POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

North East

CrimeAlert

Keeping Communities in the North East Safe

June 2023

North East CrimeAlert

Keeping Communities in the North East Safe

June 2023

Welcome to the June edition of North East Crime Alert.

A quarterly bulletin produced by the Police Scotland North East Division Crime Reduction Team aimed at keeping you up to date with what's happening in our community.

In this edition of North East Crime Alert

We look at our Shut Out Scammers campaign working alongside Trading Standards.

Sextortion continues to be popular with scammers.

Since our last issue when have seen several high value losses to Crypto Currency fraud.

Amazon impersonation scams - what to look out for.

Recycling old devices, is it safe to do so?

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

From the latest frauds and scams, to general security measures, each issue will bring you advice on how to keep your property safe.

Crime across Scotland is increasing and criminals are using ever more sophisticated methods. By working in partnership we can make our communities a safer place to live and work.

Shutting Out Scammers

During April 2023 officers from the North East Division Crime Reduction Team and Trading Standards took to the road in the ‘Scam Van.’

On 18th April 2023 Police Scotland and Trading Standards Scotland launched the nationwide ‘Shut out Scammers’ campaign outside Marischal College, Aberdeen.

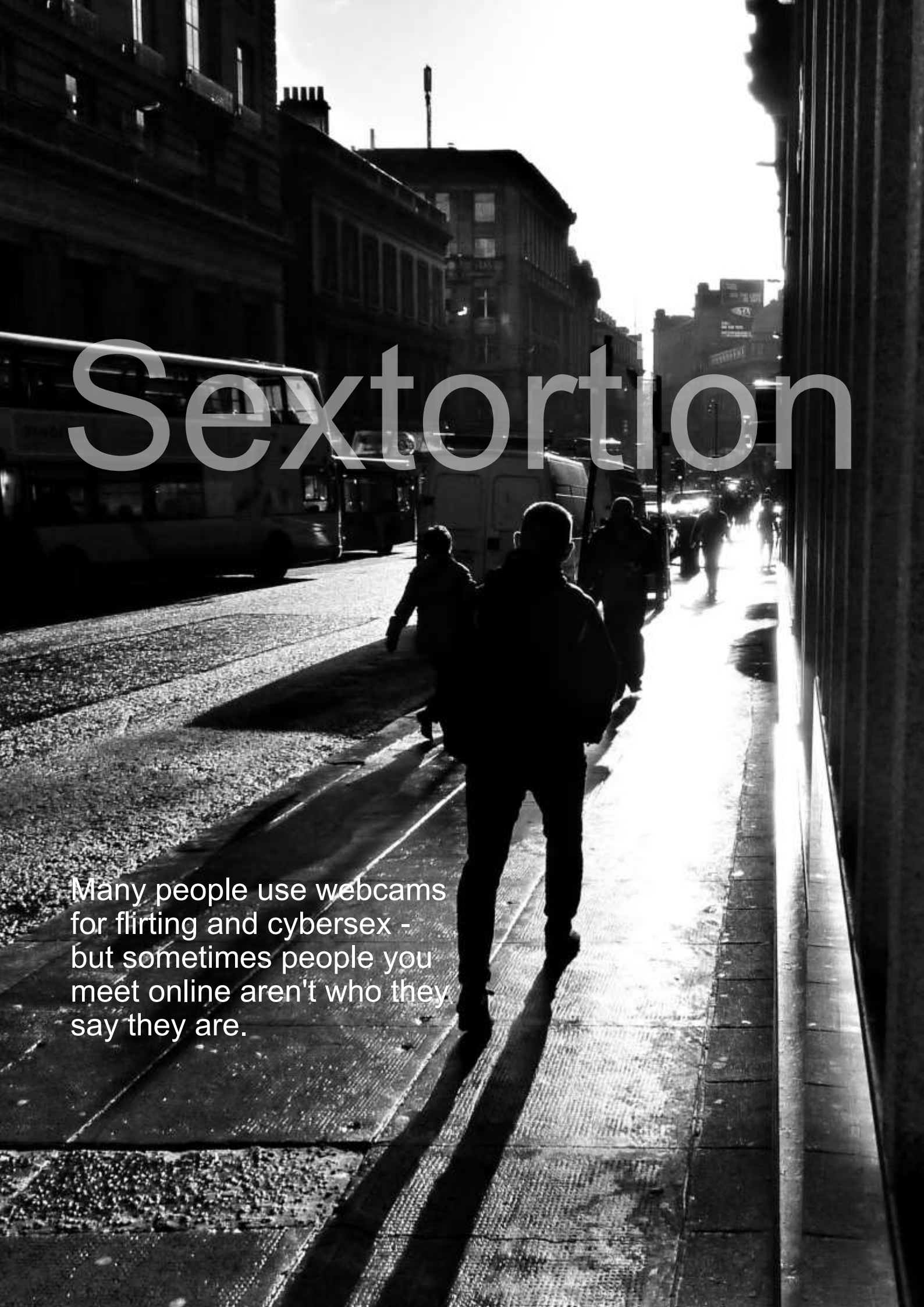
The campaign aims to raise awareness of the mis-selling of energy efficiency measures, doorstep crime, rogue trading scams and other forms of financial harm to which consumers are susceptible.

The campaign aims to empower consumers rather than make them fearful and to encourage the reporting of doorstep crime. During the week, North East Crime Reduction officers and Aberdeen City, Aberdeenshire and Moray Local Authorities Trading Standards officers were in the ‘Scam Van’ visiting town centres, retail parks and rural communities across the Grampian region. They shared information on how to prevent being affected by bogus callers and rogue traders.

The campaign aims to ensure that consumers know where to find trusted information and what their consumer rights are. The team also highlighted the most common doorstep scams and tactics rogue traders and bogus callers use.

Always contact 101 if you believe you, friends or relatives have been affected by bogus workmen.

For more information visit
www.tsscot.co.uk/shut-out-scammers/



Sextortion

Many people use webcams for flirting and cybersex - but sometimes people you meet online aren't who they say they are.

What is Sextortion? Criminals will befriend victims online by using a fake identity and then persuade them to perform sexual acts in front of their webcam.

These webcam videos are recorded by the criminals who then threaten to share the images with the victims' friends and family. This can make the victims feel extremely ashamed and embarrassed and, tragically, here in the UK at least four young men have taken their own lives after being targeted in this way.

Both men and women can be victims of this crime. The best way to stop yourself from becoming a victim is to be very careful about who you befriend with online, especially if you're considering sharing anything intimate with them.

Who is behind this crime?
We have evidence that organised crime groups – mostly based overseas - are behind this crime. For them it's a low risk way to make money and they can reach many victims easily online. Victims are often worried about reporting these offences to the police because they are embarrassed.

What to do if you've been targeted:
Don't panic, the first big step is to recognise you are the 'victim' in this help and support is available.

Don't pay, experience shows where victims have paid then there is no guarantee that offenders will not still post the recording and are in fact more likely to come back with further demands.

Don't keep communicating: By replying to these threats it indicates to the criminals that you are someone who may be persuaded to pay their ransom.

Save the evidence: Take screenshots. Save messages and images. Collect URL links to where the information is being shared online.

Report it to social media companies if communication happened on their channels, for example, Facebook or Instagram.

Report the incident to your internet service provider.

Block all communication with the person targeting you.

Most social media sites have rules against sharing intimate content without consent. You should be able to get the material removed.

Report it	Further help and support
We understand that it might be difficult to report this type of crime. Our officers are here to listen and to support you in any way we can. You can report intimate image abuse to us by calling 101. For issues of a non-urgent nature use our Contact Us form. www.police.scotland.uk/contact-us	PAPYRUS provides confidential advice and support and works to prevent young suicide in the UK. www.papyrus-uk.org Samaritans to talk any time you like in your own way and off the record. www.samaritans.org Get Safe Online www.getsafeonline.org

Guaranteed Returns Too good to be true?

This month we look at how to safeguard your finances against crypto fraud.

Cryptocurrencies have gained significant popularity in recent years, attracting both investors and fraudsters. While the digital currency ecosystem offers exciting opportunities, it's crucial to remain vigilant and protect yourself from crypto fraud schemes. In this article, we will explore key strategies to help you avoid becoming a victim and safeguard your hard-earned money.

Educate Yourself: Understanding the fundamentals of cryptocurrencies and how they function is essential before getting involved. Familiarize yourself with common terms, such as blockchain, wallets, and private keys. Stay informed about the latest trends, security practices, and potential risks associated with crypto investments.

Choose Reliable Exchanges: Selecting a reputable and secure cryptocurrency exchange is paramount. Research well-known platforms that have a proven track record of reliable service, strong security measures, and transparent operations. Check for user reviews and recommendations from trusted sources.

Verify Authenticity: Be cautious of fraudulent websites and phishing attempts. Always double-check the URL of cryptocurrency platforms and ensure they have a secure connection (https://). Beware of suspicious emails, social media messages, or ads that prompt you to share personal information or invest in dubious schemes.

Protect Your Wallet: A cryptocurrency wallet is where you store your digital assets. Choose a reputable wallet provider that offers robust security features, such as two-factor authentication (2FA) and multi-signature functionality. Regularly update your wallet software to benefit from the latest security patches.

Secure Your Private Keys: Your private keys are crucial for accessing and managing your cryptocurrency holdings. Never share your private keys with anyone and store them in a secure offline location, such as a hardware wallet or encrypted USB drive. Avoid storing them digitally or on cloud-based platforms, as they may be vulnerable to hacking.

Be Wary of Investment Schemes: Exercise caution when approached with lucrative investment opportunities or schemes promising high returns with little risk. Beware of Ponzi schemes, multi-level marketing schemes, and individuals claiming to have insider information. Remember the old adage: "If it sounds too good to be true, it probably is."

Research ICOs and Projects: Initial Coin Offerings (ICOs) can be an attractive investment avenue, but they also present risks. Thoroughly research ICO projects before investing, including the team behind the project, their experience, and the legitimacy of their claims. Look for whitepapers, roadmaps, and a strong community presence as indicators of a genuine project.

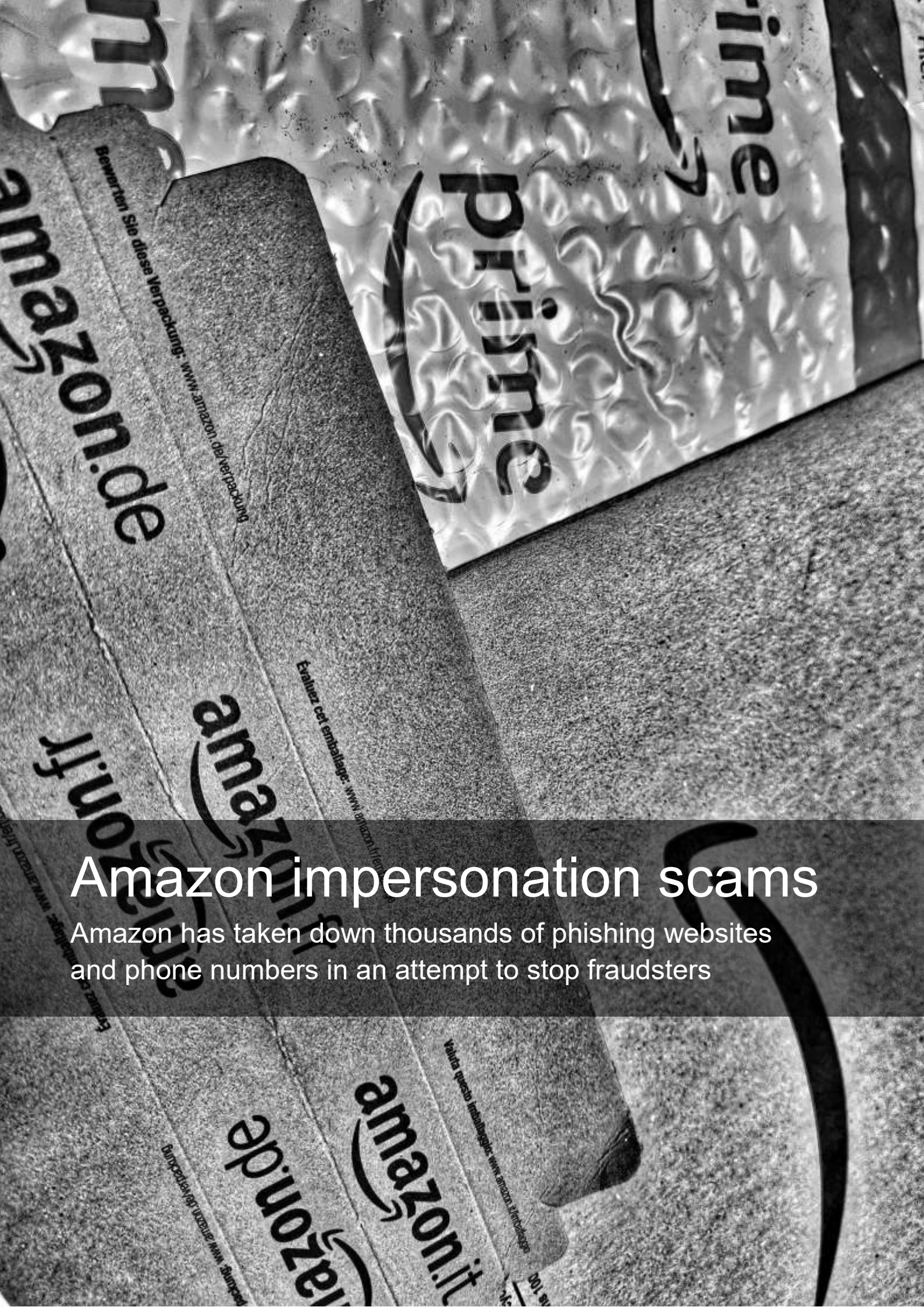
Use Two-Factor Authentication: Enable two-factor authentication wherever possible, especially on your exchange accounts and cryptocurrency wallets. 2FA adds an extra layer of security by requiring a second verification step, typically a unique code sent to your mobile device or generated by an authenticator app.

Stay Informed and Remain Sceptical: Stay updated on the latest news and developments in the cryptocurrency space. Follow reputable crypto news sources, participate in forums, and engage with the community. Develop a healthy scepticism towards unsolicited investment advice or unsolicited offers that seem too good to be true.

Seek Professional Advice: Consider consulting with a financial advisor who specializes in cryptocurrencies if you are new to the space or unsure about investment decisions. They can provide personalized guidance based on your financial goals and risk tolerance. While cryptocurrencies offer exciting opportunities, the prevalence of crypto fraud schemes necessitates caution and due diligence. By educating yourself, securing your wallets and private keys, and staying vigilant, you can reduce the risk of falling victim to crypto fraud and protect your financial interests in the digital realm. Remember, your financial security is in your hands.

Useful Links

www.cifas.org.uk	Advice on protecting your identity
www.getsafeonline.org	Advice on managing your digital footprint
www.fca.org.uk	Financial Conduct Authority
www.experian.co.uk	Credit checks
www.mpsonline.org.uk	Remove your address from mass marketing mailing lists
www.tpsonline.org.uk	Remove your telephone number from mass marketing call lists
www.royalmail.com	Report nuisance mail



Amazon impersonation scams

Amazon has taken down thousands of phishing websites and phone numbers in an attempt to stop fraudsters

Scammers have repeatedly targeted Amazon, looking to deceive its customers via calls, texts and emails, sometimes persuading victims into downloading software to give them access to their devices.

On other occasions advising them that their Amazon Prime account has expired and that their bank cards have been charged a £95 renewal fee. If the call recipient has concerns they are urged to press options on their keypad to speak to Customer Support staff. This results being left on hold, potentially to a premium rate phone numbers.

How to avoid Amazon impersonation scams

We recommend following these tips to stay safe:

Don't install apps or software. Amazon will never ask you to install anything on your device to get a refund or help from customer service.

Don't pay over the phone. Amazon will never ask you to provide payment information for products or services over the phone.

Don't be rushed. Scammers may try to create a sense of urgency to rush you into making decisions without thinking them through.

Verify orders with Amazon

Check the 'Your Orders' section on Amazon's website or the Amazon Shopping app. Amazon won't call, text or email you about orders you aren't expecting.

How to report Amazon impersonation scams

You can report Amazon impersonation scams directly to the retailer by using its online reporting service.

Dodgy calls and texts

On an iPhone, you can report scam calls by texting the word 'call' followed by the scam number to 7726.

On an Android phone, you can text the word 'call' to 7726. You will then be asked for the phone number the scam was sent from. Scam text messages can also be forwarded to 7726 to report them.

Scam emails

Scam emails can be forwarded to report@phishing.gov.uk.

To report them to your email provider, select 'Report phishing' on Gmail or Hotmail, or from a Yahoo account you can forward emails to abuse@yahoo.com.

What to do if you fall victim

If you are scammed, contact your bank immediately and report the scam to the police on 101 or via the online 'contact us' section on the Police Scotland website. www.police.scotland.uk/contact-us

Amazon says it has initiated takedowns of more than 20,000 phishing websites and 10,000 phone numbers that were being used for impersonation scams.


Re-cycling devices
Can they expose your personal information?
For your security, enter your PIN
Learn more
Your PIN contains at least 4 digits
OK
amazon

Can your recycled devices expose your personal data?

Our devices, especially our smartphones, contain more work, personal and financial data than ever before.

If you are selling, giving away, or trading in your smartphone (or other device), you should erase all of this personal data so the information stored on the device/s doesn't fall into the wrong hands.

This can result in identity theft and fraud, unauthorised sharing of intellectual property and trade secrets to individual and corporate embarrassment.

If you are changing devices, refer to the manufacturer's website (or search online) to find out how to erase your data from your device and reset it - often called a 'factory reset.' Doing a factory reset will bring the device back to its' original settings when initially purchased, removing all your personal data.

Before you erase any of your data or move towards a factory reset on your device, there are a number of checks you should attend to.

Make sure you have a backup copy of all the personal data that you want to keep.

If you use your device to access online services (such as banking, shopping, email or social media), you might be logging into these services without entering your password each time. If this is the case, make sure you know which accounts you access (and the logins and passwords for each of these accounts) before you erase your data.

If you use your device to control any of your 'smart' devices around the house (such as security cameras or thermostats), you'll no longer be able to manage them using your phone. Again, make sure you're able to manage them using a different device, before you erase your data.

If you use your device to verify your online accounts (for example, by confirming SMS codes, Authentication app), you'll need to make sure this works on another device. Make sure you do this (and check that it works) before you erase the data on the device that you're selling/giving away.

Scam Update #10

Phishing

Phishing is a popular form of cybercrime because of how effective it is. Cybercriminals have success using emails, text messages and direct messages on social media or in video games, to get people to respond with their personal information. The best defence is awareness and knowing what to look for.

How to recognize a phishing email:

- Urgent call to action or threats - Be suspicious of emails that claim you must click, call, or open an attachment immediately. Creating a false sense of urgency is a common trick of phishing attacks and scams.
- First time or infrequent senders - While it's not unusual to receive an email from someone for the first time, this can be a sign of phishing. When you get an email from somebody you don't recognize, take a moment to examine it extra carefully.
- Spelling and bad grammar. If an email message has obvious spelling or grammatical errors, these are sometimes the result of awkward translation from a foreign language.
- Generic greetings - If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.
- Mismatched email domains - If the email claims to be from a reputable company, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name.
- Suspicious links or unexpected attachments - If you suspect that an email message is a scam, don't open any links or attachments that you see. Instead, hover your mouse over, but don't click, the link to see if the address matches the link that was typed in the message.

What can you do?

Use anti-virus software to check for malware on your device and stop SPAM e-mails.

Remove suspicious apps and extensions.

Don’t give your information to an unsecured site.

Don’t be tempted by those pop-ups, most browsers allow to install ad blockers.

Don’t ignore those security updates, security patches are to keep up with new cyber attack methods.

Install firewalls to prevent external attacks.

In our regular series bringing you first hand experiences of victims of crime from across the North East we look at two recent victims of high value fraud.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

An 85-year-old man from the city was recently the victim of a scam after fraudsters managed to con £200,000 from him.

He was contacted by a man claiming to be from his bank. The man advised that the victim's bank account was being investigated due to fraudulent activity and asked him to transfer £20,000 to an account provided by the scammer. The victim complied and provided vast sums on a near-daily basis. He was also encouraged to set up internet banking.

The victim was then contacted by a woman claiming to be from the Police, working as a part of the investigation. The victim became suspicious and told a family member.

A 59-year-old business owner was defrauded of £210,000 after being informed by scammers that his various bank accounts had been compromised and was instructed to transfer his money to a 'safe account' via internet banking.

He transferred the entire balance of his business and personal accounts into criminal control.

Chief Inspector Darren Bruce said: "The people who carry out these crimes are despicable. They target members of our community and steal their life savings.

"The scammers gained the victims confidence to ensure they parted with large sums of money.

"Criminals pretend to be from a legitimate bank, then contact the victims by telephone to warn of suspicious activity on their accounts. They convince the victim to transfer money to 'safe accounts'. This type of fraud is known as 'Authorised Push Payment'.

"We would like to make the public aware of these calls to ensure that their elderly or vulnerable family members, friends and neighbours are also aware of these types of scams.

"Reputable banks and financial institutions will not ask you for your banking details or password by phone. If in doubt, do not share any personal **information or financial** details."

How could this have been prevented?

Your bank will NEVER ask you to transfer money or set up a secure account.

The bank scam normally follows a scam email, so they may know who you bank with and how much money is in your account.

Seek advice or a second opinion. Speak to family or friends if you are unsure. Take 5 minutes to be sure. A genuine caller won't mind you checking.

Criminals will often ask you to download software that enables that to take control of your computer.

Don't assume a call is safe just because the number matches the number on your card or statement.

If in doubt HANG UP.

The names of victims have been changed but all other circumstances are accurate.

What's happening in Aberdeenshire

NEPARC – Strategy launch

On 1st March 2023, the North East Partnership Against Rural Crime (NEPARC) launched its 2023 – 2025 strategy at the Royal Northern Agricultural Society Spring Show at Thainstone Centre, Inverurie. The PARC brings together 35 local and national organisations to tackle various types of rural crime including fuel, timber, plant and machinery thefts.

Scottish Self-Build and Renovation Tradeshow

On 11th March 2023, the North East Crime Reduction Team were at the Scottish Self-Build and Renovation Tradeshow held at Thainstone, Inveurie. Officer were hand to provide crime prevention advice and promote 'Construction Watch' and 'Rural Watch Scotland.'

Break-ins – Inverurie

A teenage boy, aged 15, has been arrested and charged in connection with break-ins and thefts in Inverurie. The incidents happened between 2nd and 30th April in the Market Place area of the town. A report will be submitted to the Youth Justice Management Team.

Theft of Quad Bikes

A 29-year-old man has been arrested and charged in connection with a series of quad bike thefts in Aberdeenshire. The incident happened during March and April at rural properties in Meikle Wartle, Tarves and Banff. The man was expected to appear at Aberdeen Sheriff Court on Friday 5th May 2023.

Housebreaking – Foveran

We are appealing for information about a Housebreaking at Blairythan Smithy, Foveran, Aberdeenshire. Between 25th and 26th April 2023 persons gained access to a local building, removing high-value engines, vehicles and heavy equipment.

Theft of Bowser Trailer – Turriff

We are appealing for information in relation to a theft at Sheilburn Farm, Fortrie, Turriff. Between Saturday 22th April 2023 and Monday 24th April 2023, a Yanmar L100 Diesel 18/200 Bowser trailer was stolen from the farm.

Witness Appeal – Stonehaven

Officers in Stonehaven are appealing for witnesses after a woman reported being verbally abused by a man within St Cyrus nature reserve around 4.15pm on Saturday 13th May 2023.

Housebreakings – Inverurie

A teenage boy, aged 15, has been arrested and charged in connection with break-ins and thefts in Inverurie. The incidents happened between 2nd and 30th April 2023 in the Market Place area of the town. A report will be submitted to the Youth Justice Management Team.

What's happening in Moray

Housebreaking, Lochhills, Elgin

Between 23rd and 24th March 2023, a rural property was broken into, pipes, wires and boiler was stripped from the property.

Attempted Murder – Elgin

Two teenage boys have been charged in connection with an attempted murder in Elgin. The incident happened around 10.45pm on Sunday, 30th April, near the fountain in the High Street area of the town. A 25-year-old man was taken to hospital with serious injuries. The two boys, aged 14 and 15, have been arrested and charged in connection with the incident. A report will be submitted to the Procurator Fiscal and they are expected to appear before Elgin Sheriff Court at a later date.

Puppy Fraud – Moray

Police Scotland warns those looking for a new puppy or kitten to be wary of online 'deposit scams.' A Moray resident has become the latest victim of such a crime after trying to buy a puppy and being defrauded of just over £1000. The victim thoroughly researched numerous websites before leaving contact details with one breeder through their official-looking website. The breeder contacted the victim by text, sent videos and photographs of the puppy, and even agreed to a future video chat to put the buyer's mind at ease. It was only when the victim asked for a payment receipt and medical certificate, that it became apparent it was a scam, and all contact by the scammer stopped.

Housebreaking – Elgin

We are appealing for information following a break - in to a house at the Findrassie estate, off Lossiemouth Road, Elgin. The incident is believed to have taken place overnight between 28th and 29th April 2023. A number of decorative items were stolen from the property.

Wilful fire-raising, Forres

Two male youths have been charged in connection with wilful fire-raising in Forres. Officers were made aware of shrubs and woodland being set alight around 6pm on Tuesday 18th April and Wednesday 19th April 2023 within Sanquhar Woods, Forres with Scottish Fire and Rescue Service having to attend and extinguish the fires.

Theft of Whisky – Ballindalloch

One year on from a break-in to a distillery in Ballindalloch, officers in Elgin have issued a fresh appeal for information. Twenty bottles of whisky, valued at approximately £150,000, were stolen. Detective Constable Lucy Cuthbert from Elgin said: "Enquiries into the theft from the Glenfarclas Distillery are still very much ongoing and I would like to thank everyone who has come forward with information so far. "We would encourage anyone with any further information about the break-in to get in touch. No matter how small it may seem, it may be the crucial piece of information we need in order to catch those responsible. "We would also urge anyone who has been offered a bottle of the stolen Glenfarclas branded whisky to contact us. is a criminal offence to buy stolen goods."

What's happening in Aberdeen

Bike thefts

In March, nine high value mountain bikes, were stolen from two separate garages in Aberdeen's west end, in the early hours of the same night. Entry was forced via garage side doors and basic internal security was overcome allowing thieves to remove the bikes.

Follow up fraud

We have seen a recent increase in 'follow up fraud' to people who have lost money. Unscrupulous scammers are contacting victims of fraud offering to investigate their loss and pursue the matter on their behalf for a fee, which again is a scam. Be very wary of any scheme or advert on social media or company calling you out of the blue making unrealistic claims.

Crypto frauds

We have seen several crypto currency type frauds in Aberdeen over the last few months, monies lost range for £1200 to £48,000. Many of the scammers advertise on social media with links to very convincing websites, don't be fooled by this, always carry out detailed research before investing. If you are looking to invest in an investment platform, it is vitally important, to research that platform prior to exchanging any money.

Facebook marketplace

Facebook Marketplace continues to be a lucrative area for fraudsters to operate. Many Aberdeen residents have lost out not only by purchasing but also selling on this platform. So what should you be looking for if you think the person you're talking to is a scammer? Here are some warning signs for Facebook Marketplace scams, sellers offer suspiciously low prices for high-ticket items, they refuse to meet in person, they try to take the conversation outside of Facebook Messenger, buyers send you prepaid shipping labels, buyer overpays for a product, buyers or sellers ask for your phone number, they don't have a profile photo or want you to pay with a gift card.

Facebook fraud

An Aberdeen resident lost £4000 when he paid upfront for a car he had seen advertised on Facebook, without actually seeing the vehicle. The seller offered to deliver the vehicle for an additional fee, but both seller and car never appeared.

.

Romance fraud

A 26-year-old man has been arrested and charged in Kent in connection with a high-value cyber-enabled fraud targeting a vulnerable woman in Aberdeen. The fraud targeted the victim's online finances, resulting with a sum in excess of £200,000 being stolen. An investigation was carried out by officers from North East Division's Cyber-Enabled Crime Team, resulting in enforcement activity at a property in Kent on Wednesday, 3rd May 2023. A report will be submitted to the Procurator Fiscal and the 26-year-old is expected to appear at Aberdeen Sheriff Court at
a later date.

County lines

Five people have been arrested and convicted for their part in drugs offences and organised crime in Aberdeen. In 2020, officers from North East Division's Organised Crime Unit launched Operation Dismantle, targeting a criminal group involved in county lines and organised crime. Over a six-month period, between February and July 2020, officers pieced together evidence of a county line supply of crack cocaine and heroin from London to Aberdeen, at addresses predominantly throughout Aberdeen City Centre and Rosemount.

Drug seizure

On Friday 28th April 2023 officers from the Organised Crime Unit, stopped a taxi in Gort Road. The male passenger's rucksack was searched and a quantity of Class A drugs and cash were recovered. The drugs have a potential street value of approximately £39,000. Around £9,000 was also seized. A 19-year-old man was arrested and charged in connection with the recovery. He appeared at Aberdeen Sheriff Court on 7th May 2023.

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 (Keith)
PC Richard Russell
Richard.russell@scotland.police.uk

Aberdeen City (Nigg)
PC Mark Irvine
Mark.irvine@scotland.police.uk

Aberdeenshire (Stonehaven)
PC Mike Urquhart
Michael.urquhart@scotland.police.uk

Wildlife Crime Officer (Keith)
PC Hannah Corbett
Hannah.corbett@scotland.police.uk

POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA