

**The 12 Frauds of Christmas**

Police Scotland North East Division will be launching their 12 Days of Christmas Fraud Campaign aimed at keeping people safe during the festive period.

North East Division Crime Reduction Officer PC Mark Irvine said ‘Criminals are increasingly focussing their activities on various types of frauds and scams whether it be online, by telephone or door to door. These criminals are experts at impersonating people, organisations and the police. We want everyone to have a great festive period but be mindful and stop and think if a call or email could be fraudulent.’

**Police Scotland North East Division’s ‘First Fraud of Christmas’ **

**Fraud Enablers**

Criminals will often take advantage of our natural tendency to trust. They prey on peoples’ emotions and get them *feeling* rather than *thinking*. A common tactic criminals use is pressure, for example, ‘if you don’t do this in 5 minutes you’re going to be in big trouble.’

**How to protect yourself**

The best defence against these type of attacks is knowledge; once you know someone is trying to con you the con will fail. However, even if we are suspicious, we are often bad at saying ‘no.’ If you are uncertain you could try these alternatives:

‘I can’t make that decision without authorisation. Let me get back to you.’

‘I will not make any decisions without speaking to someone first.’

Never be afraid to simply say ‘NO.’ If they are a genuine professional they won’t mind. If the person on the phone becomes pushy or insistent then the odds are fairly high it’s a fraud.

**Police Scotland North East Division’s ‘Second Fraud of Christmas’ **

**Types of Fraud**

Criminals often convince victims to make upfront payments for goods or services that don’t exist. Here are some examples:

**Inheritance Fraud** – the criminal tells you that you’re in line to receive a huge inheritance but you’ll need to pay a fee to release the funds.

**Loan Fraud** – the criminal asks you to pay an upfront fee for a loan.

**Recovery Fraud** – once you’ve been a victim of fraud the criminal contacts you claiming they can recover your losses for a fee.

**Lottery Fraud** – you’re told you’ve won a prize in the lottery but you’ll need to pay an admin fee.

**Work from home Fraud** – the criminal offers you a chance to make easy money working from home but you need to pay a fee in advance for business leads or a website.

**How to protect yourself**

Be extremely wary about giving money to anyone upfront.

If they claim to be an official double check their identity.

But don’t do so using any contact details they give you.

Don’t be pressurised into making a decision. Always take time to think, remember, Take 5.

**Police Scotland North East Division’s ‘Third Fraud of Christmas’ **

**Money Mules (Criminal Money Laundering)**

Where financial gain comes from crime, criminals use banking systems to move their proceeds i.e. stolen money. The account used to launder the criminal funds becomes a ‘Mule Account,’ making the account holder a ‘Money Mule.’ People are often targeted to provide access to their accounts either on the promise of a share of the funds or by coercion.

**How to protect yourself**

Never give anyone details of your bank or any other financial account, your bank card, PIN code, password or passcode – your bank and financial accounts are private.

Don’t be lured or persuaded to receive money into your account, even as a one off, no matter how plausible it sounds.

Be suspicious, question what you are being asked to do and do your research on any advertised jobs.

**Police Scotland North East Division’s ‘Fourth Fraud of Christmas’ **

**Online Fraud**

The vast majority of all frauds now use computers or technology in some way. There are a number of ways cyber criminals can attack you and your device. They may search the internet to find insecure devices, send an email containing malicious software or even set up fake websites.

**How to protect yourself**

Be wary about the personal information you post online and ensure you check your privacy settings on social media sites.

Use three random words to make sure your password is strong.

Storing passwords in your browser is a good tactic.

Password managers are a good idea.

If available, set up two factor authentication.

Use anti-virus software and update it regularly.

Update your software when new patches are released.

**Police Scotland North East Division’s ‘Fifth Fraud of Christmas’ **

**Banking and Card Fraud – Cash Machines**

People are targeted at cash machines by criminals who distract users and steal their cards or cash. Fraudsters also fit devices to the machines that trap cards, copy the card details and record the PIN.

**How to protect yourself**

Be wary of anyone approaching you when you are trying to withdraw cash.

Shield your PIN from criminal cameras or prying eyes. Stand close to the cash machine and cover the keypad with your spare hand.

If there appears to be anything unusual about a cash machine such as signs of tampering do not use it and report your concerns.

If your card is retained by a cash machine report it immediately to your card issuer while still at or near the machine. Store your card issuers 24 hour number in your mobile phone.

**Police Scotland North East Division’s ‘Sixth Fraud of Christmas’ **

**Banking and Card Fraud – Cards and Contactless Payment**

Contactless payment uses a wireless chip containing the users’ payment details which is embedded in a mobile phone or on a bank payment card. Every contactless card has an in-built security check, which means occasionally you have to enter your PIN number to confirm payment. Contactless only works within a few centimetres of the reader making it virtually impossible for details to be intercepted whist in use.

**How to protect yourself**

Don’t’ let anyone take your card out of sight while taking a payment – even for a few seconds. They could be using a skimming device to copy data from your card’s magnetic strip or copying the CCV code on the back. Consider purchasing a blocking wallet to protect your card whilst in your wallet/purse.

Monitor your bank statements regularly for unauthorised payments.

If your contactless payment card or contactless enabled smart phone/watch is lost or stolen inform your bank immediately.

**Police Scotland North East Division’s ‘Seventh Fraud of Christmas’ **

**Banking and Card Fraud – Online Banking**

To stay safe online you must protect your password and personal details to stop criminals from accessing your account. Many banks provide one time passcodes sent to your device when setting up new payments. These should never be shared with anyone, even from the bank. If you’re speaking to your bank and they ask for it you are certainly speaking to a criminal.

**How to protect yourself**

Choose, use and protect passwords and memorable words with great care.

Keep online banking software and banking apps up to date. Always download updates when prompted.

When logging in whilst in public take extra care to shield and PIN codes or passwords.

Always log out of your online banking account or banking app when you have finished using it. Closing the app or web page or turning off your device may not be sufficient.

Do not use publicly available Wi-Fi networks for banking or passing personal details.

If your bank has called you take a reference number and hang up before calling back on a number you know to be safe after a few minutes in order to clear the line.

**Police Scotland North East Division’s ‘Eighth Fraud of Christmas’ **

**Online shopping and auction sites**

Online shopping can save time, money and effort. However, among the genuine buyers and sellers there are criminals who use the anonymity of the internet to offer goods for sale they do not have or are fake.

**How to keep yourself safe**

Be wary of offers that look too good to be true.

Read the consumer advice on any website you are using to make a purchase. Use the recommended payment method or you may not be refunded for any losses to fraud.

Research the buyer / seller and their bidding history.

Don’t’ be convinced by pictures alone, they may have been taken from elsewhere on the internet.

Be suspicious of any requests to pay by bank transfer or virtual currency.

Never buy a vehicle without seeing it.

If you are selling online be wary of any emails stating funds have been sent.

Ensure you have adequate anti-virus protection on your device.

**Police Scotland North East Division’s ‘Ninth Fraud of Christmas’ **

**Courier Fraud**

Fraudsters cold call you pretending to be from your bank or from the police. They claim there is an issue with your bank account or request your assistance with an ongoing bank or police investigation. The ultimate aim of the call is to trick you into parting with your money either in person, online, via a money service bureau or in a bank.

**How to protect yourself**

Be extremely wary of unsolicited phone calls from your bank or the police, particularly if they are requesting personal information. The Police will never ask to call at your door to uplift money on behalf of your bank.

End the call and call back on a different phone line or mobile. If this is not possible wait at least one minute before calling back. Use either the telephone number on your bank card or go to the banks website or for the police dial 101.

Speak to friends or family before carrying out any actions. Don’t trust claims made by cold callers.

Your bank will never ask to convert your money into Amazon vouchers or similar to avoid a fraud.

Never hand over your money, bank cards or make purchases following an unexpected call.

Never share your PIN with anyone.

**Police Scotland North East Division’s ‘Tenth Fraud of Christmas’ **

**Door-to-Door Fraud**

Door-to-door scams involve criminals knocking on your door and unexpectedly offering products or services. Fraudsters convince you to pay for goods or work which is often overpriced, of poor quality or is never carried out. In many cases the work isn’t even necessary. They may use intimidation and pressure you to make quick decisions so that you agree to their demands.

**How to protect yourself**

Always check their identity. If you are not happy do not let them into your house under any circumstances.

Never leave your front door open / unlocked and unattended so a second individual can’t enter without your knowledge.

Take time to consider your options and research costs from other providers. If in doubt contact your local Trading Standards office.

If you feel pressured have the confidence to say NO.

**Police Scotland North East Division’s ‘Eleventh Fraud of Christmas’ **

**Scam Mail**

Many victims of scam mail, also known as mass market fraud, are drawn in by the thrill of a guaranteed win. You will part with money in order to claim a prize that does not exist. Often, victims of this type of crime are elderly or vulnerable. They are targeted because they may live alone or have access to savings or pension funds.

**How to protect yourself**

You cannot win a competition or lottery you have not entered. If you are asked to pay an upfront fee for such a ‘win’ do not pay.

If you purchase goods in response to a mail offer, make sure you review your bank or credit card statements.

If you have any doubts speak to a friend or relative.

**Police Scotland North East Division’s ‘Twelfth Fraud of Christmas’ **

**Identity Fraud**

Identity fraud involves the misuse if an individual’s personal details to commit crime. Your details are valuable to criminals and can be misused by them, or sold on to others. If your data is obtained by criminals it may be used to obtain credit cards or bank accounts in your name, as well as numerous other financial products.

**How to protect yourself**

Sign up to a reputable credit rating agency. After doing so you will be notified when a credit check is completed using your details. This can identify if someone is using your details without your knowledge.

Be extremely wary of unsolicited phone calls, emails or text messages claiming to be from your bank or your phone provider. Particularly if they are requesting personal information such as dates of birth or passwords.

Review your bank and credit card statements for suspicious activity.

Have security software installed on your computer and mobile devices to prevent malicious software being downloaded.

Do not open attachments or click on links in unexpected emails.

Dispose of any documents which contain personal information securely.

Always shred or burn mail/paperwork that includes personal data or bank details.