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 January 2026 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 January Summary

Android App 'TrustBastion' is a malware campaign disguised as a security app to steal sensitive data.

The malware can evade detection while capturing PINS, passwords and overlaying fake login screens on legitimate apps and tracks almost every action taken on a smartphone.
Victims of the attack are presented with advertisements or pop ups claiming that their smartphone is infected and the user is prompted to install the app to remove the alleged threats.
Immediately after installation, TrustBastion displays a supposedly necessary update. The window is visually similar to official Android or Google Play dialogs, and anyone who agrees to the update ends up downloading a manipulated APK file in the background.
Here is how to stay ahead of threats like TrustBastion:

- Stick to official app stores: Only download apps from Google Play or the Samsung Galaxy Store. These platforms have scanning and moderation that catch many malicious apps before they reach users.
- Scrutinize app details: Check reviews, download counts, and developer credentials before installing anything. Fake security apps often have sparse or suspicious feedback.
- Be wary of urgent pop-ups: Legitimate software rarely demands immediate updates or warns of infections with scare tactics. If it feels pushy or invasive, pause and verify.
- Enable built-in protections: Android devices include Google Play Protect, which can identify and block known malicious behavior even outside the Play Store. Keep it enabled and combine it with cautious habits.

Olympics 2026 merchandise scams

There has been a surge in fraudulent online stores imitating the official Milano Cortina 2026 Olympics merchandise shop. The fake online websites replicate the official storefront using identical layouts, promotional videos, branding and background music.

The criminals behind these fake websites look to steal payment information, harvest personal data, send secondary phishing emails and deploy malware without delivering the advertised items.

Consumers should only purchase goods through verified websites and treat unexpected discounts or unfamiliar domains, especially those selling sold out merchandise, as high-risk indicators of malicious activity.

Online Gaming Account Hacking

With approximately 1.2bn global online gaming users and an estimated global online gaming market of 29.5bn USD online gaming platforms and accounts provide opportunity for cyber criminals as these accounts hold personal data and money that can be used by cyber criminals. The National Cyber Security Centre provides the following advice to help safeguard you and your personal data when gaming.

1. Secure your device- keep operating systems and other software up to date.
2. Account Protection- Use 2 step verification and a strong password.
3. Protect your privacy- Apply privacy settings to ensure personal data isn't visible and do not give out personal information to other players 'in game'.
4. Use official source or stores- Whatever device you are using to play games, you should always attempt to verify the source of anything you install.

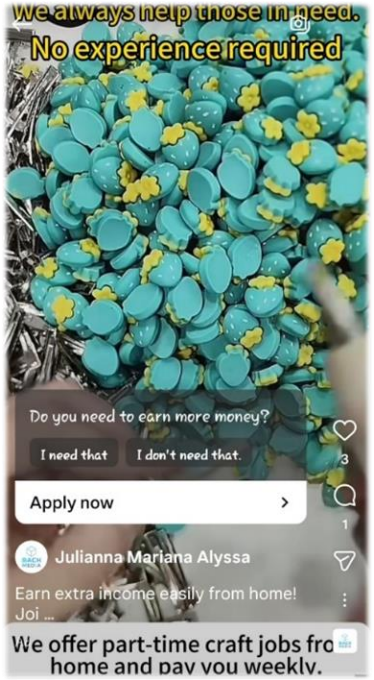
You can visit:
https://www.ncsc.gov.uk/guidance/online-gaming-for-families-and-individuals
For more online gaming advice and support.

North East Fraud November Summary

Scam part-time crafts at home jobs

Usually advertised on social media, the number of craft assembly part time jobs offered with home working is increasing. These job opportunities are often scams designed to steal money or personal information, with very few, if any, legitimate assembly jobs existing in this form. These scams, often called "craft assembly" or "work-from-home assembly" scams, often require you to pay upfront for materials, training, or certification, after which the company will reject your work and refuse to pay you.

Scammers are prevalent in Facebook craft and hobby groups and people should remain vigilant.



Gold Bullion Courier Fraud

Your bank and the police will never ask you to buy bars of gold or jewellery to assist with an investigation.

In other areas in the UK, victims of Courier Fraud have been told to purchase gold bullion bars online or expensive jewellery to assist with investigations into Fraud on their bank accounts. Couriers are then sent to their address to collect the gold. Similar crimes are now being reported in the North East.

Vinted Scams

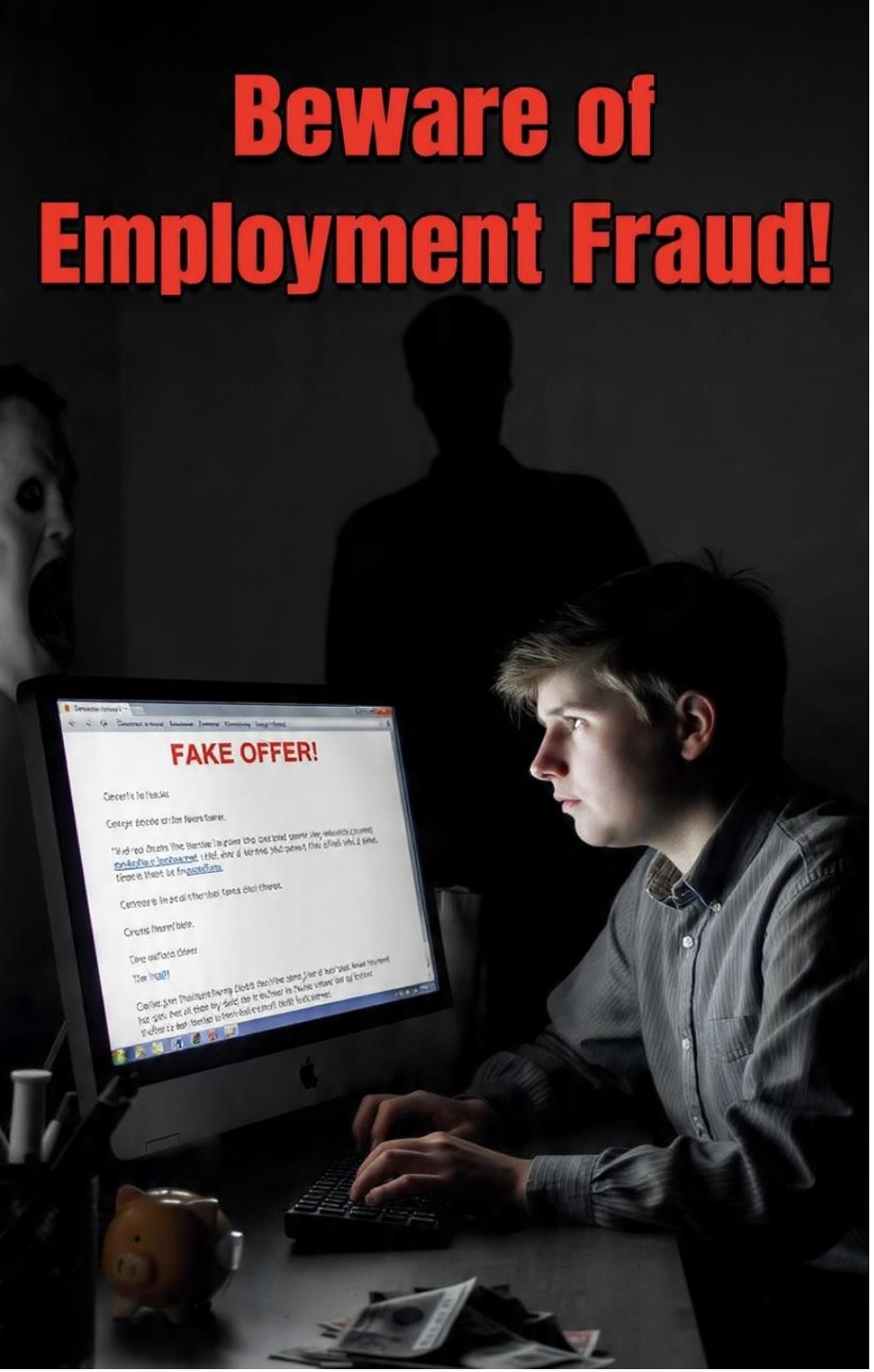
A new trend is emerging targeting sellers on Vinted. It is believed that this is to harvest personal and banking information.

Reports from victims state that after they sold an item and the buyer confirmed they were happy, they were contacted again saying there was a fault, and they wished to make a return. The fraudster messaged the victim asking to communicate outside of Vinted and requested information such as the victims address and banking information.

Bogus Tradesperson Following Bad Weather

This year, with the incessant wet weather we have had across the North East, homeowners are reminded to be vigilant when looking for a tradesperson to make repairs for any water damage to their property. Scammers, sadly, take advantage of storms and bad weather to target potential victims under the guise of cheap and speedy repairs.

Never pay cash upfront, demand at least three written quotes, and use recommended, accredited contractors. Verify their identity, insurance, and references, and ignore high-pressure tactics for "urgent" work.



Red Flags can include;

Job offers with no interview

Being asked to pay fees upfront for training, equipment or visas

Pressure to act quickly or keep it a secret

Told to move money through your personal bank account

Contact from unofficial or free email addresses (Gmail, Outlook etc)

Poor spelling/grammar in official communications

Common Types of Job or Employment Fraud;

Advance Fee Fraud (told to make a payment of some kind before starting work)

Money Mule Recruitment (being recruited – usually online – to move money through your bank account)

Fake work-from-Home or Parcel Forwarding Jobs

Impersonation of Real Companies

Protect yourself;

Check the company on Companies house

Never pay to secure a job

Don’t share bank or passport details without verification

Check job listings on official company websites

Contact your bank immediately if you’ve shared payment details

Red Flags can include;

- Asked to pay a bill, fine, tax or debt with gift cards
- Told to buy gift cards urgently and share the codes on the back
- Caller claims to be from HM Revenue & Customs, a bank, police or utility company
- Pressure to stay on the phone while purchasing the gift cards

Common Types of Gift Card Fraud;

- Fake tax or National Insurance problems
- “Missed delivery” or utility disconnection threats
- Romance / online relationship fraud, whereby they ask you to buy gift cards on their behalf
- An Email from within work, from a supervisor, asking you to purchase the gift cards on their or the company’s behalf

Protect yourself;

- Genuine organisations do not request payment via gift cards
- Never share gift card codes with someone you don’t know
- Stop contact and take the time to verify who you’re talking to using official contact details
- Contact your bank immediately if you’ve shared payment details

Refund Diversion Fraud!

Vinted

Red Flags for online sellers!

- Buyer pressurises for quick refunds.
- Buyer requests refund to different payment method than original
- Excuses made, such as, “I can’t access my old account” or “my card has stopped working”
- Buyer is new or has a limited history/reviews on the platform

How to protect yourself!

- Always refund via the platform in use – do not send money outside of the platform
- Avoid refunds to different accounts
- Document all messages, photos, receipts, etc
- Report suspicious activity to the platform and to Report Fraud
- Contact your bank immediately if you’ve shared your bank details

Courier Fraud!

How it works;

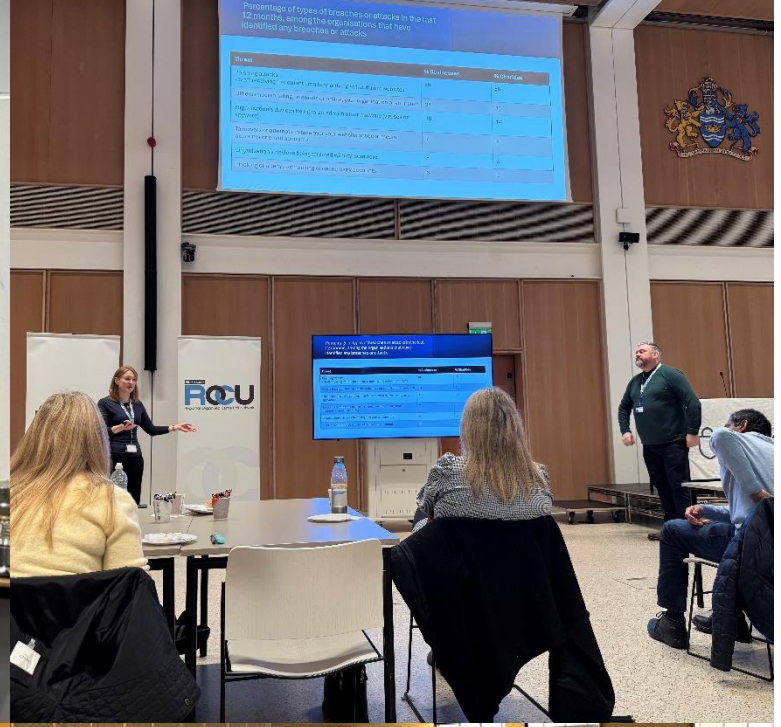
- The victim receives a phone call, email or text claiming to be from the police, bank fraud team, or government department.
- They claim the victim is in danger of losing money if they don't act immediately.
- The Fraudster tells the victim to get their cash out of the bank so that a 'courier' can come collect it and make it safe or tells them to transfer it to another account which they provide the details.
- The victim then awaits details of a 'new account' which never arrives and finds their money has been stolen.

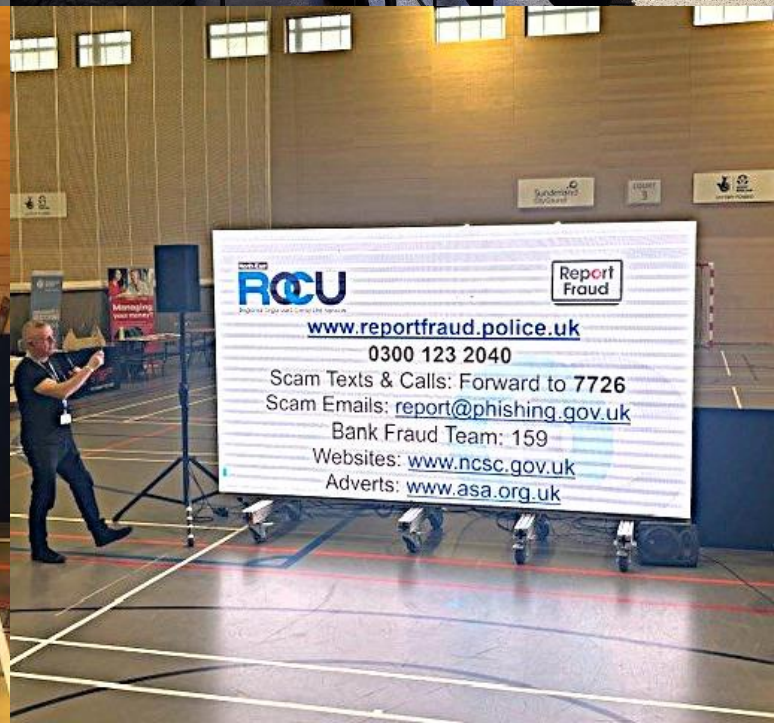
Red Flags;

- Anyone claiming to be from the police, bank or government and asking you to send money, Gold or Jewellery.
- Being pressured to act quickly.
- Unusual courier requests to send money.
- Claims its all for your own protection.

How to protect yourself;

- Never send money (or Gold or Jewellery) - the police, bank or government would never ask you to hand over these items or ask you to send it on.
- Verify independently – contact your bank on a safe number and check it is legitimate.
- If you have forwarded money, contact your bank ASAP.





ENGAGEMENT EVENTS

Below are just some of the events the team have attended this month…

- Beacon of Light financial wellbeing conference
- Cyber breakfast event at Sunderland City Hall
- Sunderland university refreshers fayre
- Northumbria university student events
- Durham agricultural society meeting
- Tyne Coast college student lectures
- Newcastle libraries digital inclusion events
- Fraud Roadshow At Barclays, Grainger Street
- Ashington Escape Family support event
- Sunderland housing care home events

Public Wi-Fi Use

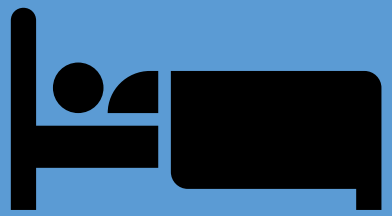
Free public Wi-Fi is available virtually everywhere but while these networks are convenient, they could leave you vulnerable online threats. Also , there is an increased chance of receiving phishing emails by fraudsters following public Wi-Fi use.

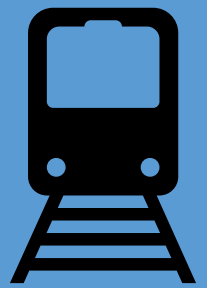
How to use it safely:

- **Before connecting** – Install the latest security updates, enable antivirus if you're using a laptop, and verify the wi-fi network's legitimacy (ask a staff member if you're unsure). You can use a VPN for additional protection, if you want to.

- **While connected** – Only visit secure websites (look for HTTPS) and avoid accessing sensitive personal data. Don't click links or download files from unknown emails.

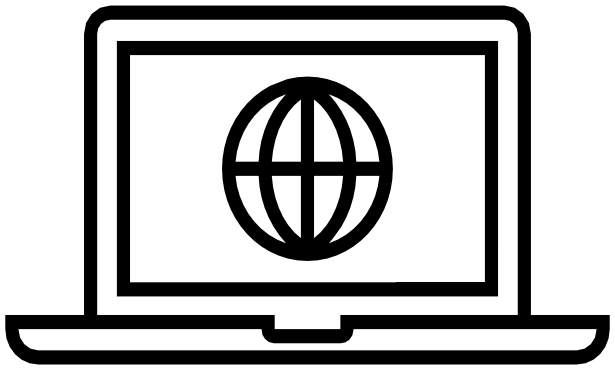
- **After disconnecting** – 'Forget' the network on your device so it doesn't auto-connect in the future without your consent





Horizon Scanning

Monitoring Threats



Investment Recovery Scams

If you have small, old investments, be mindful that Fraudsters are contacting investors and claiming they are due a windfall.

One victim was told they were owed thousands from a £100 pre-covid investment. They were contacted unexpectedly by a compensation company which appeared very professional with a good online footprint. The victim was not asked to pay up front to release their windfall which allayed any fears they had.

The victim was given a passcode to an account where they could see the large sum and were instructed on how to make a withdrawal. There was an issue with the steps to take so the Fraudster asked the victim to download an app so they could help them by accessing their PC remotely. Luckily, the victim was suspicious and hung up otherwise the Fraudster could have used this guise to empty all their bank accounts.

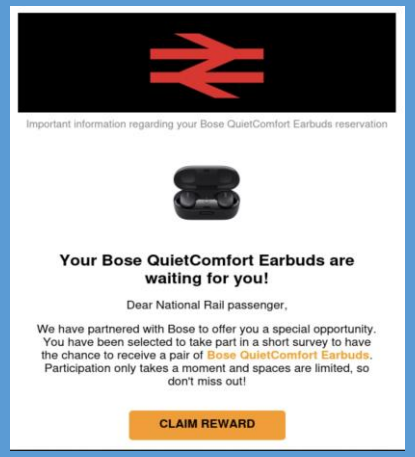
What's Happening Next?

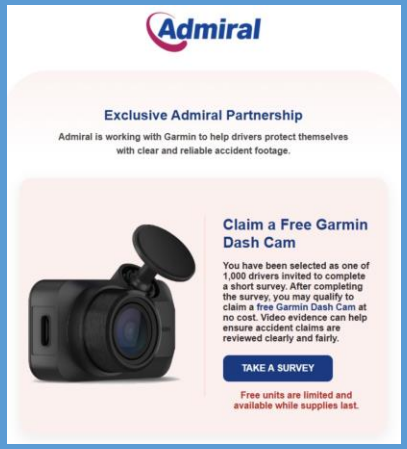
Easter Giveaways

Usually at this time of year, Fraudsters start advertising free giveaways linked to surveys for Easter hampers and chocolate eggs. Once personal details or banking details to pay for small postage costs are entered, your details can be stolen and then used to take out loans and open credit accounts in your name.

Emails offering free gifts and rewards are increasing and more widespread . With AI , some of these emails are professional and appear very real. We have seen emails from insurance companies and National Rail offering dashcams and earbuds.

If you receive such an email, do not click on the link. Such offers appear too good to be true and usually are.





DO YOU *REALLY* KNOW WHO YOU ARE TALKING TO?

Fraudsters impersonate celebrities in Investment and Romance Frauds to dupe victims into parting with cash

Celebrities will never ask you for money or advertise fantastic investment opportunities.

Beware of Deep Fakes

Tell the Police about cyber crime and fraud

reportfraud.police.uk or call 0300 123 2040

Report Fraud has replaced Action Fraud, for use in England, Wales and Northern Ireland.

Anyone searching for how to report cyber crime or fraud, or trying to use Action Fraud, will be redirected to the new service, which can be reached directly online at reportfraud.police.uk or by calling 0300 123 2040.

Report Fraud will provide:

- A clear and simple reporting process to tell the police about cyber crime and fraud.
- Guidance on what to report and how that information is used
- Further support information for victims.

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 Report Fraud by phone or online:
www.reportfraud.police.uk
0300 123 2040

Report Fraud is the central reporting point for all reports of fraud, your local police force will be informed by Report 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	**Claire Hardy– Economic Threat Desk Analyst** **Nicola Lord –Cyber Threat Desk Analyst** **PC Brian Collins – Engagement Officer**
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.