

CORPS RELAY

Prepared by: Mike Bluestone CSyP, Neil Shanks CSyP
James Henderson CSyP & Keith Denton Msyl
Date: December 2024

CORPS
— Est. 1859 —
SECURITY

SIA Targets Training Fraud in Private Security Industry

The Security Industry Authority (SIA) has launched a concerted effort to address fraudulent practices within the training sector of the private security industry. Paul Fullwood, the SIA's Director of Inspections and Enforcement, emphasised the critical role of high-quality training in maintaining public safety and upholding trust in the industry.

The initiative focuses on rooting out malpractice such as false qualifications, misuse of training credentials, and collusion between trainers and trainees. The SIA has committed to rigorous inspections and enforcement actions to ensure

compliance and integrity across the sector. This move aligns with the SIA's broader strategy to enhance professional standards and protect the public from the risks associated with inadequately trained security personnel.

This campaign reinforces the importance of transparent and honest practices within the private security training ecosystem, underscoring the SIA's commitment to fostering a well-regulated and competent workforce.

Martyn's Law Update (Third Reading in the House of Commons)

The Terrorism (Protection of Premises) Bill, known as Martyn's Law, successfully passed through the 3rd reading in the House of Commons on 9th December. The next stage will see it presented to the House of Lords, prior to obtaining Royal Assent.

The reading passed without division (division being any separate vote within the house), indicating the level of cross-party support within the House of Commons. Additionally, several MPs voiced their support and praise for Figen Murray OBE who has tirelessly campaigned for the bill.

Action Fraud's 12 Frauds of Christmas

Action Fraud, the national fraud and cybercrime reporting service, has launched a Christmas campaign highlighting 12 types of fraud to be aware of during the festive season. The public are being encouraged to remain particularly vigilant, both online and in person, as criminals look to exploit this time of year while people celebrate Christmas and the festive season.

The 12 types of fraud they highlight are:

- **Phishing:** Deceptive communications aiming to extract personal or financial information from the recipient.
- **Pet Fraud:** Fake advertisements for pets that don't exist, leading to financial loss for anyone that attempts to purchase them.
- **Online Shopping Fraud:** Non-delivery of purchased items from fraudulent sellers.
- **Social Media and Email Account Hacking:** Unauthorised access to personal accounts for malicious purposes.
- **Courier Fraud:** Impersonation scams where a fraudster contacts victims by telephone purporting to be a police officer or bank official, with the aim of deceiving the victim into handing

over bank cards or cash.

- **Romance Fraud:** Scammers feigning romantic interest to exploit victims financially.
- **Gift Card Fraud:** Requests for payment via gift cards, often linked to impersonation scams.
- **Charity Fraud:** Fraudsters posing as charitable organisations to solicit donations to their fake charity.
- **Investment Fraud:** Promises of high returns on investments that are non-existent or fraudulent.
- **QR Code Fraud:** Malicious QR codes directing users to phishing sites or prompting unintended payments.
- **Holiday Fraud:** Fake holiday deals or accommodations leading to financial loss to anyone purchasing them.
- **Ticket Fraud:** Sale of counterfeit or non-existent tickets to events.

Staying informed about these scams can help protect against financial and personal information loss during the holiday season. Action Fraud provide a greater level of detail on these on their website.

Transport for London Scam Warning

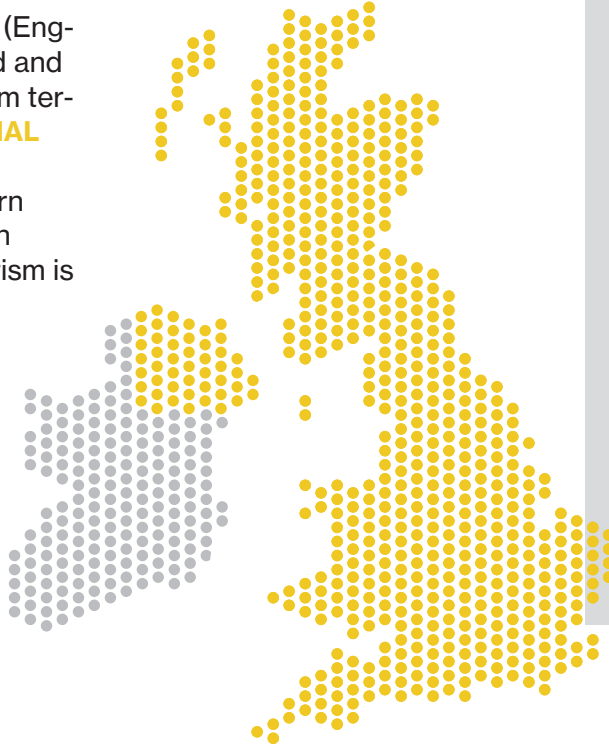
There is currently a scam text circulating which informs the recipient that their congestion charge auto pay service has been 'disabled'. The link in the text then takes the individual to a convincing duplicate of Transport for London's website. Consumers are reminded never to take any messages they receive, including emails and texts, at face value, and to always access any existing services they have via the official route rather than links sent to them.



Current National Threat Level

The threat to the UK (England, Wales, Scotland and Northern Ireland) from terrorism is **SUBSTANTIAL**

The threat to Northern Ireland from Northern Ireland-related terrorism is **SUBSTANTIAL**



NOTE:

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack

LOW means an attack is highly unlikely

MODERATE means an attack is possible, but not likely

SUBSTANTIAL means an attack is likely

SEVERE means an attack is highly likely

CRITICAL means an attack is highly likely in the near future

Warning that Children as Young as 10 are Accessing Extreme Material Online

Deputy Assistant Commissioner Vicki Evans, of the Metropolitan Police, has expressed growing concerns about children as young as 10 accessing extreme and violent material online. This development reflects an alarming trend where younger individuals are being drawn to harmful content. Evans, who oversees counter-terrorism policing at a national level, highlighted cases where people demonstrate an unhealthy fixation with violence, often revealed through their online search histories.

The police and security services have disrupted 43 significant terror plots since 2017, three of which were uncovered in the last year. Despite these successes, the UK's terrorism threat level remains at "substantial," signalling that an attack is likely.

Evans stressed the critical role of public awareness in preventing terrorism. She urged the public to remain alert and report anything suspicious, emphasising the need for collective effort in maintaining safety. Her appeal highlights the importance of shared responsibility in identifying and mitigating potential dangers.

The widespread availability of extreme online material, particularly among younger audiences, creates significant challenges for counter-terrorism efforts. The ease of access to such content underscores the need for a holistic approach, combining policing, education, and community involvement, to tackle the causes of radicalisation and curb the spread of violent ideologies.

Four Charged with Terrorism Offences following HMP Investigation

Rhea Wood (35) from Sheffield was charged with a terrorism offence as part of an inquiry into material taken into a prison. Counter Terrorism Policing Northeast charged Wood with dissemination of terrorist publications and conspiring to bring a List B prohibited article into or out of HMP Lindholme, near Doncaster. Additionally, as part of the HMP investigation three others were charged.

Abdullah Mohammed (32) from Doncaster, Menna Mohammed (36) from Sheffield and Mohammed Abdo (34) currently of HMP Wealstun were also charged with conspiring to bring a List B prohibited article into or out of a prison. Ms Wood and the others are due to appear for a pre-trial hearing regarding the conspiracy offence at Sheffield Crown Court in January next year.



WE DO NOT CROSS

CRIME SCEN

Murder of Healthcare CEO: The role of Executive Protection

Corps Focus: Security Issue of the Month

26-year-old Luigi Mangione has been charged with the murder of Brian Thompson, the 50-year-old CEO of UnitedHealthcare. Thompson was shot in the early hours of 4th December outside the New York Hilton Midtown Hotel whilst in the city to attend an annual investors' meeting of the parent company of UnitedHealthcare, UnitedHealth Group Incorporated. At his time of arrest, Mangione is reported to have had in his possession a 262-word handwritten letter/manifesto criticising the U.S. healthcare system, a passport, and multiple fake IDs. At this stage it appears that Mangione operated alone, without co-conspirators.

The targeting of high-profile individuals is nothing new, however, the murder of Thompson has highlighted the very real threat that many public figures face. UnitedHealthcare has received criticism for having nearly double the national average for denying claims. Forbes reported that the bullet casings used in the murder had "Deny", "Defend" and "Depose" written on them, in reference to some of the tactics used by health insurance companies when denying payment for healthcare claims, further suggesting a possible link between the business practices of UnitedHealthcare and Mangione's motive for targeting Thompson. This is further supported by suggestions that Mangione suffered from chronic pain following back surgery.

Mangione's motives aside, the incident has raised significant questions about why Thompson did not have executive security with him at the time of his murder. Thompson's earnings in 2023 were reportedly \$10m, and UnitedHealth Group reported \$22 billion in profit for 2023. An individual operating at this level in an industry where threats to senior executives, often linked to denial of service, are not uncommon should be provided with security assessments and appropriate security provision. This is especially important when such individuals are attending key events, such as his company's annual investors' meeting, where they will be expected to attend and the

time, date, and location are easily obtainable.

Businesses have a duty of care to their employees, including ensuring that their employees are kept safe within work or whilst undertaking work activities. When individuals are seen as senior/key figures representing a business or synonymous with a business, that duty of care extends further, as such individuals are always representing the business. The security of such high-profile individuals should be a standard consideration, with examples of standard measures being provided including, but not limited to; security assessments, security of their premises(s), appointing executive protection officers and an advanced party (to ensure the destination is safe prior to arrival), assessing travel security including routes and exfiltration plans, compiling assessments of their digital presence, identifying potential threats to associated targets (e.g. family), electronic security and monitoring services.

Following the incident, UnitedHealthcare has removed the photos, names and biographies of its top executives from its website. This approach has been followed by several other organisations as some businesses enter a state of heightened threat. Whilst the impact on the American private healthcare market may seem removed from some UK businesses, there is also an uptake in the requirement for executive protection and additional security measures for executives being seen across a number of other areas and sectors, including businesses connected to Israel, defence, fossil fuels, and energy industries.

The details of what was and wasn't available to Thompson are not common knowledge at this stage, and it is not possible to say whether an executive protection team would have prevented Mangione from killing him. It is, however, fair to say that had Thompson been working with an executive protection team and advanced party on 4th December, whilst following a suitable security plan, it would have been harder for Mangione to have accessed and shot Thompson.



Market House
85 Cowcross St
London
EC1M 6PF



07890 590352
Neil Shanks



intel@corpssecurity.co.uk
www.corpssecurity.co.uk