

North East

# CRIMEALERT Keeping Communities in the North East Safe









## Welcome to the October 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:

We explain how to secure your campervan and avoid purchasing a stolen caravan.

Relay theft is on the increase across the UK. How do you secure your vehicle and avoid becoming a victim of this keyless crime?

An Aberdeen resident shares her harrowing experience of how she became a victim of investment fraud.

Scottish Land and Estates and Aberdeenshire Council, both members of the North East Partnership Against Rural Crime, explain some of their functions.

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

Website
www.scotland.police.uk



Twitter
www.twitter.com/
NorthEPolice



Facebook www.facebook.com/ NorthEastPoliceDivision

> 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.



### Motorhome and Campervan Security

Your motorhome or campervan is a significant investment and unfortunately they are a popular target for thieves. Not only are they valuable in their own right but they are often filled with expensive contents.

Remember simple precautions like closing windows, locking all doors when you are away from the vehicle, and never leave valuables on display. Try not to leave your motorhome unattended for long periods of time.

Your insurer may require additional security measures be installed such as an alarm, immobiliser or tracking device. Some insurers will specify what device you will be required to install.

There are a wide range of options on the market to secure your motorhome and reduce the risk of theft.

#### Wheel clamps

Are a good visible deterrent. Look for a good rating from a recognised testing house such as Sold Secure to make sure it's built to withstand attack.

#### Steering wheel locks

Can be a bar-lock, circular lock or even a chain and padlock. Whichever you choose, steering wheel locks are another visual deterrent.

#### **Alarms**

Is an audio deterrent for your motorhome and will often be fitted in the base vehicle. The alarm usually comes with a window sticker which you can position appropriately to advertise that your vehicle is alarmed, thereby encouraging the would-be thief to move on.

#### **Immobilisers**

Again, this device is often found as part of the base vehicle. It is particularly helpful if a thief gains access to your motorhome, by preventing them from driving away. Each time you switch off your engine, the immobiliser activates automatically.

#### **Trackers**

If you're unfortunate enough to have your motorhome stolen, a tracker will send your vehicles location back to a control centre or your mobile device. Remember to keep the subscription active.

#### Keys

Keep key fobs in a Faraday bag or shield that blocks signals and never keep a spare set of keys in the motorhome, even while on holiday. Remember to keep your spare fob in a protective bag as well. Never keep keys next to the front door or obvious places like a kitchen drawer.

#### **CCTV**

CCTV can be a great deterrent to potential criminals as well as offering you peace of mind. It can also help the Police with investigations. 4G cameras which relay images and notifications to your mobile device can be fitted inside your motorhome providing coverage no matter where your vehicle is located. Make sure you know how to review footage if a crime has occurred. Inward facing dash cams are also available,

#### Locker doors

Locker doors are a common weak point. Doors leading to underbed spaces with an interior hatch or under lounge seats, should be protected with extra locks.

#### Pedal box

Pedal boxes are designed to prevent vehicle theft by blocking access to the van's pedals. The box encloses the pedals, making it impossible for anyone to operate the vehicle without the correct key or combination.

#### **Security posts**

Security posts are worth considering but their value depends on their location. A post will have little effect in front of a van if the rear is only protected by a flimsy fence. Thieves don't care what they destroy to remove a vehicle. Posts need to be securely fitted into the ground.

Whichever security device you chose most insurance providers will insist the product is approved by either Sold Secure or Thatcham.

#### Remember

If you have an alarm or tracking system, pay for the subscription and use it.

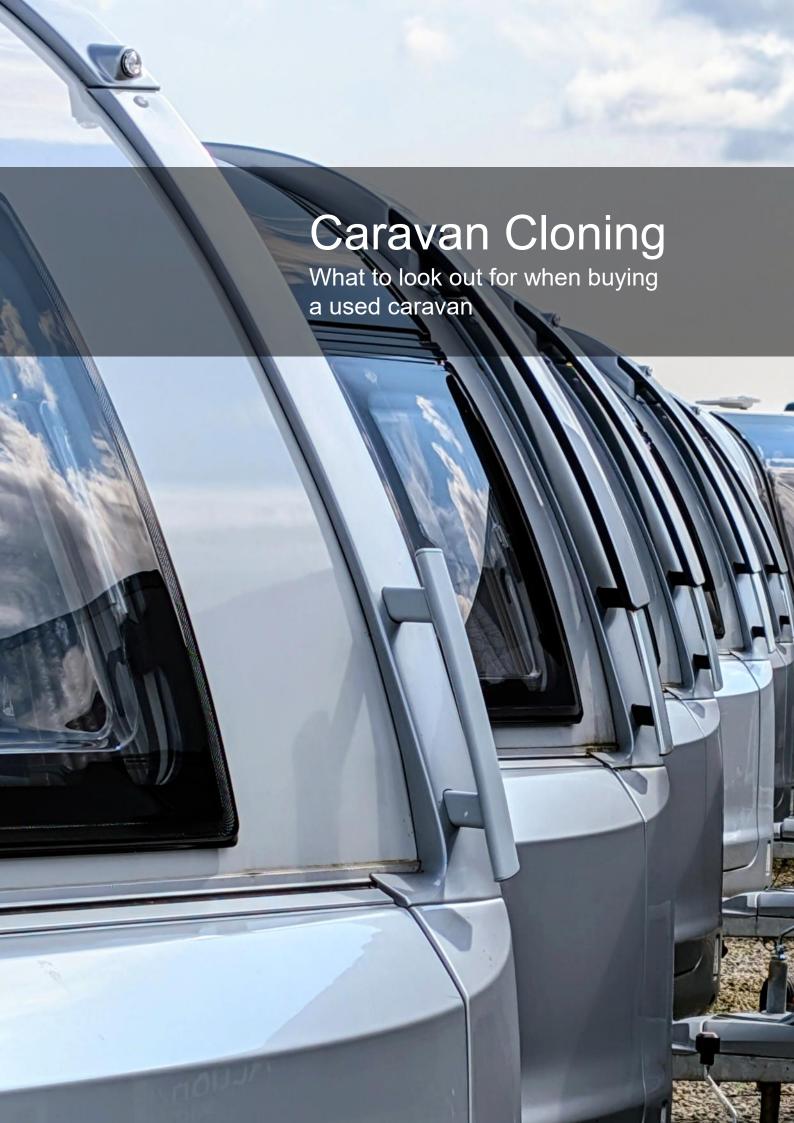
Fit visible physical devices that deter thieves.

Improve driveway security with bollards, lights and CCTV.

Add extra security to all doors, especially locker doors if they lead to the motorhome interior.

Apply window stickers to warn potential thieves there are security devices in use.

Don't leave registration documents in your camper. They can help thieves sell your vehicle.



Like campervans and motorhomes, caravans are an attractive target for thieves. They are relatively easy to steal and social media sites are awash with caravans for sale privately. So how do you check the caravan you are purchasing hasn't been stolen?



Caravans have a VIN number located on the chassis as well as ID labels such as QR codes produced by CriS and VINCHIP.

CRiS is the National Register of UK touring caravan keepers, similar to the DVLA, and is recognised by the regulatory bodies, insurance companies and Police forces.

Criminals however will commonly use fake VIN Chip caravan identification labels, coupled together with the manipulation of the stamped in number, and the production of a false manufacturer's chassis plate to give a cloned identification.

#### How it's done

Criminals are known to alter one or two of the last digits in the stamped in chassis number sequence. To support the false identification, the genuine VINCHIP markings are either removed, defaced or overlaid with false ones. These alterations are designed to make the caravan appear genuine.

The new buyer will be unable to register the caravan with CRiS, as security checks will reveal that the genuine caravan is elsewhere. Anyone who purchases a stolen caravan will not be the lawful owner and will risk it being seized or recovered. It is possible that this scam may not come to light until the caravan is next registered with CRiS.

#### **Advice**

Scan the VinChip QR code on the label fitted to the habitation door or the window next to it. (There is also a repeater QR- Vin label in the gas locker).

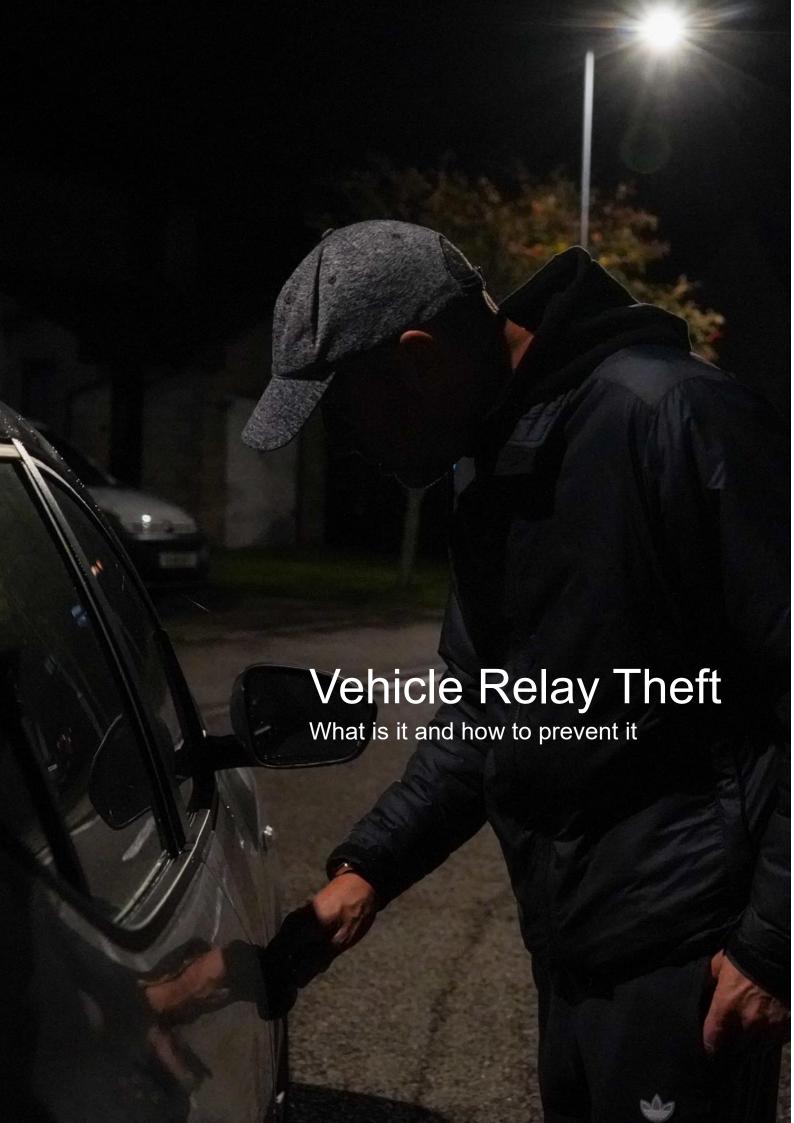
Check the URL for the secure link to CRiS. It should show the VIN number displayed on the label and direct you to the record showing make, model and colour which should match the caravan being checked.

If the URL displays SGBSG06BY70703016, and directs to a fake holding page showing error code 404-Page not found it is a fake record, designed to look like a communication fault.

Scanning a QR code that directs to 'Samsung' or the CRiS homepage rather than displaying the caravan details is fake.

If these errors are discovered the caravan will require its embedded RFID chips to be read using a CRiS handheld scanner to confirm its correct identification. Closer examination of genuine VINCHIP labels will also reveal multi-layer security features so that they can be distinguished from the fakes.

CRiS (Central Registration Identification Scheme) can provide a history check on new and pre-owned touring caravans.



Like the rest of the UK, the North East has seen an increase in the theft of motor vehicles, without forcing entry or the use of the actual true key.

## This is known as 'Relay Theft' and normally effects vehicles that operate with keyless entry.

Keyless entry allows the owner to get into their car and start it without pressing any buttons, as long as they have the vehicle fob with them.

Thieves use a device to relay the signal broadcast between the contactless key and the car. The car is tricked into thinking the key is close and unlocks the door. Typically, the relay device only needs to be within 10-15 metres of the key to work. The car will continue to run without the key until the engine is turned off.



#### How to prevent relay theft

Use a Faraday box or wallet to block any signal being sent or received by your car keys and get into the habit of always putting your keys in such a box when you return home. Make sure your spare key is also stored in a Faraday box or wallet.

The material used in Faraday pouches deteriorates over time so double-check the effectiveness of your Faraday pouch by checking it periodically. Another option is storing your keys far away from your car in a fully enclosed metal box.

Never store your vehicle keys next to the front door.

Turn off keyless ignition if possible (manufacturer dependant).

Use a mechanical security device such as steering or pedal lock.

Consider an OBD port lock (the OBD port is the diagnostic port inside your car which is often used by criminals to target the vehicle electronic systems).

Park in well-lit areas with CCTV coverage.









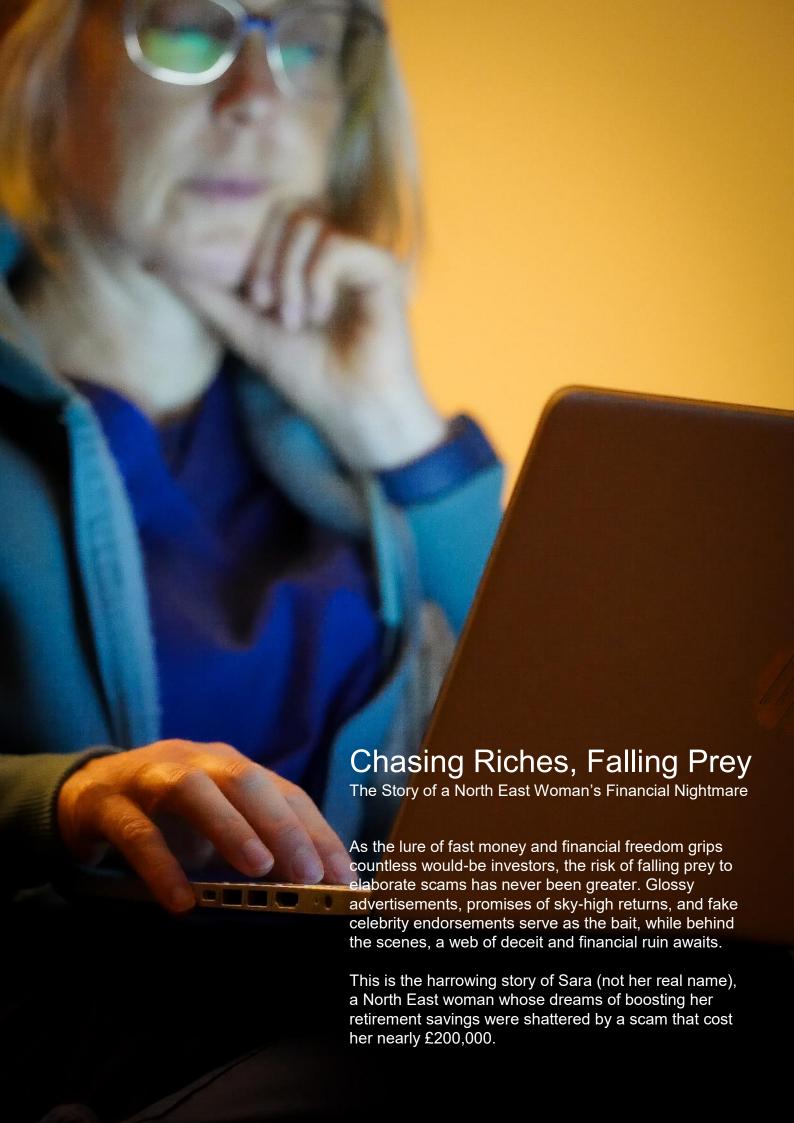
## Visitor Management Initiative

# Meet and Greet

Throughout the summer officers in Deeside were working with Rangers from a number of partner agencies to 'meet and greet' visitors to the area. As well as tackling anti social behaviour the initiative is designed to advise visitors on the best places to camp whilst promoting responsible behaviour in our beautiful countryside.

If you intend to enjoy some time in the great outdoors please familiarise yourself with the The Scottish Outdoor Access Code and follow the advice given by local Ranger services.





Sara, in her 50s and looking ahead to her retirement, was searching for ways to make the most of her savings. She had been financially responsible, with money set aside and the ambition to clear her mortgage. Like many, she turned to the internet, researching investment opportunities to help bolster her retirement fund. She discovered companies boasting celebrity endorsements from names like Elon Musk and Martin Lewis—trusted figures in the world of finance. Sara felt reassured enough to make contact.

Soon after, Emma (also not her real name), a female representative from a so-called investment firm, reached out. She was knowledgeable, friendly, and spoke perfect English despite being based somewhere in Europe. Emma's easy-going demeanour made Sara feel comfortable, and she explained the complexities of the financial markets in a way that was both clear and enticing. With £10,000 earmarked for investment—money Sara could afford to lose if the worst happened—she began her journey into currency trading with Emma's guidance.

Excitement mounted as Sara watched her investments grow. Daily updates from Emma, along with regular calls, fostered a growing sense of trust. Soon, the conversation turned to new opportunities: gold and silver, and eventually, a more advanced strategy known as the 'Gaps' market, which involved buying and selling when markets were closed before they reopened. Encouraged by her successes, Sara began to feel confident. In just one week, she 'earned' £7,000.

As Emma guided her toward bigger risks, Sara felt compelled to follow her advice. After all, it was working. At Emma's suggestion, Sara took out a £25,000 loan to capitalise on what seemed like a golden moment to invest. Positive reviews on Trustpilot, combined with her growing balance—now £100,000—eased any lingering doubts. Emma, by this point, had become more than just a financial advisor; she was a friend. They shared regular conversations, with Sara even considering flying out to meet her.

However, as Sara's investment pot grew, so too did the pressure from Emma. The tone of their relationship shifted. Now, it felt less like advice and more like coercion. Emma warned that if Sara's investment balance dipped below 75%, she stood to lose significantly. The pressure mounted, and when her account began to fall, Sara was bullied into taking out more loans to 'bridge the gap.

Desperate to protect her funds, Sara asked to liquidate her account and withdraw her earnings. It was then that she was introduced to James (again, not his real name), the company's so-called 'Finance Director.' James laid out a series of hurdles Sara would have to clear before accessing her money. The first was a 20% liquidation

fee—an eye-watering £20,000. The transaction, Sara was told, would need to be processed through a cryptocurrency exchange, adding a layer of complexity she hadn't anticipated. The fees continued to mount—trading costs, solicitor fees, all explained convincingly by James. What started as a helpful partnership now felt more threatening.

James, while persuasive, also had a darker side. He was forceful, at times even threatening, and his narcissistic tendencies began to reveal themselves. The ever-growing list of fees seemed endless, and when a solicitor handling her case became ill, yet another lawyer was assigned to Sara's account. She continued to pay, believing each payment brought her one step closer to reclaiming her funds. But every week brought new demands, and every conversation with James left her feeling more trapped.

She was now transferring money through cryptocurrency platforms like Kraken, hoping to recover her funds. But as she wired £25,000 from one 'partner' to another, silence descended. The once-helpful Emma and James had gone quiet. Sara's emails and calls were ignored, and a sinking feeling set in—she had been scammed.

Desperate to claw back some of her money, Sara turned to the internet once again, this time in search of companies specializing in cryptocurrency fraud recovery. After reading countless reviews, she found one firm that seemed trustworthy. They had glowing feedback, and after a lengthy explanation of their process, Sara paid \$600 as an initial fee. Within days, she was told they had located \$143,000. It seemed like a lifeline.

But it wasn't long before the demands for more money resumed—\$1,200 to release her funds, then \$2,000 for malware removal, then an additional \$3,000 for other expenses. A series of small test payments trickled into Sara's account, enough to keep her hopeful. But the rest never arrived.

As if the situation couldn't worsen, her bank's fraud team contacted her. They suspected Sara of criminal activity due to the movement of large sums of money through her account. She was given 60 days to close her accounts, leaving her financial future in tatters.

Today, Sara is left with a staggering £200,000 loss. Loans, savings, and a portion of her pension—gone. What began as an exciting venture to build her retirement fund has turned into a nightmare of debt, deceit, and shame. Though she has the support of her family and friends, Sara knows the harsh reality: she will never see that money again. For her, and many like her, the promise of financial freedom came at an unimaginable cost.



This summer the North East Crime Reduction Team partnered with officers from Trading Standards and the Royal Bank of Scotland to raise awareness of frauds and scams.

The national initiative, utilised the 'scam van,' and saw partners visiting villages across the North East such as Forres, Dufftown, Ballater and Turriff.

For more information on how to avoid becoming a victim of fraud visit www.scotland.police.uk











6 Secure and lock farm buildings against intruders

\*Contact your local crime prevention officer for more information





SLE is a membership organisation and our vision is to make a prosperous and sustainable future for rural Scotland, delivering publicly and politically recognised measurable benefits for society, the economy and the environment, with a focus on people, jobs, and nature.

From campsites to community owners to country estates, our members represent a diverse community passionate in promoting rural Scotland, and we've acted as their voice for over 100 years.

Our members have businesses or interests in these vital areas, and we help them to prosper through the knowledge, advice and relationships we're able to provide.

#### Wildlife Management and Muirburn (Scotland) Bill

The introduction of the Wildlife Management and Muirburn (Scotland) Bill which came into effect earlier this year, aims to regulate how certain wild birds and wild animals can be captured or killed.

The bill denoted a seismic shift in how grouse moor management operates. Estates wanting to shoot grouse now require a licence which will run for a period of up to five years. Muirburn and certain wildlife traps will also be subject to separate licensing regimes.

The licensing framework introduced by the 2024 Act, came into force in July 2024 and provides for suspension or revocation of a licence where the licence holder or a person involved in managing the land to which the licence relates:

- (A) has committed a relevant offence on the land, or
- (B) has knowingly caused or permitted another person to do so.

SLE and its members have engaged constructively with MSPs, the Scottish Government and NatureScot to ensure that the grouse moor licensing scheme is as workable and proportionate as possible, in order for Land Managers to continue delivering the decisive benefits for a range of species, including raptors.

SLE welcomed the results of the recent Raptor Transect Survey project, now in its fourth year and administered by the Game & Wildlife Conservation Trust (GWCT) for Scotland's Regional Moorland Groups.

The project is in its early stages but we can compare this year's numbers to those that were collected previously. Preliminary review show that there were 523 individual raptor records submitted by the surveyors from 15 transects, compared to 484 records on 16 transects in 2023.

This year there was an increase in Golden Eagle records, from 26 to 59 - more than double the number recorded in 2023. This was most obvious on the Grampian and Angus Glens transects, accounting for just over half of the total Golden Eagle records this year. Red Kite records also increased from 63 to 86, Hen Harrier records increased from 4 to 12, similar to those for Peregrines.

#### **Licensing for Muirburn**

SLE work closely with the GWCT Muirburn Advisory Service, which is designed to support estates in developing and monitoring simple, user-friendly muirburn plans. We can provide specialist advice to help, evaluate and manage risk of harm to the environment from muirburn activities and ensure that management complies with best practice and meets any statutory restrictions.

Scottish Land and Estates are members of the North East Partnership Against Rural Crime.



The North-East of Scotland has some of the most stunning heritage in the world. Currently there are records of just over 62,000 sites across the region, with hundreds more being added every year. These sites range from the earliest human presence in Scotland from around 14,000 years ago through to the defensive remains of World War II. Protecting these sites for future generations is vitally important. While the local authorities, Police Scotland, Historic Environment Scotland, and the Treasure Trove Unit work together to help protect and manage these sites, everyone can contribute, especially landowners.



Our heritage, whether it be upstanding castles or buried prehistoric settlements, are a finite resource. Once they, or the artefacts associated with them, are gone, their value in telling the story of who we are is lost. Many people own and use metal detectors – as individuals, as members of clubs, or on archaeological projects. Responsible metal detecting has an important part to play in researching our past. It can help identify unknown archaeological sites and locate historic finds.

However, poorly planned metal detecting can damage sites and even cause criminal damage. Some archaeological sites are protected by law and metal detecting on them is an offence. Detectorists are legally obliged to report all finds to Treasure Trove, and not take them out of Scotland without permission.

Landowners must always be asked for permission before metal detecting happens. Some organisations and landowners are happy for detecting, while others have a strict policy against such activity, such as Aberdeenshire, Aberdeen City and Moray Councils, as this helps to protect public spaces. Remember that help and advice is always available, starting with your local authority Archaeologist

(archaeology@aberdeenshire.gov.uk) or the Treasure Trove Unit (treasuretrove@nms.ac.uk).

There are three important things to remember:

If someone is metal detecting on land without permission, or causing damage to crops etc, speak up, it is criminal damage. It's important to everyone that we know who is harming our heritage. Report incidents via CrimeStoppers 0800 555111 or the Police.

Finders have no ownership rights to objects which have not been reported to the Treasure Trove Unit, and landowners have no property rights to finds unless they have a private agreement, in writing, with the detectorist. Be aware that any payment made by Treasure Trove will be to the finder alone.

Nearly all finds in Scotland are subject to Treasure Trove. They do not have to be made of precious metals. You must report your finds within one month of finding them.

Further guidance on responsible metal detecting in Scotland is now available online from Historic Environment Scotland. It has been developed in partnership between organisations as part of the effort to reduce heritage crime, to raise awareness of the issues for landowners, and to promote how everyone can enjoy the hobby responsibly.

Aberdeenshire Council are members of the North East Partnership Against Rural Crime.

# Phone Safety



Mobile technology is now an essential part of modern life, with more of our data being stored on tablets and smartphones. What's more, these devices are now as powerful as traditional computers, and because they often leave the safety of the office (and home), they need even more protection than 'desktop' equipment. Here are 5 tips that can help keep your mobile devices secure this summer.

#### 1 Switch on password protection

A suitably PIN or password (opposed to a simple one that can be easily guessed or gleaned from your social media profiles) will prevent the average criminal from accessing your phone. Many devices now include fingerprint recognition to lock your device, without the need for a password. However, these features are not always enabled 'out of the box', so you should always check they have been switched on.

## 2 Make sure lost or stolen devices can be tracked, locked or wiped

Staff are more likely to have their tablets or phones stolen (or lose them) when they are away from the office or home. Fortunately, most devices include free web-based tools that are invaluable should you lose your device. You can use them to track the location of a device, remotely lock access to the device (to prevent anyone else using it), remotely erase the data stored on the device and retrieve a backup of data stored on the device

#### 3 Keep your device and apps up to date

No matter what phones or tablets your organisation is using, it is important that they are always kept up to date. All manufacturers (for example Windows, Android, iOS) release regular updates that contain critical security updates to keep the device protected. This process is easy and free; devices should be set to automatically update. All the applications that you have installed should also be updated regularly. These updates will not only add new features, but they will also patch any security holes that have been discovered.

#### 4 Enable 2 factor authentication

Two-factor authentication, or 2FA, adds a layer of security when signing in to websites and services. The most common way this happens is when you log in from a new phone, tablet or computer, or from a new location the website doesn't recognise. Some websites also require 2FA every time you login or when you make a transaction. The website will send you a code usually via text to your mobile phone - that you have to enter before you can finish signing in. It's an effective way to protect your online data.

#### 5 Don't connect to unknown Wi-Fi Hotspots

When you use public Wi-Fi hotspots (for example in airports or coffee shops), there is no way to easily find out who controls the hotspot, or to prove that it belongs to who you think it does. If you connect to these hotspots, somebody else could access: what you're accessing whilst connected your private login details that many apps and web services maintain whilst you're logged on

The simplest precaution is not to connect to the Internet using unknown hotspots, and instead use your mobile 3G or 4G mobile network, which will have built-in security. You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet, however you should only use VPNs provided by reputable service providers.

## Crime Alert

A selection of crimes affecting residents from across Grampian

#### **Online Shopping Fraud**

A Peterhead resident had her online accounts with various retailers compromised and Apple goods fraudulently ordered to the value of £2500. The retailers spotted the suspicious activity and contacted the account holder who confirmed she had not ordered the goods.

#### **Microsoft Fraud**

A Tarland resident fell victim to a national fraud involving Microsoft account holders. Criminals hacked into a large number of accounts and used victim Paypal account details to order electronic goods which were delivered to an address in England.

#### Housebreakings, Newtonhill

A 49 year old man has been arrested and charged by the Stonehaven Community Policing team following four housebreakings in Newtonhill. A report has been submitted to the Procurator Fiscal.

#### **Online Extortion**

Criminals demanded £2000 from a 17 year old Peterhead male after exchanging explicit images via a online chat room.

#### **Sony Playstation Fraud**

A Banchory resident had her Sony Playstation account compromised and lost over £200. A number of fraudulent purchases were made using her account details on the Sony website.

#### **Badger Sett Destruction**

Officers are investigating the destruction of a badgers sett at a nature reserve in Aberdeenshire. The entrance to the sett had been deliberately blocked with boulders and earth.

#### **Any Desk Fraud**

A resident from a rural property near Lumphanan was contacted by fraudsters claiming to be from BT. They convinced the victim to download the Any Desk app claiming it would allow them to fix a fault on her line. The victim lost over £4000 from two separate bank accounts.

#### Puppy or kitten frauds

A Moray Resident was defrauded of £160 deposit after agreeing to buy a English Springer Spaniel seen on Facebook Sales. The deposit was sent, and arrangements made for delivery but the puppy never received.

#### Theft of ATV, Keith

A black Polaris Ranger, ATV was stolen from a farm near Keith.

#### Drugs recovery, Buckie

Drugs with an estimated street value of £490,000 have been recovered at an address in Buckie in August. A 36-year-old man has been arrested.

#### Wilful Fire raising, Elgin

A vehicle was wilfully set on fire in Kingsmills, Elgin causing significant damage to two vehicles.

#### **Phone Scam**

A 73 year old female Aberdeen resident received a call from her telephone provider offering a loyalty discount. She signed up for a broadband package but received three new mobiles, allegedly sent in error. She returned the phones to a specified address. It was a scam which left her paying for the phones.

#### **Online Working Fraud**

An Aberdeen resident was contacted via Whatsapp with an offer of working from home to review products. He opened a crypto account to work. When he

tried to withdraw his money, he realised it was a scam and lost £10.000.

#### **Competition Scam**

An Aberdeen female received a Facebook message from who she thought was a friend, congratulating her on winning a prize of £15,000. She was contacted by a company claiming she needed to purchase £500 of Apple vouchers to claim her prize. She purchased the vouchers and sent the codes. There was no prize and she lost £500.

#### **Investment Fraud**

An Aberdeen resident invested £6000 in a 1-year fixed ISA after finding an online investment company. 3 months later he opened another for £14,000 believing his money was doing well. The company was a scam and he lost £20,000.

#### **Royal Mail Fraud**

An Aberdeen female received a letter from Royal Mail confirming her redirected mail request had been accepted. She contacted their Fraud Department before carrying out a credit check online and found 7 credit card applications had been made in her name. £6000 had already been spent on the cards

#### **Online Dating Scam**

An Aberdeen resident used a popular dating site. A male she met advised that he was making a great return on his crypto currency investments. Following his advice the victim invested money over a 6-month period. When she went to withdraw funds, she discovered it was a scam and lost £28,000.

## 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

#### **Aberdeenshire**

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

#### **Aberdeen City**

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

