North Yorkshire Police

Cybercrime, Digital Investigations & Fraud

August 2023

Strategy & Structure

NYP Control Strategy Priorities 2025

VAWG

- Domestic abuse
- Stalking
- CSAE
- RASSO
- Online and Tech-enabled VAWG
- OIC/MSHT

Detective Superintendent Safeguarding

Serious & Organised Crime

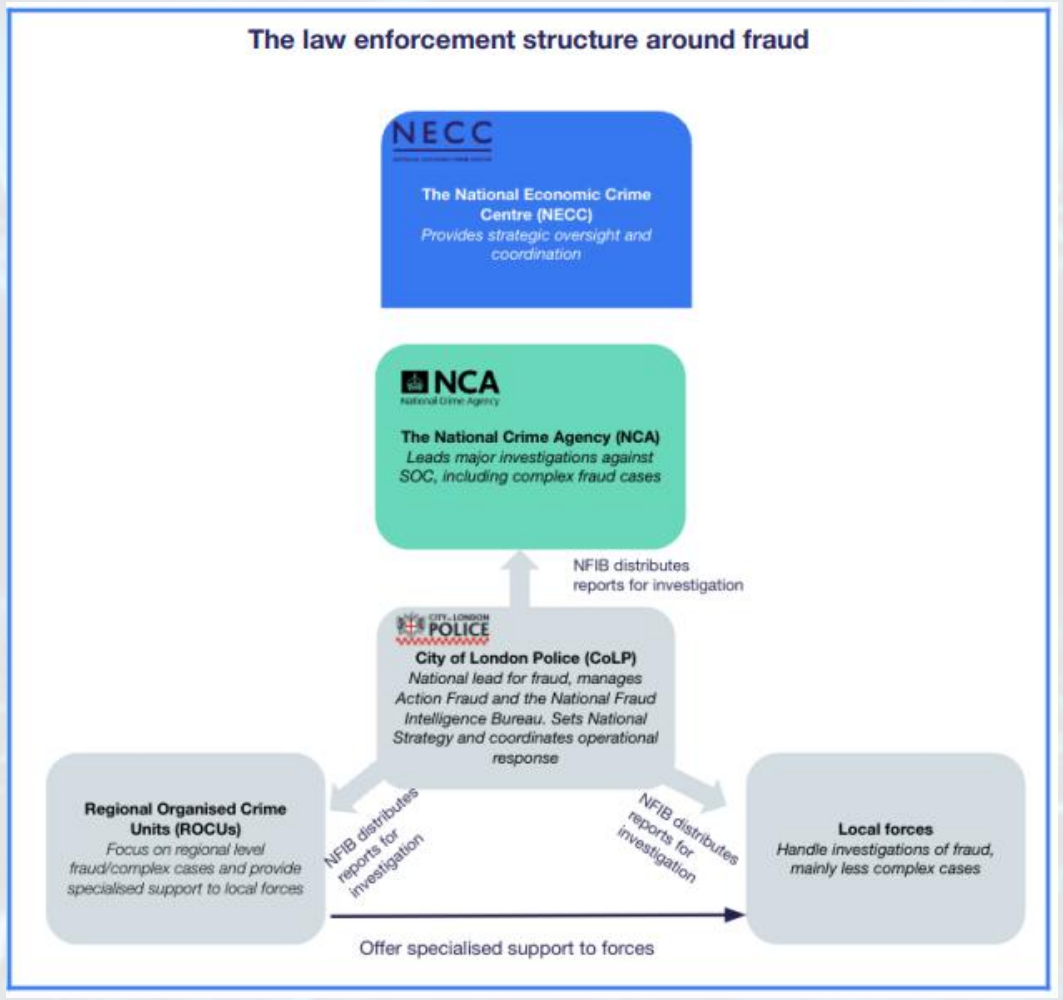
- OCGs
- Serious Violence
- Fraud

Head of MSOC

Neighbourhood Crime

- Road Safety
- Rural Crime
- Residential Burglary – City & County
- Drugs Deaths

Head of Ops, Area Commander, Supt Local Policing



Cybercrime Unit – The 4 ‘Ps’

- **PURSUE**

Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens.

- **PROTECT / PREVENT**

Protect through building cyber security and resilience of UK and its economy, including safeguarding its citizens. Prevent people from cyber offending, remove enablers and reduce incentives of cyber crime

- **PREPARE**

Strengthen capability to prepare for, respond to and recover from cyber-attacks to minimise harm caused and support victims.

Economic Crime– The 4 ‘Ps’

- **PURSUE**

Ensure there are the capabilities in place to investigate and action all NFIB packages.

- **PROTECT / PREVENT**

Dedicated Financial Crime PROTECT officer

- **PREPARE**

Ensure officers/staff have the right training & CPD to tackle the threat

Cybercrime Unit - Responsibilities

- Primary Focus - Computer Misuse Act (CMA) Investigations: Hacking, Ransomware, Distributed Denial of Service (DDOS), Malware, Website Defacement

- Investigative support to other departments “CMA-Linked Crimes”
  - Investigation opportunities
  - Support evidential captures
  - Communication data application support

- Online Fraud/Scams, Harassment, Webcam Extortion/Blackmail, Phishing, Fake Websites
- Technology facilitated abuse – Controlling/coercive behaviour, stalking/harassment
- 24/7 on-call – urgent serious/major crimes (e.g. murder, rape, organised crime, high-risk missing persons)

ECU – Pursue Responsibilities

Partnership working – June 2025

- Money mules recruited by fraudster to open bank accounts
- Binance facial recognition systems identified fraudster
- City of London Police investigation commenced, with several identified money launderers in our area
- Combination of PACE & POCA powers used

Cryptocurrency capabilities – July 2025

- Mobile phone seized and examined which showed evidence of cryptocurrency being used.
- Sufficient information enabled cryptocurrency wallet to be rebuilt, and balance seized
- S47M POCA -Realisable Property Detention Order secured

First in the UK – Cyber Pursue

- 2024 - intelligence regarding firearms printing lead to the arrest of an offender. NYP CCU were called in to assist in digital evidence identification and strategy.

- The attending officer identified a *Pwnagotchi* – a mobile phone sized device that indiscriminatingly attacks home Wi-Fi routers and steals data allowing for the password to be cracked. Bad actors can then use the Wi-Fi connection to commit crime anonymously.

First in the UK - Outcomes

- Believed to be the only investigation into this device in the UK to date. In the UK alone there are over 3000 registered devices.

- At the conclusion of the Digital Forensic Investigation into the Pwnagotchi device, the offender was offered and accepted a conditional caution with requirements to address offending through rehabilitation services partners.

- Proactive safeguarding took place after digital forensic analysis of the device revealed data that allowed NYP CCU to locate and inform victims of the attacks that had taken place.

- Examples of Safeguarded Victims:
  - Care Home
  - Local Government infrastructure
  - Multimillion pound private industry
  - Public Homes

- Published in the Team Cyber UK law enforcement network briefing.

- Contact made by other UK law enforcement officers regarding the investigation & sharing of best practice.

Cybercrime Reports – 2025 (Q1, Q2)

Reports year to date:

- 193 reports to NYP CCU for breaches of the Computer Misuse Act 1990
    - **176** Protect reports
    - **18** Pursue investigations
    - **140** Victims
    - **ALL** Victims contacted with Cyber Protect advice in line with 100% contact policy.

- Outcomes year to date:
    - **3** Arrests & Interview
    - **5** Voluntary Attendee Interviews
    - **2** Conditional Cautions (CMA & Fraud)
    - **4** Charges (CMA | Make IIOC| Possessing Extreme Pornographic Material)

ECU - Protect / Prevent Responsibilities

- FASO & Fraud Ambassadors
- Virtual Kidnapping - Presentations to York University including to overseas students (Chinese / Mandarin translation)
- Romance fraud awareness week

Operation Webhook – Protect / Prepare

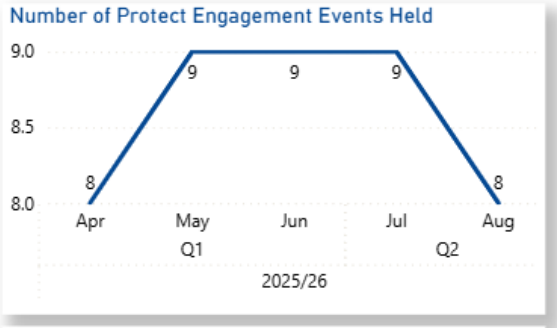
- Proactively identifying and notifying potential victims of cybercrime ***before*** they become a victim.
- Cyber target hardening by reducing vulnerable systems
- Very high success rate and very positive feedback

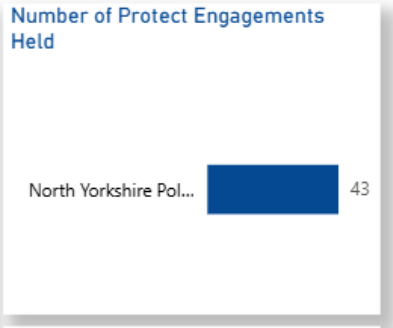
- Educational Institutions
- Local Government & Public Sector Infrastructure
- Web Hosting Company
- Several Small and medium-sized enterprises (SMEs)
- Private individuals in residential settings

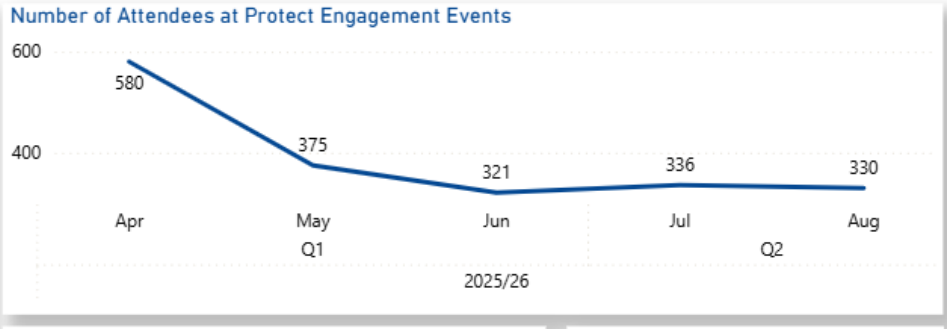
Operation Webhook – *Feedback*

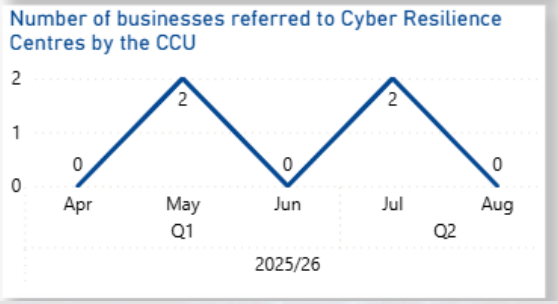
- *"I run MoD computers from here and my wife runs her NHS computer, thank you!"*
- *"May I take this opportunity to thank you and North Yorkshire police for bringing this to our attention – this is a great service that we had no idea you provided."*
- *"Thank you for your e-mail. We are impressed by the police's proactive approach and would commend this kind of activity given the security threat landscape in the UK at present."*
- *"Good to hear from you again, and thanks for letting us know about this asset. I'll speak to our Infrastructure team, and let you know their plans and any outcomes you need."*
- *"This information is definitely helpful and we really appreciate the heads up."*
- *"It's also good to find that at least North Yorkshire police are being pro-active in looking for vulnerable sites and alerting the owners, thank you."*

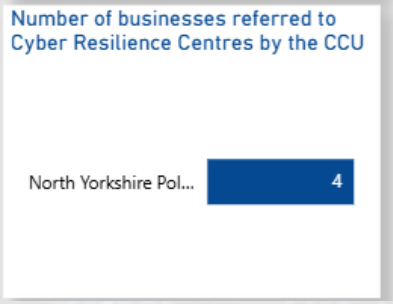
Performance Data

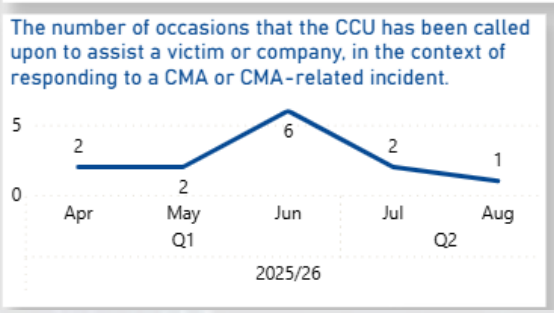


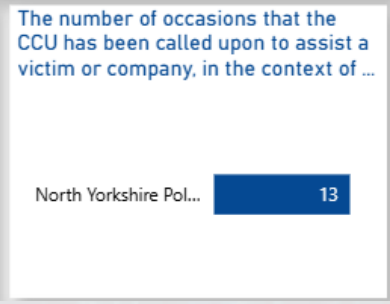












Protect & Prevent – Public/Partner Education

- Delivery of over 50 presentations to over 2000 individuals in the financial year to date. Including:
  - **16 educational facilities**
  - **6 Youth Groups**
  - **5 Women specific groups including a joint dedicated day event Dalby Forrest Girls Wellbeing Festival**
  - **Multiple Carer/Foster parent specific**
  - **Multiple general-public drop in sessions**
- Multiple *Cyber Escape Rooms* – interactive game investigation focusing on understanding weaknesses in personal cyber security and how not to be a victim.
- Half day input to all new starter police officers during their initial training.
  - Personal cyber security
  - Digital evidence recognition and seizure
  - Technology recognition
  - Social Engineering
  - Procedures & Policy
  - VAWG safeguarding considerations though Digital Safety and Target Hardening
  - Social Media Leaking
  - Wi-Fi security
  - Tracking
- Implementing everything learned into advice to the public

Prepare – Investing in our People

Economic and Cyber Crime Academy

- Six Specialist Fraud Investigators
- Three Economic Crime Investigation Managers

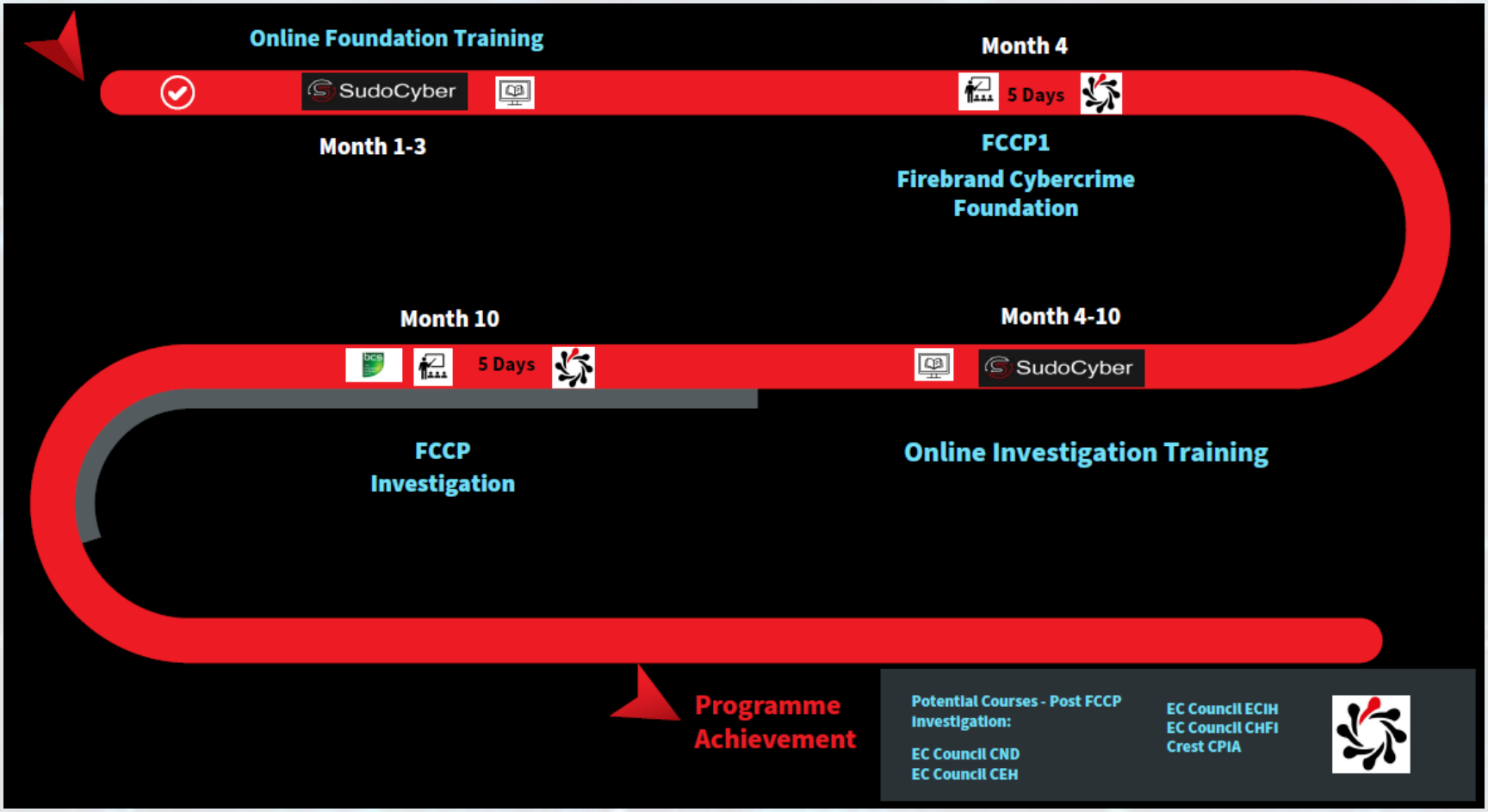
National Crime Agency

- Thirteen NCA Accredited Financial Investigators

Cryptocurrency Training

- Crypto Seizure Specialist trained officers

Investing in our People – Training Pathway



ECU - Challenges

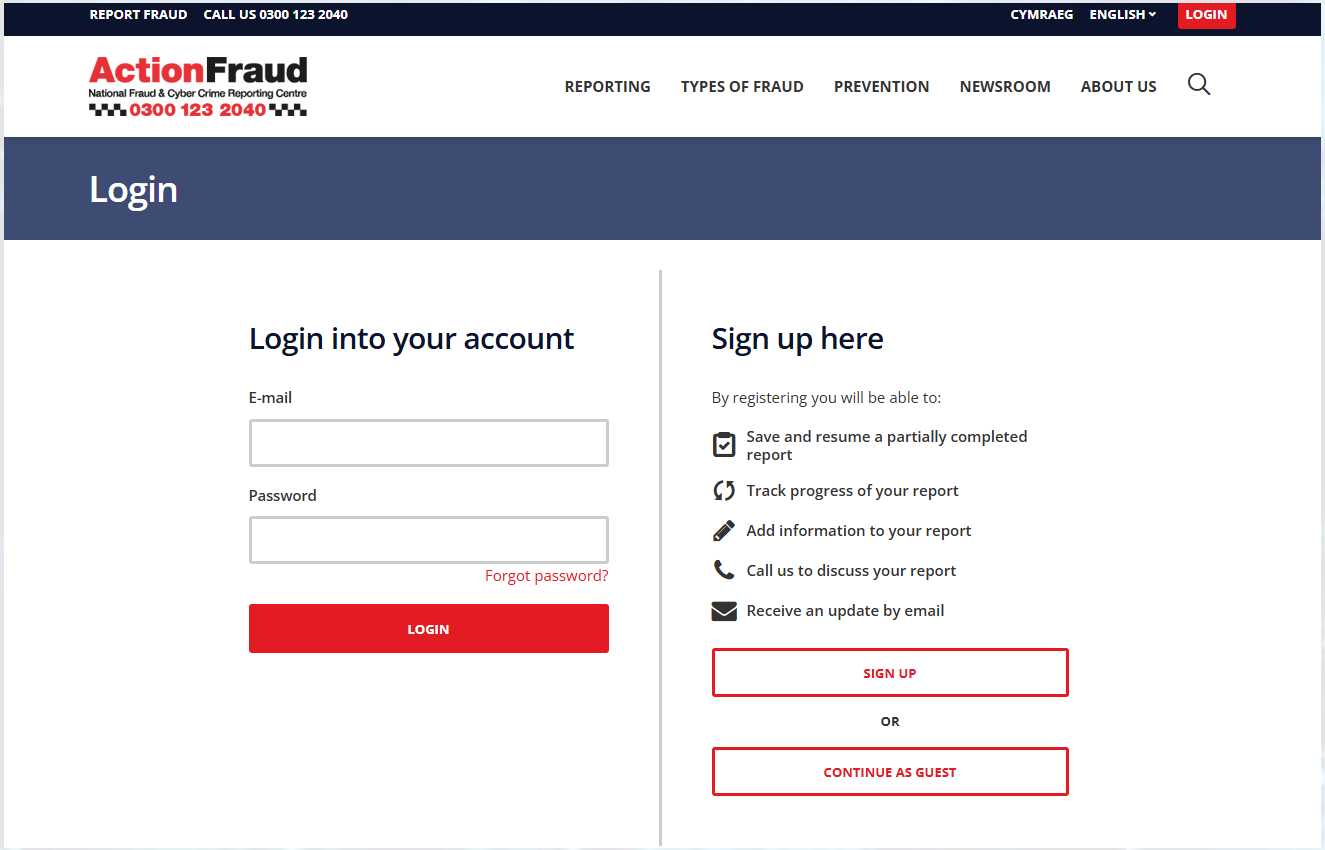
- Government report states fraud accounts for over 40% of crime but receives less than 1% of police resources
- Increasing understanding of the link between fraud and other areas of organised crime such as modern slavery and drugs
- Traditional investigation - follow the money v Proactive investigation – investigate the event itself
- Continued investment in ensuring we have a workforce with sufficient skills and capabilities
- Data sharing - Obtaining evidence from financial institutions and in particular technology companies can be difficult and lengthy
- Cross border cooperation

ECU – Deliver Improvement & Future Goals

- Reinvest recovered funds into enforcement and victim care
- Expand training and investment in Cyber and Economic Crime teams
- Increase Public Awareness and Digital Literacy

Reporting Fraud & Cybercrime

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040



Suspicious Email Reporting Service (SERS): report@phishing.gov.uk