POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

North East

CRIMEALERT

Keeping Communities in the North East Safe

JUNE 2024

Welcome to the June 2024 edition of North East Crime Alert.

Produced by the Police Scotland North East Division Crime Reduction Team it's aim is to provide advice on how to spot the latest frauds and scams as well as how to keep your home and business safe.

In this edition of North East Crime Alert:

Officers in the North East are now routinely equipped with SelectaDNA tagging spray to target those using motorbikes to commit anti-social behaviour.

Over two days Police Scotland and partners gave advice to over 1,000 rail passengers between Inverness and Galashiels about the latest frauds and scams.

We look at the most common 'top 10' frauds in the North East and explain the work of the detectives tracking down those responsible.

With the summer months upon us the theft of agricultural GPS equipment is again on the rise. We explain how to protect your property .

As well as a regular round-up of crime in the North East.

Criminals are using ever more sophisticated methods. By staying better informed and working in partnership we can ensure our communities continue to be a safe place to

Website
www.scotland.police.uk

Twitter
www.twitter.com/
NorthEPolice

Facebook
www.facebook.com/
NorthEastPoliceDivision

ANTI-SOCIAL BEHAVIOUR
SelectaDNA tagging spray

Police Scotland extended its use of SelectaDNA's tagging spray to officers in North East Division.

The handheld tagging spray, already used in other areas of the country, will be used by officers to target offenders involved in the antisocial and illegal use of motorcycles, and bicycles, including electric bikes.

The spray is aimed by officers at bikes, clothing and skin of any riders and passengers with a uniquely coded but invisible DNA that will provide forensic evidence to link them to a specific crime.

The spray is deployed as a very fine mist which does not cause any harm or damage to skin, clothing or property. The solution does not wash off surfaces, so can help forensically link offenders even after a passage of time.

Officers in the North East Division already use SelectaDNA products for marking property in efforts to deter and detect stolen goods in housebreaking and rural crime incidents.

Since it's launch, the product has already been deployed successfully and will be continue to be used in our area.

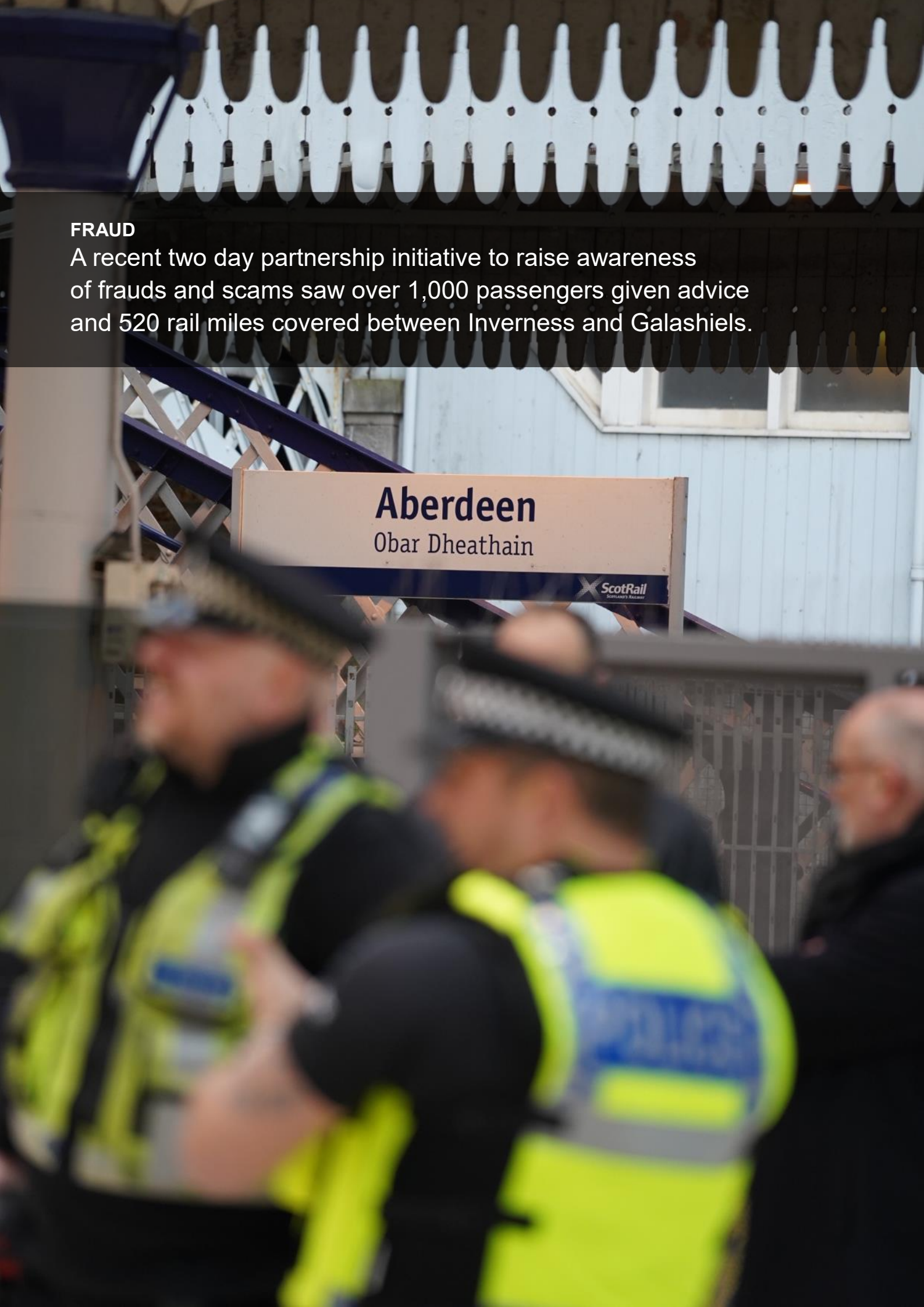
Chief Inspector Darren Bruce said: 'The use of this tagging spray is another tool officers will have at their disposal to help detect illegal and antisocial activity associated with motorcycle and bike crime.

'We know that this issue has been a concern for some communities in Aberdeen over a period of time, and we've had a number of local projects ongoing in a bid to help tackle this. Other areas of the country have seen great results in reductions of crime using these products and we hope this will be reflected in our communities.

'I'd ask the public to continue to work with us to apprehend those taking part in anti-social behaviour and hold them to account throughout our area.'

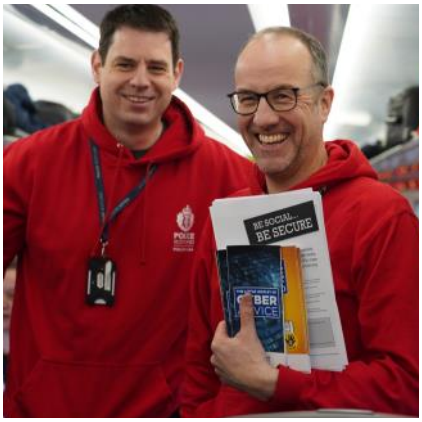
SelectaDNA also offer security marking products for a wide range of uses including your home, office and plant and construction equipment.

www.selectadna.co.uk



FRAUD

A recent two day partnership initiative to raise awareness of frauds and scams saw over 1,000 passengers given advice and 520 rail miles covered between Inverness and Galashiels.



Police Scotland officers recently launched their annual Anti-Fraud Roadshow as part of a new Stay Safe – Get on Board partnership initiative.

Alongside teams from the British Transport Police, Neighbourhood Watch Scotland and Scotrail, officers promoted fraud awareness to commuters up and down the east coast trainlines between Inverness and Galashiels.

The initiative launched at Aberdeen Railway Station with Neighbourhood Watch Scotland and officers from the Crime Reduction Unit and British Transport Police travelling onward on the Aberdeen-Dundee and Edinburgh-Dundee lines. Officers spoke with passengers offering advice on how to avoid being defrauded or what to do if they have been a victim of fraud.

Day two of the initiative saw officers and partners providing further advice to passengers on the Aberdeen-Inverness and Edinburgh -Galashiels lines.

Inspector Claire Smith of the Crime Reduction Unit said: ‘Police Scotland is committed to tackling fraud and pursuing criminals who commit fraud and providing support to victims is a priority for us. However, we hope that by working alongside partners we can deliver critical fraud prevention messaging and equip people with the information they need to prevent these crimes from occurring in the first place.’

‘Cyber-crime has increased exponentially from around 2018, almost doubling year on year.’

‘We know around 17,000 online frauds are reported each year in Scotland – or around 50 each day and according to our own figures 95% of all frauds have an online element, and it is now synonymous with cyber-crime.’

‘Behind every one of these frauds there is a victim of crime. They may have lost their savings, their business & indeed their very confidence of going online.’

Assistant Chief Constable Andy Freeburn
Executive Lead for Organised Crime,
Counter Terrorism & Intelligence for Police Scotland.

POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA

The North East Crime Reduction Team have pulled together ten of the most commonly seen frauds.

Parcel delivery scams involve tricking people into giving away personal details. They often come from seemingly legitimate companies like DHL or Royal Mail, claiming there's a fee to pay or a delivery to reschedule. Clicking a link in the message can lead to a fake website where you might be asked for your bank details, passwords, or even be tricked into transferring money to a fake account.

Watch out for **WhatsApp messages** from 'family' claiming a new phone and urgent financial need. It's a scam! Before sending money, verify their identity by calling their original number. Don't rush decisions due to pressured messages. Never send money through messaging apps without confirmation. Use two-factor authentication and warn your family about this scam.

Sextortion scams trick people online into sending nude photos or videos. The scammer pretends to be someone else, builds trust, then threatens to share the explicit material with loved ones or publicly unless the victim pays money. Don't share private information online, be cautious of strangers who turn conversations sexual quickly, and use strong privacy settings to avoid this trap.

Ticket fraud. Don't get scammed buying tickets for your next concert. Stick to official sellers and verified resellers and avoid deals that seem too good to be true. Use secure payment methods like credit cards and be wary of anyone contacting you about tickets. Check for ticket authenticity and avoid using prepaid debit cards. Buying early and ignoring unsolicited offers will also help you avoid scams.

Courier fraud targets people with fake calls and messages pretending to be from their banks or credit cards. They create urgency and trick victims into giving personal details or valuables to a fake courier. To avoid this, be sceptical of unexpected calls, verify the caller by hanging up and calling back using a trusted number, never share personal information over the phone, and don't hand over valuables to strangers. Take your time, don't be pressurised.

Online romance scammers create fake profiles to trick victims into relationships. They build trust then exploit it for money, often claiming to need help with emergencies or travel. Red flags include overly fast declarations of love, excuses to avoid meeting in person, and requests for money. To be safe, never send money online, take time to get to know someone, and be wary of inconsistencies or pressure to help financially.

Investment fraudsters create fake companies that appear legitimate, promising high returns and targeting specific groups. They might claim to have many investors or use celebrities to endorse their scams. Be wary of investment opportunities that seem too good to be true, especially those advertised on social media.

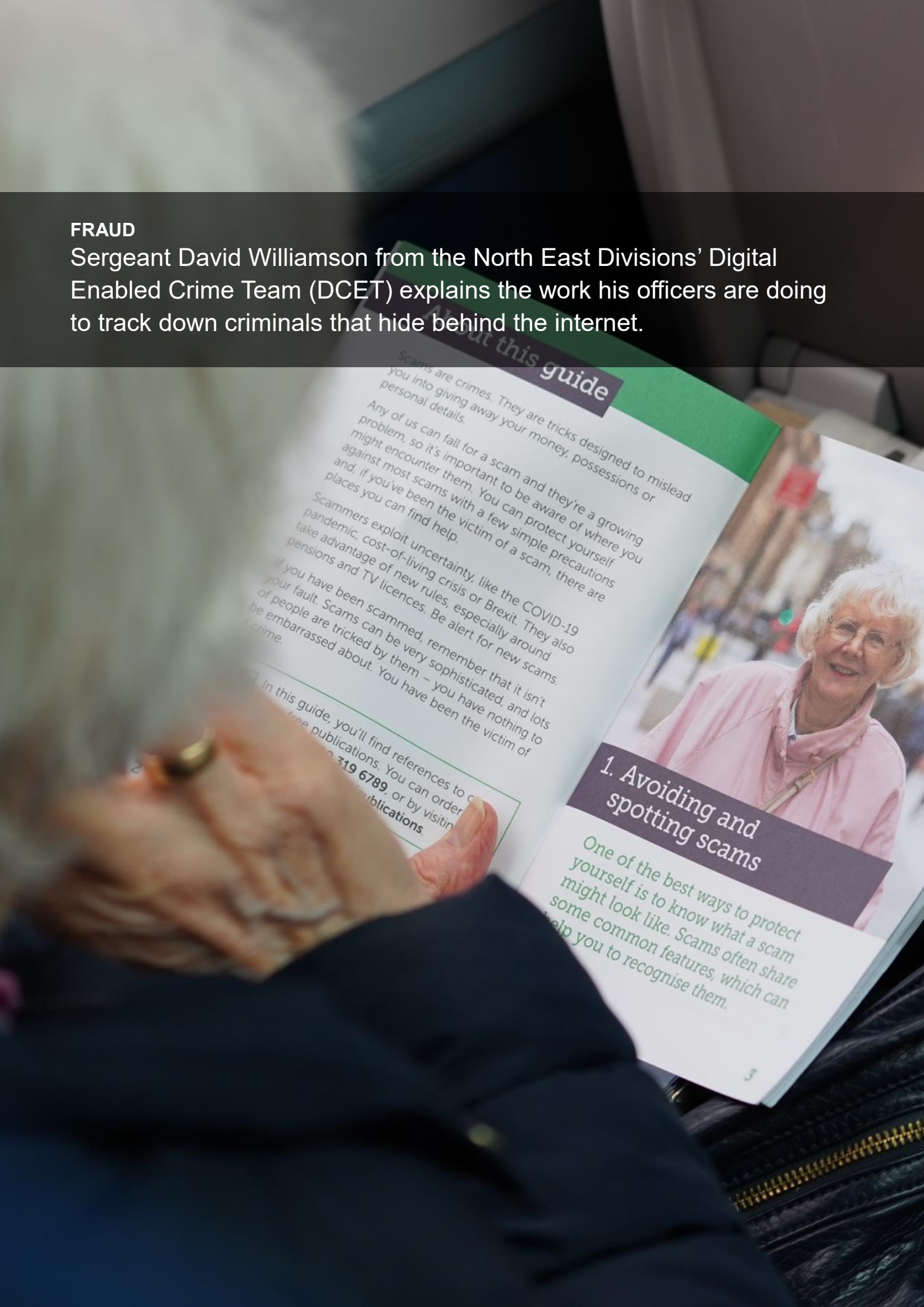
Advance fee scams promise big rewards (money, inheritance, job) for a small upfront fee. They contact you via email, social media or phone. Once you pay, they vanish or request more money with excuses. To avoid this, be sceptical of too-good-to-be-true offers, verify the company's legitimacy, never pay upfront, and don't share personal information.

Push payment scams trick you into sending money to a fake account pretending to be someone you trust, like your bank. They might pressure you to move your money to a 'safe account' controlled by them. To avoid this, be wary of calls or messages urging immediate action, use secure communication and enable security features on your accounts. If something feels off, take a moment to investigate before you send money.

Facebook Marketplace and other online sites can be dangerous for both buyers and sellers. Watch out for deals that seem unrealistically cheap. Fake sellers will often pressure you to pay outside Facebook using methods that offer no buyer protection. Never share personal info or send money before seeing the item and confirm the seller through reviews or a video call. Stick to local pickups and cash on delivery whenever possible.
If something feels wrong,
it probably is.

FRAUD

Sergeant David Williamson from the North East Divisions' Digital Enabled Crime Team (DCET) explains the work his officers are doing to track down criminals that hide behind the internet.



Taking some simple preventative measures can help protect you and your finances.

Adopting a mindset of healthy scepticism in relation to requests for money in any form can help.

Fraud and other financially motivated crime is evolving through use of technology, impacting communities across the North East of Scotland and beyond.

Within policing, there is broad recognition of the harm caused by 'non-contact' financial crime and the lasting impact it can have on individuals affected. Given the nature of technology and the internet though, there are significant complexities associated with criminal investigations into this type of crime.

In an effort to ensure local policing is equipped to respond to the challenges posed by 'non-contact' financial criminality, Police Scotland's North East Division introduced a team of Detectives to specialise in these investigations.

Since 2021, this dedicated team have been developing their collective skillset, working with colleagues from different sectors to target those responsible for orchestrating and facilitating financial crime enabled through technology. Consequently, the team has cultivated strong links with partners internationally and routinely work together with their professional network to apprehend offenders.

Along with other agencies involved in dealing with those who suffer financial harm, the crime team have taken leading roles in initiatives to improve processes to keep people safe from financial crime. Work in this area continues, with a project underway to enhance the effectiveness of the local policing and partner response to those who are identified as being victims of financial crime through their interactions with Bank staff.

Recognising trends and intelligence links is vital when investigating the criminals responsible for financial crime due to the global reach they are afforded by technology. Recent changes in our local crime team operating model has increased collaboration between different policing areas across Scotland, allowing for a comprehensive overview of crime and ensuring our response is more informed, proportionate and appropriate.

The importance of remaining alert to 'non-contact' financial crime cannot be overstated. Criminals and technology are becoming increasingly sophisticated which means that anyone can become a victim – criminals don't just target one segment of society. Taking some simple preventative measures can help protect you and your finances. Adopting a mindset of healthy scepticism in relation to requests for money in any form can help.

www.scotland.police.uk/advice-and-information/internet-safety/keep-secure-online/

North East Crime Reduction Team

Rural Roadshow

The Crime Reduction Team will be again be touring various shows in the North East this summer to answer your queries regarding rural security. Come and meet the team to get the latest advice on everything from quad bike security to keeping your office computer safe from viruses and hackers. The team will be out and about on the following dates across the North so pop along and say hello.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Fettercairn Show
6 July 2024

Banchory Show
27 July 2024

Turriff Show
4 and 5 August 2024

KeithShow
10 and 11 August 2024

RURAL

Farmers urged to be vigilant after new wave of GPS thefts

Farmers across the UK are being urged to be vigilant after a new wave of Global Positioning System (GPS) thefts in recent weeks, NFU Mutual and the National Rural Crime Unit (NRCU) have warned.

Used to provide precision positioning for cultivation and harvesting operations on farms across the world, GPS systems have become one of the most targeted pieces of farm equipment because of their high value and portability.

Superintendent Andrew Huddleston, who leads the NRCU, said: 'Organised crime groups are once again operating in the countryside, and they are targeting previous victims, especially those who have had GPS stolen in the last two years.'

- Activate PIN security on GPS kit with your own unique number if available.
- Mark your postcode on the unit's case to deter thieves and trace your property back to you.
- Keep tractors and combines with GPS fitted stored out of sight when possible.
- Remove GPS kit when possible, from tractors and other machinery and store it securely when not in use
- Record serial numbers and photograph your kit.
- Check serial numbers of second-hand kit offered for sale.

For further advice regarding rural security measures email your local crime reduction team - NorthEastCrimeReduction@scotland.police.uk

RURAL

A Forensic Marking Solution to Tackle GPS and Agricultural Equipment Theft

The cost of tractor GPS theft more than doubled to over £500,000 in the first quarter of 2023 (source: NFU Mutual), so protecting agricultural machinery, such as GPS kits is now more important than ever. To help combat this ever-growing issue, SelectaDNA released a forensic marking kit for tractor GPS systems.

SelectaDNA has long been used in rural settings on frequently targeted areas and hard-to-protect buildings, where criminals are looking for items which are easy to sell on, such as tools, GPS systems, ATVs and agricultural machinery. The solution, which has proven to reduce rural crime, and in some cases eliminating it completely, allows the police to link criminals to crime scenes and secure convictions.

However, in the unfortunate event that property does get stolen, SelectaDNA can help lead to recovery. When registered, the unique SelectaDNA code is recorded on the Secure Asset Register database. A code found on an item of property or criminal can then be identified back to a specific owner and location.

In a bid to reduce rural crime, Police Scotland and NFU Mutual extended a farm property marking scheme that saw SelectaDNA's Rural Property Marking kits distributed to highly targeted rural areas. Police Scotland has reported that a trial of SelectaDNA marking on 100 South Lanarkshire farms was a huge success, with repeat thefts on farms previously targeted by thieves eliminated.

Criminals know that DNA is one of the police's most powerful weapons in convicting criminals. Criminals view items marked with SelectaDNA as too high risk as they know they can be linked back to their owner. Using SelectaDNA to mark your property, combined with visible warning signage, is a proven and highly effective theft deterrent.

THEFT

Lock It or Lose It

Many of us have a false sense of security, especially in our own neighbourhoods.

We might leave our car unlocked in the driveway for a quick errand, thinking ‘nothing bad will happen here.’ But unfortunately, car thieves don't discriminate.

An unlocked car, regardless of location, is an open invitation for trouble.

Modern cars aren't impenetrable. While some may believe modern car alarms and security systems offer complete protection, that's not always the case. Savvy thieves can employ techniques to bypass these systems, especially if a car is left unlocked. Locking your car is the first line of defence and makes it significantly harder to steal.

Opportunity makes a thief
Thieves are constantly looking for easy targets. An unlocked car with valuables visible is a prime opportunity. It only takes a thief seconds to snatch a purse, laptop, or even the entire car itself if the keys are inside.

Insurance issues
Leaving your car unlocked could invalidate your car insurance policy or limit your coverage in case of theft. Most insurance companies require reasonable precautions to be taken by the owner, and leaving your car unlocked might be considered negligence.

Lock your car, every time
This seems obvious, but it's worth repeating. Develop the habit of locking your car every time you exit, no matter how short the trip.

Take Valuables With You.
Don't leave anything tempting in plain sight. Bags, electronics, and even loose change can attract thieves. Take valuables with you or lock them securely in the boot.

Park Smartly. Whenever possible, park in well-lit, populated areas with surveillance cameras. Avoid leaving your car parked on the street overnight if you have a garage or driveway option.

Taking these simple precautions takes minimal effort but can significantly reduce the risk of theft.

Scam Update #14

Quishing

QR code phishing or ‘quishing’ is a type of phishing attack that uses QR codes to lure victims into revealing sensitive information or even installing malware on their devices. Scammers create a QR code that looks legitimate, such as one that appears to offer a discount or special offer, but in fact directs the victim to a fake website controlled by the attacker. Fake websites can be hard to spot as attackers can create legitimate-looking sites and logos.

Red Flags to Look Out For

You shouldn’t avoid scanning QR codes entirely. Although such scams take advantage of our eyes’ incapacity to “read” QR codes, there are some signs that indicate if you are dealing with a fraudulent QR code.

Check the destination site of the QR code. Check for mistakes and misspelled words, shoddy design, low-quality photos, and insecure URLs as indicators that you’ve landed on a bogus website. Sites that are secure will use HTTPS rather than HTTP and will have a padlock icon next to their URL.

Preview the URL before accessing the link: Before directing you to the intended page, your phone will tell you the destination of the QR code. Check the URL to see if it seems safe. If the URL is shortened or unreadable, be extra cautious.

For extra caution, avoid downloading QR code scanning apps and only use your phone’s built-in QR scanner in the camera.

How to avoid becoming a victim of quishing

Be wary of QR codes in public places. If you see a QR code that looks suspicious, don't scan it.

If you're unsure whether a QR code is legitimate, try to verify it with the organisation that it supposedly represents.

Never enter your personal information into a website that you reached through a QR code.

Keep your smartphone and other devices up to date with the latest security software.

Use a strong password manager to create and store unique passwords for all of your online accounts.

Enable two-factor authentication (2FA) on all of your accounts whenever possible.

If you think you may have been a victim of quishing, contact your bank or other financial institutions immediately to report the fraud. You should also change your passwords and enable 2FA on all of your online accounts.

Crime Alert

A selection of crimes affecting residents from across Grampian

Pig Slaughtering
An Aberdeen female victim met a male on a popular online dating website and was convinced to invest in Cryptocurrency. She lost over £6000 in a fake scheme.

HMRC Scam
A 27 year old male received a phone call from someone claiming to be from HMRC who stated they had an outstanding tax bill, threatening them with jail if this wasn't paid. The caller claimed that if they paid that day they would no incur extra charges. The victim paid the fraudster and lost £2700.

Puppy Fraud
A Grampian resident replied to a Facebook Marketplace advert for a puppy. She sent a £50 deposit by Paypal without seeing the dog before paying another £100 for medical fees. She never received the dog and lost all money.

Investment Fraud
An Aberdeen resident clicked on a Facebook advertisement, for an investment apparently authenticated by Martin Lewis. This was a 'deepfake advert' and she went onto lose over £5000 in investments in what was a fraudulent scheme.

Motorbike theft
A 6 month old motorbike was stolen from the street outside the victims home. The bike had been left insecure and cost £4750.

Instagram Investment
A 39 year old male invested in an add he saw on Instagram.
He invested regular amounts over a 2 month period. The scheme was fraudulent and he lost £10, 500.

Online Earning
An Aberdeen female saw a Facebook add for earning money by carrying out reviews. She was initially given 40 tasks to complete and was advised that to earn more she needed to invest money. The scam cost her £27,000.

Extortion
An Asian student studying in Aberdeen was approached by scammers claiming to be from his home country. The fraudsters claimed he needed to pay in order to remain in the UK. Over a period of a few weeks the male lost £24,000.

Crypto Currency Trading
An Aberdeen resident started using a Crypto Trading App. Over a period of time he invested large sums and believed he was making a profit. When he went to remove funds he realised the app was a scam and lost £9000.

Push Payment Fraud
A 86 year old female was awaiting a delivery after an online purchase and received a message from a delivery company stating there was delay and that she needed to pay for a mail redirection. She paid the £1.99 but shortly afterwards received a call from a male claiming to be from her bank. He advised there was fraudulent activity and to package up her bank and credit card as well as her mobile phone with all pin numbers for them to be investigated. These were uplifted from her home address and when she checked with her bank, she found it was a scam and she had lost £25,000.

Romance Fraud
An Aberdeen female befriended a male online she believed was working on a ship in South Korea. Scammers convinced the victim to transfer over £2000.

Sextortion
A male victim met who he believed to be a similarly aged female online. The conversation quickly turned sexual and they exchanged nude images. The female was a scammer and threatened to share his images to friends and family. He paid £1600 before making family and Police aware.

Bicycle Theft
A female student left her bicycle outside a local university secured with a poor quality lock. When she returned the nearly new e-bike had been stolen. The bike cost £2600.

Business Fraud
An Aberdeen engineering company was the victim of an invoicing fraud. They lost £320,000.

Gumtree Fraud
An Alford resident lost a £100 deposit for golf clubs advertised on Gumtree. The victim transferred a deposit directly to the scammers account rather than using a secure payment method such as PayPal.

Bicycle Theft
A Giant downhill mountain bike valued at £2000 was stolen from the High Street, Banchory. The bike had been left insecure while the owner went into a local shop.

Keeping Our Communities in the North East Safe

Police Scotland's North East Division covers rural and urban areas in Moray, Aberdeenshire and Aberdeen City. The division has five territorial command areas which have their own dedicated Area Commander, who is responsible for the daily policing function. Each command area is served by a number of community policing teams whose activities are built around the needs of the local community. These teams respond to local calls and look for long term solutions to key issues. They are assisted by the division's Crime Reduction Unit who deliver against Force and local priorities in a number of areas, including physical and social crime prevention, supporting and enhancing community engagement and creating and sustaining strong and effective partnership working.

Website
www.scotland.police.uk

Twitter
www.twitter.com/NorthEPolice

Facebook
www.facebook.com/
NorthEastPoliceDivision

North East Division Crime Reduction Team

Moray
PC Richard Russell
richard.russell@scotland.police.uk

Aberdeen City
PC Mark Irvine
mark.irvine@scotland.police.uk

Aberdeenshire
PC Mike Urquhart
michael.urquhart@scotland.police.uk

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA