon as possible otherwise funds will be allocated to other citizens in need.

Additionally, victims are reporting scam calls from utilities companies offering great deals



ADVICE PAGE 16

Commission based job scams



This month, victims in the North East have lost £45000 through scam recruitment companies. Recruits are given tasks (usually cryptocurrency based) to complete with time scales and pay money in to boost their income.



ADVICE PAGE 13

ENGAGEMENT EVENTS

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

Barclay's Washington, Durham and Fawcett Street hosted two events for online safety week which we attended and helped members of the public to check their passwords and discussed Fraud protection advice.

Staff at Middlesbrough College have taken part in an input around Fraud awareness and to increase awareness of money muling. Sunderland College and Durham University invited us to their freshers event where we also talked about money muling and we spoke at Durham University international student event and to Hartlepool FE College policing students.

An online awareness session was delivered to Sunderland Council digital inclusion team.

Fraud Awareness workshops delivered to Optimum Skills apprentices at Gateshead and ProBus which is a group for retired business owners.



Criminals **steal private photos** from hacked accounts and use them to **extort victims**

Passwords

Email and social media account passwords should be **strong and different from all your other passwords.**



2-Step Verification

Enable 2-step verification (2SV), it will keep criminals out of your account even if your password is stolen.

For more information, visit: www.gov.uk/stophinkfraud





  **Join Us for Cyber Security Awareness Month!**  

This October, we're thrilled to team up with **Durham Constabulary** and **Cleveland Police** for an enlightening series of webinars designed to boost your cyber security knowledge and keep you safe online.  

◆ **What's on the Agenda?**

- **Personal Cyber Hygiene:** Tips and tricks to protect your smartphones, tablets, and computers.
 - **07/10/2024 13:00-14:00**
 - **23/10/2024 13:00-14:00**
 - **30/10/2024 10:30-11:30**
- **NCSC Small Business Guide:** Essential advice for safeguarding your business against cyber criminals.
 - **02/10/2024 10:30-11:30**
 - **16/10/2024 13:00-14:00**
 - **31/10/2021 10:00-11:00**

 **Why Attend?** In our increasingly digital world, securing your personal and business devices is more critical than ever. With cyber threats evolving rapidly, staying informed is your first line of defence. Our webinars will equip you with practical strategies and insights to defend against potential attacks and secure your digital life.

 **Don't Miss Out!** Register now and be proactive about your cyber security. Let's make this October the month you take charge of your online safety!



Unpaid Penalty Charge Notice (PCN)?

If you have received a text message containing a link claiming you have an unpaid parking fine, do not click the link. The link will take you to a fake government website and ask for payment details.

How to protect yourself :

Do not use any of the contact details provided in the text as they could be fake.

Do not enter any personal details.

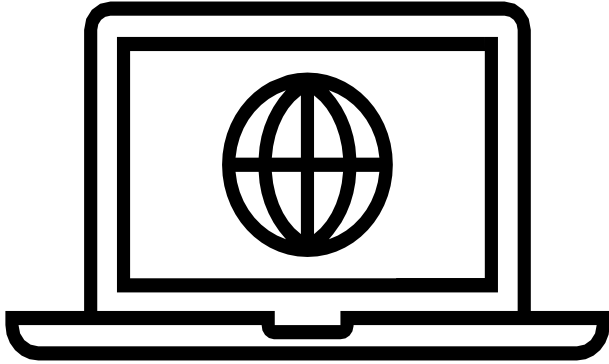
PCNs usually arrive through the post so it is likely that any requests for payments via other methods are a scam.

Always check the web address.



Horizon Scanning

Monitoring Threats



There has been an increase in the region of Employment Fraud. It has been seen that those in their 30s and 40s are being targeted by jobs advertised on WhatsApp. Victims think they are doing an online job boosting website exposure or handling cryptocurrency, however this could be a tactic to recruit money mules.



- If you are offered a 'job' that claims you can make quick or easy cash, it is likely this is Employment Fraud and could potentially lead to becoming a money mule which carries a maximum sentence of 15 years imprisonment.
- Do not let anyone transfer money through your bank account.
- Be wary of any messages received on social media platforms offering you cash in return for performing a 'job'.



Authorised Push Payment Fraud Reimbursement

Authorised push payment fraud happens when you are tricked by a criminal into sending money by bank payment to an account that they control and which you do not.

Find out more about the rules on how banks and other payment service providers reimburse victims of authorised push payment fraud, and how to protect yourself.

Visit www.takefive-stopfraud.org.uk/app-guide





i Whether it's your email, a social media account, or your online banking, losing access to a digital account can be stressful.

Check out this useful step by step guide on how to recover a hacked account:
<https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account>

#TurnOn2SV

How to tell if you've been hacked

Check your online accounts to see if there's been any unauthorised activity. Things to look out for include:

- being unable to log into your accounts
- changes to your security settings
- messages or notifications sent from your account that you don't recognise
- logins or attempted logins from strange locations or at unusual times
- unauthorised money transfers or purchases from your online accounts

In some cases, it may not be possible to recover your account with the online service. In such cases, you'll have to create a new account. Once you've done this, it's important give you your contacts your new details, and tell them you've abandoned the old account. Make sure to update any bank, utility or shopping websites with your new details.

© Crown Copyright 2022

1. Contact your account provider

Go to the account provider's website and search their help/support pages which will explain the account recovery process in detail. It's likely to be different for each account.

2. Check your email account

Check there are no unwanted forwarding rules in your email account. Cyber criminals may can set up rules which means they'll automatically receive copies of all emails sent to your account (which would allow them to reset your passwords).

3. Change your passwords

Change the password for any account that has been hacked, and also for any accounts that use the same password. Cyber criminals know that people use the same password for different accounts, and so will try the same 'hacked' password across multiple accounts.

4. Force all devices and apps to log out

This can usually be done from the 'Settings' menus of the app or website (or it may be part of the 'Privacy' or 'Account' options). Once you've done this, anyone attempting to use your account will be prompted to supply the new password.

5. Set up 2-step verification (2SV)

2SV (which is also known as two-factor authentication or 2FA) usually works by sending you a PIN or code, often via SMS or email, which you'll then have to enter to prove that it's really you. So even if a criminal knows your password, they won't be able to access your accounts.

6. Update your devices

Apply updates to your apps and your device's software as soon as they are available. Updates include protection from viruses. Applying these updates promptly is one of the most important (and quickest) things you can do to prevent your account from being hacked.

7. Notify your contacts

Contact your account contacts, friends or followers. Let them know that you were hacked, and suggest they treat any recent messages sent from your account with suspicion. This will help them to avoid being hacked themselves.

8. Check your bank statements and online shopping accounts

Keep a look-out for unauthorised purchases. Check your bank accounts for any unusual transactions. You can contact your bank directly for further support. Always use official websites or social media channels, or type the address directly into your browser. Don't use the links in any messages you have been sent.

9. Contact Action Fraud

If you've lost money, tell your bank and report it as a crime to Action Fraud, the UK's reporting centre for cyber crime (in Scotland, contact the police by dialling 101). You'll be helping the NCSC and law enforcement to reduce criminal activity.

Cost Of Living Fraud On The Rise

What has been seen so far? :

As winter fuel payments have been withdrawn and energy bills are again, beginning to rise. We are seeing an increase in cost-of-living type Frauds, where criminals are looking to exploit those in need of financial support. So far there have been unsolicited texts with links requesting personal details to receive a £900 cost of living payment with more expected to be seen within the coming months.

What can you do to protect yourself? :

- Do not click any links within texts or emails and try to use the legitimate website address.
- Always check it out first and do not enter any personal details.
- If in doubt, ignore it!
- If you do require financial help, contact your energy company to see what support they can offer.
- Be wary of anyone contacting you via text, phone call or email claiming to be from Ofgem or an energy company.

⚠ Using the same password for multiple accounts? That means criminals only need to steal one of your passwords to hack into multiple accounts.

✅ Email and social media account passwords should be strong and different from all your other passwords.

For more info on how to secure your accounts, visit:

<https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/>

#TurnOn2SV

Do your email and social media accounts have the **same password?**

Passwords

Email and social media account passwords should be **strong and different from all your other passwords.**

2-Step Verification

Enable **2-step verification (2SV)**, it will keep criminals out of your account even if your password is stolen.

For more information, visit: www.gov.uk/stopthinkfraud



What's Happening Next?



Online Shopping Fraud remains the highest reported Fraud in the North East which means the region should be extra vigilant in the run up to Christmas which are the busiest months for people spending money online.

Christmas is approaching and people will be on the lookout for bargains. There are upcoming shopping events such as Black Friday and Cyber Monday where people will be increasing their spending putting more people at risk of becoming a victim of Fraud as they seek the latest deals. With discounts being offered across lots of websites during this time it makes those 'too good to be true' deals look more believable.

Advice :

- Use a credit card where possible (especially for large purchases) as they provide more protection under Section 75 of the Consumer Credit Act.
- Read reviews of the website you are purchasing from, be wary of new websites that have only been online for a short time.
- Always type the web address into your browser and be wary of accessing links through unsolicited emails.
- If you're asked to make a bank transfer instead of using a secure payment system.





Authorised Push Payment Fraud Reimbursement

What to do if you think you've been scammed



Contact your bank immediately if you have lost money in an authorised push payment fraud. Delays can cause problems when trying to recover your funds.



You must report the fraud no more than 13 months after the last fraudulent payment was made.



The maximum amount of money you can claim is £85,000.



Your bank may ask you for information to help with your claim, including messages or screenshots. You should consent to them sharing this information with other banks where necessary.




You should co-operate fully with your bank when it comes to involving the police.

To learn more, visit
www.takefive-stopfraud.org.uk/app-guide





 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– Economic Threat Desk 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.