POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

North East

CRIMEALERT

Keeping Communities in the North East Safe

NOVEMBER 2025

Welcome to the November 2025 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:

Police and NFU Scotland urge those living and working in rural communities to report crime.

Darker Nights - follow our advice on how to keep your home safe as the nights draw in.

Are you aged between 13 and 15 years old and would like to volunteer in your community? Read about how you can gain skills and support your local policing team.

How to shop safely online for the festive season.

Learn about what makes an effective password and how to store them securely.

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 live and work.

Website
www.scotland.police.uk

Twitter
www.twitter.com/NorthEPolice

Facebook
www.facebook.com/NorthEastPoliceDivision

Retail Crime TASKFORCE

Think you're ANONYMOUS?

We're sharing information. Connecting the dots.
We're catching retail criminals.

Retailers and police now share intelligence to identify repeat offenders and organised groups.

Every piece of evidence is now connected through a national intelligence network, linking incidents and identifying offenders.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

SPACE

#NotAVictimlessCrime #RetailCrimeTaskforce

Rural Crime

Police Scotland and the National Farmers Union of Scotland urge those living and working in rural communities to report crime.

Chief Inspector George Nixon discussing the impact of rural crime with farmer Sandy Tulloch.

National Rural Crime Week 2025 was a significant initiative aimed at raising awareness and addressing the challenges faced by rural communities due to crime. The week focussed on the victims of rural crime, highlighting the challenges they face and the actions needed to protect them.

As part of the initiative, North East Division's Lead on Rural Crime Chief Inspector George Nixon, went to visit Sandy Tulloch who has a farm near Lumphanan. During the visit Sandy explained how he had been a victim of rural crime and the significant impact it had on his business.

Chief Inspector Nixon said 'Preventing, reducing and tackling rural crime is a priority for Police Scotland.

'We do this at a national level working closely with our partners from the Scottish Partnership Against Rural Crime (SPARC). The latest three-year strategy, launched in June, focusses on crime prevention, education and innovation, in addition to increasing our intelligence sharing with partners to enable effective enforcement.

'National Rural Crime Week is an important part of highlighting the work that takes place every day in our communities.'

Chief Inspector George Nixon, stressed that all crimes and suspicious sightings need to be reported:

'We can pick up useful information or sightings from one case that may help us solve another' said Chief Inspector Nixon.

'Incidents need to be reported. If you see a crime in action, it is an emergency and you must dial 999 to get an immediate response.

'Alternatively, you can call 101 or go online to the Police Scotland 'Contact Us' service for non-emergencies.'

www.scotland.police.uk/contact-us

SPARC
SCOTTISH PARTNERSHIP AGAINST RURAL CRIME

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Stonehaven Community Policing Sergeant John McOuat with local farmer Willie Officer and one of the SelectaDNA property marking kits issued by Police Scotland.

Also present at the visit were representatives from the National Farmers Union of Scotland.

Lorna Paterson, North East Regional Manager for NFU Scotland, urged farmers to report all crimes.

'Farmers need to give police information and we need these crimes recorded' said Ms Paterson.

As part of the initiative the North East Division Crime Reduction Team distributed fifty SelectaDNA forensic marking kits to farms across the North East.

Partnerships and Preventions Inspector Mark Young said 'Criminals often target isolated areas and hard-to-protect buildings looking for easily sold items such as tools and agricultural machinery. SelectaDNA products can mark such equipment and property to help prevent rural crime.

'Providing farmers with forensic marking kits and being on hand to offer face to face, practical advice on how to deter thieves forms part of our strategy to make the North East a safe environment for our rural communities.'

For further advice information regarding the Scottish Partnership Against Rural Crime visit www.scottishparc.co.uk

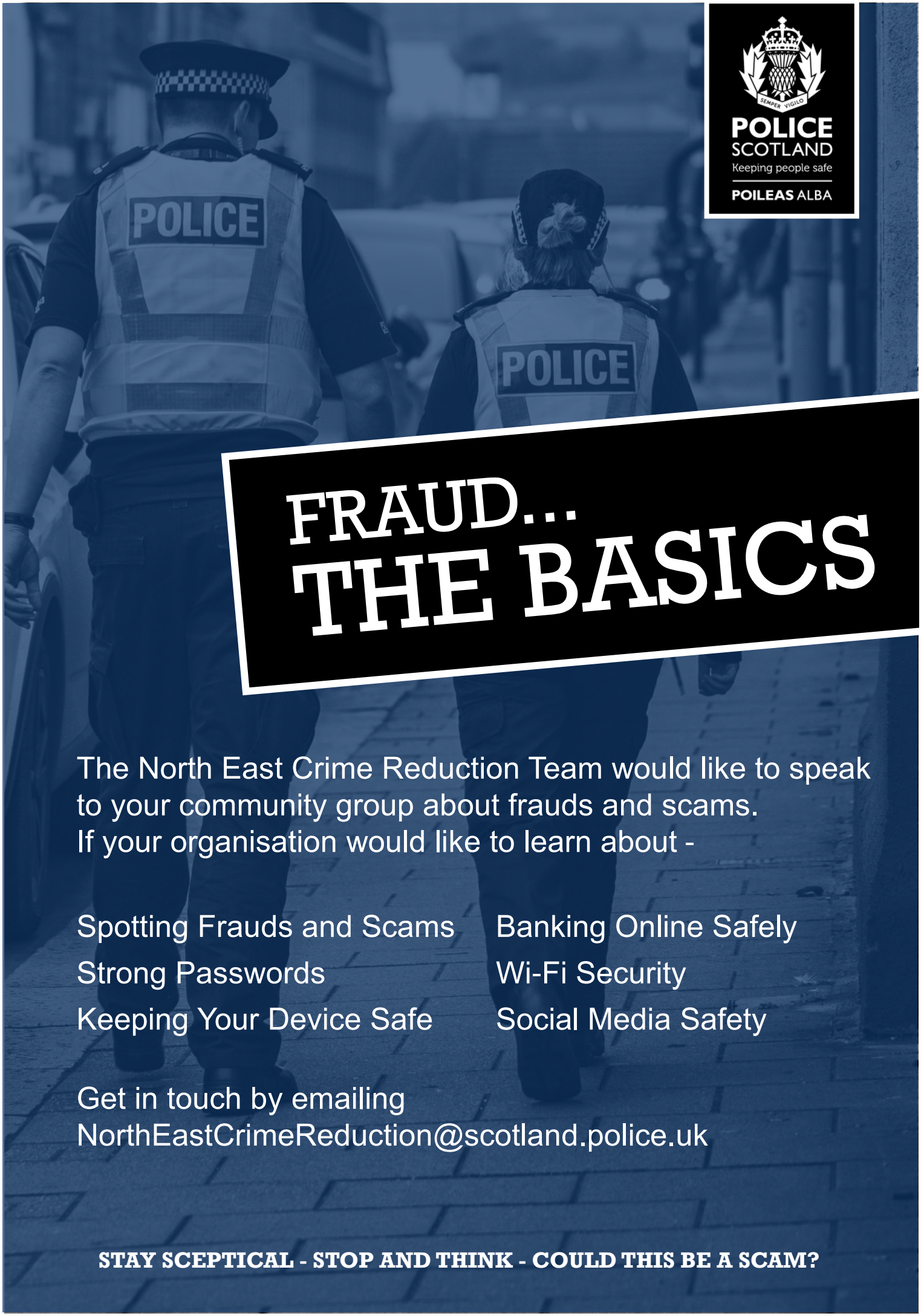
SelectaDNA property markers contain thousands of microdots. Each microdot has a DNA code unique to every kit. These codes allow police to identify property and link criminals to a crime.

UV tracers within SelectaDNA allow Police to find property that has been marked.

Police have access to the SelectaDNA database, allowing 24/7 searches when property is recovered or perpetrators apprehended.

SelectaDNA is Police accredited as 'Secured by Design.'

For more information visit www.selectadna.co.uk



POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

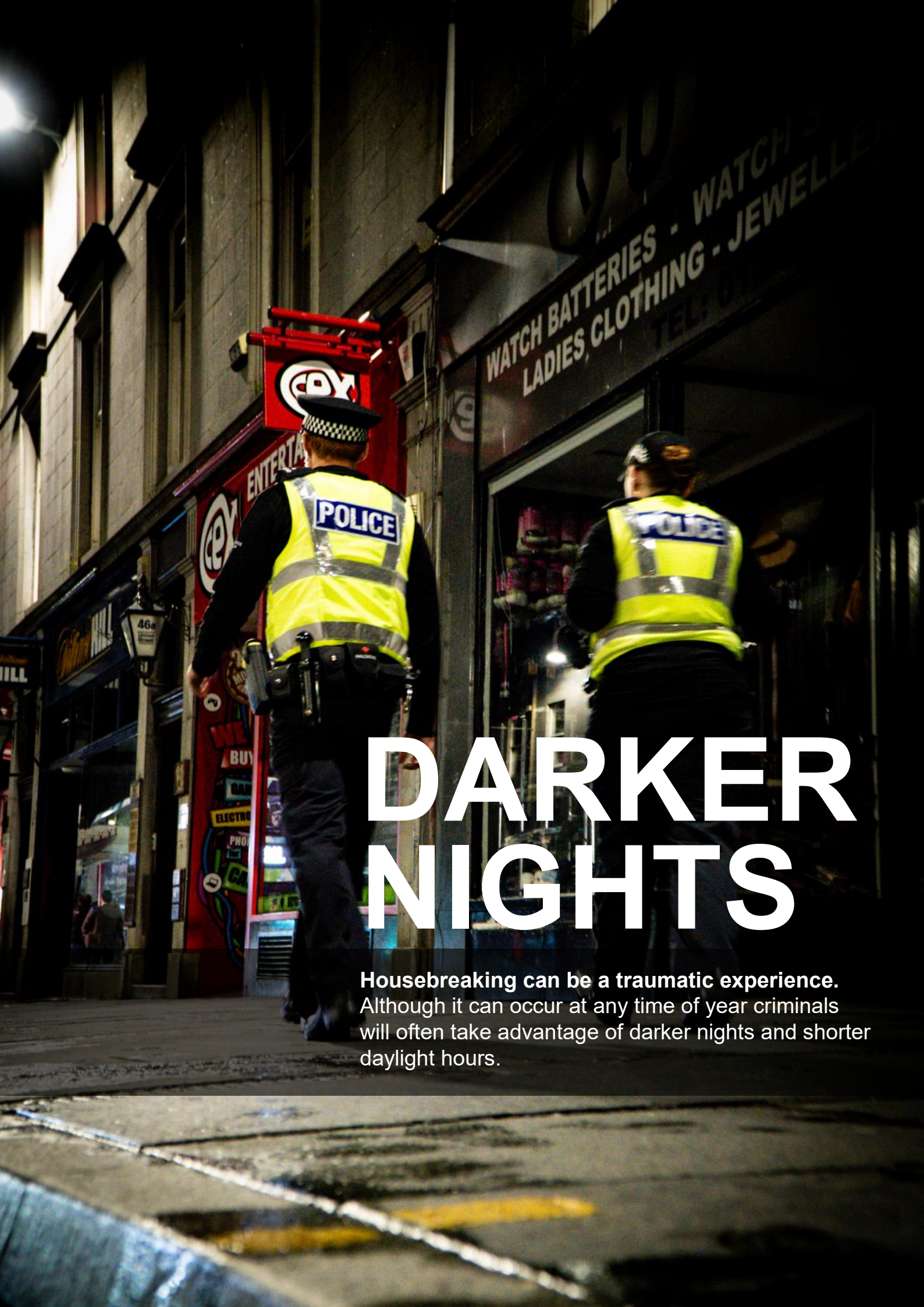
FRAUD... THE BASICS

The North East Crime Reduction Team would like to speak to your community group about frauds and scams.
If your organisation would like to learn about -

- Spotting Frauds and Scams
- Strong Passwords
- Keeping Your Device Safe
- Banking Online Safely
- Wi-Fi Security
- Social Media Safety

Get in touch by emailing
NorthEastCrimeReduction@scotland.police.uk

STAY SCEPTICAL - STOP AND THINK - COULD THIS BE A SCAM?



DARKER NIGHTS

Housebreaking can be a traumatic experience. Although it can occur at any time of year criminals will often take advantage of darker nights and shorter daylight hours.

Lock the Door
Obvious isn't it? But some people don't do it. Lock the door even if you're only out for a short time.

If you have window locks, lock those too. Keep the door locked when you are at home. This stops criminals coming in if you are in another part of the house or garden.

Don't leave your keys on the inside of locks or just inside the door. If you have a spare key, don't leave it under a mat, plant-pot or other easy to spot place at home. Never keep house keys and car keys on the same ring.

Safes and Security Boxes
Don't keep large amounts of gold, jewellery and cash at home. Bedrooms and lofts are routinely searched during housebreakings, particularly if the occupants are celebrating a cultural festival.

Consider storing valuable items at your bank. Private companies offer similar services. If this option is unavailable consider an insurance rated safe. Safes should be securely attached to the solid fabric of the building not just to a plasterboard wall or left sitting on the floor. Ideally get an insurance approved installer to fit a safe in your home.

Lighting and CCTV
House alarms and CCTV are a great visual deterrent. Modern Wi-Fi enabled CCTV systems can be combined with bright LED lighting. Any movement detected outside your home can trigger an alert to a number of mobile devices.

If considering CCTV look to cover every aspect of your home. Small discreet cameras can also be used inside. Use signage to advise that CCTV is in use.

When you're away use timers to turn on lights, radios, or TVs to put off unwanted visitors. Smart plugs allow times to be changed even whilst away.

Vehicles
High value cars are particularly vulnerable to theft and criminals will commit a housebreaking to obtain the true key of the vehicle. Where possible park vehicles inside a garage. Secure the keys inside your property out of sight. Avoid leaving them in obvious locations such as the hallway table or kitchen. Never leave valuables in your car.

Keyless Theft or Relay Theft involves criminals using hand held technology to identify whether a parked car has keyless entry. If the car 'key' is close enough the criminals can amplify the signal and send it to a transmitter which acts as the true key and opens the car allowing it to be driven off. Keep keys and fobs well away from doors and windows and purchase a signal blocker wallet to keep them in.

Property Marking and Insurance
There are a number of products you can buy which contain a unique code like DNA. This code is registered to your address. They are usually clear liquids which can be applied onto your possessions.

Check you have adequate insurance cover. Photograph and record your valuables to assist any insurance claim or Police report. This will assist police in identifying any items recovered.

General Maintenance
Never leave anything that can be used by a thief to gain entry lying around the garden. Overgrown bushes prevent neighbours seeing into your garden and allow criminals to go unseen.

Social Media
Consider what you are putting on social media, especially if you are going on holiday or attending weddings, functions or posting pictures with jewellery. Criminals search for this information to create a list of empty houses. Your social media accounts should be set to friends only.

Attached to this month's North East Crime Alert is a copy of the new Darker Nights Housebreaking Prevention Advice leaflet.

Rural Properties

Harden your perimeter. Consider one point of entry/ exit and secure with a good quality steel gate whilst taking into account any access rights.

Install Adequate Lighting. Well-placed outdoor lighting can deter criminals and help you spot them if they do approach your property.

Secure Outbuildings. Lock barns, sheds, and other outbuildings. Ensure all external doors are well maintained and fitted with good quality locks.

Remove keys from vehicles. Don't make it easy for criminals, always remove the keys and where possible lock them away in secure cabinets.

Mark your property. Keep a record of all tools and equipment with photographs and serial numbers. Consider using a DNA marking product such as Selecta DNA.

Secure your fuel. All fuel tanks should be fitted with locking fuel caps. Locate tanks away from roads, so not to be seen from passing traffic.

Unusual Activity
Report any unusual activity to Police. Criminals will often call offering to carry out work in order to identify vulnerable targets.

Neighbourhood Watch Scotland Alerts help you stay up to date with the latest crime, safety and resilience news for your local area. To receive free alerts and download a copy of the Safer Neighbourhoods Safer Communities booklet go to

www.neighbourhoodwatchscotland.co.uk

Police Scotland Youth Volunteers

Are you aged between 13 and 15 years old and would like to volunteer in your community? Read about how you can gain valuable skills and support your local policing team.

Police Scotland Youth Volunteers (PSYV) promote a practical way for young people to understand policing by supporting the Police in their local area through volunteering. As part of this, young people are given a chance for their voice to be heard and encouraged to promote good citizenship.

The programme gives young people of all backgrounds a positive means of engagement with the police service. Through regular training and participation in community safety initiatives, youth volunteers are given opportunities to overcome barriers and discover their talents whilst making a positive contribution to their communities.

PSYV North Aberdeenshire Co-ordinator Constable Sarah Grant said 'The Police Scotland Youth Volunteers Programme gives young people an insight into policing in Scotland and inspires them to participate positively in their communities.'

If you are aged between 13 and 15 years old you can register your interest. You must attend weekly sessions and attend regular volunteering events in your community and occasionally other parts of the country. Places are limited and in high demand.

You can register your interest at www.scotland.police.uk/secureforms/psyv-recruitment

Shop safely online this Christmas

Criminals use web-enabled fraud to steal our money and personal details. Follow our advice to purchase items safely and avoid fraudulent websites over the festive period.

Chose carefully where you shop
It's worth doing some research on online retailers to check they're legitimate. Read feedback from people or organisations that you trust, such as consumer websites. Reputable organisations will have information on their website about how they handle your personal data (which should only be used to fulfil your order, and not shared with third parties).

Some of the emails or texts you receive about amazing offers may contain links to fake websites. If you're unsure, don't use the link, and either:

- type a website address that you trust directly into the address bar
- search for it and follow the search results

Use a credit card for online payments
Use a credit card when shopping online if you have one. Most major credit card providers protect online purchases and are obliged to refund you in certain circumstances. Using a credit card (rather than a debit card), also means that if your payment details are stolen, your main bank account won't be directly affected.

You should also consider using an online payment platform, such as PayPal, Apple Pay or Google Pay. Using these platforms to authorise your payments means the retailer doesn't see your payment details. They also provide their own dispute resolution should anything go wrong. However, they may not provide the same protection as a card provider, so check their terms and conditions before you sign up.

When it's time to pay for your items check there's a 'closed padlock' icon in the browser's address bar. It will look like this:

The padlock icon doesn't guarantee that the retailer itself is legitimate/reputable (and that their website is secure). It means that the connection is secure.
If the padlock icon is not there, or the browser says not secure, then don't use the site. Don't enter any personal or payment details or create an account.

Only provide enough details to complete your purchase
You should only fill in the mandatory details on a website when making a purchase. These are usually marked with an asterisk (*) and will typically include your delivery address and payment details. You shouldn't have to provide security details to complete your purchase.

The store may also ask you if they can save your payment details for a quicker check-out next time you shop with them. Unless you're going to use the site regularly, don't allow this. Finally don't pay by direct bank transfer.

Keep your accounts secure
If you're using the same password for your online accounts (or using passwords that could be easily guessed) then you're at risk. Hackers could steal your password from one account and use it to access your other accounts. For this reason, you should make sure that your really important accounts (such as your email account, social media accounts, banking accounts, shopping accounts and payment accounts like PayPal) are protected by strong passwords that you don't use anywhere else.

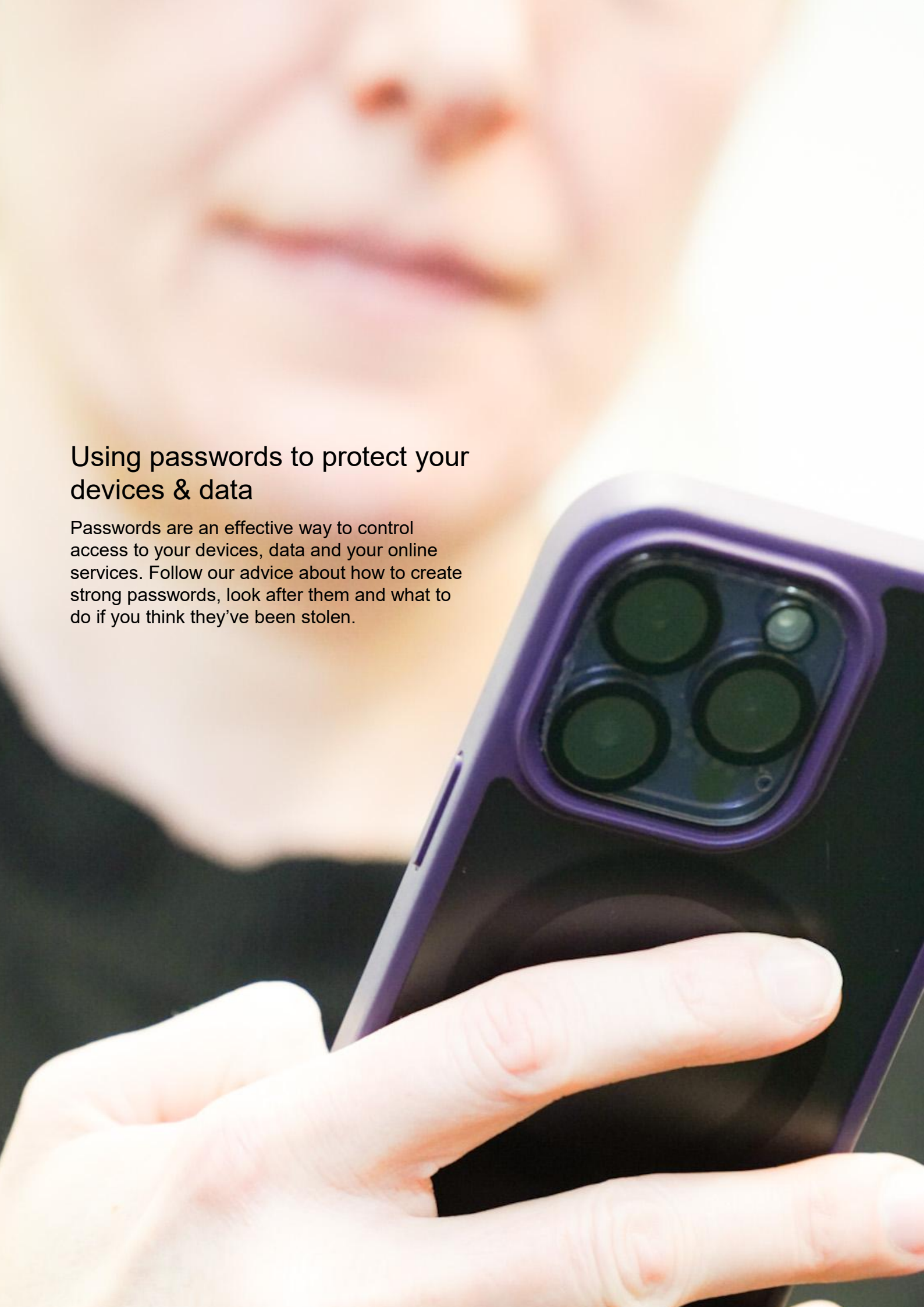
The trouble is that most of us have lots of online accounts, so creating strong passwords for all of them is hard - **read our article on page 15 about how to create and store passwords.**

You can further protect your important accounts from being hacked by turning on 2-step verification (2SV). It's also referred to as 'two-factor authentication' or 'multi-factor authentication'. Turning on 2SV stops hackers from accessing your accounts even if they know your password. It does this by asking you to confirm that it's really you in a second way - usually by asking you to enter a code that's sent to your phone.

Watch out for suspicious emails, texts and websites
You'll probably receive many messages from online stores, as a result of 'opting in' to receiving communications from them. Lurking amongst these genuine messages, there may well be fake ones (containing links designed to steal your money and personal details) that can be very difficult to spot.

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at **report@phishing.gov.uk**

If you've received a suspicious text message, forward it to **7726**. It won't cost you anything and allows your provider to investigate the text and take action (if found to be a scam).



Using passwords to protect your devices & data

Passwords are an effective way to control access to your devices, data and your online services. Follow our advice about how to create strong passwords, look after them and what to do if you think they've been stolen.

How do criminals get hold of passwords?
Passwords are often stolen when an organisation holding your details suffers a data breach. Criminals use the stolen passwords to try and access your other accounts. This page contains tips about how to create strong passwords, how to look after them and what to do if you think they've been stolen.

They will also

- try to access accounts using obvious passwords that many people still use (like 123456)
- pretend to be somebody 'official' such as a bank, the NHS, or a government department and trick you into revealing your password
- use sneaky techniques on social media (such as tricking you into sharing an SMS code)
- trick you into revealing passwords by creating fake phishing emails (or SMS messages) that link to scam websites This is why you should avoid re-using the same password for different accounts and not use passwords that a criminal can easily guess.

Create strong passwords
The more unusual your password is the harder it is for a criminal to guess.

- Combine three random words to create a single memorable password (for example CupFishBiro).

  By using a password that's made up of three random words, you're creating a password that will be 'strong enough' to keep the criminals out, but easy enough for you to remember.

  Longstanding advice around making your passwords very complex (which suggests we should create passwords full of random characters, symbols and numbers) is not helpful. This is because most of us have lots of passwords and memorising lots of complex passwords is almost impossible.

  Passwords generated from three random words is a good way to create unique passwords that are 'long enough' and 'strong enough' for most purposes, but which can also be remembered much more easily. If you want to write your password down, that's also OK, provided you keep it somewhere safe.

- Use a password manager app to create strong passwords for you (and remember them).
- Don't use predictable passwords (such as dates, family and pet names) or ones that criminals can easily guess (like '1234').
- If your smart device comes with a default password (like 0000), change it immediately.

Protect your email account
Use a strong and unique password for your email account. If a criminal accesses your email, they could:

- use it to access to all your other accounts
- access information about you (including banking and social media details)
- send emails and messages pretending to be from you

Look after your passwords
Storing your passwords safely means you won't have to remember them, so you can use strong ones:

- Most web browsers will offer to save your passwords for you. It's safe for you to do this (unless you're using a shared computer outside your home, for instance at college or a library).
- Password manager apps are a safe way to store passwords.

What to do if your password is stolen?
If you think your password has been stolen, or if it appears in any 'worst password' lists, change it as soon as possible.

Indicators of a stolen password include being unable to log in or messages sent from your account that you don't recognise.

To check if your details have appeared in public data breaches you can use online tools such as

www.haveibeenpwned.com.

Similar services are often included in antivirus or password manager tools.

For more information visit cyberaware.gov.uk

Scam Update

Crypto Scams

The world of cryptocurrency can sometimes promise high returns and financial freedom. But behind these promises often lurk sophisticated scams designed to steal your money.

How the Scam Unfolds

The Hook
The victim clicks on an enticing advert on social media, fills in a form with their contact details, and is quickly contacted by a friendly, professional-sounding individual. They'll use a seemingly legitimate company name and a professional tone to gain trust.

The Initial Investment
The scammer will persuade the victim to make a small initial investment. They'll set up an online account for the victim, which shows a small balance and some impressive-looking graphs. At this stage, your money is not invested; it has been stolen.

The 'Financial Advisor'
A new person, a so-called 'financial advisor,' will take over. They will guide the victim through setting up a legitimate crypto exchange account. They'll instruct the victim to transfer money into this account and then to a specific 'wallet address' for the scammer's fake company.

The Illusion of Growth
The scammer's website will show the victim's investment growing rapidly, sometimes to tens or even hundreds of thousands of pounds. This is a complete fabrication designed to build false confidence and make the victim believe their investment is genuinely successful.

The Withdrawal Trap
When the victim asks to withdraw their supposed earnings, the scam begins to escalate. They'll be told they must pay various fees to access their money. The fees are often a percentage of the fake balance, making them seem reasonable to the victim.

The Final Push
As the victim pays more and more fees, the scammers apply pressure and use emotional manipulation. They might claim that the withdrawal is at risk or that they could lose everything if they don't pay the next fee. They may even disappear for a while or change contact details to cover their tracks. The money paid for these fees is another loss for the victim.

The Hard Reality
Eventually, the scammer's website vanishes, the advisor disappears, and the victim is left with nothing. The money they believed was growing never existed. Their total loss includes all the initial investments and every single fee they were manipulated into paying.

How to Protect Yourself from Crypto Scams

- Be Sceptical of Social Media Adverts. If an advert seems too good to be true, it almost certainly is. Ignore adverts that promise high returns with little to no risk.
- Before investing, thoroughly research any company or individual. Check for reviews, warnings, or reports of scams online.
- Legitimate investment companies do not require you to pay fees to withdraw your own money. If you are asked to pay an upfront fee to access your funds, it is a scam.
- Legitimate financial advisors will not contact you out of the blue on social media platforms like WhatsApp.
- Never give control of your bank accounts or crypto wallets to anyone. Be suspicious of anyone who pressures you to act quickly or to open new accounts to make transfers.

If you believe you have been a victim of a cryptocurrency scam report it immediately to your bank and to Police Scotland via 101.

Crime Alert

A selection of crimes affecting residents
from across Grampian

Sextortion Fraud
An Aberdeen victim met a fraudster on an online chatroom. After a brief period, they shared explicit images. The fraudster threatened to share the images so the victim paid £750.

Stolen Motorbike
On 18 September a black and white Sinnis Shuttle motorbike was stolen from Damway Head, Peterhead.

Investment Fraud
A North East resident was contacted by scammers claiming to be investigating online fraud. The victim was convinced to move his savings into 'safe' ISA accounts and lost £165,000.

Theft by Housebreaking
A man has been charged following a break-in to a residential property on Linn Avenue, Buckie on 8 October.

Theft of Plant Machinery & Tools
Plant machinery and tools were stolen from a secure yard on Harlaw Drive, Inverurie. Items stolen include an Ifor Williams, tipping trailer, Stihl saws, Belle petrol cement mixers, petrol generators and drills.

Drugs Recovery, Aberdeen
A 25-year-old man has been arrested and charged following the recovery of class A drugs in Aberdeen. The man was found in possession of cocaine with an estimated street value of £29,500.

Stolen E-Bike
A black Talaria Komodo e-bike with distinctive gold suspension bars was stolen from a locked shed in Jarvis Place area of Fraserburgh between on 24 September.

Drugs Recovery, Moray
A 16-year-old male and a 53-year-old male have been arrested and charged in connection with the seizure of cannabis in the Urquhart area, near Elgin.
The recovery has an estimated street value of around £73,000.

Puppy Deposit Fraud
An Aberdeenshire resident has become the latest victim of a puppy deposit scam. The victim saw Dachshund puppies 'for sale' online. After paying a deposit the seller stopped all contact.

Theft and Recovery of Quad Bikes & Tractors
A 31-year-old man has been arrested and charged following the theft of quad bikes and tractors from various rural farm locations in the Huntly and Alford areas.
The vehicles were recovered in the Durham area.

Safe Account Fraud
A Portlethen resident lost £500 after being contacted by a male claiming to be from his bank.
The caller told the victim that his account had been compromised and that he needed to transfer his funds into a new account to secure his money.

Marketplace Fraud
A farmer from the Tarland area lost £700 after sending a deposit for a trailer advertised for sale on Marketplace. The seller failed to respond after the money was sent.

Sim Swap Fraud
An Aberdeen resident changed mobile suppliers for what they believed was a better deal.
The deal was a fraud and they lost £14,000; spent on a credit card by fraudsters.

Bike Theft
A cyclist returned from a trip and left their insecure mountain bike on the roof of their car. The bike, worth £2500, was stolen overnight.

Investment Fraud
An Aberdeen resident who was the victim of an investment scam was contacted by a company claiming to be able to return their money. This claim was also a scam and the victim lost £40,000 in total.

Bitcoin Fraud
A North East resident was lured by a fraudulent advert on social media for Cryptocurrency investment and lost £23,000.

Facebook Celebrity Fraud
An Aberdeen resident followed an online personality via Facebook. They were contacted by fraudsters claiming to be the personality and became 'friends.' After a period of time the victim was asked to assist financially and lost £12,000.

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